MyID

Version 10.8 Update 2

Intel Virtual Smart Card

Integration Guide

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

Document reference: INT1853-06 January 2018

Copyright

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

This document provides details of setting up and using Intel Virtual Smart Cards for MyID®.

Intel Virtual Smart Cards can be issued to a user and collected to a device that contains Intel's Identity Protection Technology. This virtual smart card can contain certificates issued by your certificate authority that allow you to carry out tasks such as Windows logon.

The Intel Virtual Smart Card appears within Windows as a smart card, and makes its certificates available to your applications.

MyID allows you to control the lifecycle of these credentials, from issuing, enabling and disabling, requesting replacements, to cancelation and revocation, and has been integrated with the following Intel products:

- Intel® Authenticate

  The Intel Virtual Smart Card is protected by Intel Firmware, requiring multi-factor authentication defined by a customizable policy.

  See section *2*, *Integration with Intel Authenticate*.

- Intel® Identity Protection Technology with PKI

  The Intel Virtual Smart Card is protected by Intel Firmware, requiring a user PIN to be entered for authentication.

  See section *3*, *Integration with Intel IPT-PKI*.

1.1 Change history

Version	Description
INT1853-01	First release.
INT1853-02	Updated for MyID 10.7.
INT1853-03	Updated for MyID 10.7 Update 1.
INT1853-04	Updated for MyID 10.8.
INT1853-05	Updated for MyID 10.8 Update 1.
INT1853-06	Updated with further Intel Authenticate deployment recommendations.

2 Integration with Intel Authenticate

Intel Authenticate allows the user to enroll multiple authentication factors (for example, a fingerprint, Bluetooth device, or PIN) to protect the certificates associated with their Virtual Smart Card issued by MyID. The required authentication factors are defined by a policy file that is distributed to each user's computer.

When MyID issues an Intel Virtual Smart Card, the certificate issued is automatically associated with the OSLogin action defined within the policy file.

Note: You must select OSLogin when creating the policy file using Intel's Profile Editor Application. Other actions available with Intel Authenticate are not currently associated with the Virtual Smart Card.

The user can enroll their authentication factors separately, using Intel's factor management application. This can take place before or after receiving their Virtual Smart Card and certificate from MyID. When the user attempts to log on to Windows, they are prompted for their enrolled authentication factors.

For further details on installing, configuring, and using these features, see the documentation supplied with Intel Authenticate.

2.1 Hardware and software requirements

2.1.1 Client operating system requirements

MyID supports Intel Authenticate on Windows 8.1 (64-bit) and Windows 10 (64-bit) clients.

2.1.2 Intel hardware and software requirements

The client PC onto which you want to install the Intel Virtual Smart Card must have the appropriate Intel hardware, and support Intel Authenticate software. See the Intel Authenticate documentation for details.

See the readme in the WSVC package for details of the minimum versions required.

MyID has been tested with Intel Authenticate v2.5.

2.1.3 MyID client software requirements

You must install the following MyID software on your client PC:

- MyID Windows Integration Service – WSVC.
- MyID Self-Service App – SSP.

The MyID Windows Integration Service and MyID Self-Service App installers are provided on the MyID product CD.

Note: If the MyID minidriver for Intel Virtual Smart Cards (MYIDIAM) is installed, you must uninstall it to work with Intel Authenticate, as these components are already built into the software.

2.2 Recommended deployment configuration

Before deploying MyID with Intel Authenticate, Administrators should consider which users will be able to use this capability, as it is limited to compatible hardware only.

2.2.1 Deploying Intel Authenticate software

Intel Authenticate software must be installed alongside Intercede MyID clients to provide a streamlined issuance process.

- The MyID integration service and client must be installed prior to Intel Authenticate being installed, otherwise additional virtual smart cards will be created which will not be associated with a certificate – this may lead to authentication based on password only.
- It is recommended that the Intel Authenticate policy file is not deployed until users have been confirmed as requiring use of the feature, as it will trigger the factor enrolment process. This step should align with a request for the credential profile in MyID (see section *5.1*, *Requesting Intel Virtual Smart Cards*). Intel provide group policy scripts to install the policy file.
- Collection of certificates takes place using the MyID Self-Service App. Intercede recommends that scripts are used to manage this process, allowing a simpler process that works after the Intel Authenticate enrolment completes. For further details, see section *5.2*, *Collecting Intel Virtual Smart Cards*.

2.2.2 Intel Authenticate policy settings

The settings in the policy determine what actions are protected by Intel Authenticate, and the factors required to use them. The policy also controls how the Windows password is used during authentication processes.

MyID is used with Intel Authenticate to issue managed certificates for authentication, therefore it is important to ensure that the settings within the Intel Authenticate policy do not contradict or undermine certificate-based authentication.

Full instructions for configuring Intel Authenticate policy files are provided with the Intel Authenticate software. The following settings are expected to be used when MyID is providing certificate issuance for Intel Authenticate.

- Actions: OSLogin

  Currently, only the OSLogin action supports certificate based authentication.

  - OS Login: Advanced Settings
    - Block the user from using their Windows Password to log in

      Enable this setting. If this is *not* set, Intel Authenticate will use cached passwords, undermining the benefits of certificate based authentication.
    - Ask for the Windows Password only once and store it until it changes

      Select this option.
    - Require the system drive to be encrypted

      Select this option.

3 Integration with Intel IPT-PKI

Intel Identity Protection Technology with PKI (IPT-PKI) uses a secure PIN to protect the certificates associated with the Virtual Smart Card issued by MyID. When MyID generates a certificate request, the Intel Protected Transaction Display is used to set the PIN that will protect the certificate. When the user attempts to log on to Windows, or access an SSL-protected web site, the user is prompted for their PIN.

3.1 Hardware and software requirements

3.1.1 Client operating system requirements

MyID supports Intel IPT-PKI on Windows 8.1 (64-bit) and Windows 10 (64-bit) clients.

If you want to use Intel Virtual Smart Cards on Windows 7 clients, contact Intercede customer support quoting reference SUP-245.

3.1.2 Intel hardware and software requirements

The client PC onto which you want to install the Intel Virtual Smart Card must have the appropriate Intel hardware:

- Intel Broadwell 5th generation processor, Intel Skylake 6th generation processor, or Intel Kaby Lake 7th generation processor.
- The computer must be vPro compatible.

  Intel provide tools to check the compatibility of your client PC.

  The PC must support a minimum of Intel IPT-PKI as the result from this check.
- The following Intel software:
  - Intel Management Engine Firmware.
  - Intel Management Engine Software.
  - Intel IPT-PKI Cryptographic Service Provider (CSP).
  - Intel HD Graphics Driver.

  See the readme in the WSVC or MYIDIAM package for details of the minimum versions required.

3.1.3 MyID client software requirements

You must install the following MyID software on your client PC:

- MyID Windows Integration Service – WSVC.
- MyID Self-Service App – SSP.
- MyID minidriver for Intel Virtual Smart Cards – MYIDIAM.

The MyID Windows Integration Service and MyID Self-Service App installers are provided on the MyID product CD.

To obtain the MyID minidriver for Intel Virtual Smart Cards, contact Intercede customer support, quoting reference SUP-240.

4 Configuring Intel Virtual Smart Card Support

To set up MyID to issue virtual smart cards for use with Intel Authenticate or Intel IPT-PKI, you must carry out the following:

- Set the configuration option to allow Intel Virtual Smart Cards to be supported.
- Create a key to be used to protect the PIN when the credential is issued.
- Set up a credential profile for Intel Virtual Smart Cards.

4.1 Windows services

To collect an Intel Virtual Smart Card, the client PC must have the following Windows services available or running:

Windows	Service Name	Start Type	Must be running?
Windows 8.1/10	Smart Card	Automatic	N – triggered start
	Certificate Propagation	Automatic	N – triggered start
	Device Install Service	Manual	N – triggered start

For Windows 8.1 and Windows 10, the services must be available, but will be started automatically when required.

4.2 Setting the Intel Virtual Smart Card configuration option

To allow MyID to issue Intel Virtual Smart Cards:

1. From the **Configuration** category, select **Operation Settings**.
2. On the **Devices** tab, set the following:
   - **Enable Intel Virtual Smart Card support** – set this option to `Yes`.
3. Click **Save changes**.

4.3 Creating the PIN protection key

You must use the Key Manager workflow to create a key to be used to protect the PIN when the credential is issued. This PIN is not used by administrators or users; it is used internally by MyID to protect the issuance of the Intel Virtual Smart Card.

To set up the PIN protection key:

1. From the **Configuration** category, select **Key Manager**.
2. From the **Select Key Type to Manage** drop-down list, select **PIN Generation Key**.
3. Click **Next**.
4. Click **Add New Key**.
5. Type a **Key Name** and **Description**.

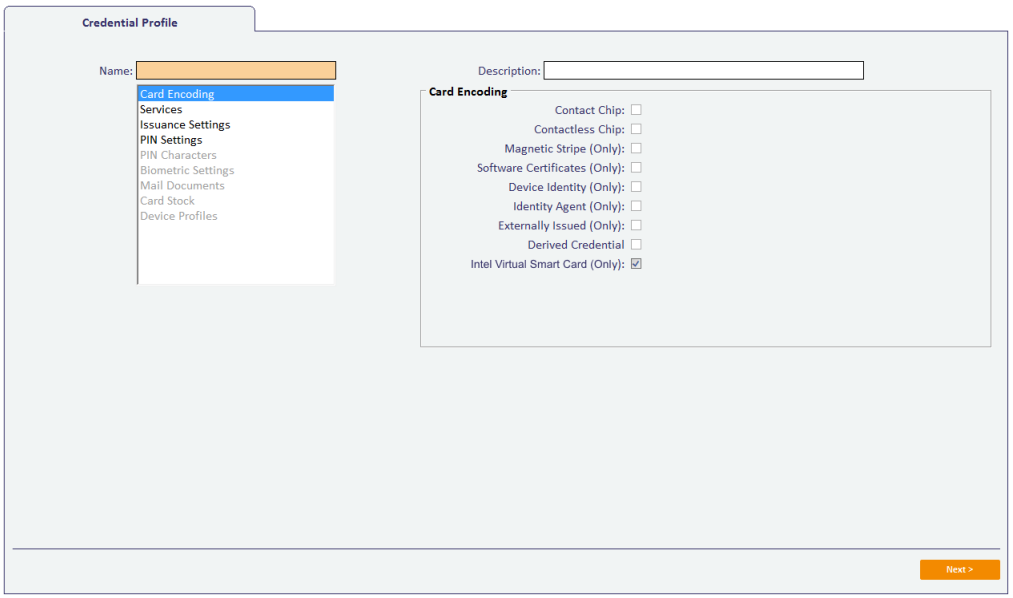
   Set the following options:
   - **Encryption Type** – **3DES**.
   - **Automatically Generate Encryption Key in Software and Store on Database** – selected.
   - **Exportable** – not selected.
6. Click **Save**.

4.4 Creating the credential profile

You must set up a credential profile within MyID to be used only for Intel Virtual Smart Cards.

To set up the credential profile:

1. From the **Configuration** category, select **Credential Profiles**.
2. Click **New**.
3. Type a **Name** and **Description**.
4. In the **Card Encoding** section, select **Intel Virtual Smart Card (Only)**.



5. In the **Issuance Settings** section, you can select the following options:
   - **Validate Issuance**
   - **Lifetime**
   - **Terms and Conditions**
   - **Generate Logon Code**

   See the ***Administration Guide*** for details of these options.

   The other options in this section are not suitable for Intel Virtual Smart Cards.
6. In the **PIN Settings** section, set the following:
   - **PIN Algorithm** – **EdeficePinGenerator**
   - **Protected Key** – select the PIN generation key you created to protect the Intel Virtual Smart Card PINs. See section *4.3*, *Creating the PIN protection key*.
7. If you are issuing the virtual smart card for use as a derived credential, in **Device Profiles**, from the **Card Format** drop-down list, select the following data model:
   - **PIVDerivedCredential.xml**.

     See the ***Derived Credentials Installation and Configuration Guide*** for details.
   - For all other uses, this option is not available.
8. Click **Next**.
9. Select the certificates you want to issue to the Intel Virtual Smart Card.

   Do not select any certificates that are set for key archival.

Note: For each certificate you select, an Intel Protected Transaction Display PIN entry dialog will appear when you issue the credential.

10. Click **Next** and complete the workflow.

    See the ***Administration Guide*** for details.

5 Working with Intel Virtual Smart Cards

MyID treats Intel Virtual Smart Cards in the same way as smart cards, and lets you manage the lifecycle of the credentials through the MyID user interface. The MyID Self-Service App on the user's PC manages the collection and cancelation of the credentials, and MyID communicates directly with the certificate authority to enable, suspend, or revoke certificates.

Note: You cannot use MyID Desktop to collect Intel Virtual Smart Cards.

Note: Currently, certificate renewal is not supported – if your certificates are due to expire, you must request a replacement Intel Virtual Smart Card.

5.1 Requesting Intel Virtual Smart Cards

To request an Intel Virtual Smart Card for a user, use one of the following methods:

- The **Request Card** workflow.
- The **Batch Request Card** workflow.

  See the ***Administration Guide*** for details of the **Request Card** and **Batch Request Card** workflows.
- The Lifecycle API.

  See the ***Lifecycle API*** document for details.

In each case, if you select a credential profile that you have configured for Intel Virtual Smart Cards, MyID creates a request for an Intel Virtual Smart Card for the user.

Note: If you have set the **Validate Issuance** option on the credential profile, you must use the Validate Request workflow before the user can collect the Intel Virtual Smart Card.

5.2 Collecting Intel Virtual Smart Cards

Once you have requested the Intel Virtual Smart Card (and optionally validated the request), the user can collect their credential onto a suitable PC.

Use the MyID Self-Service App to collect the Intel Virtual Smart Card and store it on the PC's hardware.

You can run the MyID Self-Service App in Intel Virtual Smart Card-only mode to restrict the list of available credentials – see the ***Self-Service App Installation and Configuration*** document for details of the `/iptonly` command-line option.

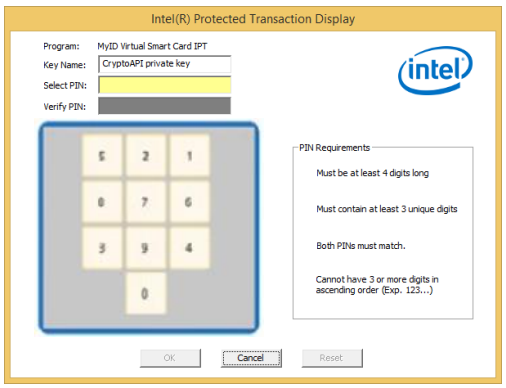
5.2.1 Using Intel Authenticate

Once issued, the Virtual Smart Card will use the authentication factors registered using the Intel Authenticate factor management application. No factor enrollment takes place using the MyID Self-Service App.

Note: If you installed Intel Authenticate before MyID, you must remove any older Intel Virtual Smart Cards before issuance starts. For more information on removing the Intel Virtual Smart Card, contact customer support, quoting reference SUP-192.

5.2.2 Using Intel IPT-PKI

During collection using the MyID Self-Service App, the Intel Protected Transaction Display will require the user PIN to be set for each certificate that is being issued to the device.



5.3 Enabling, disabling, and canceling Intel Virtual Smart Cards

You can enable, disable, and cancel Intel Virtual Smart Cards using the following methods:

- The **Enable/Disable Card** workflow.
- The **Erase Card** workflow.

  You can use the **Erase Card** workflow in MyID Desktop to erase a VSC that is present on the PC on which Desktop is running.
- The **Cancel Credential** workflow.

  You can use the **Cancel Credential** workflow to revoke a VSC even if it is not present; however, this revokes the VSC and its certificates without removing the VSC from the PC itself. To remove the VSC from the PC, you must use **Erase Card**.
- The **Issued Certificates** workflow.
- The **Edit Person** workflow – if you disable a user, the Intel Virtual Smart Card is disabled or cancelled, and its certificates suspended or revoked, depending on the revocation status mapping you select.

  See the ***Administration Guide*** for details of the **Enable/Disable Card**, **Erase Card**, **Cancel Credential**, **Issued Certificates**, and **Edit Person** workflows.
- The Lifecycle API.

  See the ***Lifecycle API*** document for details.

These procedures will result in the credential certificates being suspended or revoked as appropriate; note, however, that the certificates on the user's PC will not be affected.

You can also use the **Credential Group** and **Cancel Previously Issued Device** options on the credential profile to cancel any previously-issued VSCs from the same credential group automatically when you issue a new VSC.

When you collect a new VSC using the Self-Service App, if you have the **Erase Unused VSCs** permission for your role (as configured in the **Edit Roles** workflow), the Self-Service App will delete any previously-cancelled VSCs; for example, VSCs cancelled using **Cancel Credential** or the **Credential Group** settings.

See the ***Administration Guide*** for details of using the **Erase Card** and **Cancel Credential** workflows, and the **Credential Group** options.

5.4 Requesting replacement Intel Virtual Smart Cards

If the certificates on an Intel Virtual Smart Card are approaching expiry, or a user has forgotten their PIN, you can request a replacement credential with updated certificates.

You can use the following methods:

- The **Request Replacement Card** workflow.

  See the ***Administration Guide*** for details of the **Request Replacement Card** workflow.

  For a forgotten PIN, the recommended reason for replacement is **Revocation (other)**. Include the information about the forgotten PIN in the **Details** box.

- The Lifecycle API.

  See the ***Lifecycle API*** document for details.

Note: Currently, certificate renewal is not supported.

Once you have requested a replacement credential (and optionally validated the request) the user can collect the replacement credential using the Self-Service App. The original credential will be removed and the certificates will be revoked.

5.5 Windows Logon

An Intel Virtual Smart Card can be used for Windows logon when issued with a suitable certificate.

Note: If you want to use a certificate for Windows Logon, make sure it has 2048-bit keys.

MyID can force this to be used by setting the user's active directory attribute "Smart card is required for interactive logon" once the Virtual Smart Card has been issued successfully.

This feature requires careful configuration. For more information, contact customer support, quoting reference SUP-227.

5.5.1 Logging on using Intel Authenticate

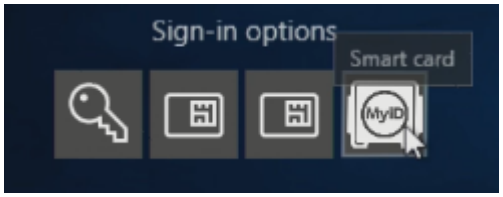
At the Windows logon screen, the user will be prompted to:

- Press Enter to login with Intel Authenticate

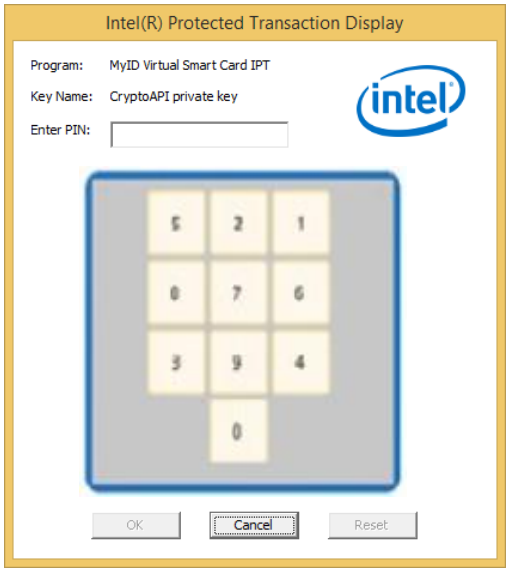
This uses the registered factors to log on to Windows; for example, fingerprint, PIN, and so on.

5.5.2 Windows Logon using IPT-PKI

At the Windows logon screen, select the **Sign-in options**, then select the MyID Virtual Smart Card icon.



Once you have selected the credential, click **Next**, and the Intel Protected Transaction Display will be displayed to enter your PIN:



Windows logon will then continue as normal.

6 Limitations

Intel Authenticate and Intel Virtual Smart Cards will appear as smart cards to the operating system; however, they do not support all of the features or lifecycle management capabilities as a physical smart card.

For example:

- MyID Credential Profile limitations:
  - PIN settings/PIN characters will have no effect on Intel Virtual Smart Cards as this is controlled outside of MyID.
  - You cannot lock or unlock the PIN.
  - Issuance or recovery of certificates with archived certificates is not supported.
  - Selecting Intel Authenticate or Intel IPT-PKI for MyID Logon and MyID Encryption is not supported.
  - Additional Identity certificates are not supported.
- Automatic renewal of certificates is not supported for Intel Virtual Smart Cards. You are advised to disable this feature on your profile.
- Cancelling the Intel Virtual Smart Card using the **Cancel Credential** workflow will cause a revocation on the certificate authority, but not remove the certificates from the local PC. The user will be revoked once the CRL has been updated from the certificate authority, and Windows will stop the authentication.
- The Self-Service App can be aborted while the Intel Protected Transaction Display (PTD) is on screen. As the PTD is driven from the Intel processor, there is no connection between these windows; therefore, you may encounter issues. You are recommended to cancel the PTD before aborting the Self-Service App.

7 Troubleshooting

- **Minimum hardware requirement check fails**

  In the Self-Service App, the error is:

  ```
  An enabled IPT is required to continue
  ```

  The error may be caused by a variety of reasons. Use the audit message to diagnose the problem:

  - `Could not Establish Named Pipe Connection`

    Check that the MyID Windows Integrated Service is running.

  - `Service provider not found`

    Check that the Intercede VSC configuration utility has been installed.

  - `Check IPT Failed. IPT – PKI CSP Provider name has not been configured`

    Check that the Intel IPT with PKI – Exportable Keys CSP is installed.

- **Cannot find the locally-created VSC card.**

  In the Self-Service App, this error will cause the application to terminate. The following audit message is reported:

  ```
  Unable to find locally created VSC
  ```

  This is likely to occur due to the total number of cards (including VSCs) exceeding the system's limit. In Windows, the maximum number of cards is 10. Remove any unused cards from the system.

- **MyID Intel Authenticate drivers are not installed or the MyID VSC Service is not running**

  In the Self-Service App, the error is:

  ```
  An error occurred logging into the card: The entered PIN is either longer or shorter than is accepted by the card
  ```

  Check that the MyID Intel Authenticate drivers are installed and that the MyID VSC Service is running.

- **IPT-PKI uses anti-hammering when repeated incorrect PINs are used**

  An incorrect PIN message appears when getting an incorrect PIN.

  A timeout warning and duration is displayed (for example, two minutes) when the anti-hammering is activated. This applies to all MyID Intel Virtual Smart Cards on the PC, as this a PC-level lock-out and affects all users.

- **Untrusted Publisher dialog**

  You may see an issue where you are prompted to trust the signature of the publisher of the minidriver and virtual reader, even when the certificate is installed to the Trusted Publishers store. This is a known issue; see the following knowledge base article for a Microsoft hotfix:

  https://support.microsoft.com/en-us/kb/2921916

- **Unable to use newly-issued credential**

  After issuing an Intel Authenticate credential, the user must log off and log back on with the new credential before they can use the new certificates fully.

8 Known Issues

- **IKB-190 – Issues with Windows 10 Anniversary Update**

  Some problems have been identified with Intel VSCs on Windows 10 operating systems that have been updated to version 1607 (Anniversary Update).

  The symptoms include:

  - Intel Protected Transaction Display opening then immediately closing.
  - Intel Protected Transaction Display keypad being offset, preventing access to some numeric keys.
  - Intel Virtual Smart Card disappearing.

  If you intend to use Windows 10 Anniversary Update, contact customer support quoting IKB-190 for further information on the resolution of these issues.

- **IKB-191 – Logon, witnessing, or approving with an Intel VSC**

  You cannot currently use an Intel Virtual Smart Card for authentication in MyID. On the logon page, this device type will show the following message:

  ```
  This card cannot be used
  ```

  Once logged in to MyID, operations that have a witness or approval stage may include an Intel Virtual Smart Card in the list of credentials that can be used; however, any attempt to use the Intel VSC will fail.

  Support for logon, witnessing or approving will be added in a future release.

- **IKB-209 – Multiple users**

  The current release of Intel Authenticate supports only a single Virtual Smart Card on one computer. MyID has the capability to issue multiple VSC to one computer.

  If multiple VSC are issued, then users may experience failure to logon to Windows, or Windows requiring passwords for one of the accounts.