MyID Enterprise
Version 12.10

FIDO Authenticator Integration Guide

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:

  For example:
  - Copy the file *before* starting the installation.
  - Do *not* remove the files before you have backed them up.
- ***Bold and italic*** hyperlinks 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 installation media.
- A `fixed width` font is used where the identification of spaces is important, including filenames, example SQL queries and any entries made directly into configuration files or the database.
- **Notes** are used to provide further information, including any prerequisites or configuration additional to the standard specifications.

  For example:

  Note: This issue only occurs if updating from a previous version.
- Warnings are used to indicate where failure to follow a particular instruction may result in either loss of data or the need to manually configure elements of the system.

  For example:

  Warning: You must take a backup of your database before making any changes to it.

Contents

1 Introduction

This guide provides details of how to integrate your MyID® system with FIDO (Fast IDentity Online) authenticator devices.

FIDO authenticators are removable devices (smart cards or USB tokens) or devices built into a computer (for example, a mobile phone). These authenticators may provide single-factor, two-factor, or multi-factor authentication.

You can use MyID to request, register, or cancel FIDO authenticators, and you can configure MyID to use an issued FIDO authenticator to log on to your MyID system. You can use the Self-Service Request Portal with an already-issued smart card to request (and optionally register) a FIDO authenticator for yourself.

For information on configuring the Self-Service Request Portal, see the ***Derived Credentials Self-Service Request Portal*** guide.

Intercede also provides a plug-in for AD FS (the MyID AD FS Adapter OAuth) that allows you to use the MyID authentication service in conjunction with a registered FIDO authenticator to access AD FS (Active Directory Federation Services); see the *MyID AD FS Adapter OAuth* section in the ***MyID Authentication Guide*** for details.

You can integrate MyID's authentication service with your own system to authenticate a person's identity using their FIDO authenticator using OAuth 2.0 OpenID Connect; see the *Authenticating using OpenID* section in the ***MyID Authentication Guide*** for details.

You can also set up the MyID authentication service as a standalone service (for high availability FIDO authentication operations); see the *Setting up the standalone authentication service* section in the ***MyID Authentication Guide*** for details.

1.1 Supported authenticators

MyID can work with any FIDO compatible authenticator that meets the technical standards set by the FIDO Alliance.

FIDO authenticators may provide single-factor, two-factor, or multi-factor authentication.; you can configure MyID to treat FIDO basic assurance authenticators and high assurance authenticators with different levels of trust; for example, you can enable logon to MyID for high assurance authenticators, but disable logon for basic assurance authenticators.

See section *2.5*, *Setting up credential profiles for FIDO authenticators* and section *2.7*, *Configuring MyID for FIDO logon* for details.

1.2 Supported browsers

The FIDO authenticator registration process is supported on the following browsers:

- Google Chrome
- Microsoft Edge (Chromium version)
- Mozilla Firefox.

Note: The pre-Chromium version of Microsoft Edge is not supported.

2 Configuring MyID for FIDO authentication

To configure MyID for FIDO authentication, you must carry out the following:

- Set the MyID configuration options.

  See section *2.1*, *Setting the configuration options*.

- Set up your MyID system for email notifications.

  See section *2.2.1*, *Configuring your system for email notifications*.

- Configure your email templates for the FIDO issuance notification and the registration code.

  See section *2.2.2*, *Editing the notification templates*.

- Optionally, set up SMS for mobile notifications.

  See section *2.2.3*, *Configuring the registration code to be sent by SMS*.

- Configure the MyID authentication service with the FIDO metadata.

  See section *2.3*, *Setting up the FIDO metadata*.

- If necessary, amending the server settings.

  See section *2.4*, *Configuring the server settings*.

- Set up a credential profile for FIDO authenticators.

  See section *2.5*, *Setting up credential profiles for FIDO authenticators*.

- Configure your end-user roles to allow for FIDO registration.

  See section *2.6*, *Configuring roles for registering FIDO authenticators*.

- Optionally, configure MyID for logon using a FIDO authenticator.

  See section *2.7*, *Configuring MyID for FIDO logon*.

2.1 Setting the configuration options

To set the configuration options required for registering FIDO authenticators:

1. Log on to MyID Desktop as an administrator.

2. From the **Configuration** category, select **Operation Settings**.

3. On the **General** tab, set the following option:

   - **URL path** – make sure this is set to the URL of the MyID web server. Include the protocol and server name only; for example:

     `https://myserver.example.com`

     MyID uses this option to generate the link to the registration page for FIDO authenticators on the authentication service.

     Important: Your MyID system must be set up to use https.

4. Click **Save changes**.

5. From the **Configuration** category, select **Security Settings**.

6. On the **Logon** tab, set the following option:

   - **Allow Logon Codes** – set this option to `Yes` ✅.

     MyID uses this option to generate a single-use code for the FIDO authenticator registration process.

7. Click **Save changes**.

2.2 Setting up email templates for FIDO registration

When a person requests a FIDO authenticator through the MyID Operator Client or the Self-Service Request Portal (assuming the credential profile is not set up for immediate registration), MyID sends two email messages; the first contains a link to the registration web page, and the second contains a single-use registration code.

You can edit the templates used for these messages; see section *2.2.2*, *Editing the notification templates*.

For increased security, you can configure MyID to send the registration code by SMS instead of email; see section *2.2.3*, *Configuring the registration code to be sent by SMS*.

2.2.1 Configuring your system for email notifications

You must configure your system with an SMTP server; see the *Setting up email* section in the ***Advanced Configuration Guide***.

You must also ensure that everyone who is going to request a FIDO authenticator has an email address stored in their user account. You can use the **Requisite User Data** feature of the credential profile to prevent people who do not have email addresses from requesting FIDO authenticators; see section *2.5*, *Setting up credential profiles for FIDO authenticators*.

2.2.2 Editing the notification templates

To edit the content of the FIDO registration messages:

1. Log on to MyID Desktop as an administrator.

2. From the **Configuration** category, select **Email Templates**.

3. Select one of the following templates, and click **Modify**:

   - **Register FIDO Authenticator** – this template contains the link to the MyID authentication web page.

     You can provide the following information in this message:

     - `%x` – the URL of the MyID web server. This is taken from the URL Path configuration option; see section *2.1*, *Setting the configuration options*.

     - `%jobguid` – the ID of the request for the FIDO authenticator.

       Important: The registration URL you provide in the message *must* have the following format:

       `%x/web.oauth2/fido/register/begin?requestId=%jobguid`

   - **FIDO Authenticator Registration Code** – this template contains the single-use registration code that the end user will enter to complete their registration.

     You can provide the following information in this message:

     - `%logonName` – the person's logon name.

     - `%logonCode` – the FIDO registration code.

2.2.3 Configuring the registration code to be sent by SMS

To allow MyID to send SMS messages, set the **SMS email notifications** on the **General** tab of the **Operation Settings** workflow to `Yes`.

By default, SMS messages are sent to an Email to SMS gateway, in the format `<cellnumber>@<gateway>`, where:

- `<cellnumber>` – the cell phone number from the user's record.

- `<gateway>` – the URL from the **SMS gateway URL for notifications** option on the **General** tab of the **Operation Settings** workflow.

For example: `00447700900123@smsgateway.com`

If this is not suitable, you can customize the `sp_CustomPrepareSMS` stored procedure in the MyID database.

You must also edit the email template containing the registration code, and change it to use SMS instead of email for its transport:

1. Log on to MyID Desktop as an administrator.

2. From the **Configuration** category, select **Email Templates**.

3. Select the **FIDO Authenticator Registration Code** template, and click **Modify**.

   The Edit Email Template screen appears.

4. From the **Transport** drop-down list, select **sms**.

5. Click **Save**.

Important: If you configure the registration codes to be sent by SMS, you must ensure that everyone who is going to request a FIDO authenticator has a mobile phone number stored in their user account. You can use the Requisite User Data feature of the credential profile to prevent people who do not have mobile phone numbers from requesting FIDO authenticators; see section *2.5*, *Setting up credential profiles for FIDO authenticators*.

2.3 Setting up the FIDO metadata

To allow MyID to carry out attestation checks on FIDO authenticators during registration, it requires access to the FIDO Alliance Metadata Service metadata. You can obtain FIDO metadata online (this is the default) or from a local file system repository.

Access to online metadata is controlled from the configuration file for the MyID authentication web service (web.oauth2) using the `OnlineMetadata` Fido setting:

```
"Fido": {
"Config": {
// If OnlineMetadata is true FIDO metatdata will be downloaded from
https://mds.fidoalliance.org/
"OnlineMetadata": true,
// Optionally provide a FIDO metadata Blob root certificate in base64 format
"MetadataBlobRootCert": "",
// Control whether the certificates in the chain of trust for the FIDO metadata service
BLOB is CRL checked.
"DisableCrlCheck": false,
}
}
```

The installer sets `OnlineMetadata` to `true` by default in the `appsettings.json` file, meaning that FIDO metadata is obtained from the online source. If you need to change any settings, you can edit the `appsettings.Production.json` file to override the settings in the `appsettings.json` file.

The MyID FIDO implementation uses an built-in FIDO Alliance ROOT certificate which is part of the certificate chain of trust for the signed metadata `blob.jwt` (see section *2.3.1, Setting up a local metadata repository*). This certificate has an expiry date of 2029. If this certificate expires, or the FIDO Alliance certificate chain changes, you can provide an external root certificate as a base64 string through the `MetadataBlobRootCert` setting above. The root certificate is then used to verify cryptographically any `blob.jwt` obtained online or used by the local metadata repositories.

For online metadata during FIDO registration, you can disable CRL checking of the metadata chain of trust certificates by setting `DisableCrlCheck` to `true`. The default value is `false` which means that CRL checking is enabled by default. The `DisableCrlCheck` setting applies only to online metadata; no CRL checking is done on a local metadata repository.

Previous versions of FIDO on MyID used the FIDO Alliance MDS2 metadata service, which required an access token to be able to download the metadata. With the newer MDS3 FIDO Alliance metadata service, this is no longer the case, with metadata now freely available as a direct download from:

mds.fidoalliance.org

The MyID web server must be able to access the above FIDO Alliance URL to download the metadata. If your server cannot access this URL, or if you are experiencing performance issues when verifying metadata, you can create a local repository; see section *2.3.1, Setting up a local metadata repository*.

Note: If you are using the standalone authentication service (web.oauth2.ext) in conjunction with the AD FS Adapter OAuth to allow for FIDO authentication to your AD FS, the web.oauth2.ext service configuration for `OnlineMetadata` is ignored, because attestation checks are relevant only for registration, and the standalone authentication service provides only authentication and not registration for FIDO authenticators.

2.3.1 Setting up a local metadata repository

You can create a local metadata repository, which you can then configure the authentication service to use instead of the live metadata from the FIDO Alliance website.

To create a local repository:

1. Download the MDS3 FIDO Alliance metadata.

   In your browser, navigate to:

   mds.fidoalliance.org

   This downloads a single `blob.jwt` file that contains, amongst other things, the FIDO Alliance metadata statements for all registered FIDO authenticators.

2. Open the `appsettings.Production.json` file for the authentication service in a text editor.

   By default, this is:

   `C:\Program Files\Intercede\MyID\web.oauth2\appsettings.Production.json`

3. Edit the file to include the following settings:

```
"Fido": {
"Config": {
// If OnlineMetadata is true FIDO metatdata will be downloaded from
https://mds.fidoalliance.org/
"OnlineMetadata": false,
// If a filesystem FIDO metadata repository is provided by the customer
its path should be entered here.
"MDSCacheDirPath": "<path of cache folder",
// If a filesystem FIDO metadata repository is provided by the customer
and the customer wishes to override
// the nextUpdate time in the metadata BLOB file then this can be done by
setting the cache time in days from
// the time now.  A default value of 2 days ensures that during fido
registration the file is read only once
// from the file system with all subsequent times read from memory cache
until the system is restarted.
"CacheTimeDays": <validity period>
}
}
```

where:

- `<path of cache folder>` is the path of the folder where the `blob.jwt` is located. Use forward slashes or double backslashes in the path. A non-empty value here enables the local file system metadata repository.

- `<validity period>` is the number of days from the current time after which the cache will no longer be valid, and the authentication service will revert to re-reading the metadata from the file system rather than its own in-memory cache.

The installer sets a default value of 2 days for `CacheTimeDays` in the `appsettings.json` file. This means, after reading the file system metadata into memory cache, it will keep using the memory cache for two days (or until the server app pool is recycled) then re-read the file system metadata into memory cache and then use memory cache for

another 2 days and so on. If you set the `CacheTimeDays` value to 0 it will be ignored and the `nextUpdate` time specified in the `blob.jwt` file will apply; when that expires it will keep reading from the file system.

Important: Merge these settings into your existing `Fido:Config` section. Do not delete any existing settings.

If you want to use the local repository in preference to the live data, you can set the `OnlineMetadata` option to `false` as shown above.

If you leave the `OnlineMetadata` set to `true` in the configuration file, MyID uses both live metadata and metadata from the local repository. You can use either or both options.

4. Save the `appsettings.Production.json` file.

5. Recycle the web service app pool:

   a. On the MyID web server, in Internet Information Services (IIS) Manager, select **Application Pools**.

   b. Right-click the myid.web.oauth2.pool application pool, then from the pop-up menu click **Recycle**.

   This ensures that the web service has picked up the changes to the configuration file.

Note: Earlier versions of FIDO on MyID used a `MyID.FIDO.Metadata.App` to obtain a local metadata repository from the MDS2 server. With MDS3 no such app is required as the metadata is all in a single `blob.jwt` file that is freely available from the FIDO Alliance MDS3 server.

Existing MDS2 metadata JSON files are not compatible with the MDS3 metadata specification. This means customers who already have MDS2 metadata JSON files in their local repository must replace them with a single MDS3 compatible `blob.jwt` metadata file.

You can place individual MDS3-compliant JSON metadata statement files alongside the `blob.jwt` in the file system repository folder and they are read in and appended to the metadata extracted from the `blob.jwt` file. This is useful if you want to use metadata for authenticators that have not been registered with the FIDO Alliance.

JWT metadata files are cryptographically verified as originating from the FIDO Alliance before being accepted as a source of metadata.

Only one JWT file is supported in the local repository path. If more than one file is present, only the first found alphabetically will be used.

2.4 Configuring the server settings

This section contains information on configuring the server settings in the `appsettings.Production.json` file.

2.4.1 FIDO configuration file options

The server settings are derived from the value you provided for the **MyID Server URL** in the MyID installation program, and are initially stored in the `appsettings.json` file. If you need to change these settings, you can edit the `appsettings.Production.json` file to override the settings in the `appsettings.json` file.

Note: If you subsequently install or upgrade MyID again and provide a different value in the **MyID Server URL** in the MyID installation program, and you have set the `Origin`, `Origins`, or `ServerDomain` options in the `appsettings.Production.json` file, the values you enter in the installation program are ignored; the `appsettings.Production.json` file is never updated by the installation program, and always takes precedence over the `appsettings.json` file.

- `ServerDomain` is used when registering the FIDO to instruct the FIDO token the domain that may be used during authentication. It must be either:

  - The exact web domain name that will be used during authentication. In this case, only this domain may be used during authentication, *or*:

  - A registrable domain suffix of the web domain that will be used during authentication. In this FIDO authentication will be possible either using this exact domain, or any sub-domain of that domain

- `Origin` or `Origins` specify the origins that are allowable to be used during FIDO authentication.

  Use `Origin` if you have a single origin, or `Origins` if you have multiple origins; if you specify a value for `Origins`, it overrides any setting you provide for `Origin`.

For example: web.oauth2 is running on `https://myid.customer.com`

In this case, set `Origin` to `https://myid.customer.com` and `ServerDomain` to `myid.customer.com` – this allows tokens to be registered on the `myid.customer.com` domain so that they can authenticate only on `myid.customer.com`.

Alternatively: you intend to register FIDO tokens in web.oauth2 on `https://customer.com` and for those tokens to authenticate to that instance of MyID, but that instance of MyID is also reachable through a sub-domain `https://subdomain.customer.com`

In this case, on web.oauth2 set the `Origins` to:

```
["https://customer.com","https://subdomain.customer.com"]
```

This allows authentication on either of those origins. Then set `ServerDomain` to:

```
customer.com
```

That is, the registrable domain suffix, which means that the FIDO token can be used to authenticate on the `customer.com` domain or any sub-domain of `customer.com`, subject to the `Origin` also being listed in the `Origin` or `Origins` section.

2.4.2 Single origin

To configure the server settings for a single origin:

1. As an administrator, open the `appsettings.Production.json` file in a text editor.

   By default, this is:

   ```
   C:\Program Files\Intercede\MyID\web.oauth2\appsettings.Production.json
   ```

   This file is the override configuration file for the `appsettings.json` file for the web service. If this file does not already exist, you must create it in the same folder as the `appsettings.json` file.

2. Edit the file to include the following:

   ```json
   {
       "Fido":{
           "Config":{
               "Origin":"https://<server>:<port>",
               "ServerDomain":"<server>"
           }
       }
   }
   ```

   where:

   - `<server>` – the name of the server to which users will authenticate.

   - `<port>` – optionally, the port to which users will authenticate, if you are using a non-standard HTTPS port.

   You must add the `Origin` and `ServerDomain` to any existing entries in the `Fido:Config` section. Your `appsettings.Production.json` file may already contain commented-out entries for these values; remove the double-slash `//` to uncomment the entries.

   Important: The `Origin` and `ServerDomain` options are case sensitive, and must be consistent with the casing of the DNS Name in the web server's TLS certificate.

   For example:

   ```json
   {
     "Fido":{
       "Config":{
         "Origin": "https://myserver.example.com:30443",
         "ServerDomain": "myserver.example.com"
       }
     }
   }
   ```

3. Save the `appsettings.Production.json` file.

4. Recycle the web service app pool:

    a. On the MyID web server, in Internet Information Services (IIS) Manager, select **Application Pools**.

    b. Right-click the **myid.web.oauth2.pool** application pool, then from the pop-up menu click **Recycle**.

    This ensures that the web service has picked up the changes to the configuration file.

2.4.3 Multiple origins

MyID has support for multiple origins, where multiple sub-domains of a registrable domain can be used for authentication.

To configure the server settings for multiple origins:

1. As an administrator, open the `appsettings.Production.json` file in a text editor.

    By default, this is:

    `C:\Program Files\Intercede\MyID\web.oauth2\appsettings.Production.json`

    This file is the override configuration file for the `appsettings.json` file for the web service. If this file does not already exist, you must create it in the same folder as the `appsettings.json` file.

2. Edit the file to include the following:

    ```
    {
      "Fido":{
        "Config":{
          "Origins":["https://<server>:<port>",
    "https://<subdomain1>:<port>", "https://<subdomain2>:<port>" ... ],
          "ServerDomain":"<server>"
        }
      }
    }
    ```

    where:

    - `<server>` – the name of the server that contains the sub-domains to which users will authenticate.

    - `<subdomainx>` – A list of sub-domains of the server domain that will be allowed to authenticate.

    - `<port>` – optionally, the port to which users will authenticate, if you are using a non-standard HTTPS port.

    Important: The `Origins` and `ServerDomain` options are case sensitive, and must be consistent with the casing of the DNS Name in the web server's TLS certificate.

3. Save the `appsettings.Production.json` file.

4. Recycle the web service app pool:

    a. On the MyID web server, in Internet Information Services (IIS) Manager, select **Application Pools**.

    b. Right-click the **myid.web.oauth2.pool** application pool, then from the pop-up menu click **Recycle**.

    This ensures that the web service has picked up the changes to the configuration file.

Note: If `Origins` is specified then it overrides any value in `Origin`.

2.5 Setting up credential profiles for FIDO authenticators

You must set up one or more credential profiles for your FIDO authenticators.

The options you select depend on whether you intend to request the FIDO authenticator through the MyID Operator Client or through the Self-Service Request Portal.

2.5.1 Setting up a FIDO credential profile for the MyID Operator Client

To set up a credential profile for FIDO authenticators that you can use for requests made in the MyID Operator Client:

1. Log on to MyID Desktop as an administrator.

2. From the **Configuration** category, select **Credential Profiles**.

3. Click **New**.

4. In the **Card Encoding** list, select **FIDO Authenticator (Only)**.

   Note: The other options are disabled. The **Derived Credential** option is not disabled; however, it is used only for requests made through the Self-Service Request Portal. See section *2.5.2*, *Setting up a FIDO credential profile for the Self-Service Request Portal*.

5. In the **Services** section, you can set the following:

   • **MyID Logon** – select this option if you want to be able to log on to MyID with the authenticator.

   Note: The **MyID Encryption** option is disabled. You cannot use a FIDO Authenticator to store an encryption certificate.

6. In the **Issuance Settings** section, the following options are available:

    *   **Validate Issuance**

    *   **Validate Cancellation** – do not select this option. Validating cancellation is not supported with FIDO authenticators, and setting this option may result in being unable to cancel the device.

    *   **Lifetime**

    *   **Credential Group**

    *   **Block Multiple Requests for Credential Group**

    *   **Cancel Previously Issued Device**

    *   **Enforce Photo at Issuance** – do not select this option. Request checks are performed for FIDO authenticators, but issuance checks are not; instead of standard MyID issuance, authenticators use a FIDO-specific registration process.

    *   **Notification Scheme**

    *   **Require user data to be approved**

    See the *Working with credential profiles* section in the ***Administration Guide*** for details of these options.

    You must also set the following option:

    *   **Generate Code on Request** – set this to one of the following options:

        *   **Simple Logon Code** – the FIDO registration code is generated using the complexity rules as defined by the **Simple Logon Code Complexity** configuration option on the **Auth Code** tab of the **Security Settings** workflow.

            By default, this is `12-12N`, which means a 12-digit number.

        *   **Complex Logon Code** – the FIDO registration code is generated using the complexity rules as defined by the **Complex Logon Code Complexity** configuration option on the **Auth Code** tab of the **Security Settings** workflow.

            By default, this is `12-12ULSN[BGI1OQDSZ]`, which means a 12-character code containing upper case, lower case, special characters, and numbers, and a set of commonly-confused characters excluded.

    Important: Do not select **None**. MyID must generate a FIDO registration code to be used in the FIDO authenticator registration process.

    For more information about the format of these codes, see the *Setting up logon codes* section in the ***Administration Guide***.

7. In the **FIDO Settings** section, set the following:

- **Assurance Level** – select one of the following options:

  - **Basic** – the FIDO authenticator uses single factor authentication, and is suitable for use with some external systems, but not for access to crucial systems.

  - **High** – the FIDO authenticator uses multi-factor authentication, and is suitable for use with secure systems, such as logging on to MyID.

    You are recommended to set **Assurance Level** to **High** only when you have also set the **User Verification** to **Required**.

  MyID differentiates between FIDO authenticators that have been issued with a credential profile where the **Assurance Level** is set to **Basic** or **High** – for example, you can enable logon to MyID for **FIDO High Assurance**, but disable logon for **FIDO Basic Assurance**. See section *2.7*, *Configuring MyID for FIDO logon* for details.

- **User Verification** – select one of the following options:

  - **Required** – the FIDO authenticator supports two-factor authentication. If the authenticator does not support two-factor authentication, it cannot be registered.

  - **Preferred** – the FIDO authenticator will use two-factor authentication if the authenticator supports that feature, but will still be registered if it supports only one-factor authentication.

  - **Discouraged** – the FIDO authenticator will use single-factor authentication, unless the authenticator cannot work without multi-factor authentication.

- **Authenticator Type** – select one of the following options:

  - **Internal** – you can issue this credential profile to internal FIDO authenticators; for example, authenticators included in mobile devices such as cell phones.

  - **Removable** – you can issue this credential profile to external removable authenticators; for example, USB tokens or smart cards.

  - **Internal or Removable** – you can issue this credential profile to internal or removable FIDO authenticators.

- **Require Client Side Discoverable Key** – select this option to ensure that the FIDO authenticator supports Resident Keys. If you select this option, and the FIDO authenticator supports client side discoverable keys, you can choose not to provide the username manually when using the FIDO authenticator to log on to MyID; see section *3.4*, *Logging on to MyID with FIDO authenticators*.

- **Enforce Authenticator Attestation Check** – select this option to carry out an authenticator attestation check during the registration process.

- **Immediate registration via Self-Service Request Portal** – used only for requests made through the Self-Service Request Portal. See section *2.5.2*, *Setting up a FIDO credential profile for the Self-Service Request Portal*.

8. In the **Requisite User Data** section, set any user attributes that you want to require for the people who will request FIDO authenticators.

   For example, as the FIDO notification is sent as an email, you are recommended to select **Email** in the **Required for Request** column.

   If you have configured your system to send the registration code in an SMS, you are recommended to select **Mobile** in the **Required for Request** column.

   For more information about this features, see the *Requisite User Data* section in the ***Administration Guide***.

9. Click **Next**.

10. In the **Select Roles** screen, select the roles you want to be able to receive, request, or validate FIDO registrations.

    - Make sure that people who will receive the FIDO authenticator have a role that is selected in the **Can Receive** list.

    - Make sure that operators who will request FIDO authenticators have a role that is selected in the **Can Request** list.

    - If you have selected the **Validate Issuance** option, make sure that operators who will approve requests for FIDO authenticators have a role that is selected in the **Can Validate** list.

    Note: You do not need to select any roles in the **Can Collect** list. Collecting FIDO authenticators is carried out by the person who is receiving the authenticator using a self-service registration process.

11. Click **Next**.

12. Type your **Comments**, then click **Next** to save the credential profile and complete the workflow.

2.5.2 Setting up a FIDO credential profile for the Self-Service Request Portal

To set up a credential profile for FIDO authenticators that you can use for requests made in the Self-Service Request Portal:

1. Log on to MyID Desktop as an administrator.

2. From the **Configuration** category, select **Credential Profiles**.

3. Click **New**.

4. In the **Card Encoding** list, select the following:

- **Derived Credential**

- **FIDO Authenticator (Only)**

Note: The other options are disabled.

5. In the **Services** section, you can set the following:

- **MyID Logon** – select this option if you want to be able to log on to MyID with the authenticator.

Note: The **MyID Encryption** option is disabled. You cannot use a FIDO Authenticator to store an encryption certificate.

6. In the **Issuance Settings** section, the following options are available:

- **Validate Issuance**

- **Validate Cancellation** – do not select this option. Validating cancellation is not supported with FIDO authenticators, and setting this option may result in being unable to cancel the device.

- **Lifetime**

- **Credential Group**

- **Block Multiple Requests for Credential Group**

- **Cancel Previously Issued Device**

- **Enforce Photo at Issuance** – do not select this option. Request checks are performed for FIDO authenticators, but issuance checks are not; instead of standard MyID issuance, authenticators use a FIDO-specific registration process.

- **Notification Scheme**

- **Require user data to be approved**

See the *Working with credential profiles* section in the ***Administration Guide*** for details of these options.

You must also set the following option:

- **Generate Code on Request** – set this to one of the following options:

  - **Simple Logon Code** – the FIDO registration code is generated using the complexity rules as defined by the **Simple Logon Code Complexity** configuration option on the **Logon** tab of the **Security Settings** workflow.

    By default, this is `12-12N`, which means a 12-digit number.

  - **Complex Logon Code** – the FIDO registration code is generated using the complexity rules as defined by the **Complex Logon Code Complexity** configuration option on the **Auth Code** tab of the **Security Settings** workflow.

    By default, this is `12-12ULSN[BGI1OQDSZ]`, which means a 12-character code containing upper case, lower case, special characters, and numbers, and a set of commonly-confused characters excluded.

Important: Do not select **None**. MyID must generate a FIDO registration code to be used in the FIDO authenticator registration process.

For more information about the format of these codes, see the *Setting up logon codes* section in the ***Administration Guide***.

7. In the **FIDO Settings** section, set the following:

- **Assurance Level** – select one of the following options:

  - **Basic** – the FIDO authenticator uses single factor authentication, and is suitable for use with some external systems, but not for access to crucial systems.

  - **High** – the FIDO authenticator uses multi-factor authentication, and is suitable for use with secure systems, such as logging on to MyID.

    You are recommended to set **Assurance Level** to **High** only when you have also set the **User Verification** to **Required**.

  MyID differentiates between FIDO authenticators that have been issued with a credential profile where the **Assurance Level** is set to **Basic** or **High** – for example, you can enable logon to MyID for **FIDO High Assurance**, but disable logon for **FIDO Basic Assurance**. See section *2.7*, *Configuring MyID for FIDO logon* for details.

- **User Verification** – select one of the following options:

  - **Required** – the FIDO authenticator supports two-factor authentication. If the authenticator does not support two-factor authentication, it cannot be registered.

  - **Preferred** – the FIDO authenticator will use two-factor authentication if the authenticator supports that feature, but will still be registered if it supports only one-factor authentication.

  - **Discouraged** – the FIDO authenticator will use single-factor authentication, unless the authenticator cannot work without multi-factor authentication.

- **Authenticator Type** – select one of the following options:

  - **Internal** – you can issue this credential profile to internal FIDO authenticators; for example, authenticators included in mobile devices such as cell phones.

  - **Removable** – you can issue this credential profile to external removable authenticators; for example, USB tokens or smart cards.

  - **Internal or Removable** – you can issue this credential profile to internal or removable FIDO authenticators.

- **Require Client Side Discoverable Key** – select this option to ensure that the FIDO authenticator supports Resident Keys. If you select this option, and the FIDO authenticator supports client side discoverable keys, you can choose not to provide the username manually when using the FIDO authenticator to log on to MyID; see section *3.4*, *Logging on to MyID with FIDO authenticators*.

- **Enforce Authenticator Attestation Check** – select this option to carry out an authenticator attestation check during the registration process.

- **Immediate registration via Self-Service Request Portal** – select this option if you want to register the authenticator immediately when the cardholder makes the request in the Self-Service Request Portal. If you do not select this option, MyID sends the standard registration messages, and the person can register their authenticator later.

8. In the **Requisite User Data** section, set any user attributes that you want to require for the people who will request FIDO authenticators.

   For example, if you are not using immediate registration, as the FIDO notification is sent as an email, you are recommended to select **Email** in the **Required for Request** column.

   If you have configured your system to send the registration code in an SMS, you are recommended to select **Mobile** in the **Required for Request** column.

   For more information about this features, see the *Requisite User Data* section in the ***Administration Guide***.

9. Click **Next**.

10. In the **Select Roles** screen, select the **Derived Credential Owner** role for each of the following:

    - **Can Receive**
    - **Can Request**
    - **Can Collect**

    Note: You do not need to select any of the roles held by the person who will receive the FIDO registration request.

11. Click **Next**.

12. Type your **Comments**, then click **Next** to save the credential profile and complete the workflow.

2.6 Configuring roles for registering FIDO authenticators

Any person who wants to register a FIDO authenticator must have a role that has permission to use the Register FIDO Security Key option.

To configure a role for registering FIDO authenticators:

1. Log on to MyID Desktop as an administrator.

2. From the **Configuration** category, select **Edit Roles**.

3. Click **Show/Hide Roles** to display the role to which you want to add the FIDO registration permission.

   Note: This role *must* have access to the Password logon mechanism; the FIDO registration code is a special case of a logon code, and logon codes use the Password logon mechanism.

4. From the **Cards** section, select the following option:

   • **Register FIDO Security Key**

   Note: If you are using the Self-Service Request Portal to request and register FIDO authenticators, you must set up the **Derived Credential Owner** role to have access to the Password logon mechanism and the **Register FIDO Security Key** option.

5. Click **Save Changes**.

Any person who has the selected role can now access the authentication service to register a FIDO authenticator.

2.7 Configuring MyID for FIDO logon

If you want to allow people to log on to your MyID system using their registered FIDO authenticators, you can configure MyID to allow this feature.

Configuring FIDO logon requires the following:

• Setting up global configuration options for FIDO logon.

• Configuring individual roles for FIDO logon.

Note: You are recommended to restrict logon to multi-factor authenticators; MyID allows you to differentiate between Basic assurance authenticators and High assurance authenticators. If you allow logon for Basic assurance authenticators, you are recommended to allow those users access only to read-only features with limited scope.

2.7.1 Setting the FIDO logon configuration options

You can enable or disable FIDO logon globally using the configuration options.

To enable or disable FIDO logon:

1. Log on to MyID Desktop as an administrator.

2. From the **Configuration** category, select **Security Settings**.

3. On the **Logon Mechanisms** tab, set the following options:

   - **FIDO Basic Assurance Logon** – set this option to `Yes` ✅ to enable logon to MyID with a FIDO authenticator that has been issued with a credential profile where the **Assurance Level** is set to **Basic**.

   - **FIDO High Assurance Logon** – set this option to `Yes` ✅ to enable logon to MyID with a FIDO authenticator that has been issued with a credential profile where the **Assurance Level** is set to **High**.

4. Click **Save changes**.

2.7.2 Setting up FIDO logon mechanisms

For each role in MyID, you can decide whether people who have been assigned that role can log on to MyID using their registered FIDO authenticator and access the features that are configured for that role.

Note: If a person has multiple roles, but has a FIDO logon mechanism configured for only some of them, when they log on to MyID using their FIDO authenticator they can access only those features that are configured for the roles that have the FIDO logon mechanism configured. For example, if Susan has a Cardholder role with access to **View Person**, and Reporter role with access to **Management Information Reports**, if only the Cardholder role has a FIDO logon mechanism configured, when she logs on to MyID using her FIDO authenticator, she can access only View Person; to access her reports, she must log on with a smart card.

1. Log on to MyID Desktop as an administrator.

2. From the **Configuration** category, select **Edit Roles**.

3. Click **Logon Methods**.

   The Logon Mechanisms screen appears.

Logon Mechanisms	Password	Smart Card	Windows Logon	Biometric Logon	Client Credentials OAuth2	Windows Hello	FIDO Basic Assurance	FIDO High Assurance
Cardholder (1)	☐	☐	☑	☑	☑	☐	☑	☑
Manager (2)	☐	☑	☑	☐	☑	☐	☐	☑
Security Chief (3)	☐	☑	☑	☐	☑	☐	☐	☐
Personnel (4)	☐	☑	☑	☐	☑	☐	☐	☐
Help Desk (6)	☐	☑	☑	☐	☑	☐	☐	☐
Contractor (20)	☐	☑	☐	☐	☐	☐	☐	☐
Foreign (21)	☐	☑	☐	☐	☐	☐	☐	☐
Emergency (22)	☐	☑	☐	☐	☐	☐	☐	☐
Signatory (23)	☐	☑	☐	☐	☐	☐	☐	☐
Adjudicator (24)	☐	☑	☐	☐	☐	☐	☐	☐
Operator (25)	☐	☑	☑	☐	☑	☑	☐	☐
SecurityGroupA (26)	☐	☐	☐	☐	☐	☐	☐	☐
SecurityGroupB (27)	☐	☐	☐	☐	☐	☐	☐	☐
SecurityGroupC (28)	☐	☐	☐	☐	☐	☐	☐	☐
Employee (29)	☐	☐	☐	☐	☐	☐	☐	☐
Applicant (101)	☐	☑	☐	☐	☐	☐	☐	☐
Issuer (102)	☐	☑	☐	☐	☐	☐	☐	☐
Security Officer (103)	☐	☑	☐	☐	☐	☐	☐	☐

OK

4. For each role you want to be able to log on to MyID using FIDO, select one of the following options:

   - **FIDO Basic Assurance** – access to the features configured for this role is allowed when logging on with a FIDO authenticator that has been issued with a credential profile where the **Assurance Level** is set to **Basic**.

   - **FIDO High Assurance** – access to the features configured for this role is allowed when logging on with a FIDO authenticator that has been issued with a credential profile where the **Assurance Level** is set to **High**.

5. Click **OK**.

6. Click **Save Changes**.

MyID is now configured for logon using FIDO authenticators. For information on using FIDO authenticators to log on, see section *3.4*, *Logging on to MyID with FIDO authenticators*.

2.8   Checking IIS configuration

You must make sure that your Internet Information Services (IIS) is set up with the correct feature delegation options.

In Internet Information Services (IIS) Manager, carry out the following:

1. In the **Connections** pane, select the web server.

2. In **Features View**, in the **Management** section, double-click the **Feature Delegation** option.

3. Ensure that the following are set:

    *   **Authentication - Anonymous** – make sure this is set to **Read/Write**.

    *   **Authentication - Windows** – make sure this is set to **Read/Write**.

    To change the setting, right-click the option, then from the pop-up menu select **Read/Write**.

If your system has these options set to **Read Only**, you may experience a problem using FIDO to authenticate, with a `500 30` server error message.

3 Working with FIDO authenticators

Once you have configured MyID for FIDO authenticators, you can:

- Request FIDO authenticators for people.

  See section *3.1*, *Requesting FIDO authenticators*.

- Register your authenticator with MyID.

  See section *3.2*, *Registering FIDO authenticators*.

- Canceling authenticators.

  See section *3.3*, *Canceling FIDO authenticators*.

- Log on to MyID using your registered authenticator.

  See section *3.4*, *Logging on to MyID with FIDO authenticators*.

3.1 Requesting FIDO authenticators

You can request a FIDO authenticator for a person using the MyID Operator Client. Alternatively, if a person already has a smart card issued, they can use the Self-Service Request Portal to request (and optionally register) a FIDO authenticator for themselves.

3.1.1 Requesting FIDO authenticators using the MyID Operator Client

You can use the MyID Operator Client to request a FIDO authenticator for a person.

1. Log on to the MyID Operator Client.

2. Click the **People** category and search for a person.

   See the *Searching for a person* section in the **MyID Operator Client** guide.

3. Click the **Request Device** option in the button bar at the bottom of the screen.

   You may have to click the **...** option to see any additional available actions.

4. From the **Credential Profile** drop-down list, select the FIDO credential profile you want to use.

   See section *2.5*, *Setting up credential profiles for FIDO authenticators* for details of FIDO credential profiles.

5. Click **Save** to make the request.

For more information about requesting devices, see the *Requesting a device for a person* section in the **MyID Operator Client** guide.

If your FIDO credential profile is configured to require validation, you must approve the request before MyID notifies the person that they can register their FIDO authenticator; see the *Approving requests* section in the **MyID Operator Client** guide for details.

See section *3.2*, *Registering FIDO authenticators* for details of carrying out the registration process.

3.1.2 Requesting FIDO authenticators using the Self-Service Request Portal

If you have an already-issued smart card, you can use this to request a FIDO authenticator through the Self-Service Portal.

For information on configuring the Self-Service Request Portal, see the **Derived Credentials Self-Service Request Portal** guide.
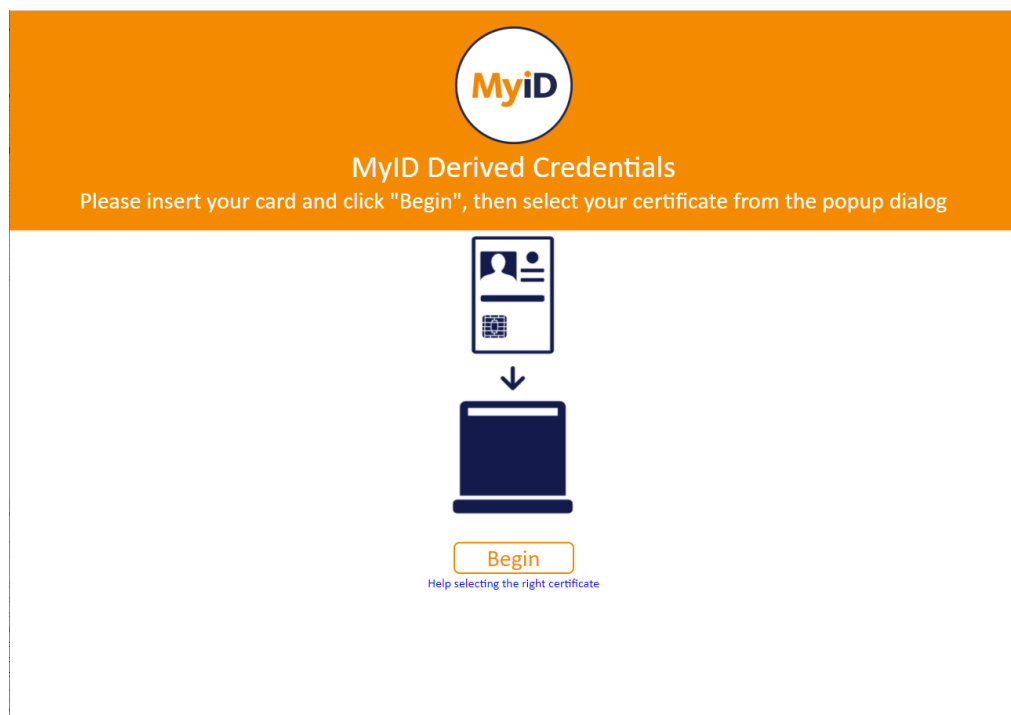
To request a FIDO authenticator through the Self-Service Portal:

1. Open a web browser and navigate to the StartPage on the SSRP web server:

    `https://<myserver>/StartPage`

    where `<myserver>` is the address of the MyID server hosting the Self-Service Portal.

    The start page appears.

2. Insert your card, click Begin, then select a certificate from your card.

The credential profile selection page appears.
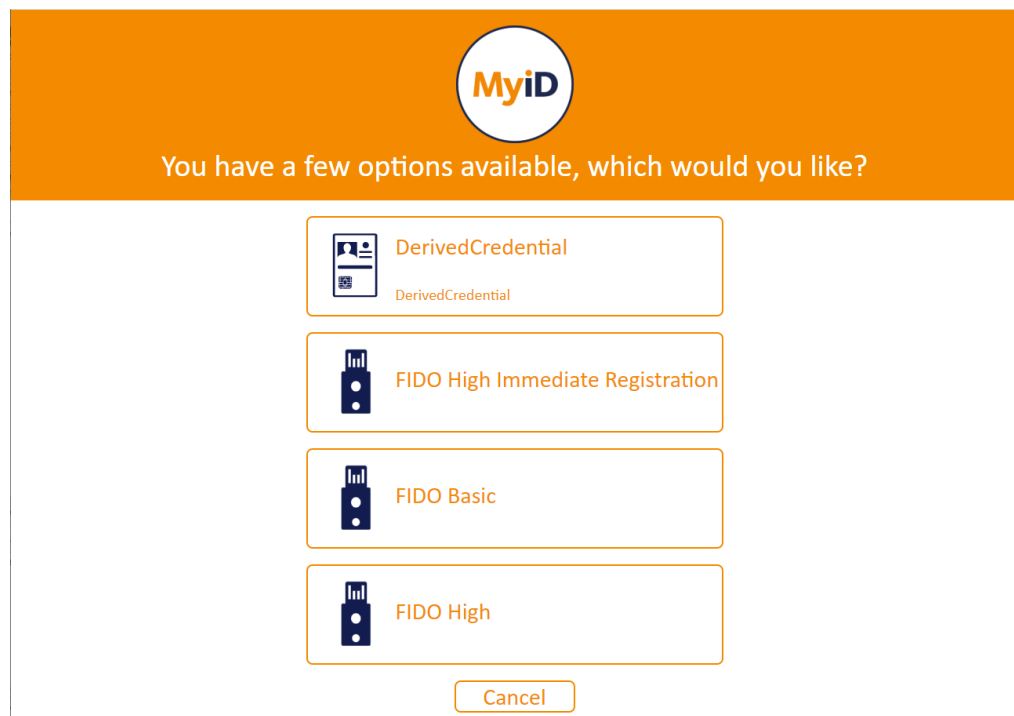
3. Select the credential profile you want to use.

See section *2.5.2*, *Setting up a FIDO credential profile for the Self-Service Request Portal* for details of setting up your FIDO authenticator credential profiles.

The next stage depends on how you have set up the **Immediate registration via Self-Service Request Portal** option in the credential profile:

- If the **Immediate registration via Self-Service Request Portal** option is set, you can register your FIDO authenticator immediately; see section *3.2.2*, *Registering FIDO authenticators using the Self-Service Request Portal*.

- If the **Immediate registration via Self-Service Request Portal** option is *not* set, MyID sends a registration link and a registration code; see section *3.2.1*, *Registering FIDO authenticators through notifications*.

3.2 Registering FIDO authenticators

You can register your FIDO authenticator using the following methods:

- Using a link and a registration code provided through notifications to your email address or cell phone.

- Using the Self-Service Request Portal for immediate registration after requesting an authenticator.

3.2.1 Registering FIDO authenticators through notifications

MyID sends two notifications to the person when a FIDO authenticator has been requested for them:
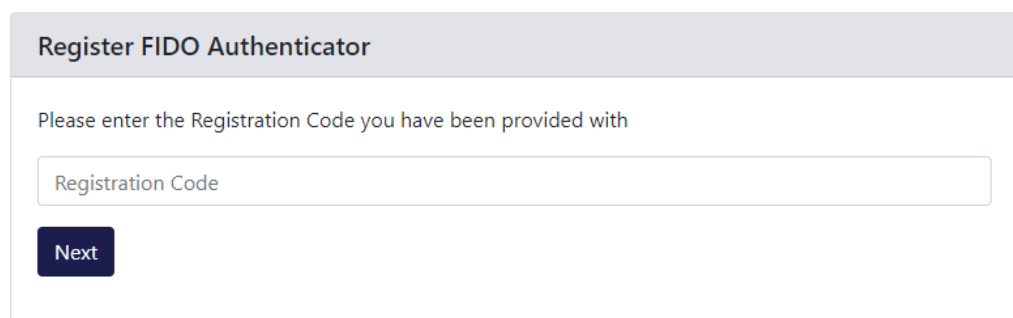
- An email message containing a link to the registration web page.

- An email message (or SMS, depending on configuration) containing a single-use registration code.

To register your FIDO authenticator:

1. Click the link in the FIDO registration email.

   This should take you to a web page with an URL similar to:

   ```
   https://<myserver>/web.oauth2/fido/register/begin?requestId=BADF1894-
   266B-4B80-9084-6ECD721347BD
   ```

   Register FIDO Authenticator

   Please enter the Registration Code you have been provided with

   Registration Code

   Next

2. Type your registration code from the email or SMS you received, and click **Next**.

   Windows Security takes you through the registration process for your FIDO authenticator. This process depends on the capabilities of your FIDO authenticator, and is independent of MyID.

   For example, Windows Security prompts you to present your authenticator:

   Windows Security ✕

   Making sure it's you

   Set up your security key to sign in to react.domain31.local as susan.smith.

   This request comes from Chrome, published by Google LLC.

   Tap your security key on the reader or insert it into the USB port.

   Cancel
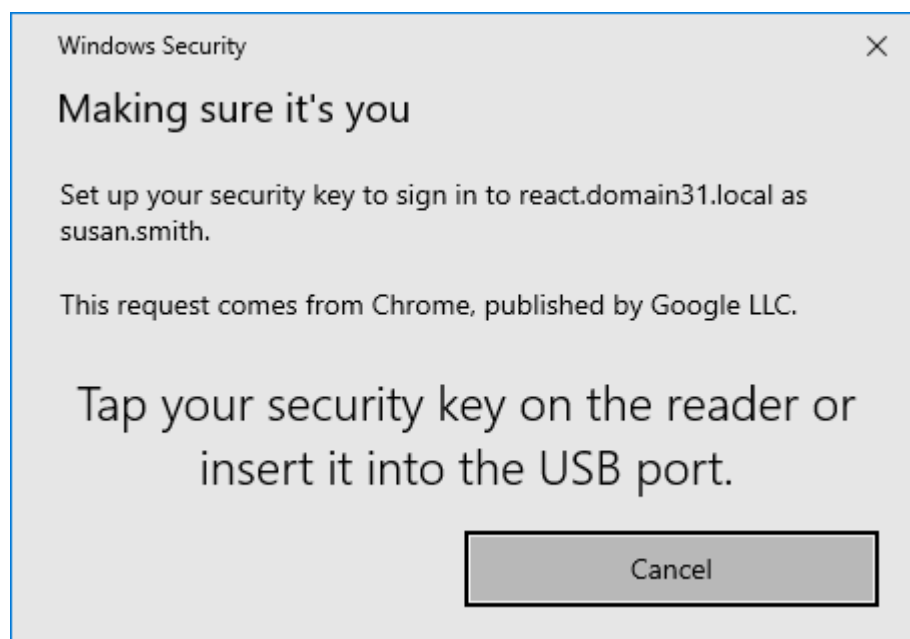
a. Present your authenticator.

You may be required to set up a PIN:

b. Type a **New PIN**, then confirm it, and click **OK**.

You may be required to provide additional authentication. For example, some FIDO authenticators require a PIN *and* for the user to touch the device physically for each authentication attempt; this provides an extra layer of security.
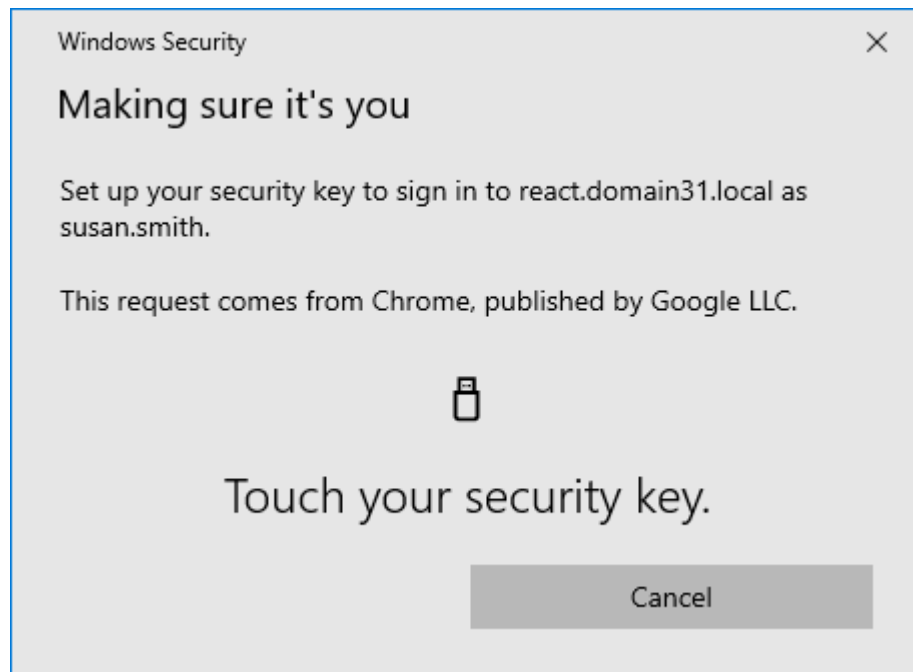
c. If your FIDO authenticator requires it, touch the device.

Your browser may request that you allow the website to see the authenticator; for example, in Google Chrome:
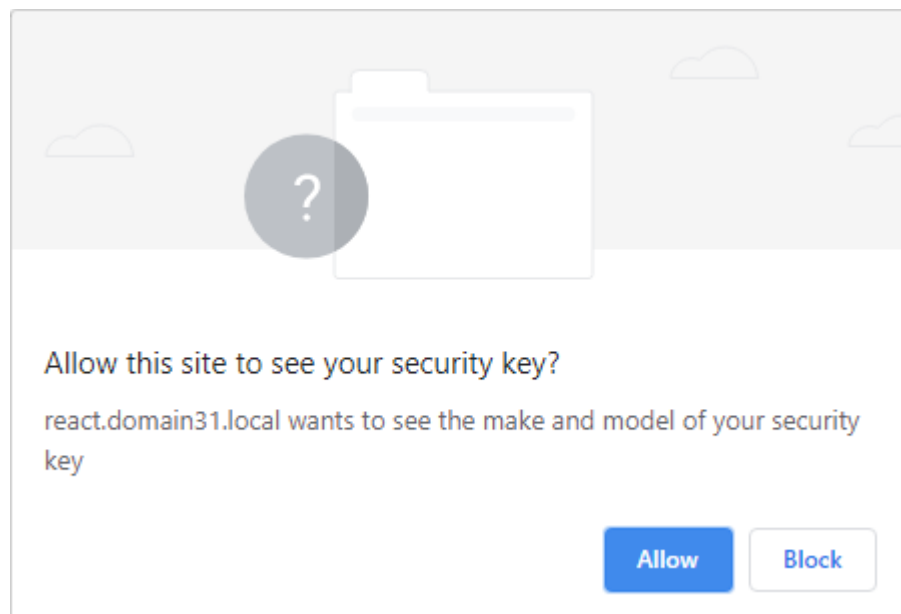
d. Click **Allow**.

When you have completed all the steps requested, your authenticator is registered with MyID, and is available for use. You can close the browser window.

3.2.2 Registering FIDO authenticators using the Self-Service Request Portal

If the credential profile used for the request had the **Immediate registration via Self-Service Request Portal** option set, and you requested the FIDO authenticator using the Self-Service Request Portal, click **Collect Now** to begin the registration process.
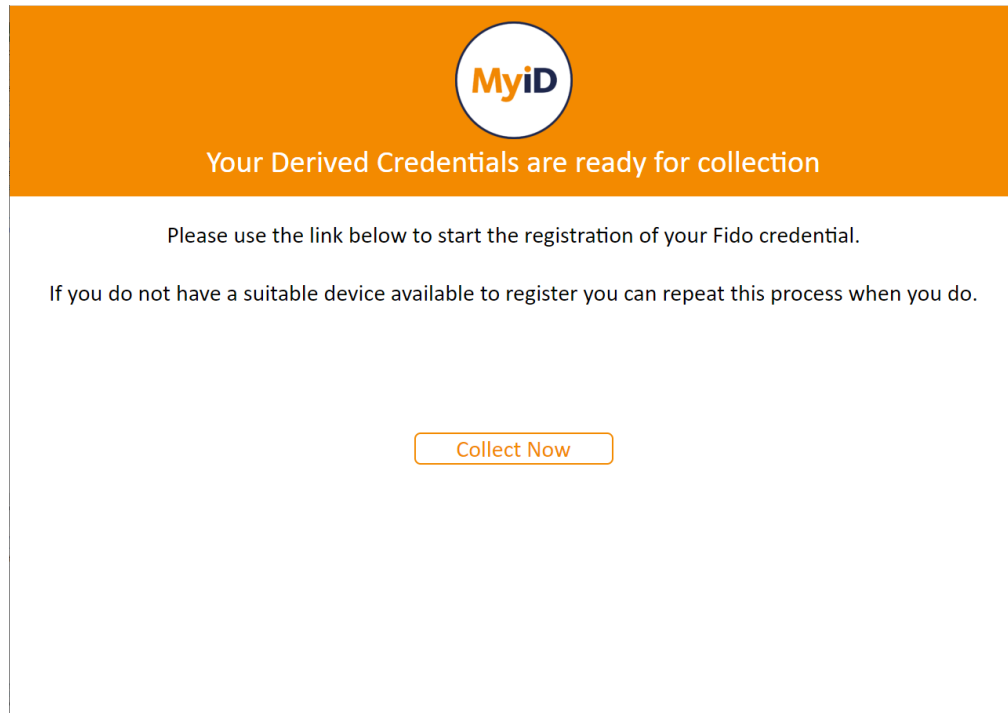
MyiD

Your Derived Credentials are ready for collection

Please use the link below to start the registration of your Fido credential.

If you do not have a suitable device available to register you can repeat this process when you do.
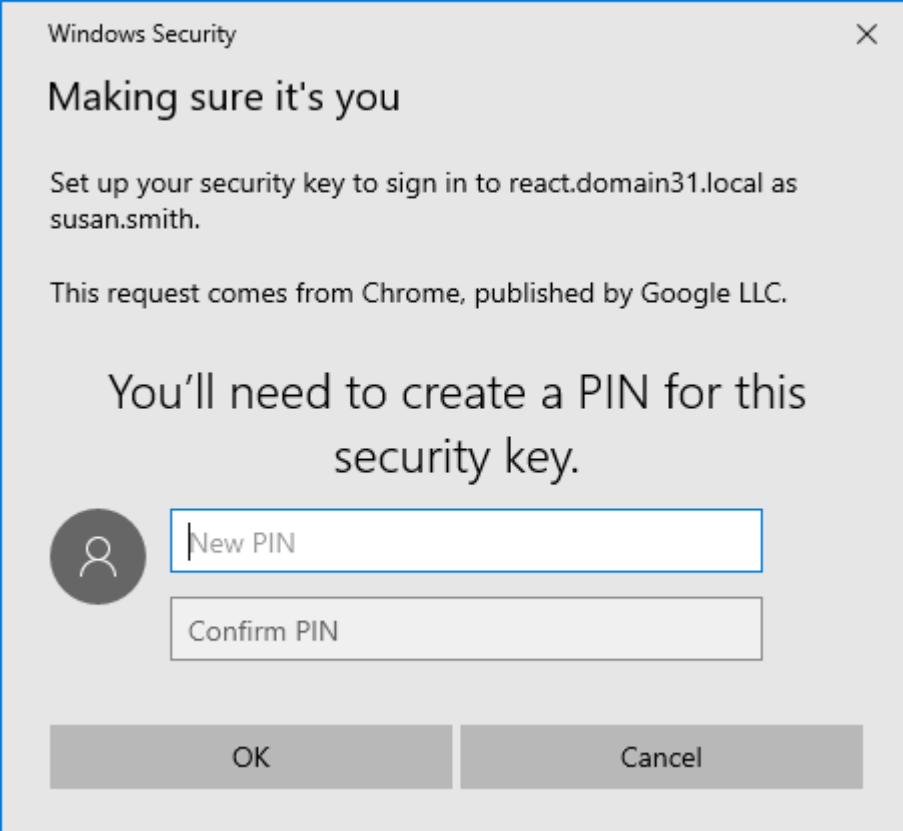
Collect Now

Windows Security takes you through the registration process for your FIDO authenticator. This process depends on the capabilities of your FIDO authenticator, and is independent of MyID.

Note: The timeout for immediately collection is determined by the **FIDO Immediate Collect Timeout** option on the **PINs** tab of the **Security Settings** workflow. By default, the timeout is set for 120 seconds.

3.3 Canceling FIDO authenticators

Once a FIDO authenticator has been registered, you can use MyID to control its lifecycle.

Note: This process is remote, and does not require physical access to the FIDO authenticator. Additionally, this process does not affect the content of the authenticator; instead, it changes the status of the authenticator on the MyID authentication service. If you want to change the content of the authenticator, for example to carry out a complete reset, your authenticator manufacturer provides tools for this purpose.

3.3.1 Searching for a FIDO authenticator

To search for a FIDO authenticator:

1. Log on to the MyID Operator Client.

2. Click the **Devices** category and search for the FIDO authenticator you want to work with.

3. From the **Device Type** drop-down list in the search criteria, select one of the following options:

- **FIDO Basic Assurance**
- **FIDO High Assurance**

4. Click **Search**.

You can also view a device from any form that contains a link to the device.

For example:

- Click the item in the list on the **Devices** tab of the View Person form.

- Click the link icon ⧉ on the **Device Serial Number** field of the View Request form.

See the *Searching for a device* section in the ***MyiD Operator Client*** guide for more information about searching for devices.

3.3.2   Canceling a FIDO authenticator

When you cancel a FIDO authenticator, it can no longer be used to authenticate using the MyID authentication service. If you want to use the authenticator again, you must request a FIDO authenticator for the user, then re-register the authenticator.

To cancel a FIDO authenticator:

1. Search for the authenticator you want to cancel.

   See section *3.3.1*, *Searching for a FIDO authenticator*.

2. Click the **Cancel** option in the button bar at the bottom of the View Device screen.

   You may have to click the **...** option to see any additional available actions.

3. On the Confirm Details screen:

   - Select a **Reason** from the drop-down list.

     As FIDO authenticators do not contain certificates issued by MyID, this option is for auditing purposes only.

   - Type any **Notes** on the cancellation in the provided box.

4. Click **Save**.

Note: You can also use the **Cancel Credential** workflow in MyID Desktop to cancel a FIDO authenticator. See the *Canceling a credential* section in the ***Operator's Guide*** for details of using this workflow.
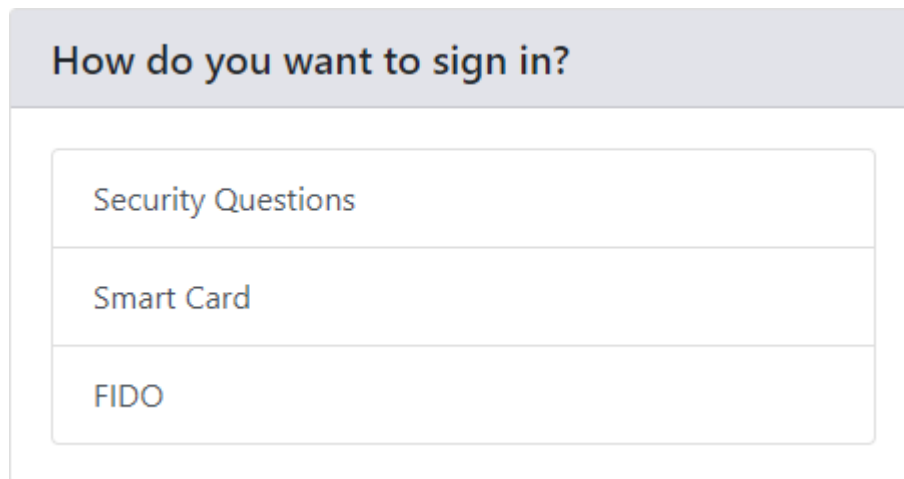
3.4 Logging on to MyID with FIDO authenticators

If you have configured MyID to allow logon using FIDO authenticators (see section *2.7*, *Configuring MyID for FIDO logon*) you can use a registered FIDO authenticator to log on to the MyID Operator Client.

To log on to MyID using a FIDO authenticator:

1. From the MyID Operator Client landing page, click **SIGN IN**.

   If more than one logon mechanism is configured for your system, you are prompted to select which one to use.
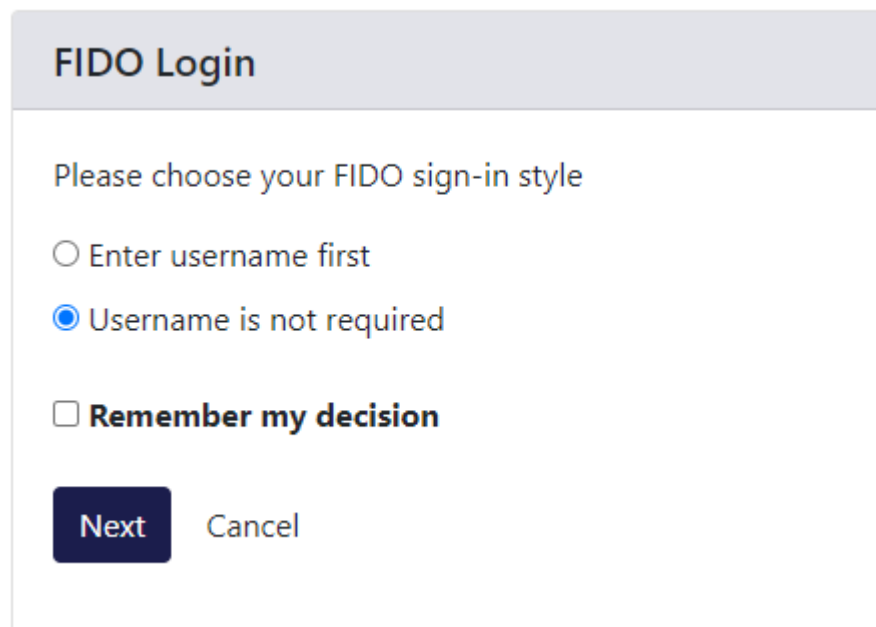
   ### How do you want to sign in?

   Security Questions

   Smart Card

   FIDO

   Select **FIDO** from the list, and the FIDO Login screen appears:

   ### FIDO Login

   Please choose your FIDO sign-in style

   ○ Enter username first
   ◉ Username is not required

   ☐ **Remember my decision**

   [Next] Cancel

2. Choose whether or not to provide a username:

   • **Enter username first**

     You must type your username when authenticating to MyID.

   • **Username is not required**

If your FIDO authenticator supports it, and has been issued with a discoverable key for the user and the domain (for example, by issuing using a credential profile that has the **Require Client Side Discoverable Key** option set) you can opt not to provide a username. If there is more than one identity for the current domain on the FIDO authenticator, the Windows Security dialog provides you with a list to select the appropriate one to use:

Windows Security

Making sure it's you

Please sign in to react.domain31.local.

This request comes from Chrome, published by Google LLC.

Susan.Smith

Susan.Smith

react.domain31.local

More choices

Susan.Smith

Jane.Jones
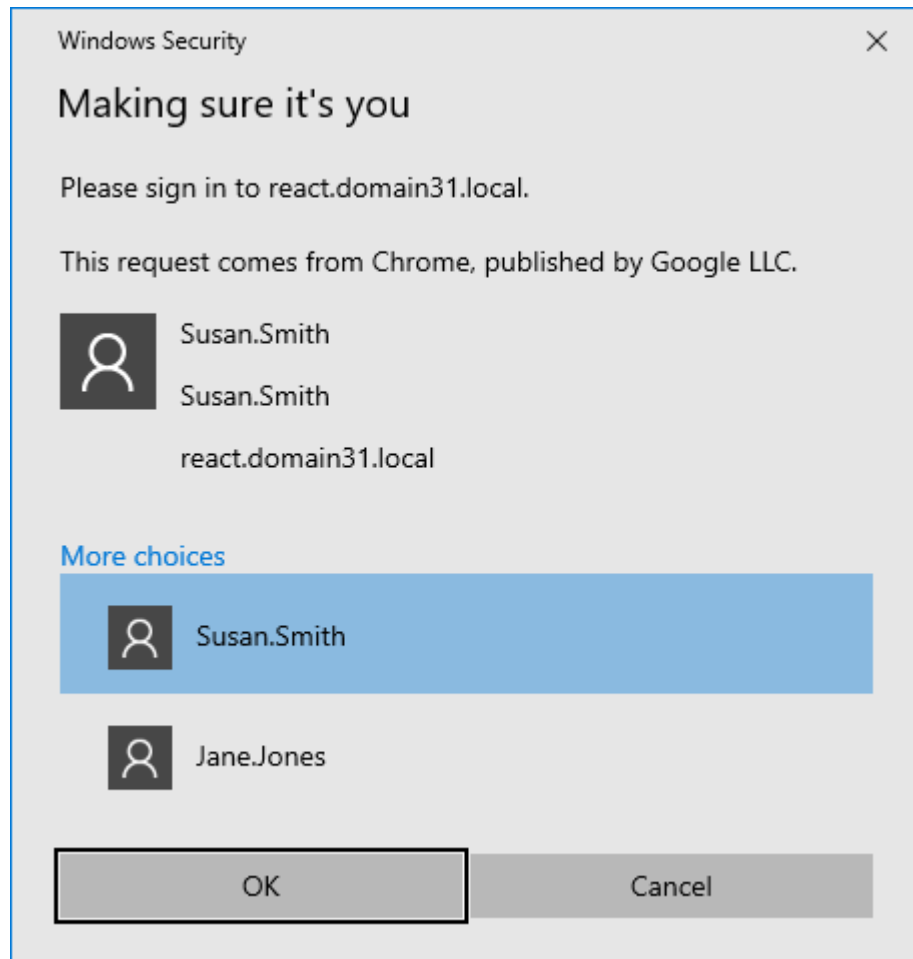
OK   Cancel

If you select **Remember my decision**, you will not be prompted again when using this browser under this user account on this PC. If you subsequently change your mind, you can click **Cancel** on a FIDO system authentication dialog box, or delete the cookies stored in your browser from the MyID website.

3. Complete your FIDO authentication.

Note: The specifics of the process depend on the capabilities of your FIDO authenticator, your selected FIDO logon style (username or no username) and how your credential profile is set up for user verification.

For example:

a. Type your **Username** and click **Next**.

The Windows Security dialog appears, requesting your PIN:
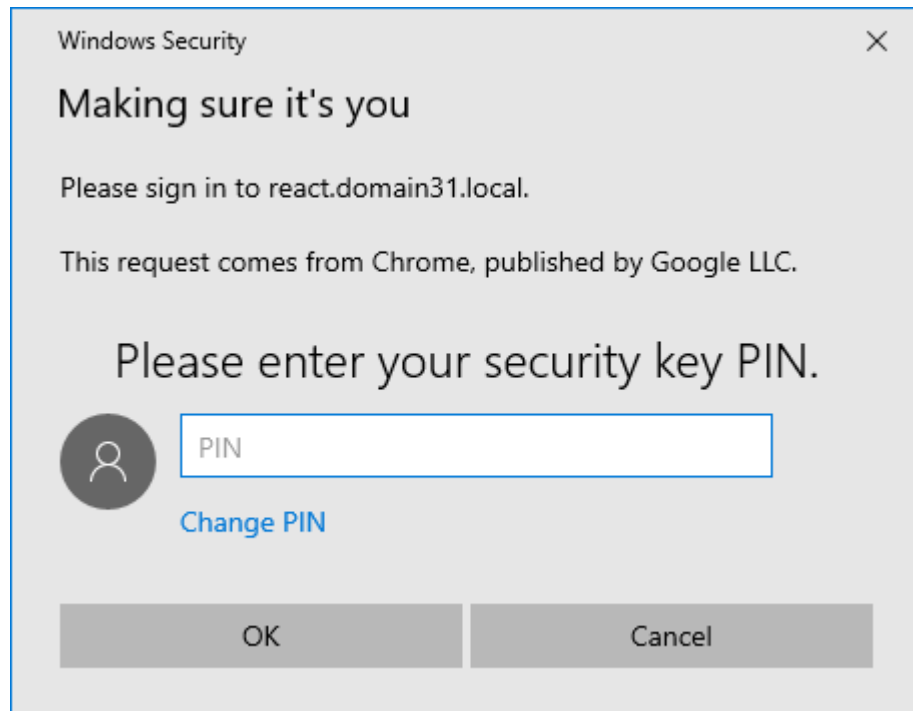
b. Enter your PIN and click **OK**.

The Windows Security dialog requests that you touch your authenticator:
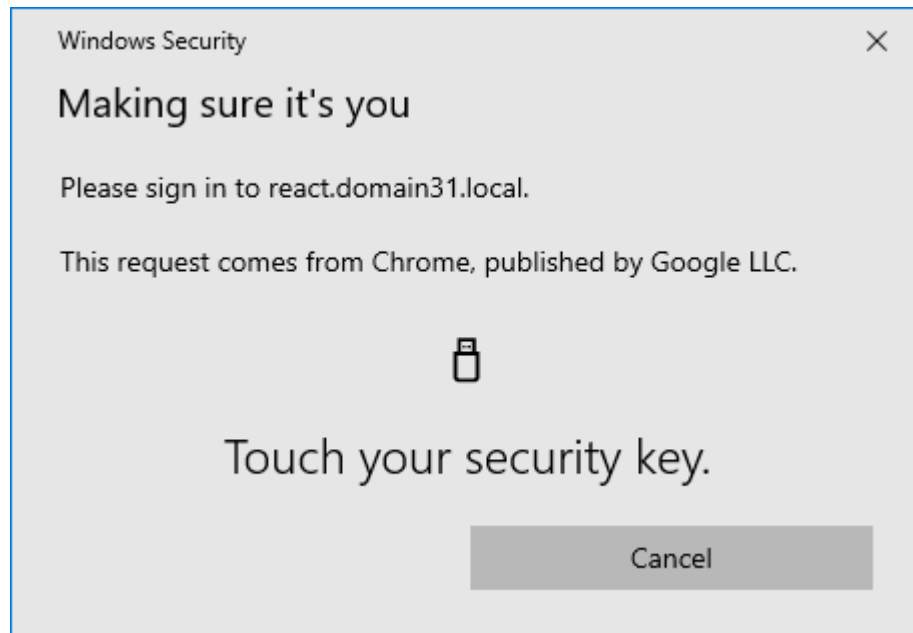
c. Touch your authenticator.

You can now use the MyID Operator Client.

Note: If the list of features available in the MyID Operator Client does not match what you expect, check that the logon mechanisms have been set up correctly for your roles; see section *2.7.2*, *Setting up FIDO logon mechanisms*.

4 Troubleshooting

This section contains troubleshooting information and frequently asked questions related to working with FIDO authenticators.

- **I requested a FIDO token, but there are no notifications**

  Check your email SMTP server settings in the **External Systems** workflow; see the *Setting up email* section in the ***Advanced Configuration Guide***.

  Check that the person has an email address stored in MyID. If you are using SMS to distribute the registration codes, check that the person also has a cell/mobile number set up.

  In Windows Services, check that both the MyID Notifications Service and eCertificate Services Server are running.

- **I requested a FIDO token and one notification arrives instantly but the other notification takes longer to arrive**

  The two notifications are sent by different processes on the MyID server (one through the MyID Notifications Service and the other through the eCertificate Services Server) so the notifications may arrive on slightly different schedules depending on the polling time of the services.

- **The link in the registration email does not work**

  If the link does not start with `https://<your server name>` check that the **URL path** option is set; see section *2.1*, *Setting the configuration options*.

  Note: This link *must* be an https address.

- **My FIDO registration code is not accepted**

  Make sure that the **Allow Logon Codes** option is set; see section *2.1*, *Setting the configuration options*.

  Make sure that the person has permission to the **Register FIDO Security Key** option in Edit Roles, and that the role has the Password logon mechanism; see section *2.6*, *Configuring roles for registering FIDO authenticators*.

- **My FIDO registration code was accepted, but I get error OA10009**

  Check that your browser and authenticator support FIDO2 Web Authentication (WebAuthn) standard.

  For more information about browsers, operating systems, and authenticators that support this, see:

  fidoalliance.org/fido2/fido2-web-authentication-webauthn/

  Check that the FIDO credential profile is compatible with the type of FIDO authenticator you want to use; not all FIDO authenticators support all FIDO features.

- **When registering, I get error OA10017 – a problem accessing the FIDO metadata**

  Make sure that the web server has access to the Internet, and there is no firewall preventing access to the FIDO metadata service; for example, make sure you can access the `mds.fidoalliance.org` domain. (This domain is controlled by the FIDO Alliance, and may be subject to change.)

  See section *2.3*, *Setting up the FIDO metadata*.

- **I want to supply my own metadata, as the authenticator I used is not on the FIDO metadata service, or I want to restrict issuance to a specific FIDO authenticator**

  If you want to use your own file-based FIDO metadata repository, follow the instructions in section *2.3.1*, *Setting up a local metadata repository*.

- **When logging on to the MyID Operator Client, I do not get the option to select FIDO as a means of logging on**

  Make sure that you have enabled at least one of the FIDO logon mechanisms; see section *2.7*, *Configuring MyID for FIDO logon*.

  Check the `appsettings.json` file for the web.oauth2 service; by default, this is:

  `C:\Program Files\Intercede\MyID\web.oauth2\appsettings.json`

  Check that the `EnableFido2LoginBasicAssurance` and `EnableFido2LoginHighAssurance` options have not been set to false for the MyID Operator Client (`myid.operatorclient`).

- **I cannot log on to MyID with my FIDO authenticator**

  Check the credential profile – the **MyID Logon** option in the `Services` section must be enabled to allow MyID logon.

  Check that the person and device are enabled, and that the device has not expired.

  The **Audit Reporting** and **System Events** workflows may provide additional information.

  You can also check the `AuthenticationAudits` table in the authentication database); see the *Reporting on the authentication database* section in the **MyID Authentication Guide** for details.

- **When trying to log on with FIDO, there is an error complaining about the domain or origin**

  FIDO tokens are domain locked to the domain that registered them; that is, if a website at `https://myserverdomain` registered the FIDO authenticator, that FIDO authenticator can be used only to authenticate at websites that are also at `https://myserverdomain`. However, the same FIDO authenticator can hold FIDO credentials for other systems that MyID does not know about, enabling a user to use that FIDO authenticator for many systems; MyID will ignore these other FIDO credentials.

  Therefore it is important to not change the server domain of the MyID system, as doing so will render already registered FIDO credentials unusable; if this happens, you must request and register new FIDO credentials.

  Note: It is the URL the client sees that is important; this may be the URL of the load balancer or reverse proxy they access rather than the URL of the actual MyID web server.

  There is special consideration if alternative web servers are used for a standalone MyID authentication service (for externally facing systems such as ADFS to authenticate to) but the FIDO authenticator is registered on a different MyID web server by web.oauth2. In this situation, you must set up a load balancer or proxy so the same domain is accessed in both cases and routed to the appropriate servers.

  Note: MyID now supports multiple origins, where sub-domains of a registrable domain can also be authenticated; see section *2.4.3*, *Multiple origins*.

<image src="">
</image>

- **When trying to log on with FIDO I get the error HTTP 431 Request Header Fields Too Large**

  Your FIDO authenticator has too many credentials on it, which is causing the combined length of the credential IDs to exceed the HTTP header size restriction; you are recommended to cancel any older unwanted FIDO credentials for that user.

- **I cannot log on using my older FIDO credentials**

  This is related to the HTTP 431 Request Header Fields Too Large error. When the combined length of credential IDs is too large and runs the risk of exceeding the HTTP header size restriction, the older tokens are ignored.

- **Why are there two logon mechanisms – FIDO Basic Assurance and FIDO High Assurance?**

  This provides flexibility. You may want to issue one-factor authenticators (basic assurance) for logging on to some external systems, but only allow two-factor authenticators (high assurance) for logging on to MyID.

- **I registered two FIDO credentials to the same FIDO authenticator, but MyID shows them as two separate devices – why?**

  FIDO has privacy built in that prevents a system from identifying the authenticator to which the credential is issued; this means that each registered FIDO credential has its own device record.

- **Does this mean each FIDO credential uses a MyID device license, even if they are on the same physical device?**

  Yes, MyID tracks device license usage based on issued credentials, not physical devices.

- **I get database errors when registering or authenticating a FIDO authenticator**

  Make sure that the authentication database is set up correctly. Ensure that the authentication `.udl` file (by default, `MyIDAuth.udl`) in the Windows `System32` folder of the MyID application server is pointing to the authentication database.

- **I get HTTP Error 500.30**

  If you see an error similar to:

  ```
  HTTP Error 500.30 - ANCM In-Process Start Failure
  ```

  Check that your `appsettings.Production.json` file is valid.

Note especially that copying code samples from a browser may include hard spaces, which cause the JSON file to be invalid.

To assist in tracking down the problem, you can use the Windows Event Viewer. Check the **Windows Logs > Application** section for errors; you may find an error from the .NET Runtime source that contains information similar to:

```
Exception Info: System.FormatException: Could not parse the JSON file.
---> System.Text.Json.JsonReaderException: '"' is invalid after a
value. Expected either ',', '}', or ']'. LineNumber: 13 |
BytePositionInLine: 6.
```

which could be caused by a missing comma at the end of a line.

An error similar to:

```
Exception Info: System.FormatException: Could not parse the JSON file.
---> System.Text.Json.JsonReaderException: '0xC2' is an invalid start
of a property name. Expected a '"'. LineNumber: 7 | BytePositionInLine:
0.
```

is caused by a hard (non-breaking) space copied from a web browser, which is not supported in JSON.

Note: Some JSON files used by MyID contain comment lines beginning with double slashes `//` – these comments are not supported by the JSON format, so the JSON files will fail validation if you attempt to use external JSON validation tools. However, these comments *are* supported in the JSON implementation provided by asp.net.core, and so are valid in the context of MyID.

- **I get errors relating to attestation when registering a GoTrust FIDO authenticator**

  There have been issues noticed when registering GoTrust Idem Key FIDO authenticators due to a problem with the GoTrust root certificate. Contact GoTrust technical support for assistance.