MyID

Version 10.8 Update 2

Symantec (Digicert) Managed PKI
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 and to indicate references to other sections within the current document:

  For example:
  - "Copy the file *before* starting the installation"
  - "See *Issuing a Card* for further information"

- ***Bold and italic*** are used to identify the titles of other documents.

  For example: "See the ***Release Notes*** for further information."

  Unless otherwise explicitly stated, all referenced documentation is available on the installation CD.

- A `fixed width` font is used where the identification of spaces is important, including filenames, example SQL queries and any entries made directly into configuration files or the database.

- **Notes** are used to provide further information, including any prerequisites or configuration additional to the standard specifications.

  For example:

  Note: This issue only occurs if updating from a previous version.

- Warnings are used to indicate where failure to follow a particular instruction may result in either loss of data or the need to manually configure elements of the system.

  For example:

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

Contents

1 Introduction

This document is a step-by-step guide to integrating the Symantec MPKI Certificate Authority with MyID®.

Note: Following the acquisition of Symantec PKI solutions by Digicert, there may be differences in the branding of documentation and information supplied to you by Digicert when compared to MyID. Throughout MyID, the brand name Symantec is used in user interface and lower level components. This approach has been taken to avoid backwards compatibility issues for customers who are upgrading from earlier product versions.

1.1 Hardware and software requirements

The current version of MyID has been tested with:

- Symantec MPKI version 7.x.
- Symantec MPKI version 8.17.4.

Please refer to your Symantec MPKI documentation for recommendations of the hardware and software needed for Symantec MPKI.

1.2 Prerequisites

The MyID application server must be able to communicate using secure HTTP with the main Symantec CA.

If you are using the Key Management Server, the MyID application server also must be able to communicate using secure HTTP with the KMS server.

You must obtain an appropriate RA certificate for a configured Symantec jurisdiction.

1.3 Key Management Server

You can optionally set up MyID to work with a Symantec Key Management Server (KMS). You must have a KMS if you want to archive and recover certificates.

1.4 Upgrading to Symantec MPKI

Note: Symantec Certificate Authority was previously known as VeriSign.

If you want to upgrade your system from Local Hosting 6.1.3 to Web Service 7.3, you must first set up your Symantec MPKI – you can either upgrade your existing Local Hosting CA to MPKI, or set up an MPKI CA separate to the existing Local Hosting CA.

Note: Local Hosting is no longer supported as a CA with MyID as of version 9.0 SP1.

Whether you upgrade your existing CA or set up a new CA, you must still create a new entry in the **Certificate Authorities** workflow within MyID for the MPKI CA.

If you are upgrading an existing jurisdiction, you must set up your Symantec MPKI CA and enable its policies (see section *2.2*, *Configure MyID* for details), then run a procedure on the MyID database to associate the existing certificates with the new CA entry.

Contact Intercede customer support for details quoting reference SUP-37.

1.5 Differences between Symantec MPKI 7.x and 8.x

- Support for MPKI 8.x in MyID relates explicitly to policies configured for Web Services usage. If the policies have not been configured for Web Services usage, you may see an A300 error.

- The PKI attributes have been extended to enable the `seat_id` attribute to be included; typically, this is the email address. Note, however, that while MPKI 8.x supports revocation based on the `seat_id`, MyID continues to revoke certificates at the device/user level by certificate rather than `seat_id`.

- If the MPKI 8.x CA has been configured to allow multiple instances of the certificate to be recovered, or issued to multiple devices for a user, the certificate can be revoked only once. If a certificate like this has been issued (either within or outside of MyID), when MyID attempts to revoke it (for example, due to user removal or device cancellation) MyID will not treat finding the certificate as already revoked as an error.

- MPKI 8.x has two forms of escrow:

    - Enterprise – this is the traditional KMS usage.

    - Cloud – does not require a local Enterprise Gateway to be installed.

    Note: In general, you are expected to use either Enterprise or Cloud. If you want to use *both* forms of escrow for a single policy on a single jurisdiction, contact Symantec to determine whether your CA supports this. An attempt to use both may result in a message containing error:

    ```
    A604 – A certificate has already been issued with this enrolment
    information.
    ```

    where an issuance using either Cloud or Enterprise escrow would succeed.

- Changes in MPKI 8.x mean that the `friendlyname` describing a policy is shared across multiple copies of the policy; in MPKI 8.x terms, the unique identifier is the `oid`.

- In previous versions of MPKI support, certificate policies on the CA side were typically one year, and so on. With MPKI 8.x, more customization is provided by Symantec over particular instance lifetime. While MyID may constrain certificate lifetimes within the credential lifetime with which it is associated, if the policy has an even shorter lifetime configured on the CA, then MyID uses the lesser time that the CA will authorize. In previous releases, MyID would have failed/rejected a severely constrained lifetime request.

- You can disable suspensions on the CA. MyID does not treat an attempt to suspend a certificate that cannot be suspended as a failure.

2   Configuring MyID

2.1   Requesting RA certificates

Before you configure your Symantec MPKI CA within MyID, you must request a Registration Authority certificate to secure communications between MyID and the Managed PKI web services. If you are using Dual Control for key recovery, you must request a second Registration Authority certificate. When requesting these certificates, make sure that the requests have **Export Private Key** set.

Note: These certificates are in addition to the RA certificate that secures communications between the KMS and Managed PKI web services.

When communicating with the Symantec MPKI CA, MyID uses the RA certificate as a TLS/SSL client authentication certificate. You can store your RA certificate in a software keystore or on an HSM; the method you use has implications on how you obtain your RA certificate.

See your Symantec documentation for details.
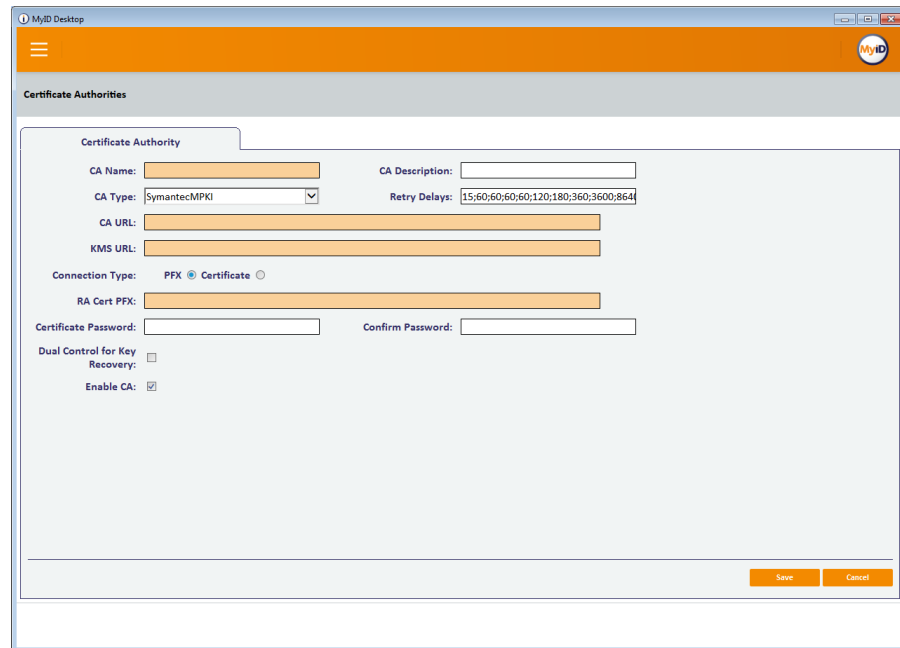
Note: For software keystores, you are recommended to use a CER file instead of a PFX file to avoid any overhead. Import the RA certificate into the MyID COM+ user's personal user store, then export the CER file and use that instead. Importantly, to import the certificate, you must use the `certutil` utility and specify a CSP that supports SHA256; for example:

```
certutil –csp "Microsoft Enhanced RSA and AES Cryptographic Provider" -user –importpfx RACert.pfx
```

2.2   Configure MyID

Configure the Symantec CA using the **Certificate Authorities** workflow.

1.   Put the RA certificate on the MyID application server.

     Note: The MyID named COM+ user must have access to this file.

2.   From the **Configuration** category, select **Certificate Authorities**.

3.   Click **New**.

4.   From the **CA Type** drop-down list, select **SymantecMPKI**.

5. Type a **CA Name** and **CA Description**.

6. Type the **CA URL**.

    This is the URL for the Symantec-hosted certificate authority.

    For MPKI 7 pilot systems:

    ```
    https://pilot-pkiservices.verisign.com
    ```

    For MPKI 7 production systems:

    ```
    https://pkiservices.verisign.com
    ```

    For MPKI 8 systems:

    ```
    https://pki-ws.symauth.com/
    ```

7. If you are using a KMS, type the **KMS URL**.

    This is the URL for your locally-hosted Key Management Server. For example:

    ```
    https://myserver.example.com:8443
    ```

    Note: This option is a mandatory field; you cannot leave it blank. If you are not using a KMS, type the following:

    ```
    n/a
    ```

8. If you are using a CER file; for example, for an HSM-based RA certificate, or for a software-based certificate that has been installed to the MyID COM+ user's personal user store:

    a) For the **Connection Type**, select the **Certificate** option.

    b) Type the location of the **RA Cert**.

        For example:

        ```
        C:\Symantec\RACert.cer
        ```

        Note: The file must not be read-only.

    c) Type and confirm the password for the certificate.

        Note: The password cannot contain a pipe ǀ character.

9. If you are using a PFX file for a software-based RA certificate:

   a) For the **Connection Type**, select the **PFX** option.

   b) Type the location of the **RA Cert PFX**.

      For example:

      `C:\Symantec\RACert.pfx`

      Note: The PFX file must not be read-only.

   c) Type and confirm the password for the certificate.

10. If you are using dual control for key recovery:

   a) Select the **Dual Control for Key Recovery** option.

      Note: You cannot configure dual control for a CA you have already set up in MyID. See section *3, Known Issues* for more details.

   b) Type the location of the **2nd RA Cert**.

      For example:

      `C:\Symantec\RACertTwo.pfx`

      Or

      `C:\Symantec\RACertTwo.cer`

      Note: The PFX or CER file must not be read-only.

   c) If you are using a software-based certificate, type and confirm the password for the certificate.

      Note: The password cannot contain a pipe | character.

11. Set the **Retry Delays**.

    This is a semi-colon separated list of elapsed times, in seconds.

    For example, `5;10;20` means:

    ◆ If the first attempt to retrieve details from the CA fails, a second attempt will be made after a 5 second delay.

    ◆ If this second attempt fails, the CA will be contacted again after 10 seconds.

    ◆ Subsequent attempts will be made to retrieve information every 20 seconds, until a response is received.

    If you want to limit the number of retry attempts, enter 0 as the last number in the sequence.

    The default is:

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

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

12. Make sure that the **Enable CA** checkbox is selected.

13. Click **Save**.

    You can now go back into the **Certificate Authorities** workflow and set up your certificate templates.

2.2.1 Enabling certificates on a CA

Note: Because of the way Symantec MPKI 8 handles certificate template names, the friendly name is not available in MyID. The certificate names provided are not guaranteed to be unique; however, MyID displays the unique OID as part of the name (for example: `2.16.840.1.113733.1.16.1.2.3.5.1.239836912`), and you can use this to match up with the certificate templates on the Symantec server.

Although all certificate templates are detected when you add the CA to MyID, they are all initially disabled. To enable them:

1. From the **Configuration** category, select **Certificate Authorities**.

2. From the **CA Name** drop-down list, select the certificate authority you want to work with.
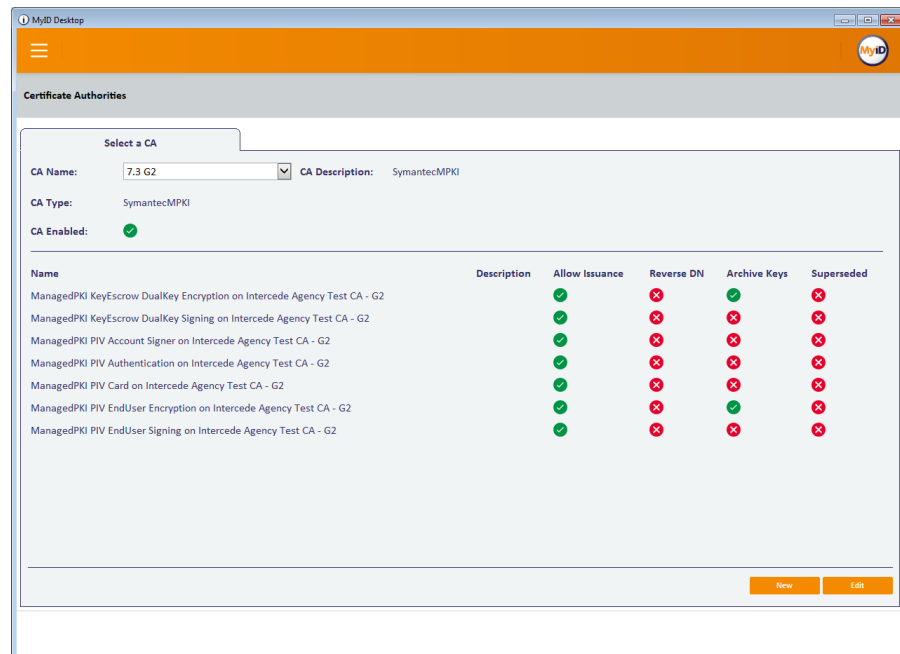
3. Click **Edit**.
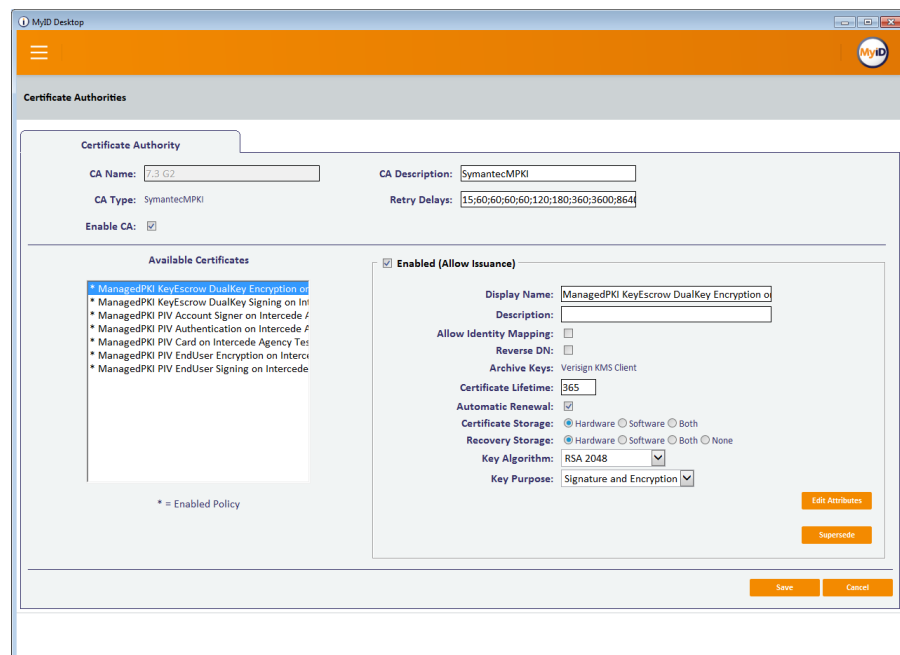
4. Make sure **Enable CA** is selected.

5. Select a certificate template you want to enable for issuance within MyID in the **Available Certificates** list.

6. Click the **Enabled (Allow Issuance)** checkbox.

7. Set the options for the policy:

◆ **Display Name** – the name used to refer to the policy.

   If you have more than one KMS, you may not be able to distinguish between the same type of certificate on different KMS servers when selecting certificates in a card profile, as the display names are the same. To avoid this problem, change the **Display Name** of each certificates for one of your KMS servers.

◆ **Description** – a description of the policy.

◆ **Allow Identity Mapping** – used for additional identities. See the *Administration Guide* for details.

◆ **Reverse DN** – select this option if the certificate requires the Distinguished Name to be reversed.

◆ **Archive Keys** – select whether the keys should be archived.

◆ **Certificate Lifetime** – the life in days of the certificate. You can request a certificate from one day up to the maximum imposed by the CA. For example, type `365` to request one-year certificates.

◆ **Automatic Renewal** – select this option if the certificate is automatically renewed when it expires.

◆ **Certificate Storage** – select one of the following:

   □ **Hardware** – the certificate can be issued to cards.

   □ **Software** – the certificate can be issued as a soft certificate.

   □ **Both** – the certificate can be issued either to a card to as a soft certificate.

◆ **Requires Validation** – select this option if the certificate requires validation.

   Note: This option is available only if you select **Software** or **Both** for the **Certificate Storage** option.

◆ **Recovery Storage** – select one of the following:

   □ **Hardware** – the certificate can be recovered to cards.

   □ **Software** – the certificate can be recovered as a soft certificate.

   □ **Both** – the certificate can be recovered either to cards or to a soft certificate.

   □ **None** – allows you to prevent a certificate from being issued as a historic certificate, even if the **Archive Keys** option is set. If the **Certificate Storage** option is set to **Both**, the certificate can be issued to multiple credentials as a shared live certificate, but cannot be recovered as a historic certificate.

◆ Additional options for storage:

   If you select **Software** or **Both** for the **Certificate Storage**, or **Software**, **Both**, or **None** for the **Recovery Storage**, set the following options:

   □ **CSP Name** – select the name of the cryptographic service provider for the certificate. This option affects software certificates issued or recovered to local store for Windows PCs.

   □ **Requires Validation** – select this option if the certificate requires validation.

□ **Private Key Exportable** – when a software certificate is issued to local store, create the private key as exportable. This allows the user to export the private key as a PFX at any point after issuance.

It is recommended that private keys are set as non-exportable for maximum security.

Note: This setting affects only private keys for software certificates – private keys for smart cards are never exportable.

□ **User Protected** – allows a user to set a password to protect the certificate when they issue or recover it to their local store.

This means that whenever they want to make use of the soft certificate, they will be prompted for a password before they are allowed to use it. This is a CSP feature that is enabled when you set this option, and affects only software certificates that are issued or recovered to local store for Windows PCs.

◆ **Key Algorithm** – select the type and length of the key-pairs used for certificate generation. A longer key length is more secure but certain manufacturers' CSPs do not support longer lengths. Select the appropriate key length from the list. This must match the key type and length set up in your CA.

Note: ECC types are not supported with Symantec MPKI 7, but are supported with Symantec MPKI 8.

◆ **Key Purpose** – select one of the following:

□ **Signature** – the key can be used for signing only.

□ **Signature and Encryption** – the key can be used for either signing or encryption.

Note: The **Key Purpose** option has an effect only where the device being issued supports the feature. PIV cards do not support this feature, while smart cards issued with minidrivers and software certificates issued to local store for Windows PCs do support this feature.

8. If you need to edit the policy attributes, click **Edit Attributes**.

Policy Attributes

Attribute	Type	Value
mail firstName	Dynamic	First Name
mail lastName	Dynamic	Surname
mail email	Dynamic	Email
Seat Id	Dynamic	Email
Common Name (Searchable)	Not Required	Not Required
Email (Searchable)	Not Required	Not Required
Additional Field 4 (Non-searchable)	Not Required	Not Required
Additional Field 5 (Non-searchable)	Not Required	Not Required
Employee ID (Non-searchable)	Not Required	Not Required
Address (Non-searchable)	Not Required	Not Required
Two letter country code. For example, US, UK. (Non-searchable)	Not Required	Not Required
AddField6 (Non-searchable)	Not Required	Not Required
Job title (Non-searchable)	Not Required	Not Required
Locality (Non-searchable)	Not Required	Not Required
state (Non-searchable)	Not Required	Not Required

* = Mandatory attribute
# = Recommended attribute

Hide Attributes

a) For each attribute, select one of the following options from the **Type** list:

□ **Not Required** – the attribute is not needed.

□ **Dynamic** – select a mapping from the **Value** list to match to this attribute.

□ **Static** – type a value in the **Value** box.

b) Click **Hide Attributes**.

For information on mapping attributes for PIV systems, see section *2.4*, *Attribute mapping for PIV systems*.

Note: MyID may not override the settings of the CA. You need to obtain the correct settings from the administrator of your CA.

9. Click **Save**.

Note: Changes made to certificate profiles do not take effect immediately, as the normal interval for MyID to poll for updates is 50 minutes. To force MyID to poll for changes immediately, you must manually restart the **eKeyServer** service, then restart the **eCertificate** service.

2.3   Configuring additional attributes

You can set up MyID to provide additional attributes to Symantec MPKI in the certificate request.

You can then use these fields in Symantec Managed PKI Control Center – you can use some fields to search for certificates, and the values for the other fields are displayed in the search results.

The Symantec documentation provides a list of which attributes you can use in the enrollment request. Some fields are searchable, while other fields are non-searchable but will be returned in the search results.

Currently, you can use the following fields as searchable fields:

Name	Type	Description
common_name	VT_PRINTABLE_STRING	Common name
mail_email	VT_IA5_STRING	Email

You can also use the following non-searchable fields:

Name	Type	Description
additional_field4	VT_T61_STRING	Additional Field 4
additional_field5	VT_T61_STRING	Additional Field 5
employeeID	VT_T61_STRING	Employee ID
mailStop	VT_T61_STRING	Address
country	VT_PRINTABLE_STRING	Two letter country code. For example, US, UK.
additional_field6	VT_T61_STRING	AddField6
jobTitle	VT_T61_STRING	Job title
locality	VT_T61_STRING	Locality
state	VT_T61_STRING	State

2.3.1   Setting up the additional attributes

The availability of additional searchable and non-searchable attributes in the MyID **Certificate Authorities** workflow is determined by the SymantecMPKIConnector.xml configuration file in the MyID Components folder on the MyID application server; by default, this is:

C:\Program Files (x86)\Intercede\MyID\Components\

By default, the configuration file contains all of the available additional attributes. However, you can configure this file if necessary.

For example, for the Common Name searchable attribute, use an `<Extension>` block like:

```
<Extension displayType="recommended">
  <Name>common_name</Name>
  <DisplayName>Common Name (Searchable)</DisplayName>
</Extension>
```

with a `displayType` of `"recommended"`.

For the Employee ID non-searchable attribute, use an `<Extension>` block like:

```
<Extension displayType="optional">
  <Name>employeeID</Name>
  <DisplayName>Employee ID (Non-searchable)</DisplayName>
</Extension>
```

with a `displayType` of `"optional"`.

Note: After you have made any changes to this file, you must restart the service:

1. From the Windows Administrative Tools, double-click **Services**.

2. Right-click the **eCertificate Services Server** service, then from the popup menu click **Restart**.

Note: The provided XML file introduces `seat_id` as a mandatory field, as it is required for MPKI 8. You are recommended to set up `seat_id` for *both* MPKI 7 and MPKI 8; however, the `seat_id` is not submitted to an MPKI 7 system; for MPKI 7 you are recommended to map it to `email`.

2.3.2 Mapping the additional attributes

You must use the **Edit Attributes** option for each certificate policy in the **Certificate Authorities** workflow to set up a mapping or a static value for each of the additional attributes that you want to pass in the certificate request. See section *2.2.1*, *Enabling certificates on a CA* for details.

2.4 Attribute mapping for PIV systems

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

The following tables provide an example configuration for PIV cards.

Note: The PIV Card Authentication certificate policy *must not* contain a mapping for Email.

2.4.1 Publishing policies

You are recommended to set the jurisdiction to allow the user to decide whether policies should be published, rather than setting the jurisdiction to Always Publish or Never Publish. The PIV signing and encryption certificates should be published, while the PIV authentication certificates should not be published.

The **publish flag** attribute appears if the jurisdiction is set to allow the user to decide whether the individual policies are published; The attribute must be set to **Static**, and can contain one of the following:

- `Yes` – the policy is published.

- `No` – the policy is not published.

The case is not important. If you use a value other than `Yes` or `No`, an error similar to one of the following will occur:

```
<Parameters>
    <Status>-6</Status>
    <CAType>SymantecMPKI</CAType>
    <Message>Error found in SendRequest: Unable to cast object of type
'Symantec.Cert.Policy.PublishCert' to type 'System.String'.</Message>
</Parameters>
```

or:

```
<Parameters>
    <Status>-6</Status>
    <CAType>SymantecMPKI</CAType>
    <Message>Error found in SendRequest: cACertPublishNameValuePair must
be yes or no, not clientProvided</Message></Parameters>
```

or:

```
<Parameters>
    <Status>-6</Status>
    <CAType>SymantecMPKI</CAType>
    <Message>Error found in SendRequest: Must specify valid information
for parsing in the string.</Message></Parameters>
```

Note: Using a value of `1` or `0` will not generate an error; however, as `0` is equivalent to `Yes` and `1` is equivalent to `No`, to prevent confusion, you are recommended to use `Yes` and `No` only.

2.4.2   Attribute tables

The following tables show the recommended options for attribute mapping.

ManagedPKI KeyEscrow DualKey Encryption	
Attribute	**Value**
mail email	Email
common name	Common Name
state	Not Required
country	Not Required
org unit	Organisational Unit
mailStop	Not Required
employeeID	EmployeeID
locality	Not Required
jobTitle	Not Required
corp company	Applicant Group
publish flag (Static)	No

ManagedPKI KeyEscrow DualKey Signing

Attribute	Value
mail email	Email
common name	Common Name
state	Not Required
country	Not Required
org unit	Organisational Unit
mailStop	Not Required
employeeID	EmployeeID
locality	Not Required
jobTitle	Not Required
corp company	Applicant Group
publish flag (Static)	No

ManagedPKI PIV Account Signer

Attribute	Value
common name	Common Name
publish flag (Static)	No

ManagedPKI PIV Authentication

Attribute	Value
common name	Common Name
FASC-N	FASC-N (Hex)
UserPrincipalName	User Principal Name
Email	Not Required
UUID	UUID (ASCII)
NACI Check	NACI Status
publish flag (Static)	No

ManagedPKI PIV Card

Attribute	Value
fascn printable	FASC-N (ASCII)
FASC-N	FASC-N (Hex)
UserPrincipalName	Not Required
Email	Not Required
UUID	UUID (ASCII)
NACI Check	NACI Status
publish flag (Static)	No

ManagedPKI PIV EndUser Encryption

Attribute	Value
common name	Common Name
mail email	Email
publish flag (Static)	Yes

ManagedPKI PIV EndUser Signing

Attribute	Value
common name	Common Name
mail email	Email
publish flag (Static)	Yes

2.4.3   PIV-I systems

The FASC-N mapping is required for standard PIV cards, but is not permitted for PIV-I cards. The Printable FASC-N mapping is set to FASC-N (ASCII) for PIV cards, and UUID (ASCII) for PIV-I cards. NACI is not required for PIV-I.

For example, for a PIV-I system, the following certificate policies would need to be different from the example for a PIV system above:

ManagedPKI PIV Authentication

Attribute	Value
common name	Common Name
FASC-N	Not Required
UserPrincipalName	User Principal Name
Email	Not Required
UUID	UUID (ASCII)
NACI Check	Not Required
publish flag (Static)	No

ManagedPKI PIV Card

| Attribute	Value
fascn printable	UUID (ASCII)
FASC-N	Not Required
UserPrincipalName	Not Required
Email	Not Required
UUID	UUID (ASCII)
NACI Check	Not Required
publish flag (Static)	No

2.5 Setting up KMS

2.5.1 Setting up KMS for MPKI 7

If you are using the Key Management Server, you must set up shared secrets for your KMS user and password.

Note: MyID maintains a single set of KMS credentials which must be the same to work across all of the CAs available on your site. This limitation does not exist on MPKI 8.

To set up shared secrets:

1. Install the Key Management Server according to the documentation provided by Symantec.

2. Make a note of the basic authentication username and password (`kms.authenticate.username`, `kms.authenticate.password`).

3. Set the KMS to use PKCS12 passwords (`pkcs12.password.generate=YES`, `pkcs12.password.length=8`).

4. On the MyID application server, start the GenMaster utility.

5. Set up the KMS username as a shared secret.

   a) Select **Configure Secret Keys**, then click **Next**.

   b) In the **Name** box, type `KMSUser`.

   c) From the **Type** drop-down list, select **Password**.

   d) Type your KMS basic authentication username in the box.

   e) For the **Description**, type `SymantecMPKI username`.
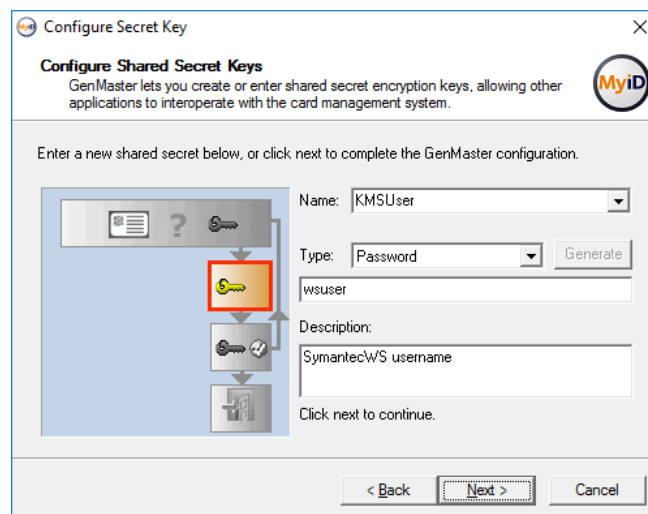
   f) Click **Next**, review the changes you are about to make, then click **Next** again.

6. Set up the KMS password as a shared secret.

   a) Select **Configure Secret Keys**, then click **Next**.

   b) In the **Name** box, type `KMSPwd`.

   c) From the **Type** drop-down list, select **Password**.

   d) Type your KMS basic authentication password in the box.

   e) For the **Description**, type `SymantecMPKI password`.

   f) Click **Next**, review the changes you are about to make, then click **Next** again.

7. Click **Cancel** to close GenMaster.

Note: You must restart the eKeyServer service before the shared secrets are picked up by MyID.

2.5.2 Setting up KMS for MPKI 8 Cloud

No additional steps are required to set up KMS for MPKI 8 Cloud.

Note: This means that Symantec are hosting your key material.

2.5.3 Setting up KMS for MPKI 8 Enterprise

You must install and configure Symantec Enterprise Gateway, and reconfigure your Symantec MPKI 8. You no longer need to set up shared secrets, as for MPKI 7.

Unlike MPKI 7, MPKI 8 uses *two* RA certificates: one is for the IIS sites, and the other is for the Apache Tomcat site.

If you are using SSL, you must also have the local Symantec IIS websites' SSL server certificate as a trusted certificate. Add this certificate to the Trusted Root Certification Authorities certificate store for the MyID COM user on the MyID application server.

See your Symantec documentation for details.

Note: You cannot use Windows Server 2016 for Enterprise Gateway.

2.6 Setting up an authorized user list

For MPKI 8, you must set up an authorized user list in the Symantec portal for your LMKS usage. If you do not set up a list, issuance will fail.

See the *Manage authorized user lists* topic in the PKI Manager documentation provided by Symantec.

3 Known Issues and Troubleshooting

- **Error when adding a new CA**

  You may see an error in the `LogEvents` table similar to the following after attempting and failing to add a new CA:

  ```
  Error found in CheckPolicy: Request Enrollent Policy failed:
  SetClientAuth fail. Certificate Store , C:\Symantec\ra2014.pfx.  The
  given path's format is not supported.
  ```

  This is caused by the PFX file being read-only.

- **Multiple CAs with the same CA Path**

  If you have multiple CAs sharing a CA Path, the first CA that is updated has all of the Published flags for its policies set to `0`.

  This is an issue for Symantec MPKI integration where different jurisdictions may be against the same back-end issuing CA.

- **Dual Control for key recovery**

  If you have an existing Symantec MPKI connection in MyID, and you want to change it to use Dual Control for key recovery, you must contact Intercede customer support for help with reconfiguring your MyID system, quoting reference SUP-23.

- **Error A601**

  Error A601 can appear when the `common_name` or `mail_email` name value pairs are missing; the message that appears is similar to:

  ```
  Enrollment request is incomplete or incorrect. Correct the
  enrollment request and retry the operation.
  ```

  However, this error may also occur when the lifetime requested results in an invalid expiry date; for example, if the validity period of the certificates exceeds the expiration date of the issuing CA.