



MyID PIV
Version 12.8

PrimeKey EJBCA Integration Guide

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

Copyright

© 2001-2023 Intercede Limited. All rights reserved.

Information in this document is subject to change without notice. The software described in this document is furnished exclusively under a restricted license or non-disclosure agreement. Copies of software supplied by Intercede Limited may not be used resold or disclosed to third parties or used for any commercial purpose without written authorization from Intercede Limited and will perpetually remain the property of Intercede Limited. They may not be transferred to any computer without both a service contract for the use of the software on that computer being in existence and written authorization from Intercede Limited.

No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or any means electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of Intercede Limited.

Whilst Intercede Limited has made every effort in the preparation of this manual to ensure the accuracy of the information, the information contained in this manual is delivered without warranty, either express or implied. Intercede Limited will not be held liable for any damages caused, or alleged to be caused, either directly or indirectly by this manual.

Licenses and Trademarks

The Intercede® and MyID® word marks and the MyID® logo are registered trademarks of Intercede in the UK, US and other countries.

Microsoft and Windows are registered trademarks of Microsoft Corporation. Other brands and their products are trademarks or registered trademarks of their respective holders and should be noted as such. All other trademarks acknowledged.

Apache log4net

Copyright 2004-2021 The Apache Software Foundation

This product includes software developed at

The Apache Software Foundation (<https://www.apache.org/>).

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

PrimeKey EJBCA Integration Guide	1
Copyright	2
Conventions used in this document	3
Contents	4
1 Introduction	6
1.1 Supported PrimeKey EJBCA versions	6
1.1.1 PrimeKey integration with other certification authorities and HSMs	6
1.2 ECC support	6
2 Prerequisites	7
3 Configuring MyID	9
3.1 Administering EJBCA CA	9
3.2 Establishing a secure connection with the CA	9
3.3 Configuring the MyID RA user	9
3.3.1 Configuring end entity and certificate profiles for an RA User certificate	10
3.3.2 Creating a MyID RA User	11
3.3.3 Configuring MyID RA user access	12
3.3.4 Adding the MyID RA user to the RA Administrator role	14
3.4 Configuring certification authorities	15
3.5 Configuring certificate profiles	17
3.6 Configuring end entity profiles	21
3.6.1 Certificate Request Subject DN generation	24
3.7 Key escrow policy configuration overview	24
3.8 Configuring the CA within MyID	24
3.8.1 Enabling certificates policies on a CA	27
3.8.2 Mapping the additional attributes	31
3.8.3 Configuring attributes	31
3.8.4 Removing attributes	32
3.8.5 Deleting a CA	32
3.8.6 Repeated policy attributes	32
3.9 Configuring custom certificate extensions	34
3.9.1 Setting up the custom extensions in MyID	34
3.9.2 Certificate extension OIDs	35
3.9.3 Additional attribute settings	36
3.10 Attribute mapping for PIV systems	37
3.10.1 Common Name	38
3.10.2 Publishing policies	38
3.10.3 Attribute tables	38
3.10.4 PIV-I Systems	39
4 Troubleshooting	41
4.1 Logging	41
4.1.1 EJBCA audit logging	41
4.1.2 EJBCA connector logging	41
4.2 Displaying certificates in RA Web	42

4.3 Troubleshooting certificate policies 43

1 Introduction

This document is a step-by-step guide to integrating the PrimeKey EJBCA Enterprise PKI® certification authority with MyID®.

1.1 Supported PrimeKey EJBCA versions

The current version of MyID has been tested with:

- PrimeKey EJBCA Enterprise PKI version 7.11.01.

See your PrimeKey EJBCA Enterprise PKI documentation for recommendations of the hardware and software needed for PrimeKey EJBCA Enterprise PKI.

1.1.1 PrimeKey integration with other certification authorities and HSMs

The PrimeKey EJBCA server can integrate with other certification authorities and HSMs. Intercede expects that these are managed by the EJBCA server and may differ from the versions Intercede has tested. You are recommended to test compatibility with MyID before deploying to production.

Note: MyID has not been tested with EJBCA server integration with HSMs, and does not publish the certificates issued by the server.

1.2 ECC support

MyID has been tested with the following ECC capabilities of the PrimeKey EJBCA Enterprise PKI certificate authority:

- Smart card key generation using ECC using P256, P384, and P521 curves.

Note: Support for this feature is limited by smart card type – see the [Smart Card Integration Guide](#) for details.

The following features are not currently supported with the PrimeKey EJBCA Enterprise PKI certificate authority:

- Issuing certificates with ECC keys to a software local store (CSP).
- Issuing certificates with ECC keys as a .pfx file.
- Issuing certificates with ECC keys to a mobile device.
- Issuing certificates with ECC keys using the MyID SCEP interface.
- Issuing certificates with ECC keys to a Microsoft Virtual Smart Card.
- Issuing or recovering certificates with archived keys that use ECC.

2 Prerequisites

The MyID application server must be able to communicate using secure HTTP/TLS with the web service that is hosting the CA.

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

PrimeKey EJBCA Enterprise PKI is a public-key PKI certification platform for registration agents and remote users.

- Create and configure the following entities:

- CA functions:

- Certification Authority (CA).
- Crypto tokens (for storing CA keys).
- Publishers (if required).

EJBCA provides support for publishing certificates to LDAP and Active Directory. Custom publishers require customized plug-ins.

See section [3.4, Configuring certification authorities](#) when configuring a CA for use within MyID.

- System functions:

- Administration Roles.

These roles are used to control access to CAs and administrator functions.

- Services.

Various timed services are available to carry out periodic system functions and checks. Services for publishing CRLs and publishing certificates must be enabled. The HSM service is required if using HSM for storing cryptographic tokens.

The supported services you may need to configure are:

- `CRLUpdater` to periodically update the CRL from the required CAs.
- `PublisherQueueChecker` to periodically check the publication queue.
- Configure the following Custom Certificate Extensions:
 - `NACI` (PIV-only)
 - `UserSid` (PIV and Enterprise)

See section [3.9.2, Certificate extension OIDs](#).

- Configure the certificate profiles.

These determine the non-user specific content and behavior of certificates. The largest part of the settings controls the information that is included in a certificate that is issued using the certificate profile, and the source of the information. See section [3.5, Configuring certificate profiles](#) for constraints when configuring a certificate profile for use within MyID.

- Configure end entity profiles.

These are used to control the information that is present when configuring an end entity. An end entity profile specifies one or more certificate profiles that is used when generating certificates. The combination of an end entity profile and a certificate profile is used to control the information that is present in an issued certificate.

Although an end entity profile may reference multiple certificate profiles, MyID treats the combination of an end entity profile and a certificate profile as a certificate policy, and therefore end entity profiles used within MyID *must* reference only a single certificate profile.

See section [3.6, *Configuring end entity profiles*](#) for constraints when configuring end entity profiles for use within MyID.

See the PrimeKey EJBCA documentation for details on how to configure the above entities.

3 Configuring MyID

This section describes how to configure the PrimeKey EJBCA Enterprise PKI to provide RA function for the management of user entities and certificate issuance through MyID.

Several constraints on the configuration of PrimeKey EJBCA Enterprise PKI entities are imposed to ensure that the configuration is compatible for RA management through MyID. These constraints are described in this section.

3.1 Administering EJBCA CA

Before you configure the CA through the web browser UI, you must request a certificate for a CA administrator. The CA administrator certificate is used to provide a secure connection with the EJBCA,

An administrator certificate is created as part of the EJBCA PKI installation process.

You can administer the CA through the installation server command line interface or through the web browser UI. The UI provides two main pages for administering the CA:

- An Admin Web interface for various CA, RA and system level configuration functions.

The admin web is typically located at:

`https://my.primekey.com:8443/ejbca/adminweb`

- An RA Web for managing users and user certificate requests.

The RA web is typically located at:

`https://my.primekey.com:8443/ejbca/ra`

3.2 Establishing a secure connection with the CA

The certificate path for the RA and CA administrator certificates *must* be trusted to establish a secure connection with the CA. Where the certificate issuing CA is a PrimeKey EJBCA CA, you can retrieve the certificate for the issuing CA from the public part of the PrimeKey EJBCA web site; for example:

`http://my.primekey.com:8080/ejbca/retrieve/ca_certs.jsp`

You must then add the certificate to the Trusted Root Certification Authorities store.

3.3 Configuring the MyID RA user

Before MyID can access your PrimeKey PKI, you must have an RA user, with appropriate access, to enable MyID to manage certificates on the CA. A Registration Authority (RA) certificate is required for this RA user to provide a secure communication between MyID and the web service hosting the CA. You can store your RA certificate in a software keystore or on an HSM. When requesting the certificate, make sure that the request has the **Export Private Key** option set.

You must copy the RA certificate to the MyID application server. You use the location of the certificate to set the key store location when configuring the CA; see section 3.8, [Configuring the CA within MyID](#).

Although you can specify the location and password of a PFX key store when configuring the CA, you are recommended to enroll the PFX into a CSP or KSP for the MyID COM+ user. Then, export the imported certificate to a certificate file. Use the location of this file when

configuring the CA.

3.3.1 Configuring end entity and certificate profiles for an RA User certificate

You must configure a suitable end entity and certificate profile to use when issuing an RA user certificate.

The end entity profile must have the following configuration:

- Subject DN Attributes
 - Common Name

The certificate profile *must* have the following configuration:

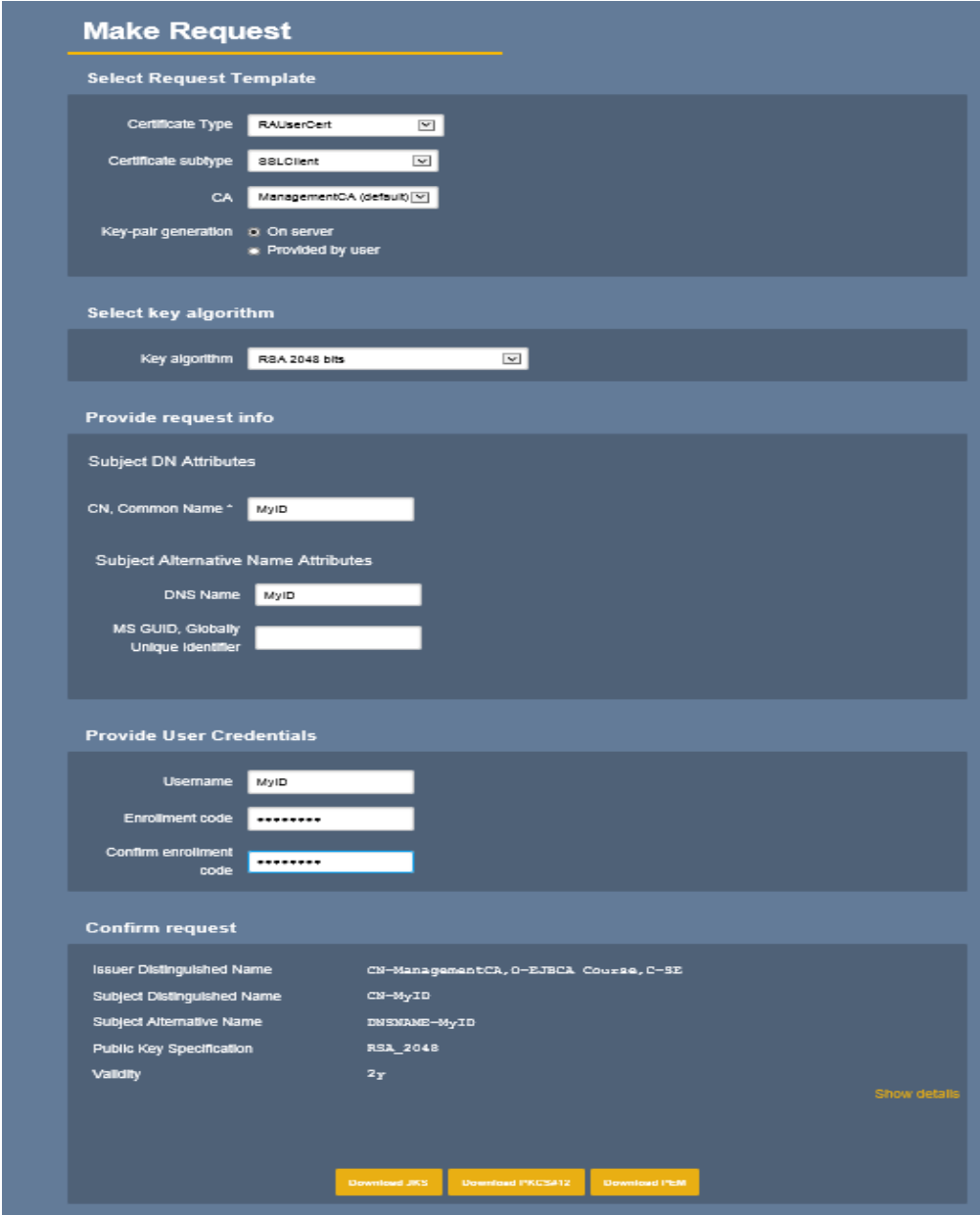
- Key Algorithm – **RSA 2048 bits**.
- Allow subject DN override by End Entity Information – **Enable**.
- Key Usage – **Digital Signature, Non-Repudiation, Key Encipherment**.
- Extended Key Usage – **Client Authentication**.

Both the end entity and certificate profile must reference the CA that is going to be used to issue the certificate in section [3.3.2, *Creating a MyID RA User*](#).

See the PrimeKey EJBCA documentation for details on how to configure the above entities.

3.3.2 Creating a MyID RA User

Create a MyID RA user through the EJBCA RA Web using the **Enroll > Make New Request** option. The MyID RA user certificate must be signed by an appropriate CA in the EJBCA; for example:



Make Request

Select Request Template

Certificate Type:

Certificate subtype:

CA:

Key-pair generation: ☐ On server ☒ Provided by user

Select key algorithm

Key algorithm:

Provide request info

Subject DN Attributes

CN, Common Name *:

Subject Alternative Name Attributes

DNS Name:

MS GUID, Globally Unique Identifier:

Provide User Credentials

Username:

Enrollment code:

Confirm enrollment code:

Confirm request

Issuer Distinguished Name	CN=ManagementCA, O=EJBCA Course, C=SE
Subject Distinguished Name	CN=MyID
Subject Alternative Name	DNSNAME=MyID
Public Key Specification	RSA_2048
Validity	2y

[Show details](#)

[Download JKS](#) [Download PKCS#12](#) [Download PEM](#)

Enroll the user certificate by clicking the **Download PKCS#12** button. You can then use the downloaded certificate with MyID; the password is provided in the **Enrollment code** field.

Note: To allow the establishment of a secure connection, you must configure the EJBCA server to trust the CA that is used to issue the certificate.

3.3.3 Configuring MyID RA user access

The roles assigned to the RA user used by MyID define the MyID administrative capabilities. You can assign access rules for a role when creating the role, as described below, or after creating the role using EJBCA GUI **Roles > Access Rules** option.

Although MyID acts as an RA administrator, the default RA Administrator template access rules do not provide sufficient access to enable MyID to validate and synchronize the policies of the EJBCA. As such, you need the Advanced Mode to configure the access rules.

At minimum the user must have the following access rules assigned:

Configuration Option	Setting
Role	MyID RA Administrator
Authorized CAs	Access to all Certificate Authorities.
Regular access rules	<ul style="list-style-type: none"> • Default RA Administrator access rules • View certificate profile • View end entity profiles
End Entity Rules	<ul style="list-style-type: none"> • Create, Delete, Edit, Revoke, and View End Entities. • Key Recover End Entities.
End Entity Profiles	Provide access to all the end entity profiles, or at least those end entity profiles associated with MyID. Even if access is provided to all end entity profiles, only those profiles that reference one or more of the CAs used by MyID will be visible within MyID as certificate policies.
Validators	None.
Internal key binding	None.
Other rules	None.

The following shows the minimum configuration options in the **Regular Access Rules** settings when configuring the access rules in advanced mode:

Edit Access Rules[?]

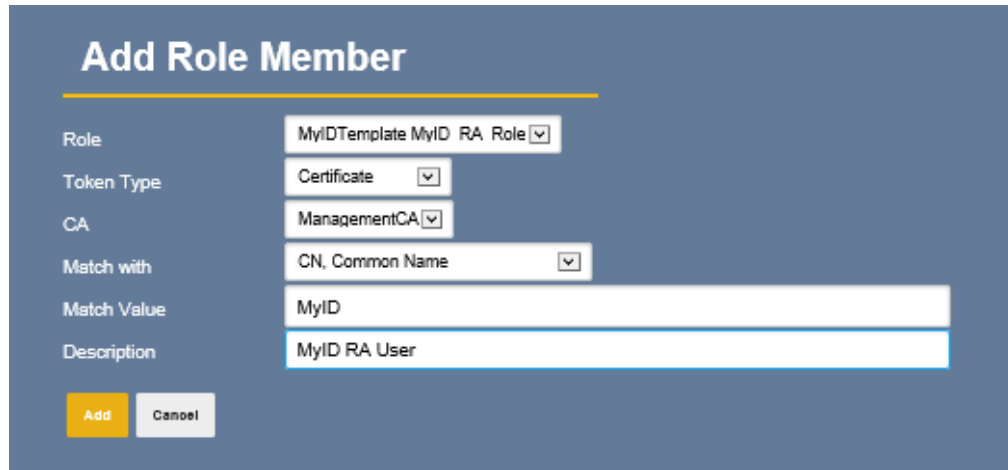
Administrator Role : RA Administrator

Role Based Access Rules	
/	<input type="radio"/> Allow <input type="radio"/> Deny <input checked="" type="radio"/> Inherit (Deny)
/administrator/	<input checked="" type="radio"/> Allow <input type="radio"/> Deny <input type="radio"/> Inherit
Regular Access Rules	
/ca_functionality/	<input type="radio"/> Allow <input type="radio"/> Deny <input checked="" type="radio"/> Inherit
/ca_functionality/activate_ca/	<input type="radio"/> Allow <input type="radio"/> Deny <input checked="" type="radio"/> Inherit
/ca_functionality/approve_caaction/	<input type="radio"/> Allow <input type="radio"/> Deny <input checked="" type="radio"/> Inherit
/ca_functionality/create_certificate/	<input checked="" type="radio"/> Allow <input type="radio"/> Deny <input type="radio"/> Inherit
/ca_functionality/create_crl/	<input type="radio"/> Allow <input type="radio"/> Deny <input checked="" type="radio"/> Inherit
/ca_functionality/edit_approval_profiles/	<input type="radio"/> Allow <input type="radio"/> Deny <input checked="" type="radio"/> Inherit
/ca_functionality/edit_blacklist/	<input type="radio"/> Allow <input type="radio"/> Deny <input checked="" type="radio"/> Inherit
/ca_functionality/edit_ca/	<input type="radio"/> Allow <input type="radio"/> Deny <input checked="" type="radio"/> Inherit
/ca_functionality/edit_certificate_profiles/	<input type="radio"/> Allow <input type="radio"/> Deny <input checked="" type="radio"/> Inherit
/ca_functionality/edit_publisher/	<input type="radio"/> Allow <input type="radio"/> Deny <input checked="" type="radio"/> Inherit
/ca_functionality/edit_validator/	<input type="radio"/> Allow <input type="radio"/> Deny <input checked="" type="radio"/> Inherit
/ca_functionality/renew_ca/	<input type="radio"/> Allow <input type="radio"/> Deny <input checked="" type="radio"/> Inherit
/ca_functionality/view_approval_profiles/	<input type="radio"/> Allow <input type="radio"/> Deny <input checked="" type="radio"/> Inherit
/ca_functionality/view_ca/	<input type="radio"/> Allow <input type="radio"/> Deny <input checked="" type="radio"/> Inherit
/ca_functionality/view_certificate/	<input type="radio"/> Allow <input type="radio"/> Deny <input checked="" type="radio"/> Inherit
/ca_functionality/view_certificate_profiles/	<input checked="" type="radio"/> Allow <input type="radio"/> Deny <input type="radio"/> Inherit
/ca_functionality/view_publisher/	<input type="radio"/> Allow <input type="radio"/> Deny <input checked="" type="radio"/> Inherit
/ca_functionality/view_validator/	<input type="radio"/> Allow <input type="radio"/> Deny <input checked="" type="radio"/> Inherit
/ra_functionality/	<input type="radio"/> Allow <input type="radio"/> Deny <input checked="" type="radio"/> Inherit
/ra_functionality/approve_end_entity/	<input checked="" type="radio"/> Allow <input type="radio"/> Deny <input type="radio"/> Inherit
/ra_functionality/create_end_entity/	<input checked="" type="radio"/> Allow <input type="radio"/> Deny <input type="radio"/> Inherit
/ra_functionality/delete_end_entity/	<input checked="" type="radio"/> Allow <input type="radio"/> Deny <input type="radio"/> Inherit
/ra_functionality/edit_end_entity/	<input checked="" type="radio"/> Allow <input type="radio"/> Deny <input type="radio"/> Inherit
/ra_functionality/edit_end_entity_profiles/	<input type="radio"/> Allow <input type="radio"/> Deny <input checked="" type="radio"/> Inherit
/ra_functionality/edit_user_data_sources/	<input type="radio"/> Allow <input type="radio"/> Deny <input checked="" type="radio"/> Inherit
/ra_functionality/keyrecovery/	<input checked="" type="radio"/> Allow <input type="radio"/> Deny <input type="radio"/> Inherit
/ra_functionality/revoke_end_entity/	<input checked="" type="radio"/> Allow <input type="radio"/> Deny <input type="radio"/> Inherit
/ra_functionality/view_approvals/	<input checked="" type="radio"/> Allow <input type="radio"/> Deny <input type="radio"/> Inherit
/ra_functionality/view_end_entity/	<input checked="" type="radio"/> Allow <input type="radio"/> Deny <input type="radio"/> Inherit
/ra_functionality/view_end_entity_history/	<input checked="" type="radio"/> Allow <input type="radio"/> Deny <input type="radio"/> Inherit
/ra_functionality/view_end_entity_profiles/	<input checked="" type="radio"/> Allow <input type="radio"/> Deny <input type="radio"/> Inherit
/services/edit/	<input type="radio"/> Allow <input type="radio"/> Deny <input checked="" type="radio"/> Inherit
/services/view/	<input type="radio"/> Allow <input type="radio"/> Deny <input checked="" type="radio"/> Inherit

You can configure an RA administrator role, if not already provided by default, using the administrator RA Web **Role Management > Roles** option.

3.3.4 Adding the MyID RA user to the RA Administrator role

Add the MyID RA user to the MyID RA Administrator role using the **Add Role Member** option in the RA Web **Role Management > Role Members** option; for example:



The screenshot shows a web form titled "Add Role Member" with a blue header. The form contains several fields and buttons:

- Role:** A dropdown menu with the selected value "MyIDTemplate MyID RA Role".
- Token Type:** A dropdown menu with the selected value "Certificate".
- CA:** A dropdown menu with the selected value "ManagementCA".
- Match with:** A dropdown menu with the selected value "CN, Common Name".
- Match Value:** A text input field containing "MyID".
- Description:** A text input field containing "MyID RA User".
- Buttons:** Two buttons at the bottom left: "Add" (yellow) and "Cancel" (gray).

In the above example, the subject common name is used to determine the user role, and hence their capabilities.

You can also add a user to a role through the EJBCA Adminweb using the **Administrator Roles > Members** option.

3.4 Configuring certification authorities

Before you add a PrimeKey EJBCA CA into MyID, you must configure the CA on the PrimeKey EJBCA.

See your PrimeKey EJBCA documentation for details.

The following restrictions are imposed on configuring a CA to ensure that MyID can manage certificates using the CA, and to prevent performance degradation due to unnecessary database queries.

Configuration Field	Purpose	Enforcement
Type of CA	Controls the type of certificates that can be issued by the CA, X509 or CVC.	X.509
Crypto Token	Token where the CA's key mappings are expected to exist.	PKCS#11 HSM slot mapping, or a Soft PKCS#12 keystore in the database. A PKCS#11 crypto token requires additional common fields to be set to identify the location of the crypto token. See the PrimeKey EJBCA documentation for details.
Enforce unique public keys	When enabled, checks are performed that the same public key is not used to issue certificates using different certificate policies (users are associated with certificate policy when used by MyID).	Disable When enabled may affect performance if the database is not configured with (subjectKeyId, issuerDN) database index.
Enforce unique DN	Enforces that the same DN cannot be used when issuing policies using different certificate policies.	Disable Enabling this option would prevent a user being issued certificates using different policies but the same DN.
Enforce unique Subject DN Serial Number	Ensures that only one end entity, with a specific Subject DN Serial Number, can be issued from this CA.	Disable (default) Enabling this option can affect certificate issuance performance and prevent the same user being issued certificates using different certificate policies if Subject DN serial number is used.
Use Certificate Request History	Maintain a history of Certificate Requests.	Disable (default) Enabling this option will lead to reduced certificate issuance performance.

Configuration Field	Purpose	Enforcement
Use User Storage	Allows users (end entities) to be searched. When enabled, a certificate can only be requested for stored users (end entity).	Enable You can disable the option to improve performance when the CA is not being used for escrow. You <i>must</i> enable this option when using the PrimeKey PKI CA for key escrow.
Use Certificate Storage	Stores issued certificates to enable certificates to be retrieved and provide revocation information.	Enable (default) Required to provide CRLs although it does have the effect of reducing performance. You <i>must</i> enable this option when using the PrimeKey PKI CA for key escrow.
Default CA defined validation data	Configure a CRL distribution point OCSP default service URI. A CRL publishing service is required to periodically publish the CRL.	If you need to validate certificates against a CRL, the CRL publishing service must be enabled to publish the updated CRL periodically; the MyID application server must be able to access the Certificate Revocation List (CRL) location, and if configured, the OCSP default service URI. Certificate profiles used to issue certificates that are published with the CA <i>must</i> have the Access Information Access , as well as the Use CA defined CA issuer and/or the Use CA defined OCSP locator options enabled; see section 3.5, Configuring certificate profiles .
Approval Settings	Provides default approval settings for the relevant options.	None Enabling these prevents operations being completed until the operation has been approved.
Finish User	Checks if an end entity should transit from New to Generated after issuing a certificate.	Enable Disabling this setting prevents the end entity from being created in a specific table within PrimeKey database. This will prevent the EJBCA "republish all" CLI command from failing when attempting to publish an issued certificate to an external database.

3.5 Configuring certificate profiles

The following restrictions are imposed on configuring certificate profiles that are used for issuing certificates to users to ensure that MyID can manage certificates using the CA.

Configuration Field	Purpose	Enforcement
Type	Type of entity using the certificate profile.	End Entity
Available key algorithm	List of allowed key algorithms that public key used in the certificate request.	Select RSA if the profile is to be used for issuing RSA certificates. Select ECDSA if the profile is to be used for issuing ECC certificates. You can use a profile for both RSA and ECDSA keys.
Available bit lengths	List of allowed key sizes that the public key used in the certificate requests must comply with.	Ensure that the required bit lengths are selected. Bit lengths supported by MyID are: RSA: 1024, 1536, 2048 and 4096 ECDSA: 256, 384 and 521
Validity Offset	A validity offset can be configured to handle to handle clock skew. The offset adjusts the certificate validity start/end times when the corresponding validity time is specified as a relative time. The default validity offset is used if an offset is not specified.	To prevent a certificate lifetime exceeding the required certificate lifetime, MyID specifies the certificate start time only in terms of relative time. The certificate end time is specified as a fixed time. Hence the validity offset is applied only to the certificate start time.
Allow validity override	Enables the default certificate validity period, specified in the certificate profile, to be overridden by the validity period in the certificate request.	Enable MyID allows the required validity period to be overridden by the setting the credential profile used to issue the certificate. The policy validity period should not be modified through the Certificate Authorities workflow, as the change would get overwritten on the next policy synchronization.

Configuration Field	Purpose	Enforcement
Allow extension override	<p>When enabled, allows X.509 certificate extensions featured in a certificate request to be honored. Externally supplied extensions are added "as-is". Matching extensions already supplied in the certificate profile are overridden.</p> <p>Further override control can be provided by providing a comma separated list of OIDs specifying the extensions that may (or may not) be overridden.</p> <p>When this option is disabled, the default certificate profile extensions are used and the end entity subject DN is taken from the registered entity LDAP setting.</p>	<p>Enable</p> <p>MyID provides dynamic extension data that is written to the certificate.</p>
Allow subject DN override by CSR	<p>Allows the X.509 subject DN in a certificate to come directly from the PKCS#10 included in the certificate request rather than from the registered end entity LDAP DN entry.</p>	<p>You must disable this option for certificate profiles that are used for key escrow policies, as PKCS#10 is not provided in the certificate request for these policies.</p> <p>Normally this option is enabled for non-key escrow policies, although you can disable the option if the subject DN is being generated using the policy attributes or custom DN order is required using the certificate profile's Custom DN Order setting.</p> <p>See section 3.8.3, Configuring attributes for information on configuring policy attributes.</p>

Configuration Field	Purpose	Enforcement
Allow subject DN override by End Entity Information	Allows the X.509 subject DN in a certificate to come from the end entity information supplied in the certificate request rather than from the registered end entity LDAP DN entry.	Enabled MyID configures the end entity being used for the certificate request with same subject DN as that provided in the request, although this may not be the same as that provided in the CSR for a non-key certificate request. An End Entity that is being used for non-key archive certificate request can get used for multiple users. As such the DN held against the end entity gets updated for each certificate request. Therefore the recommendation is, if not using the DN supplied in the CSR, to use the DN supplied in the request rather than that stored against the end entity information. Both this and the Allow subject DN override by CSR option must be disabled if use of the custom DN order is required in the certificate profile's Custom DN Order setting
Allow Key Usage Override	When enabled, allows the key usage to be overridden by the certificate request.	Disabled (default) The option is not currently used by MyID.
Use certificate storage	Issued certificates are stored in the database to provide certificate management and CRLs.	Enabled Note: This may impact on certificate issuance performance.
CRL Distribution point	The CRL Distribution point information enables a client to verify a certificate using the provided URI.	Enable
Certificate Policies	Policy OIDs may be set to indicate that certificates issued using this profile are for a specific purpose.	Enable the Use option and specify the required policy OIDs to ensure that certificates issued using the profile assert the required policy OID as specified by the appropriate common policy requirement; for example, PIV model policies may be required to assert policy OIDs to satisfy the X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework.

Configuration Field	Purpose	Enforcement
X.509v3 extensions	This group of configuration options is used to control which X.509v3 validation data extensions URIs are asserted by certificates issued with this profile.	Enable the Use option for the extensions according to the common policy requirements; for example, PIV model policies may be required to assert the CRL Distribution Points and the OCSP Service Locator URIs. It is recommended that the URI values are inherited from the CA configuration rather than being specified within the profile.
Used Custom Certificate Extensions	Selects custom extensions, configured through the custom data in System Configuration , as described in section 3.9, Configuring custom certificate extensions . Selected custom extensions are, by default, treated as mandatory, and the extension default value is used if an override value is not provided in the certificate request.	Select the required configured custom extensions. Custom extensions, as described in section 3.9.1, Setting up the custom extensions in MyID , are added to a policy only if at least one custom extension has been selected in the corresponding certificate profile.
Approval settings	Provides default approval settings for the relevant options.	None (default) Enabling these prevents operations being completed until the operation has been approved.
Available CAs	Determines which CAs can use this certificate profile for certificate issuance.	You must at least select the CA that was specified in the CA Path field when configuring the CA through the Certificate Authorities workflow.
Publishers	Controls where the certificate is published.	Select if certificates issued using the certificate profile are required to be published.
Single Active Certificate Constraint	Controls if multiple active certificates can be issued to an end entity.	Disable (default) Enabling this option prevents MyID from issuing multiple certificates using the same certificate policy.

3.6 Configuring end entity profiles

The following restrictions are imposed on configuring end entity profiles that are used for issuing certificates to users to ensure that MyID can manage certificates using the CA.

Configuration Field	Purpose	Enforcement
Username	Controls if the username for the end entity is automatically generated.	Disable auto-generated MyID provides the username based on the end entity profile name.
Password (Enrolment Code)	Password is used for key and certificate recovery.	Disable auto-generated Enable the Required option for profiles being used for key escrow certificates, as a password is required to recover the server-generated keypair. Passwords are not required for non-key escrow certificates, as certificates issued using the profile do not need to be recovered.
Maximum number of failed login attempts	Used when the EJBCA is also validating login attempts using the configured password.	Disable
Batch generation (clear text pwd storage)	Password is used to authenticate PKI requests.	Disable
End Entity E-mail	Email is used for notifications.	Disable The EJBCA is not used for sending notifications.

Configuration Field	Purpose	Enforcement
Subject DN Attributes	<p>Controls which DN attributes can be configured in the Subject DN.</p> <p>This configuration is used to populate the certificate policy extensions in MyID.</p>	<p>See section 3.9.3, Additional attribute settings.</p> <p>For each attribute:</p> <ul style="list-style-type: none"> Enable the Required option if the attribute is mandatory. A certificate request will fail if a mandatory attribute is not supplied in the certificate request even if the subject DN attributes are being taken from the supplied PKCS#10 data. <p>See section 3.8.1, Enabling certificates policies on a CA for details of mapping policy attributes in MyID.</p> <ul style="list-style-type: none"> Enable the Modifiable field if the value can be modified. This option is normally enabled unless there is a specific reason for wanting a static attribute value in the issued certificates. <p>You must specify a static value for any non-modifiable attribute. In this case the attribute must also be configured with the same value in MyID.</p> <p>When configuring an End Entity profile for key escrow certificates or when using a certificate profile that uses the Subject DN supplied in the certificate request, the Subject DN components must cater for any DN components that are required for the certificate.</p> <p>Any DN components that are not specified in this section will not be supplied in the certificate request.</p> <p>Where the supplied subject DN may contain repeated DN components, the number of such components, configured in the profile, must be greater than or equal to the maximum number of such components.</p> <p>For example, if the supplied DN could have three OU components, the profile must also have at least three OU components.</p>

Configuration Field	Purpose	Enforcement
Other Subject Attributes	Controls which SAN and Subject Directory attributes are required to be configured in this certificate policy. This configuration is used to populate the certificate policy extensions in MyID.	As for Subject DN Attributes. When adding RFC 822 Name attribute, the Use entity e-mail field option is automatically enabled and the Modifiable option is disabled. An email address is not set for an end entity and therefore you <i>must</i> disable the Use entity e-mail option. The Modifiable option must also be enabled but initially this may remain disabled; in this case, you must save the profile setting and then re-edit the profile to set the Modifiable option.
Default Certificate Profile	The certificate profile used if a certificate profile is not specified in the certificate request.	MyID does not specify the certificate profile in the received certificate request, therefore the default certificate profile is used.
Available Certificate Profiles	Controls which certificate profiles can be used in a certificate request using this profile.	You can leave this list unselected, as the default certificate will be added even if it has not been selected.
Available CAs	Determines which CAs can use this certificate profile for certificate issuance.	Must at least select the CA selected in the certificate profile referenced by this profile. Ensure that the profile does not reference a CA, including the default CA, that is not referenced by the referenced certificate profile.
Default Token	Controls the types of certificates that may be issued using this profile.	Must select User Generated . Must also select P12 token for key escrow certificate policies.
Key recoverable	Identifies that the profile can be used to recover the server-generated encryption keys.	Check Use if the profile is to be used for issuing key escrow certificates; otherwise, leave this option unchecked. When Use is checked, you must also check the following to prevent additional certificates being created unnecessarily: Default and Reuse old certificate .
Send Notifications	Notification is sent when a certificate is available for collection.	Leave unset PrimeKey EJBCA CA must not be used for sending notifications.

Note: For the Key Management End Entity, you must make sure that the minimum password strength is set to a value higher than 0. If you set the minimum password strength to 0, the key management certificate does not issue.

3.6.1 Certificate Request Subject DN generation

MyID automatically generates the subject DN for the certificate request using any configured certificate policy attributes and the supplied user DN. Where the same DN component is present in both the certificate policy attribute and the user DN, the attribute supplied in the attributes takes priority. Only those subject DN components that have been configured as being allowed in the corresponding End Entity Profile will be included in the generated subject DN.

3.7 Key escrow policy configuration overview

This section provides an overview of the configurations required to support key escrow policies:

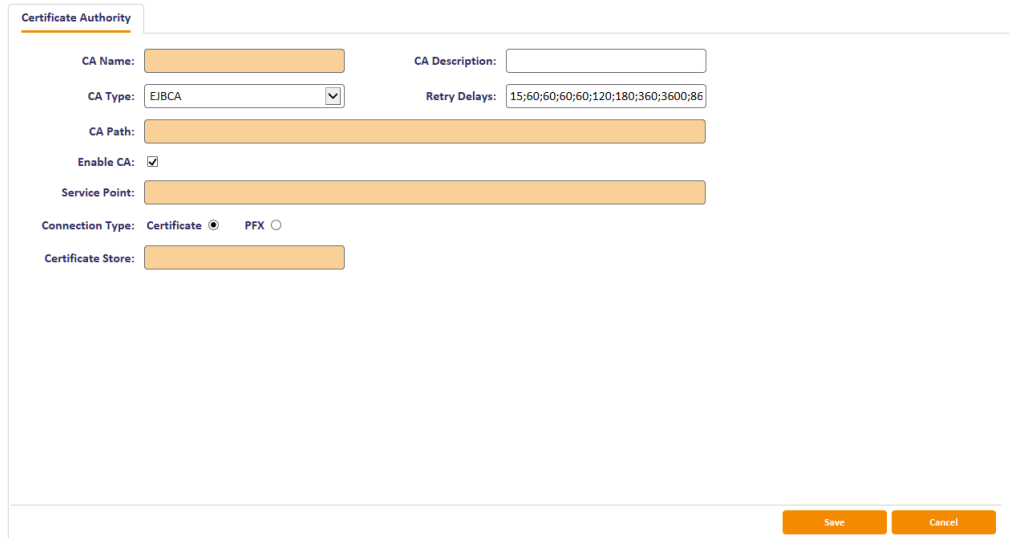
1. Enable the **Enable Key Recovery** option in the **Basic Configuration** tab under **System Configuration**.
You must set this first, as the key recoverable option is available in the end entity profile only when key recovery is enabled.
2. Set the following configuration options in the end entity profile being used for issuing key escrow certificates:
 - **Password** – check **Required**.
 - **Key recoverable** – check **Use**, **Default**, and **Reuse old certificate**.
 - **Subject DN Attributes** – configure according to the required subject DN attributes.
3. Check the following configuration options in the certificate profile being used for issuing key escrow certificates:
 - **Available key algorithm** – select **RSA**.
 - **Signature algorithm** – select the required RSA hashing algorithm.
 - **Allow subject DN override by CSR** – deselect **Allow**.
 - **Allow subject DN override by End Entity Information** – select **Allow**.

3.8 Configuring the CA within MyID

Configure the PrimeKey PKI CA using the **Certificate Authorities** workflow.

1. Put the RA certificate file 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 **EJBCA**.



5. Type a **CA Name**.

This is a friendly name that is used to identify the CA.

6. Type a **CA Description**.

This is a description for the CA.

7. 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.

8. Type the **CA Path**.

The CA name as configured on the EJBCA. The name is not case-sensitive.

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

10. Type the **Service Point**.

This is the full URL for the PrimeKey-hosted certification authority web service; for example:

`https://myserver.com:8443/ejbca/ejbcaws/ejbcaws`

Note: The EJBCA web service API is called `ejbcaws`, and is located in the directory named `ejbca/ejbcaws` – therefore, the web service full URL ends with the following:

`/ejbca/ejbcaws/ejbcaws`

11. 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 (as described in section 3.3, *Configuring the MyID RA user*):

- a. For the **Connection Type**, select the **Certificate** option.
- b. Type the location of the certificate file in the **Certificate Store** box.

For example:

`C:\PrimeKey\RACert.cer`

12. If your RA certificate is held in a PFX file:

- a. For the **Connection Type**, select the **PFX** option.
- b. Type the location of the certificate file in the **PFXCertificate Store** box.

For example:

`C:\PrimeKey\RACert.p12`

- c. Type and confirm the password for the certificate (only required for a pfx or p12 certificate store).

Note: You are recommended to enroll the private key into a CSP or KSP for establishing the secure connection to avoid the additional overhead related to using a p12 or pfx files.

13. Click **Save**.

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

Note: If your RA certificate is held in a PFX file, you must restart the eCertificate service before you can set up your certificate templates within MyID.:

1. From the Windows Administrative Tools, double-click Services.
2. Right-click the **eCertificate Services Server** service, then from the pop-up menu click **Restart**.

3.8.1 Enabling certificates policies on a CA

Note: Because of the way MyID manages PrimeKey PKI certificate template names, the displayed Friendly name is the name of the end entity profile on the PrimeKey EJBCA that references the CA as identified in the **CA Name** field.

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.

Name	Description	Allow Issuance	Reverse DN	Archive Keys	Superseded
PIV Authentication 2 On MYIDCA		X	X	X	X
PIV Key Management 2 On MYIDCA		X	X	X	X
PIV Key Management On MYIDCA		X	X	X	X
PIVAuthenticate On MYIDCA		X	X	X	X
PIVCardAuthentication On MYIDCA		X	X	X	X
PIVSigning On MYIDCA		X	X	X	X
Smartcard Logon On MYIDCA		X	X	X	X
User On MYIDCA		X	X	X	X

3. Click **Edit**.

Available Certificates

- PIV Authentication 2 On MYIDCA
- * PIV Key Management On MYIDCA
- * PIV Key Management 2 On MYIDCA
- * PIVAuthenticate On MYIDCA
- * PIVCardAuthentication On MYIDCA
- PIVSigning On MYIDCA
- Smartcard Logon On MYIDCA
- User On MYIDCA

* = Enabled Policy

Enabled (Allow Issuance)

Display Name: PIV Authentication 2 On MYIDCA

Description:

Allow Identity Mapping: ☐

Reverse DN: ☐

Archive Keys: None

Certificate Lifetime: 730

Automatic Renewal: ☒

Certificate Storage: ☒ Hardware ☐ Software ☐ Both

Recovery Storage: ☒ Hardware ☐ Software ☐ Both ☐ None

Key Algorithm: RSA 2048

Key Purpose: Signature and Encryption

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.
- **Description** – a description of the policy.
- **Allow Identity Mapping** – used for additional identities. See the *Additional identities* section in the [Administration Guide](#) for details.
- **Reverse DN** – select this option if the certificate requires the Distinguished Name to be reversed. This setting has an effect only when the EJBCA policy is configured to use the subject DN from the supplied PKCS10. A key management certificate request does not have a PKCS10.

See section [3.9.3, Additional attribute settings](#) for details.

- **Archive Keys** – select whether the keys should be archived. For policies configured for key archive, set this option to **EJBCA Client**.
- **Certificate Lifetime** – the life in days of the certificate. This is defaulted to the maximum allowed life imposed by the certificate policy on CA.
- **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.
- **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.

The CSP you select determines what type of certificate templates you can use. For example, if you want to use a 2048-bit key algorithm, you cannot select the Microsoft Base Cryptographic Provider; you must select the Microsoft Enhanced Cryptographic Provider. See your Microsoft documentation for details.

- **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.

- **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 can 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.
- **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
Common Name	Dynamic	Common Name
RFC 822 Name(e-mail address)	Dynamic	Email
NACI	Not Required	Not Required
User Security Identifier	Dynamic	User Security Identifier

* = Mandatory attribute
= Recommended attribute

[Hide Attributes](#)

For details of adding the User Security Identifier or NACI extension to your certificates, see section [3.9.2, Certificate extension OIDs](#).

- 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**.

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

Important: Where there are repeated components, do *not* leave intermediate attributes as **Not Required** (as shown below) as this may result in certificate request failure, depending on the profile configuration:

Common Name	Not Required	Not Required
Organizational Unit *	Static	Company
Organizational Unit *	Not Required	Not Required
Organizational Unit *	Static	Org
Organization *	Not Required	Not Required

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.

3.8.2 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 [3.8.1, Enabling certificates policies on a CA](#) for details.

For details of adding the User Security Identifier or NACI extension to your certificates, see section [3.9.2, Certificate extension OIDs](#).

3.8.3 Configuring attributes

The end entity profile configuration is used to determine which attributes are available for the corresponding certificate policy within MyID.

The following shows an example of configuring Subject DN Attributes:

Subject DN Attributes [?]

Subject DN Attributes	Value	Required	Modifiable	Validation
emailAddress, E-mail address in DN		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
CN, Common name		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
OU, Organizational Unit		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
O, Organization		<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
C, Country (ISO 3166)	UK	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

The following subject attributes are defined in the above example: Common Name (CN), Organizational Unit (OU), Organization (O), and Country (C). Of these, the CN and OU attributes are mandatory, and C has a non-modifiable static value.

Note: The default value for an attribute is used only if the attribute is not modifiable.

The available Subject DN and Subject Alternative Name attributes are limited to the attributes that are supported by the EJBCA, not all of which are supported by MyID. The attributes for which MyID provides a dynamic mapping, for the inserted attribute value, are listed below:

Ejbca End Entity Profile Attribute	Attribute Group	MyID Attribute Mapping
Common Name	Subject DN	Common Name
Domain Component	Subject DN	Domain
First Name	Subject DN	First Name
Full Name	Subject DN	Full Name (name)
Organizational Unit	Subject DN	Group Name or Application Group
DN Serial Number	Subject DN	Serial Number
Surname	Subject DN	Surname
Title	Subject DN	Title
RFC 822 Name (email address)	Subject Alt-Name	Email

EjbcA End Entity Profile Attribute	Attribute Group	MyID Attribute Mapping
FASC-N	Subject Alt-Name	FASC-N (Hex)
User Principal Name	Subject Alt-Name	User Principal Name
Uniform Resource ID	Subject Alt-Name	UUID (ASCII)

You can use attributes for which MyID does not have default dynamic mapping, but these would require static value or custom implementation.

Note: You must not set dynamic mappings of attributes to Organizational Unit or Distinguished Name, as these may be made of multiple attribute components and therefore will result in the certificate request being rejected by the EJBCA.

Note: You must supply a mapped value if the attribute is configured as being mandatory in the end entity profile in the EJBCA.

3.8.4 Removing attributes

If you remove an attribute component from an End Entity profile, the policy attribute is no longer visible in the **Certificate Authorities** workflow.

As such, if you have previously configured the attribute in MyID, it remains configured; however, the operator can no longer manage the attribute.

You are recommended to remove any attributes from MyID by resetting the attribute as **Not required** in the **Certificate Authorities** workflow *before* removing them from the CA End Entity profile setting.

3.8.5 Deleting a CA

You can delete a CA from the list of available CAs if you no longer need to be able to work with it, or if you created it in error.

See the *Deleting a CA* section in the [Administration Guide](#) for details.

3.8.6 Repeated policy attributes

MyID displays the policy attributes as defined in the End Entity Profile on the CA. To allow a DN with a duplicate component to be provided in a certificate request, the component is also required to be duplicated in the End Entity Profile in the CA, with the number of duplications matching the maximum number of such duplications in user DNs for that component. This results in the attributes also being duplicated within MyID. MyID is able to internally distinguish between these duplicate attributes but this distinction is not visible to the user.

Attribute	Type	Value
Common Name	Not Required	Not Required
Organizational Unit	Static	Test
Organizational Unit	Static	Adhoc
Organization	Not Required	Not Required
Organization	Not Required	Not Required
DN Serial Number	Not Required	Not Required
Domain Component	Not Required	Not Required
Domain Component	Not Required	Not Required
Postal Code	Not Required	Not Required
Organization	Not Required	Not Required

* = Mandatory attribute
= Recommended attribute

Hide Attributes

Where DN component values are provided through the policy attributes that are configured through the **Certificate Authorities** workflow in MyID, these are added to the DN that is supplied in the certificate request in the order that the attributes are received by the CA connector. Any DN component that is defined in the End Entity Profile, but for which values is not supplied in policy attributes, are automatically added by the CA connector using the supplied user DN.

Where a DN component values are fixed, and the order of the values is important, it is recommended that default, non-modifiable, values are specified in the End Entity Profile in the CA. The order of the fixed attribute values specified against the policy in MyID must then match the attribute values configured in the CA. A certificate request with the DN component values in a different order would be rejected.

Subject DN Attributes [?]	
Subject DN Attributes	emailAddress, E-mail address in DN <input type="button" value="Add"/>
CN, Common name	<input type="text"/> <input type="checkbox"/> Required <input checked="" type="checkbox"/> Modifiable <input type="checkbox"/> Validation <input type="text"/>
OU, Organizational Unit	Test <input type="checkbox"/> Required <input type="checkbox"/> Modifiable <input type="checkbox"/> Validation <input type="text"/>
OU, Organizational Unit	Adhoc <input type="checkbox"/> Required <input type="checkbox"/> Modifiable <input type="checkbox"/> Validation <input type="text"/>
O, Organization	<input type="text"/> <input type="checkbox"/> Required <input checked="" type="checkbox"/> Modifiable <input type="checkbox"/> Validation <input type="text"/>
O, Organization	<input type="text"/> <input type="checkbox"/> Required <input checked="" type="checkbox"/> Modifiable <input type="checkbox"/> Validation <input type="text"/>

The actual order in which the DN components are written to a certificate is dependent on various settings within the Certificate Policy in the CA. See section [3.9.3, Additional attribute settings](#).

3.9 Configuring custom certificate extensions

PrimeKey EJBCA Enterprise PKI provides support for custom extensions to be added to a certificate.

The required extensions are first configured in the PrimeKey EJBCA through the Custom Certificate Extensions settings in the System Configuration as shown:

ID	0
Object Identifier (OID)	<input type="text" value="0.1.0.01"/>
Label	<input type="text" value="myExtension"/>
Extension Class	<input type="text" value="Basic Certificate Extension"/>
Critical	<input type="checkbox"/>

Properties

Key	Value
dynamic	<input type="text" value="true"/>
encoding	<input type="text" value="DERBITSTRING"/>
value	<input type="text" value="A String"/>
<input type="button" value="Save"/>	

The OID is the extension that is added to the certificate.

Inclusion of a custom extension in a certificate requires that:

- The associated certificate profile references the required custom extension through its **Used Custom Certificate Extensions** setting.
- The use **Custom certificate extension data** option is enabled in the corresponding end entity profile.

Further information about managing these custom extensions is described in the PrimeKey EJBCA administration guide.

3.9.1 Setting up the custom extensions in MyID

MyID is unable to interrogate the PrimeKey EJBCA system configuration through the web service interface and, although it can identify that a certificate profile is referencing custom extensions, it cannot extract the extension details. Therefore, custom extensions cannot be automatically added to certificate policies within MyID.

Therefore, these custom extensions are identified through a custom extensions configuration file: `EjbcaPKIConnector.xml`. All custom extensions are defined in this file within an XML `<Extensions>` node. Each custom extension is defined in an `<Extension>` node.

For example, a configuration with two custom extensions would look like:

```
<Extensions>
  <Extension displayType="optional">
    <Name>MyExtnsion</Name>
    <DisplayName>My Extension</DisplayName>
    <OID>0.1.0.01</OID>
  </Extension>
  <Extension displayType="mandatory">
    <Name>MyExtnsion2</Name>
    <DisplayName>My Extension 2</DisplayName>
    <OID>0.1.0.02</OID>
  </Extension>
</Extensions>
```

The EJBCA connector attempts to load the custom extensions file from the MyID `Components` folder on the MyID application server; by default, this is:

`C:\Program Files\Intercede\MyID\Components\`

A default `EjbcaPKIConnector.xml` file, containing only the PIV NACI extension, is installed in the EJBCA installation folder on the MyID application server; by default, this is:

`C:\Program Files\Intercede\MyID\Components\PKI\EJBCA\`

You must add any additional custom extension to this file, then copy the file to the MyID `Components` folder.

As MyID cannot determine which custom extensions are being referenced by the individual policies, all custom extensions identified in the configuration file are added as policy attributes to any policy that references a custom extension on the PrimeKey EJBCA. It is up to the administrator to configure the required attributes through the **Certificate Authorities** workflow, as described in section [3.8.1, *Enabling certificates policies on a CA*](#).

Although an extension can be set to mandatory or optional within MyID, any referenced custom extensions are treated as mandatory by the EJBCA with the default value, configured in the system configuration, being used if a value is not supplied.

Note: The OID value of these custom extensions must match the extensions configured in the System Configuration in the PrimeKey EJBCA.

Note: After you have made any changes to this file, you must restart the eCertificate service to update the certificate policies within MyID.

1. From the Windows Administrative Tools, double-click Services.
2. Right-click the **eCertificate Services Server** service, then from the pop-up menu click **Restart**.

3.9.2 Certificate extension OIDs

You must configure the following certificate extensions:

Object Identifier (OID)	Label	Encoding	Comment
2.16.840.1.101.3.6.9.1	NACI	DERBOOLEAN	PIV only
1.3.6.1.4.1.311.25.2	UserSid	RAW	PIV and Enterprise

3.9.3 Additional attribute settings

The following table shows the configuration required to support the additional attributes and custom extensions:

Certificate Profile	End Entity Profile	MyID certificate policy attributes
Allow subject DN override by CSR: Enabled LDAP DN Order and Custom Subject DN Order settings are ignored.	Subject DN Attributes are used only as the subject DN of the End Entity and not used in the issued certificate.	No need to configure subject DN attributes in MyID. The subject DN is written to the certificate as supplied in the PKCS#10.
Allow subject DN override by CSR: Disabled Custom Subject DN Order: Disabled LDAP DN Order is used to control the subject DN components order.	Subject DN Attributes are used for both the subject DN of the End Entity and in the issued certificate.	Configure certificate policy attributes as described in section 3.8.1, Enabling certificates policies on a CA . The policy attribute Reverse DN has no effect. The subject DN order is controlled through the EJBCA certificate profile setting
Allow subject DN override by CSR: Disabled Custom Subject DN Order: Enabled The Apply LDAP DN order sub-option is used to control the subject DN order. LDAP DN Order setting is ignored.	Subject DN Attributes are used for both the subject DN of the End Entity and in the issued certificate.	Configure certificate policy attributes as described in section 3.8.1, Enabling certificates policies on a CA . The policy attribute Reverse DN has no effect. The subject DN order is controlled through the EJBCA certificate profile setting

Certificate Profile	End Entity Profile	MyID certificate policy attributes								
<p>Allow Extension override: Enabled</p> <p>and</p> <p>Subject Alternative Name: Enabled</p> <table><tr><th>X.509v3 extensions</th><th>Names</th></tr><tr><td>Subject Alternative Name</td><td><input checked="" type="checkbox"/> Use...</td></tr></table>	X.509v3 extensions	Names	Subject Alternative Name	<input checked="" type="checkbox"/> Use...	<p>The required attributes are required to be configured in Subject Alternative Name.</p>	<p>Configure certificate policy attributes as described in section 3.8.1, Enabling certificates policies on a CA.</p>				
X.509v3 extensions	Names									
Subject Alternative Name	<input checked="" type="checkbox"/> Use...									
<p>Allow Extension override: Enabled</p> <p>and</p> <p>Subject Directory Attributes: Enabled</p> <table><tr><th>X.509v3 extensions</th><th>Names</th></tr><tr><td>Subject Alternative Name</td><td><input checked="" type="checkbox"/> Use...</td></tr><tr><td>Issuer Alternative Name [?]</td><td><input checked="" type="checkbox"/> Use...</td></tr><tr><td>Subject Directory Attributes</td><td><input checked="" type="checkbox"/> Use</td></tr></table>	X.509v3 extensions	Names	Subject Alternative Name	<input checked="" type="checkbox"/> Use...	Issuer Alternative Name [?]	<input checked="" type="checkbox"/> Use...	Subject Directory Attributes	<input checked="" type="checkbox"/> Use	<p>The required attributes are required to be configured in Subject Directory Attributes.</p>	<p>Configure certificate policy attributes as described in section 3.8.1, Enabling certificates policies on a CA.</p>
X.509v3 extensions	Names									
Subject Alternative Name	<input checked="" type="checkbox"/> Use...									
Issuer Alternative Name [?]	<input checked="" type="checkbox"/> Use...									
Subject Directory Attributes	<input checked="" type="checkbox"/> Use									
<p>Allow Extension override: Enabled</p> <p>and</p> <p>The required custom extensions are selected in Used Custom Certificate Extensions.</p> <table><tr><td>Card Number Extension [?]</td><td><input type="checkbox"/> Use</td></tr><tr><td>Used Custom Certificate Extensions</td><td><div>EmployeeID</div><div>myExtension</div></td></tr></table>	Card Number Extension [?]	<input type="checkbox"/> Use	Used Custom Certificate Extensions	<div>EmployeeID</div> <div>myExtension</div>	<p>Enable Custom certificate extension data.</p> <p>Note: MyID cannot validate that this setting has been enabled.</p> <p>The required custom extensions are required to be configured in System Configuration as described in section 3.9, Configuring custom certificate extensions.</p>	<p>Configure the required extensions in <code>EjbcaPKIConnector.xml</code> as described in section 3.9.1, Setting up the custom extensions in MyID.</p> <p>Configure certificate policy attributes as described in section 3.8.1, Enabling certificates policies on a CA.</p> <p>The custom extensions defined in the external file are added to all PrimeKey PKI certificate policies. Only those extensions required by the policy should be configured within MyID. Configuring more custom attributes than required may result in a certificate request being rejected due to configuration mismatch.</p>				
Card Number Extension [?]	<input type="checkbox"/> Use									
Used Custom Certificate Extensions	<div>EmployeeID</div> <div>myExtension</div>									

3.10 Attribute mapping for PIV systems

For PIV systems, you must set up the attributes of the PIV certificate policies to have specific **Dynamic** mappings; see section [3.8.3, Configuring attributes](#) for details.

EJBCA allows the certificate's subject DN attributes to be extracted from the PKCS#10 or passed into the certificate request as end entity data. When using the subject DN from the end entity data, the subject DN in the end entity configuration *must* be configured to include all the required subject attributes, and the certificate profile *must* be configured to take the subject DN extensions from the end entity information, as described in section 3.9.3, [Additional attribute settings](#).

The following tables provide an example configuration for PIV cards.

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

3.10.1 Common Name

The common name is either obtained from the PKCS#10 passed in the certificate request, or through providing dynamic mapping in the subject DN attributes setting in the end entity profile; see section 3.8.3, [Configuring attributes](#) and section 3.9.3, [Additional attribute settings](#).

3.10.2 Publishing policies

Policy publishing is controlled through the Certificate Profile configuration for the certificate policy. See section 3.5, [Configuring certificate profiles](#).

3.10.3 Attribute tables

The following tables show the recommended options for attribute mapping.

ManagedPKI PIV Account Signer	
Attribute	Value
Common Name	Common Name
Publish policy	No

ManagedPKI PIV Authentication	
Attribute	Value
Common Name	Common Name
FASC-N	FASC-N (Hex)
User Principal Name	User Principal Name
Uniform Resource ID	UUID (ASCII)
NACI	NACI Status
Publish policy	No

ManagedPKI PIV Card	
Attribute	Value
DN Serial Number	FASC-N (ASCII)
FASC-N	FASC-N (Hex)

ManagedPKI PIV Card	
Uniform Resource ID	UUID (ASCII)
NACI	NACI Status
Publish policy	No

ManagedPKI PIV End User Encryption	
Attribute	Value
Common Name	Common Name
RFC 822 Email	Email (optional)
Publish policy	Yes

ManagedPKI PIV End User Signing	
Attribute	Value
Common Name	Common Name
RFC 822 Email	Email (optional)
Publish policy	Yes

3.10.4 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.

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
User Principal Name	User Principal Name
Uniform Resource ID	UUID (ASCII)
NACI	NACI Status
Publish policy	No

Note: Certificate publication is controlled through the corresponding certificate profile configuration on the EJBCA; see section [3.10.2, Publishing policies](#). This configuration is not visible in MyID.

ManagedPKI PIV Card	
Attribute	Value
DN Serial Number	FASC-N (ASCII)
FASC-N	Not required
Uniform Resource ID	UUID (ASCII)
NACI	NACI Status
Publish policy	No

4 Troubleshooting

If you are experiencing problems when using PrimeKey EJBCA with MyID, you can use the logging systems to provide further information.

You can also display the details of certificates and troubleshoot certificate policies.

See:

- section 4.1, [Logging](#).
- section 4.2, [Displaying certificates in RA Web](#).
- section 4.3, [Troubleshooting certificate policies](#).

4.1 Logging

MyID supports both EJBCA audit logging and EJBCA connector logging.

4.1.1 EJBCA audit logging

You can enable EJBCA audit logging when deploying the EJBCA, and can modify it through the server command line interface.

See your EJBCA installation and administration guides for details.

When logging is enabled, the audit logs can be viewed by an administrator using the View Log command through a web browser. You can apply a filter to reduce the number of log entries as shown:

Current conditions			
Column	Condition	Value	
Event	Not equals	Access Control	
Certificate Authority	Equals	TestCA	
Certificate Authority ▼	+ Add...		

[✖ Clear all conditions](#) ☒ Automatic reload when conditions change

[Download shown results](#)
[Download shown results as CMS](#)
CMS signing CA : RootCA ▼

[First](#)
[Previous](#)
[Next](#)
[Reload](#)
Displaying results 161 to 200. Entries per page : 40

Search results				
Time ▼ ▲	Event ▼ ▲	Outcome ▼ ▲	Administrator ▼ ▲	Module ▼
2018-03-20 10:16:11-0400	Certificate Request	Success	CN=SuperAdmin	Certificate
2018-03-20 10:16:11-0400	Public Web User Authentication	Success	CN=SuperAdmin	CA
2018-03-20 10:16:11-0400	End Entity Edit	Success	CN=SuperAdmin	Registration Au
2018-03-20 10:14:06-0400	End Entity Edit	Failure	CN=SuperAdmin	Registration Au
2018-03-20 10:12:49-0400	Certificate Create	Success	CN=SuperAdmin	Certificate

Hover over or click the required **Details** column entry to view detailed information. To download results, select the **Download shown results** option.

4.1.2 EJBCA connector logging

The MyID EJBCA connector supports logging. For information on how to enable this logging, contact customer support quoting reference SUP-286.

4.3 Troubleshooting certificate policies

If you are experiencing problems with certificate policies, check the following.

- A Key Management policy is not detected as a key management policy within MyID.

This may present as an error similar to the following:

```
BOL COM catch handler Function : ConfirmAPDUCommand, catch handler.
Error : Unspecified error An error occurred inside
PivCardServer::ConfirmCommand Card error when processing
'ChallengeResponse': 0x6e00 Invalid class -----
Exception raised in function: ConfirmTranslator::checkCommandSucceeded
In file ConfirmSequenceTranslator.cpp at line 91
```

Check that the End Entity profile on the EJBCA server has been configured correctly; see section 3.7, [Key escrow policy configuration overview](#).

- External extension attributes, such as NACI, are not available for a policy when it was expected that the extension should be available.
 - An external extension is added only when the certificate policy on the EJBCA server indicates that it supports external extensions. Check that the certificate profile on the EJBCA server has been configured correctly; see section 3.9.1, [Setting up the custom extensions in MyID](#).
 - Issuance fails with an error that the End Entity profile requirement has not been met. This type of error is indicated by the CA returning a `ValidationException` followed by text indicating the reason for the exception. Typically this would be error conditions such as:
 - All the mandatory attributes have not been supplied.
 - There is a mismatch between the expected and supplied value for an attribute.
 - An attribute verification failure, when a verification pattern has been configured against the attribute.
 - A required feature has not been enabled in the End Entity Profile.
 - Internal EJBCA server error.

This type of error may be indicated by an `IllegalStateException`. The error text may provide useful information in relation to where in the system the error occurred. The error will typically require support from EJBCA administrators to identify and resolve the issue.
 - To resolve these problems, check the corresponding error message in the audit as it generally gives information for the reason for the check failure. Check how the attributes are configured in the End Entity profile and make note of any default non-modifiable values that may have been specified. The value provided for any non-modifiable attribute must match the default value.