Certificate Autoenrollment in Windows Server 2016

Sysadmins LV

Author: Vadims Podans

Inspired by: “Certificate Autoenrollment in Windows Server 2003” whitepaper published by David B. Cross

Published: August 8, 2018

Last updated: August 8, 2018

Abstract

Provides a technical reference and planning guide for PKI administrators who wish to utilize automatic certificate deployment on Windows-based clients and servers.

This article is intended for IT managers and system administrators. It provides a technical walkthrough of the certificate autoenrollment feature, along with an in-depth explanation of how this feature works and key troubleshooting information.

Applies to

This whitepaper is written against Windows 10 and Windows Server 2016 Windows Operating Systems. The following operating systems are applicable too if not specified otherwise:

- Windows 7
- Windows Server 2008 R2
- Windows 8
- Windows Server 2012
- Windows 8.1
- Windows Server 2012 R2

Revision summary

Date	Revision version	Revision class	Comments
August 8, 2018	1.0	Major	Initial release

Feedback

Feedback for this document is accepted via contact form at: https://www.sysadmins.lv/contact.aspx

Contents

Certificate Autoenrollment in Windows Server 2016

About this guide

This document provides an in-depth description of certificate autoenrollment feature integrated in Windows 10 and Windows Server 2016 operating systems.

Target audience

- Administrators or IT operations engineers responsible for implementing and managing certificate services and certificate clients.
- Administrators or IT operations engineers responsible for the day-to-day management and troubleshooting of networks, servers, client computers, operating systems, or applications.
- IT operations managers accountable for network and server management.
- IT architects responsible for computer management and security throughout an organization.

Glossary

The following terms and abbreviations are used in this document:

- **CA certificates**: CA certificates are certificates that are issued by one CA to another CA. These CA certificates become a part of the certificate trust hierarchy, the certificate path from end entity certificates to the trusted root CA certificate.
- **CEP**: Certificate enrollment policy as defined in [MS-XCEP] (https://msdn.microsoft.com/en-us/library/dd302869.aspx).
- **certificate enrollment**: Certificate enrollment is the process of acquiring a digital certificate from a certification authority. This certificate and its associated private key establish a trusted identity for an entity using the public key-based services and applications.
- **LDAP**: In this document the term LDAP always refers to the Lightweight Directory Access Protocol (LDAP) profile specified in [MS-ADTS] section 3.1.1.3 (https://msdn.microsoft.com/en-us/library/cc223225.aspx).
- **policy server end point**: A collection of information about a policy server, such as the protocol it supports, its Uniform Resource Identifier (URI), and authentication to be used when accessing the server.
- **MAY**, **SHOULD**, **MUST**, **SHOULD NOT**, **MUST NOT**: These terms (in all caps) are used as described in [RFC2119] (https://tools.ietf.org/html/rfc2119). Note that in [RFC2119] terms, most of these specifications should be imperative, to ensure interoperability. All statements of optional behavior use either **MAY**, **SHOULD**, or **SHOULD NOT**.

Any specification that does not explicitly use one of these terms is mandatory, exactly as if it used MUST.

Certificate Autoenrollment Overview

Many systems and protocols they implement require digital certificates to operate. Those systems usually do not specify how their certificates are obtained. As long as a valid certificate for enrollment is available the server will use that certificate. Certificates have a certain lifetime and will eventually face expiration. Obtaining or renewing certificates is a burden on the server administrator. Computer certificate autoenrollment takes this burden away from the server administrator by automating certificate enrollment and renewal for server certificates.

Certificate autoenrollment was first introduced in Windows 2000 and greatly enhanced over the time by adding new features and usage scenarios. Windows 10 and Windows Server 2016 support the capability to automatically enroll users and computers for certificates including TPM and smart card-based certificates.

Using the autoenrollment feature, organizations can manage the certificate lifecycle for users and computers, which includes but not limited to:

- Certificate enrollment and automatic renewal
- Pending request retrieval
- Local certificate store management
- Superseding of certificates
- Multiple signature requirements

Certificate autoenrollment is based on the combination of Group Policy settings and version 2 (or higher) certificate templates. This combination allows the Windows client to enroll users when they log on to their domain, or a machine when it boots, and keeps them periodically updated between these events.

Automatic enrollment of user certificates provides a quick and simple way to issue certificates to users and to enable public key infrastructure (PKI) applications, such as smart card logon, Encrypting File System (EFS), Secure Sockets Layer (SSL), Secure/Multipurpose Internet Mail Extension (S/MIME), and others. User autoenrollment minimizes the high cost of normal PKI deployments and reduces the total cost of ownership (TCO) for a PKI implementation when Windows clients are configured to use Active Directory.

Certificate autoenrollment evolution

The following table outlines the most important features added to autoenrollment feature over the time. This table will help administrators to identify notable features supported by particular operating system family.

Operating system	Key Features
Windows 2000 Professional Windows 2000 Server	• Automatic Certificate Request (ACR) introduced. ACR supports only unmanaged (version 1) computer certificate templates. No user certificate templates supported
Windows XP Professional Windows Server 2003	• Managed certificate template (version 2) support • Computer and user certificate autoenrollment based on version 2 templates
Windows Vista Business Windows Server 2008	• Brand new Cryptography Next Generation (CNG) cryptographic stack and rich CertEnroll application programming interfaces • Version 3 certificate templates that support CNG cryptography • Private key access control list (ACL) management with certificate template and autoenrollment • Autoenrollment timing changed from GPO update to system tasks in Task Scheduler

Operating system	Key Features
Windows 7 Professional Windows Server 2008 R2	• Active Directory Certificate Services Web Services (ADCS-WS) and WSTEP enrollment stack introduced • Workgroup environment support for certificate enrollment and autoenrollment • Cross-forest certificate enrollment support • Short-lived certificate support without writing them to CA database
Windows 8 Pro Windows Server 2012	• Version 4 certificate templates with key-based renewal • Renewal with same key (key pair reuse) • Desired issuance policies can be provided in the request • Additional certificate stores can be updated by autoenrollment • Automatic certificate renewal by including subject in the request from renewal certificate. Allows to automatically renew certificate when certificate template requires subject information in the request
Windows 8.1 Pro Windows Server 2012 R2	• Version 4 certificate templates with key attestation and TPM support • Automatic SSL certificate re-bind in IIS when certificate automatically renewed using autoenrollment
Windows 10 Pro Windows Server 2016	• Certificate transparency (CT) support

Dependencies

The autoenrollment feature has several infrastructure requirements. These include:

- Windows Server 2008 R2 (or higher) Active Directory schema and Group Policy updates;
- Windows Server 2008 R2 (or higher) domain controllers;
- Windows 7 (or newer) or Windows Server 2008 R2 (or newer) clients;
- Windows Server 2008 R2 (or higher) running as an Enterprise CA.

Additional requirements are applied to support autoenrollment feature on clients that are not joined to Active Directory domain:

- Windows Server 2008 R2 (or higher) or [MS-XCEP] compatible server running as Certificate Enrollment Policy service;
- Windows Server 2008 R2 (or higher) or [MS-WSTEP] compatible server running as Certificate Enrollment Server service.

The Certificate Enrollment Architecture

In order to understand automatic certificate enrollment, it is required to understand certificate enrollment in general as described in this section. At the very abstract level and as illustrated in the following diagram, the administrator enters a policy as a machine-readable certificate enrollment policy (CEP) stored in a policy server.

The CEP is made available from the policy server to certificate enrollment clients, which consume this CEP to determine which certificates the client is supposed to have and which issuers are available to provide those certificates. Clients then create certificate requests and submit them to issuers that issue certificates back to the clients.

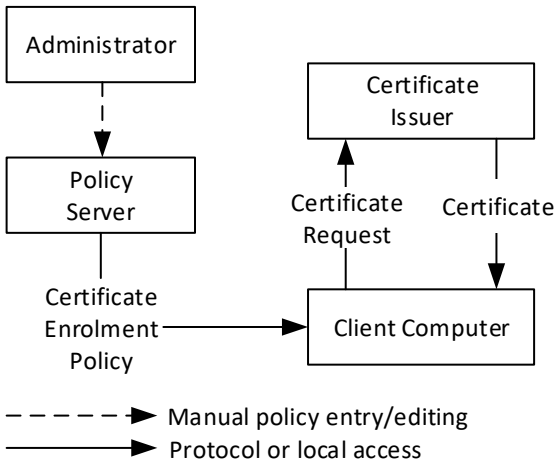

Figure 1: Certificate enrollment architecture

Microsoft Windows 10 and Windows Server 2016 support two enrollment protocol stacks.

The first stack, named *WCCE*, was originally introduced in Windows 2000 and uses Windows Client Certificate Enrollment Protocol [MS-WCCE] for certificate requests. It uses the LDAP to obtain a CEP from a domain controller (DC). Finally, the CEP is expressed via certificate template structures specified in [MS-CRTD] and certification authority (CA) information. This stack is supported by all Windows operating systems starting with Windows 2000 and is supported by all modern Windows operating systems, including Windows 10 and Windows Server 2016. The following figure illustrates the enrollment process using WCCE stack:

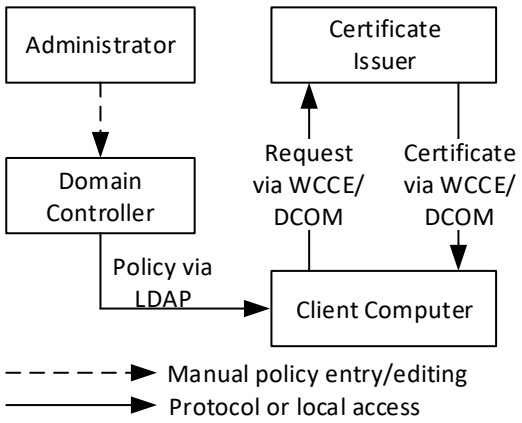

Figure 2: Certificate requests using WCCE enrollment stack

Figure 2 outlines the WCCE enrollment architecture, where domain controller acts as policy server and client uses LDAP to retrieve enrollment policy from domain controller. Client then uses this policy to determine available certificate templates and certification authorities. Certificate enrollment client uses this

information to determine which certificates should be requested and/or renewed. WCCE stack uses RPC/DCOM to communicate with CA server. Although, WCCE stack is pretty simple and requires minimum administrative efforts, its simplicity leads to a number of major limitations:

- The computer can be a member of only single Active Directory domain at a time, thus only single WCCE enrollment policy can be configured on a client;
- The certificate issuer (CA server) must be accessible to client via RPC/DCOM protocol;
- WCCE stack is not available on workgroup computers.

With Windows 7 and Windows Server 2008 R2, a new certificate enrollment stack called *XCEP* was introduced. This stack does not necessary use Active Directory to retrieve CEPs and certificate templates and do not communicate with Certificate Issuer by using RPC/DCOM transport protocol. Instead, Windows client communicates with CEPs and Certificate Issuer by using [MS-XCEP] and [MS-WSTEP] protocols respectively. These protocols use HTTP/SOAP underlying transport:

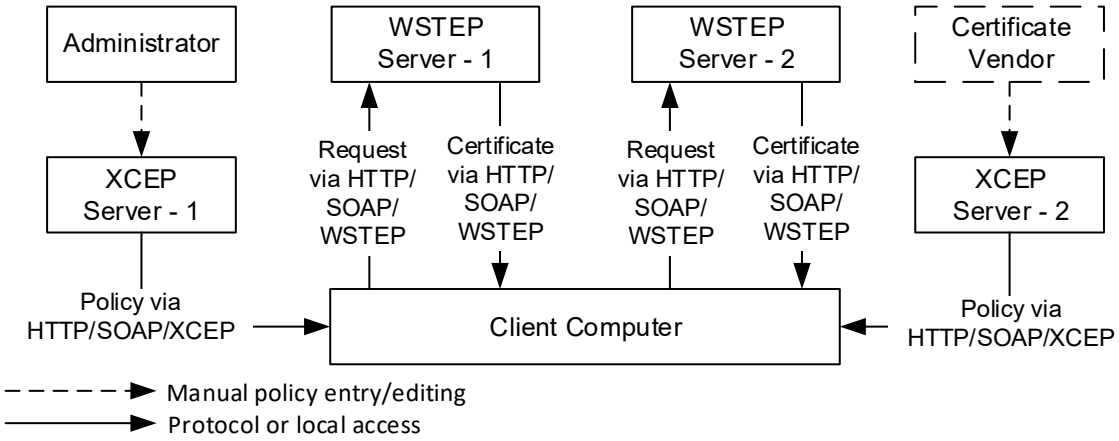

Figure 3: Certificate requests using XCEP certificate enrollment stack

Figure 3 outlines the XCEP enrollment architecture, where XCEP server acts as policy server and client uses HTTP/SOAP to retrieve enrollment policy from policy server by using [MS-XCEP] protocol. Client then uses this policy information to determine available certificate templates and certificate issuer endpoints. XCEP stack uses HTTP/SOAP to communicate with certificate issuers by using [MS-WSTEP] protocol.

> Microsoft implements XCEP component in ADCS Certificate Enrollment Policy Service (CEP) and WSTEP in ADCS Certificate Enrollment Service (CES) server roles. More details on ADCS Web Services: Certificate Enrollment Web Services in Active Directory Certificate Services

As it is shown, there are no dependencies on Active Directory environment, thus XCEP enrollment stack leverages limitations of WCCE stack and allows the use of autoenrollment feature for workgroup computers (which are not parts of Active Directory domain). In addition, client computer can be configured with multiple enrollment policies, thus allowing to receive certificates from different certificate providers (WSTEP Server).

Computers starting with Windows 7 and Windows Server 2008 R2 can use both protocol stacks to enroll for certificates based on the same company policy. This process is shown in Figure 4:

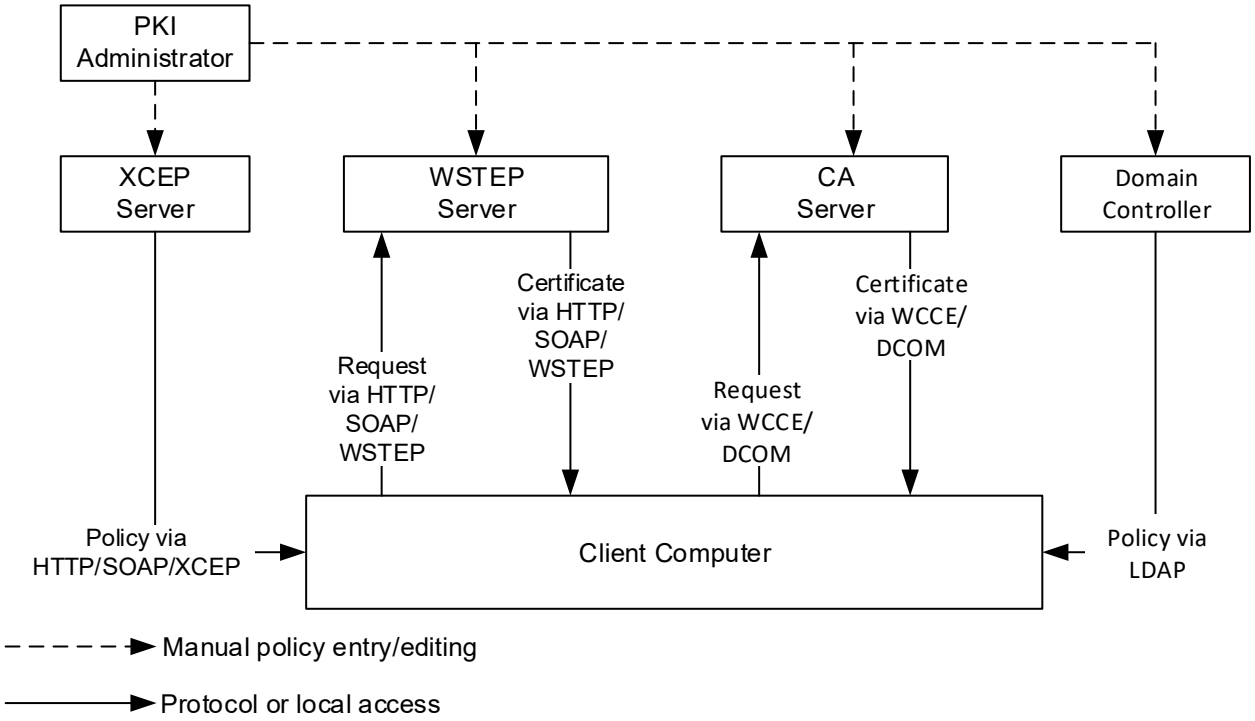

Figure 4: Certificate enrollment requests using WCCE and XCEP certificate enrollment stacks

A client computer starts by discovering a policy server. With WCCE enrollment stack, the policy server is always a domain controller. For the use of ADCS Web Services (ADCS-WS), the web service address has to be configured out of band (for example, manually or by Group Policy).

Certificate enrollment clients can use Group Policy to obtain policy server endpoints that were configured by the administrator in the enterprise. Clients can also use a local configuration store that contains policy server end points specific to a particular client. The following figure illustrates this concept.

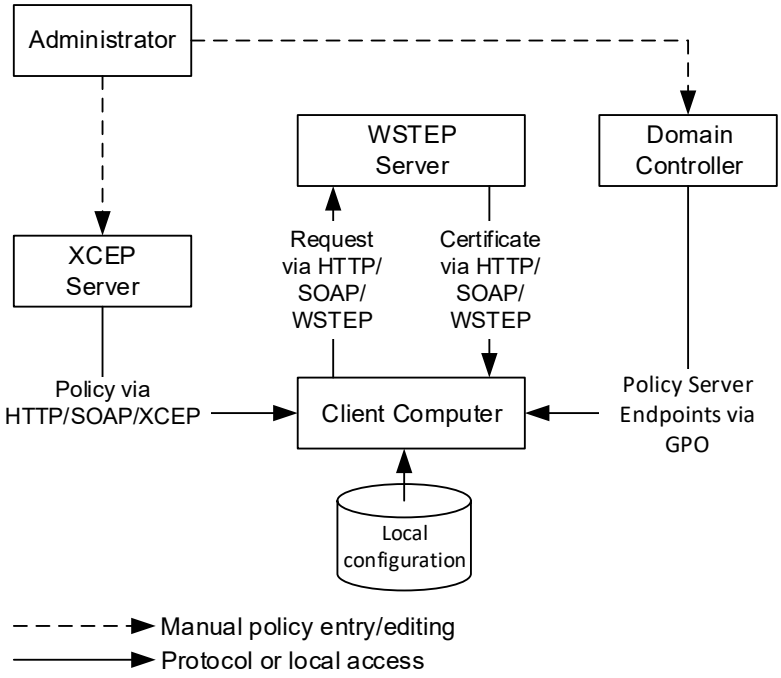

Figure 5: Certificate enrollment using Group Policy

Figure 5 shows the enrollment process in Active Directory domain with use of XCEP stack. XCEP server endpoints are configured by an administrator on domain controller through Group Policy. Client computer retrieves enrollment policies and XCEP server endpoints from domain controller.

Non-domain computers cannot use domain controllers to retrieve enrollment policies and XCEP server endpoints. Instead, they must be configured on client computer manually:

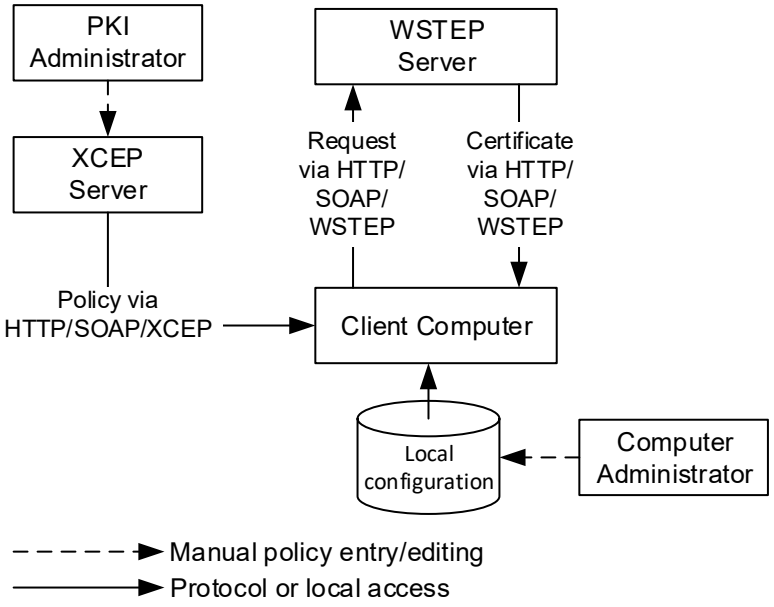

Figure 6: Certificate enrollment using local configuration

Computer administrator manually configures local configuration with enrollment policy and XCEP server endpoints. This can be done by using various ways, including local Group Policy, Certificates MMC snap-in, `certutil.exe` tool. The following diagram shows an example of one possible deployment:

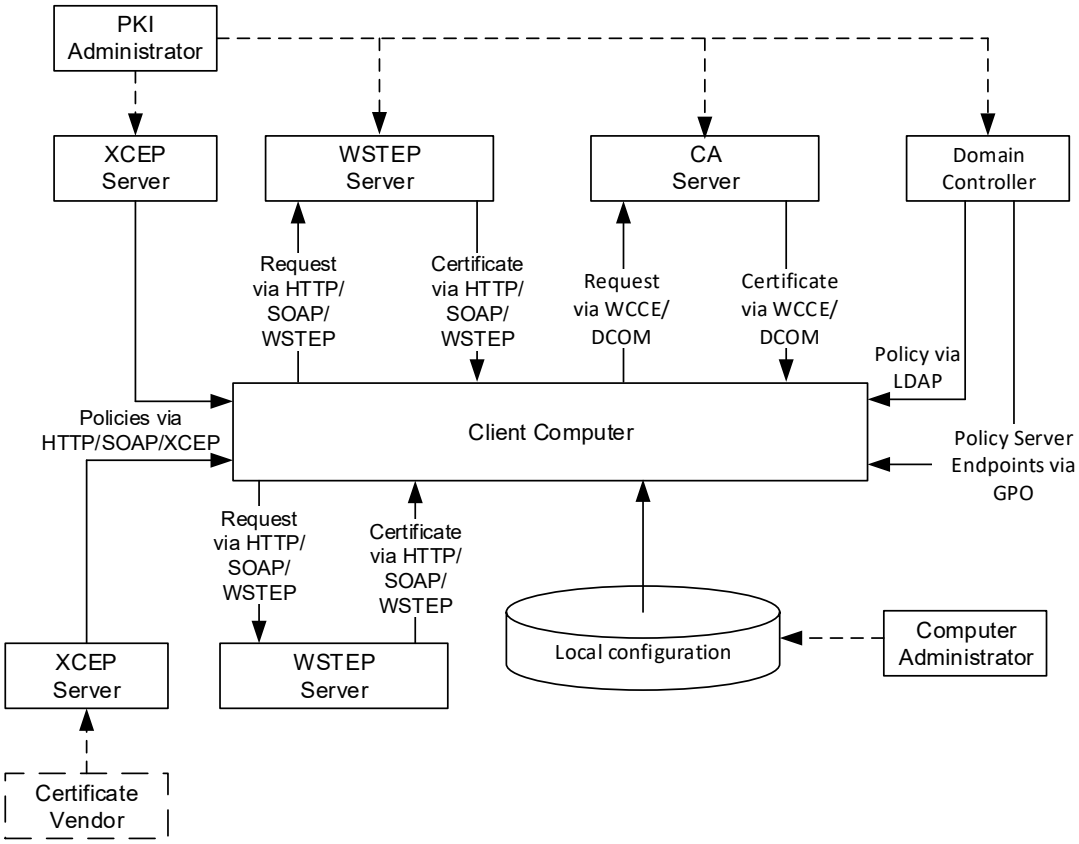

Figure 7: Domain member client requesting certificate enrollment through a Group Policy deployment

XCEP server endpoints are normally obtained by client through Group Policy. Computer administrator may provide client-specific endpoints manually. Autoenrollment feature will use all endpoints available in the local configuration. XCEP endpoint configuration is outside the scope of this whitepaper.

Considering that any client can be configured to work with multiple CEPs where each CEP may have multiple policy server end points, can define multiple certificate templates, and are used by multiple issuers, it is clear that enrolling for certificates manually can be a difficult task. The job of autoenrollment is to traverse all of the CEPs and enroll for certificates as needed.

Certificate Autoenrollment Architecture

This section discusses the autoenrollment architecture, an analysis of the components of the autoenrollment process, and working with certificate authority interfaces.

Autoenrollment internal components

Autoenrollment consist of several components installed on each computer. Depending on environment (Active Directory or workgroup) some components may present or not present. The following diagram outlines autoenrollment components and their high-level interactions in both environments:

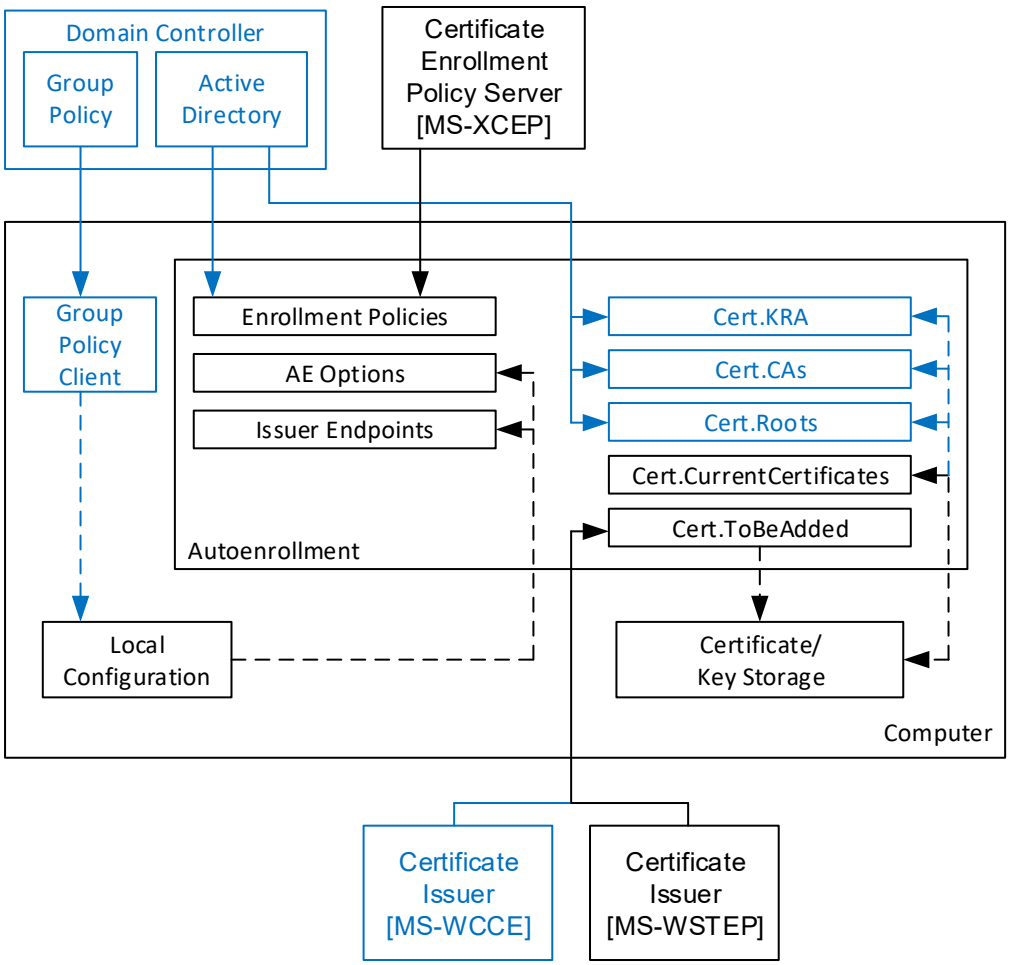

Figure 8: Autoenrollment component diagram. Blue color shows components available only in Active Directory environment

The meaning of each component is provided in next sections.

Group Policy client

> This component is not available in workgroup environments.

Client module that is responsible for Group Policy retrieval and processing from domain controller, policy storage and policy maintenance on a local computer. Group Policy client updates local configuration with certificate enrollment policy (CEP) information.

Local configuration

System Registry storage that contains information about certificate enrollment policies (CEP). This information is then used to populate configuration for: **Enrollment Policies**, **AE Options** and **Certificate Issuers** components. Local configuration is stored in System Registry in HKLM and HKCU registry hives:

```
SOFTWARE\Policies\Microsoft\Cryptography\AutoEnrollment\
```

Enrollment Policies

Contains a collection of CEPs. In Active Directory environment, a LDAP domain policy is added by default. XCEP policies must be configured by an administrator in Group Policy on domain controllers (available only in Active Directory) and/or using local configuration tools. Each policy contains the following notable properties:

- **Enrollment stack**. Can be either, WCCE or XCEP;
- **URI**. An URI to a policy server. If URI begins with LDAP:// prefix, **Enrollment Stack** is set to WCCE and CEP server is set to domain controller. If URI begins with HTTPS:// prefix, **Enrollment Stack** is set to XCEP and URI points to XCEP server.
- **PolicyId**. Allows the grouping of policy server end points that serve the same CEP together. It is also used to record which CEP contained a certificate template on which a particular certificate was based;
- **Authentication method**. Kerberos authentication is available only in Active Directory environment;
- **IsDefault**. Boolean flag used to identify default CEP. A default CEP is used to renew certificates for which the original PolicyId is unknown;
- **Cost**. Is used during CEP sorting;
- **Templates**. A list of certificate templates available to client for enrollment.

AE Options

Specifies options that control autoenrollment behavior. These options contain the following flags:

- **Enabled** — specifies the status of the autoenrollment feature. The value 1 enables autoenrollment feature, value 0 disables autoenrollment feature;
- **Enroll** — enroll and renew certificates based on certificate templates that have been set up for autoenrollment;
- **Manage** — renew certificates when the certificate templates are not set up for autoenrollment;
- **RetrievePending** — retrieve pending requests.

Certificate template is set up for autoenrollment when its settings are compatible with silent initial enrollment and renewal operations. Certificate is not set up for autoenrollment when its settings are not compatible with initial certificate enrollment, but allow silent certificate renewal operation.

Enroll setting is controlled by a “Update certificates that use certificate templates” checkbox in autoenrollment configuration dialog in GPO (see Configuring autoenrollment policy section below)

Manage and **RetrievePending** settings are controlled by a “Renew expired certificates, update pending certificates, and remove revoked certificates” checkbox in autoenrollment configuration dialog in GPO (see Configuring autoenrollment policy section below).

Local Certificate Storage

Autoenrollment requires the computer on which it is executing to provide some implementation-specific persisted local certificate storage that can be logically organized into groups of certificates.

Local Private Key Storage

Autoenrollment requires that the computer on which it is executing provide some implementation-specific persisted local private key storage where it could store private keys associated with the certificates it is requesting.

Certificates

Cert.ToBeAdded: a list of certificates to be added to the local certificate storage after renewing existing and enrolling new certificates.

Cert.ToBeDeleted: a list of certificates to be deleted when existing certificate gets successfully renewed.

Cert.CurrentCertificates: a list of the current end entity certificates.

Cert.Roots: a list of certificates that holds certificates from the **Trusted Root CAs** store.

Cert.CAs: a list of certificates that holds certificates from the **Intermediate CAs** store.

Cert.KRA: a list of certificates that holds CA certificates which are allowed to perform client private key archival in CA database. KRA feature is used only when certificate template requires private key archival in CA database. Private key material is transferred to CA in a secure way. Transfer security is accomplished by encrypting the key with CA Exchange certificate provided by a CA server. More details on key archival: Active Directory Certificate Services Longhorn Beta3 Key Archival and Recovery.

Balloon User Interface

For each request that requires user interaction as per the certificate template, the balloon user interface (UI) is invoked in system tray and is added in the notification center:

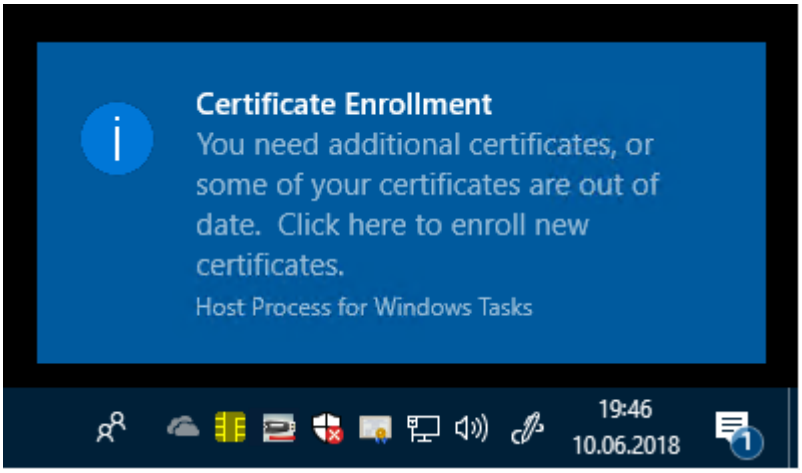

Figure 9: Certificate enrollment balloon user interface that requires user input

Balloon UI notification is displayed approximately 60 seconds after logon. If no user interaction is explicitly defined on the certificate template, no UI will be displayed to the user. This delay is incorporated to allow

for speedy application and shell response times during the logon and booting of the client machine. If the 60-second delay is not desired, the following registry key may be added on a per-user basis:

```
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Cryptography\AutoEnrollment\AEExpress
```

Using this key in a normal production environment is not recommended. If it is used, it must be created on a per-user basis.

> Machine certificates do not support user interaction and must not be configured to require this setting.

The balloon UI waits for the user to see the balloon and is activated by a mouse click. Note that after approximately 15 seconds, the balloon pop-up window is replaced in the system tray by a certificate icon that may be activated by a mouse click. If no activation occurs within seven hours, the taskbar icon will disappear and the silent thread will re-activate at the next logon, machine reboot, or next autoenrollment trigger, whichever is first. Once the user activates the UI, the REQUEST store is checked first for pending requests.

The Autoenrollment Process

This section describes a detailed process performed by autoenrollment each time it is activated.

Autoenrollment timing

The autoenrollment process is normally triggered by a set of built-in scheduled tasks which are stored under `Task Scheduler Library\Microsoft\Windows\CertificateServicesClient` container in Task Scheduler:

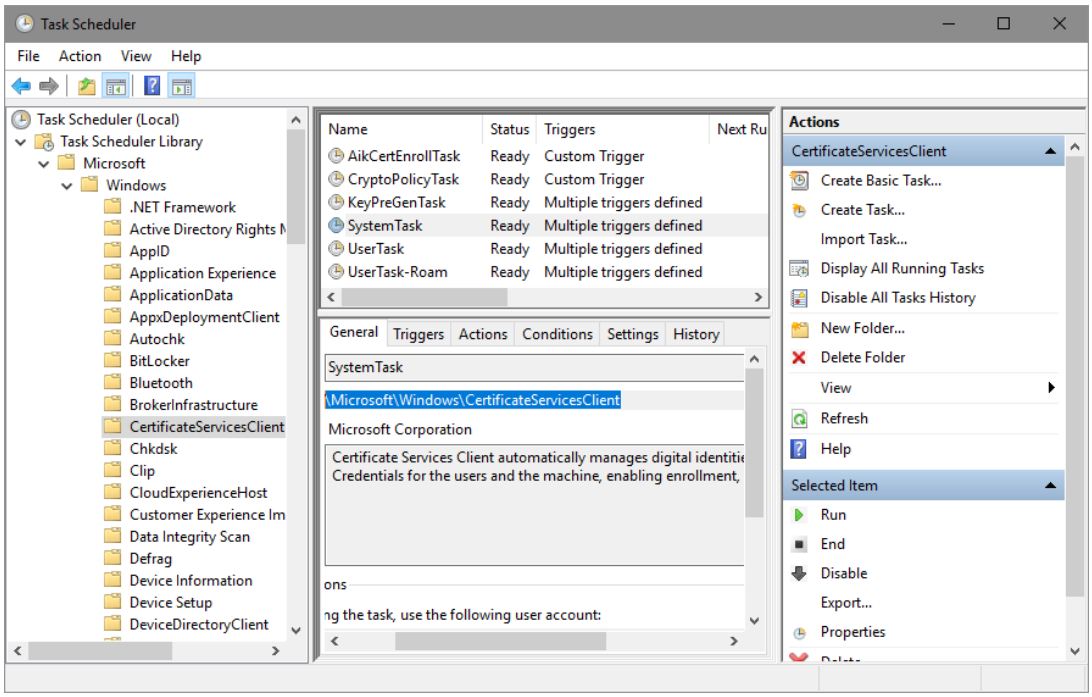

Figure 10: Autoenrollment triggers in Task Scheduler

This container stores several scheduled tasks that can activate autoenrollment for machines and users. By default, autoenrollment is triggered at reboot for machines, or at logon for users, and is refreshed every eight hours. The refresh interval can be configured using Group Policy. Autoenrollment is also triggered by an internal timer that activates every eight hours after the last time autoenrollment was activated.

Autoenrollment trigger for computer and user contexts can be activated manually, by running the following commands:

```
Certutil -pulse
Certuil -user -pulse
```

Unlocking the workstation does not trigger autoenrollment.

Forcing re-enrollment

An administrator may force all users to re-enroll for a given template by updating the major version number of the template. When Active Directory is queried during logon for required certificate templates, the version number is examined. If the version number has incremented, the certificate template is considered to be updated and the user must re-enroll for that template.

To manually force the template version to be updated (thereby forcing re-enrollment): right-click the template and select **Reenroll All Certificate Holders** (Figure 11):

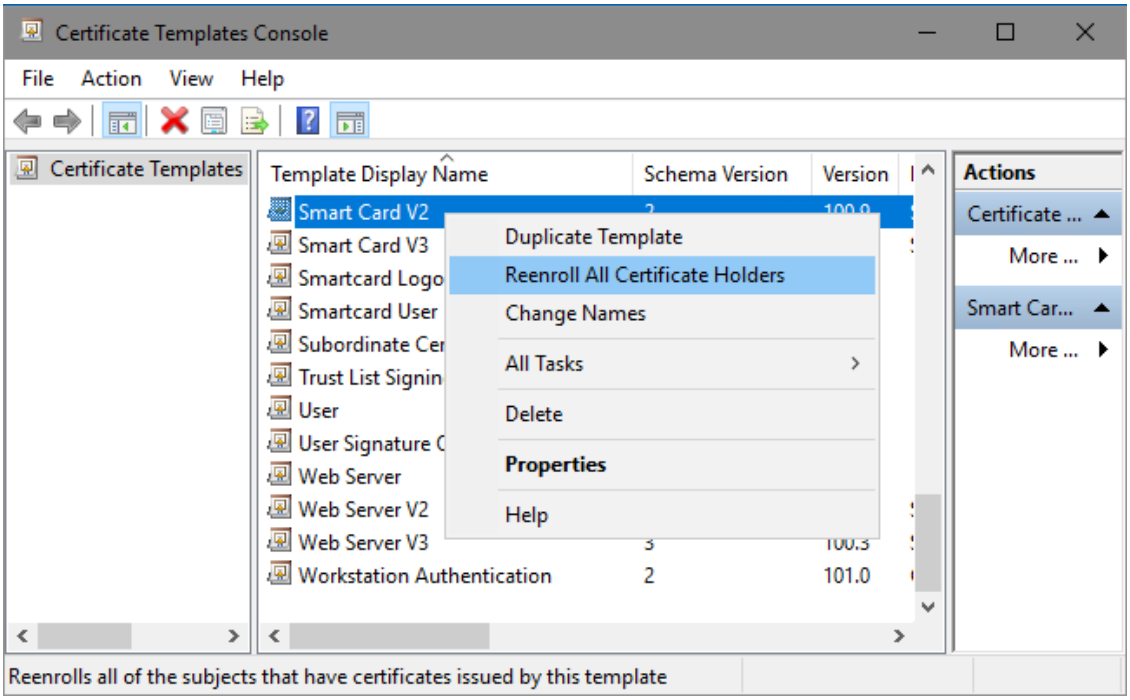

Figure 11: Manually Forcing Certificate Re-Enrollment

This procedure will increase template's **Major Version** attribute. Autoenrollment client will handle this attribute to force existing certificate renewal when **Major Version** is changed. When modifying certificate template, its **Minor Version** is incremented, but it doesn't force client certificate reenrollment.

Templates are not updated automatically. By default, templates are updated at a minimum interval of 10 minutes.

Renewal intervals

Windows clients will perform automatic renewal of certificates as specified on a per-template basis. Renewal intervals are dictated by the certificate template, which is set to six weeks (before expiration) by default. When certificate renewal is performed, the old (previous) certificate enrollment is always archived on the client machine, and the user directory object is updated. Even if "Delete revoked or expired certificates" checkbox is selected in certificate template settings. In this case, previous certificate will be deleted after expiration or revocation. Important certificate renewal criteria include the following:

- Automatic certificate renewal will only occur when 80 percent of the certificate lifetime has passed, or when the renewal interval period specified on the template has been reached whichever timeframe is smaller.
- If the renewal period is greater than 20 percent of the certificate lifetime, autoenrollment will not automatically attempt certificate renewal until the 80 percent threshold has been reached.

Autoenrollment task sequence

This section describes the process and operation sequence during autoenrollment initialization. Depending on autoenrollment configuration not all steps are performed. Each subsection provides conditions when particular task is executed.

Initialize autoenrollment options

In this step, autoenrollment feature examines local configuration storage (which is updated via Group Policy and/or manually by a computer administrator) to determine the process behavior. If autoenrollment state is set to **Disabled**, the process terminates, otherwise it continues with the next step. Autoenrollment initialize **Enroll**, **Manage** and **RetrievePending** flags.

Update certificates and object identifiers from Active Directory

> This step is performed only by domain members. Workgroup members skip this step.

Autoenrollment automatically downloads and manages trusted root certificates, cross-certificates, and NTAuth certificates from Active Directory into the local machine registry for domain-joined machines. All users who log on to the machine inherit the trust and downloaded certificates that are downloaded and managed by autoenrollment. The following stores are located under the following DS path: `CN=Public Key Services, CN=Services, {ConfigurationNamingContext}`:

Local Certificate Storage	Certificates MMC container	Corresponding Active Directory container
Cert.Roots	Trusted Root Certification Authorities	CN=Certification Authorities
Certs.CAs	Intermediate Certification Authorities	CN=AIA
Certs.KRA	N/A	CN=NTAuthCertificates

Additionally, autoenrollment fetches object identifier (OID) registration information and writes it to the local cache. Administrators use Active Directory to register object identifiers for new application policies (enhanced key usages or EKU), certificate policies and certificate templates. OID information is downloaded from the following Active Directory container:

```
CN=OID, CN=Public Key Services, CN=Services, {ConfigurationNamingContext}.
```

Update local stores

During this step, autoenrollment initializes runtime stores: **Cert.CurrentCertificates**, **Cert.ToBeAdded**, **Cert.ToBeDeleted**. **Cert.CurrentCertificates** will include all the certificates from client's **Personal** store and, optionally, from additional stores if such are configured in local configuration. Other runtime stores are initialized to empty lists.

Initialize enrollment policies

During this step, autoenrollment uses local configuration to obtain information about CEP policies. Autoenrollment groups policies by **PolicyId** attribute. Groups are sorted by **Cost** attribute, then by **Authentication** attribute. **Kerberos** authentication has higher precedence. The rest groups are placed in arbitrary order.

After grouping and sorting CEPs, each CEP is queried. During the query, client obtains the following information:

- List of certificate templates available to client and their settings;
- List of certificate issuers supported by this CEP with a list of supported certificate templates by each issuer.

If CEP uses WCCE enrollment stack, then certificate templates and certificate issuers are downloaded from Active Directory, otherwise, this information is downloaded from XCEP server. Upon retrieval, every certificate issuer certificate is validated according to validation rules specified in RFC 5280. Certificate issuers that fail validation are excluded from processing.

After downloading certificate templates and certificate issuers, autoenrollment constructs a list of certificate templates applicable for autoenrollment. At a minimum, certificate template is considered applicable for autoenrollment when client has **Autoenroll** permissions on that template, and template is supported by any of certificate issuers in the current CEP group. Additional restrictions apply and will be covered in "Autoenroll based on certificate templates" section below.

Retrieve pending requests

If autoenrollment options has **RetrivePending** flag enabled, autoenrollment checks **Certificate Enrollment Requests** (REQUEST) local store for non-complete certificate requests. Pending requests are requests that require explicit CA manager approval. When client submits such request, it is placed in CA database and waiting for review and approval. CA manager can approve the request and issue the certificate, or cancel request.

For each pending request, autoenrollment checks the age of the request. If request is in pending state for 60 or more days, pending request is deleted from **Certificate Enrollment Requests** and excluded from further processing.

When stale pending requests are deleted, remaining pending requests are updated. Each pending request contains all relevant information to update request status. Autoenrollment contacts certificate issuer associated with the particular request and updates the request status. There are three possible outcomes:

1. If status is not changed (still pending) or autoenrollment failed to contact certificate issuer, the request entry is skipped;
2. If certificate was issued by certificate issuer, autoenrollment downloads issued certificate, links private key to it and moves completed request to **Personal** certificate store. Request entry is completed and removed from **Certificate Enrollment Requests** store.

   If request is renewal request (not initial) and certificate template requires to delete the renewal certificate, it is deleted from **Personal** store, otherwise, renewal certificate is marked as "archived". Archived certificates are not added in the default certificate store view, but they still can be queried when asked by client application.
3. If CA manager declined the request, or CA failed to issue the certificate, error status is returned. Although the certificate was not issued, request is considered completed and removed from **Certificate Enrollment Requests** store.

When all pending requests are processed, autoenrollment performs existing certificates renewal.

Autoenroll based on certificate templates

If autoenrollment options has enabled **Enroll** flag, autoenrollment will perform a two-step **Personal** certificate store update. First step renews existing certificates (if applicable) and second step enrolls for certificates which don't exist in certificate store, but are required by enrollment policy. These two steps are performed against certificate templates that have been set up for autoenrollment (support silent initial enrollment). Certificate autoenrollment consists of three steps:

1. Certificate renewal against certificate templates that are configured for autoenrollment;
2. New certificate requests against certificate templates that are configured for autoenrollment;
3. Certificate renewal against certificate templates that are not configured for autoenrollment.

Each step is described in the following sections

Automatic certificate renewal

In the first step, autoenrollment enumerates all existing certificates (from Personal and additional stores provided in the configuration) that use certificate templates and checks its validity by passing it to a certificate chaining engine. Certificate is validated according to validation rules as specified in in RFC 5280. If certificate fails validation checks, it cannot be renewed. Instead, a new certificate request is issued as described in next section. If existing certificate passes validation checks, autoenrollment examines whether certificate template is set up for autoenrollment. Certificate template is set up for autoenrollment is none of the following conditions are true:

- Client does not have **Autoenroll** permissions on certificate template;
- Certificate template is available to client, but it is not supported by any available certificate issuer;
- Certificate template requires private key archival in CA database and CA (that supports this template) certificate is not presented in the **Certs.KRA** local store or fails validation check;
- Certificate template requires multiple (2 or more) registration authority (RA) signatures in the **Issuance Requirements** tab. When this condition is true, the certificate is not renewed, instead a new certificate request procedure is initiated as described in the next section;
- Certificate template requires subject name to be supplied with request in the **Subject Name** tab;
- User interaction is required for machine certificate templates in the **Request Handling** tab;
- Certificate template is superseded by another template in the **Superseded Templates** tab.

If any of these conditions are true, existing certificate cannot be renewed, and autoenrollment will skip such certificate. Otherwise, autoenrollment checks passes the certificate to certificate chaining engine (CCE) to determine its validity.

> Autoenrollment will ignore revocation errors if a CRL Distribution Point (CDP) extension does not exist in the CA certificate or if the revocation status is offline.

If certificate is valid according to chain validation rules (as described in RFC 5280) autoenrollment estimated validity of the existing certificate:

- Automatic certificate renewal will only occur when 80 percent of the certificate lifetime has passed, or when the renewal interval period specified on the template has been reached whichever timeframe is smaller;
- If the renewal period is greater than 20 percent of the certificate lifetime, autoenrollment will not automatically attempt certificate renewal until the 80 percent threshold has been reached.

If existing certificate's validity meets renewal threshold, autoenrollment will submit renewal request to CA server.

If certificate lifetime hasn't reached renewal threshold, autoenrollment checks certificate template **Major Version** attribute in existing certificate and certificate template obtained from XCEP server. If **Major Version** of certificate template is higher than **Major Version** in existing certificate, this will instruct autoenrollment to perform existing certificate renewal even if renewal threshold is not yet reached. Major

Version attribute manipulation allows systems administrators to force existing certificate renewal when critical changes were made in certificate template settings.

Submitting a new request

After renewing existing certificates based on templates, autoenrollment examines a list of certificate templates that have been set up for autoenrollment (as described in previous section) and attempts to find a matching certificate in the **Personal** store. New request is not issued against certificate template if any of the following conditions are true:

- Valid and non-expired certificate is found;
- Certificate template is configured to check Active Directory for an existing certificate and valid and non-expired certificate is found in `userCertificate` Active Directory attribute of the current client account;
- RA signature count in certificate template's **Issuance Requirements** tab is set to 2 or greater value;
- RA signature count in certificate template's **Issuance Requirements** tab is set to 1 and no matching certificate to co-sign the request is found in **Personal** certificate store.

If no valid certificate is found, or certificate chaining engine failed to validate existing certificate, a new certificate request is issued.

When new certificate request is created, autoenrollment checks if CA servers provided by a default CEP policy supports specified certificate template. If at least one CA supports specified certificate template, a request will be sent to CA server with lower **Cost** value. If no CAs in the default CEP policy are found, autoenrollment arbitrary enumerates all available CAs that support specified certificate template. If at least one CA is found, a first (arbitrary selected) CA is used to submit certificate request. If no CAs that support specified certificate templates are found, certificate template is skipped.

Renew manually enrolled certificates

Some certificates require manual initial enrollment, but later can be automatically renewed. If autoenrollment options has **Manage** flag enabled, autoenrollment will examine current certificates in **Certs.CurrentCertificates** store to determine if any such certificates exist and attempt to renew them. Manually enrolled certificate renewal if none of the following conditions are true:

- Certificate has not passed 80% of its validity or the renewal interval period specified on the template has not been reached;
- Existing valid and non-expired certificate based on this certificate template is found;
- Certificate template requires private key archival in CA database and CA (that supports this template) certificate is not presented in the **Certs.KRA** local store or fails validation check;
- Certificate issuer endpoint that supports certificate template is configured in "Renewal Only" mode. This configuration is possible only when using **WSTEP** enrollment stack;
- Certificate template requires subject name to be supplied in the request subject information from existing certificate retrieval is not allowed in the **Subject Name** tab;
- User interaction is required for machine certificate templates in the **Request Handling** tab;
- Certificate templates requires multiple RA (2 or more) signatures in the **Issuance Requirements** tab and no suitable RA signing certificate is found in **Personal** store.

> Clients prior to Windows 8 and Windows Server 2012 do not support the use of existing name in the renewal certificate and autoenrollment against the template that requires the subject to be supplied in the request will fail.

If neither of these blocking conditions met, autoenrollment submits certificate request. If initial enrollment results in an issued certificate, it is installed in the **Personal** store. If request results in a pending state,

client keeps request information in the **Certificate Enrollment Requests** store and will check its status upon next autoenrollment trigger.

Certificate store cleanup

This section describes the certificate store cleanup process after each successful certificate renewal or new certificate enrollment.

If certificate renewal for existing certificate occurred and resulted in an issued certificate, autoenrollment performs existing certificate cleanup in local storage. Cleanup will either, mark existing certificate as "archived" or delete it. Cleanup action is configured in the certificate template's **Request Handling** tab. The following image illustrates cleanup setting:

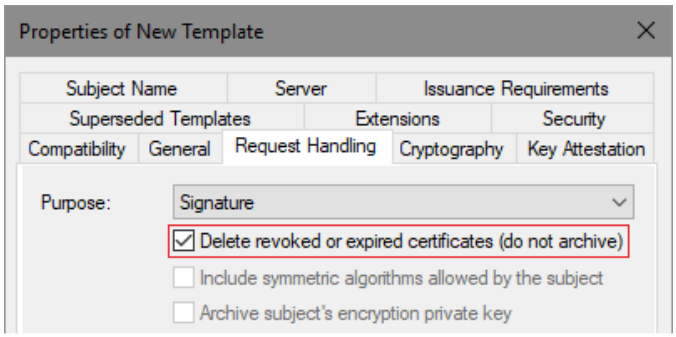

Figure 12: Certificate cleanup setting in certificate template

If autoenrollment options has **Manage** flag enabled, autoenrollment deletes revoked certificates in the `userCertificate` attribute on the client object in Active Directory. Expired or superseded certificates are not deleted automatically from Active Directory, they must be deleted manually.

If certificate purpose is **Encryption**, existing certificate is always marked as "archived" and cannot be deleted by autoenrollment.

Configuring Autoenrollment

Autoenrollment configuration in general consist of three steps: configure autoenrollment policy, prepare certificate templates and prepare certificate issuers. Each configuration step is described in next sections.

Configuring autoenrollment policy

The recommended way to configure autoenrollment policy is to use Group Policy feature. Group policy feature is available in both, domain and workgroups environments. This section provides information about autoenrollment configuration using Group Policy editor. It is recommended to turn on autoenrollment policy in both, user and computer configuration.

1. Start **Group Policy** editor. In Active Directory environment, use **Group Policy Management Console** (gpmc.msc). In workgroup environment, use **Local Group Policy Editor** (gpedit.msc);
2. Expand `Computer Configuration\Policies\Windows Settings\Security Settings\Public Key Infrastructure`;
3. Double-click on Certificate Services Client – Auto-enrollment;
4. Set Configuration Model to **Enabled**;

5. Configure the policy as shown below and save settings:

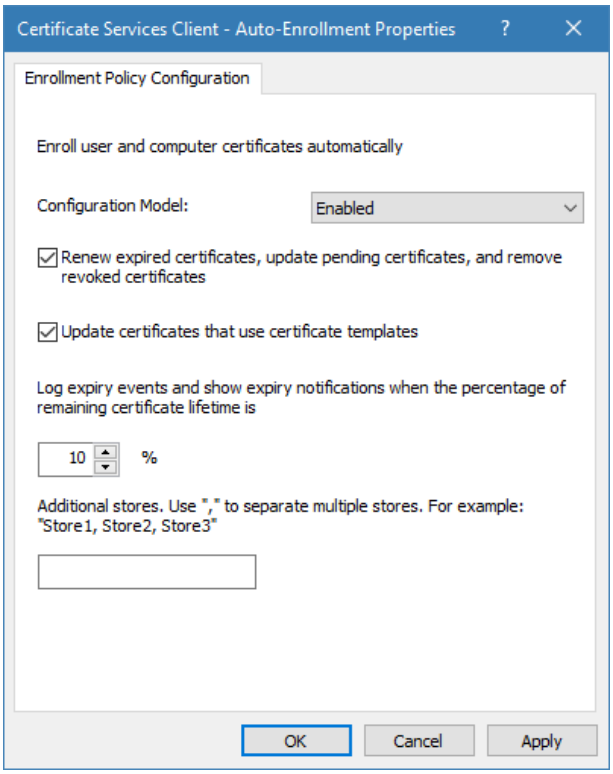

Figure 13: Configuring Autoenrollment policy in GPO

6. Repeat steps 2-5 for **User Configuration** node.

Configuration options on the dialog shown above have the following meaning:

- **Configuration model**

Configuration model selects the state of autoenrollment policy. When the value is set to **Disabled**, autoenrollment will be effectively disabled. This means that autoenrollment will not be triggered automatically and will have no effect when triggered manually. If the value is set to **Enabled**, autoenrollment will be triggered automatically based on internal timers. If the value is set to **Not Defined**, the autoenrollment status is determined by local registry information located at the following path:

```
Key: SOFTWARE\Policies\Microsoft\Cryptography\AutoEnrollment
Value: AEPolicy
Type: DWORD
```

- **Renew expired certificates, update pending certificates, and remove revoked certificates**

When checked, autoenrollment will renew certificates when the certificate's templates are not set up for autoenrollment. Such templates are which require multiple signatures (require Enrollment Agent, for example) or which accept certificate subject information from request. In addition, this setting will retrieve pending requests which were placed in pending state for CA manager approval.

When unchecked, neither of these tasks will be performed during autoenrollment activation.

- **Update certificates that use certificate templates**

When checked, autoenrollment will enroll and renew certificates based on certificate templates that have been set up for autoenrollment. When unchecked, neither of these tasks will be performed during autoenrollment activation.

Configuring certificate templates

This section covers how to configure certificate templates and provides a step-by-step example of how to create a new template for the autoenrollment of a smart card. Certificate template permissions are also explained.

Default settings

The following are default settings:

- Both domain administrators from the root domain, and enterprise administrators for fresh installations of Windows Server 2003 (and newer) domains may configure templates.
- Certificate template ACLs are viewed in the **Certificate Templates** MMC snap-in.
- Certificate templates can be cloned or edited using the **Certificate Templates** MMC snap-in.

Creating a new template for the autoenrollment of a smart card

In this exercise we will create certificate template that will be intended for client authentication and secure email (SMIME). As the additional requirement, the certificate will be stored on a smart card. To create a new template for autoenrollment of a smart card:

1. Log on to a computer where ADCS Remote Server Administration Tools (RSAT) are installed with Enterprise Admins permissions;
2. Press Win+R key combination on the keyboard.
3. In the **Run** dialog box, type *certtmpl.msc*, and then click **Ok**.

   The **Certificate Templates** MMC snap-in may also be invoked using the **Certification Authority** MMC snap-in by selecting the **Certificate Templates** folder, right-clicking, and then selecting **Manage**.
4. In the console tree, click **Certificate Templates**.
5. In the details pane, right-click the **Smartcard User** template, and then click **Duplicate Template** (Figure 14).

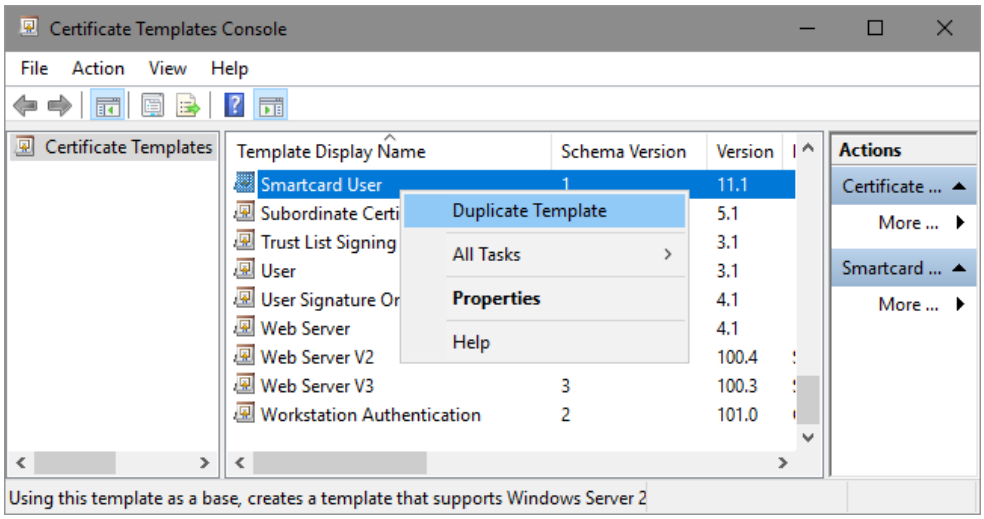

Figure 14: Creating a New Template for Autoenrollment of a Smart Card

6. The **Compatibility** tab of the new template properties dialog box appears. Configure compatibility settings to minimum OS version that will consume this template and minimum OS version of CA server that will issue certificates based on this template.
7. Switch to **General** tab.

In the **Template display name** field, type a unique name for the template, for example Smartcard User V2 (Figure 15). Specify desired certificate validity and enable checkboxes: "**Publish certificate in Active Directory**" and "**Do not automatically reenroll if a duplicate certificate exists in Active Directory**".

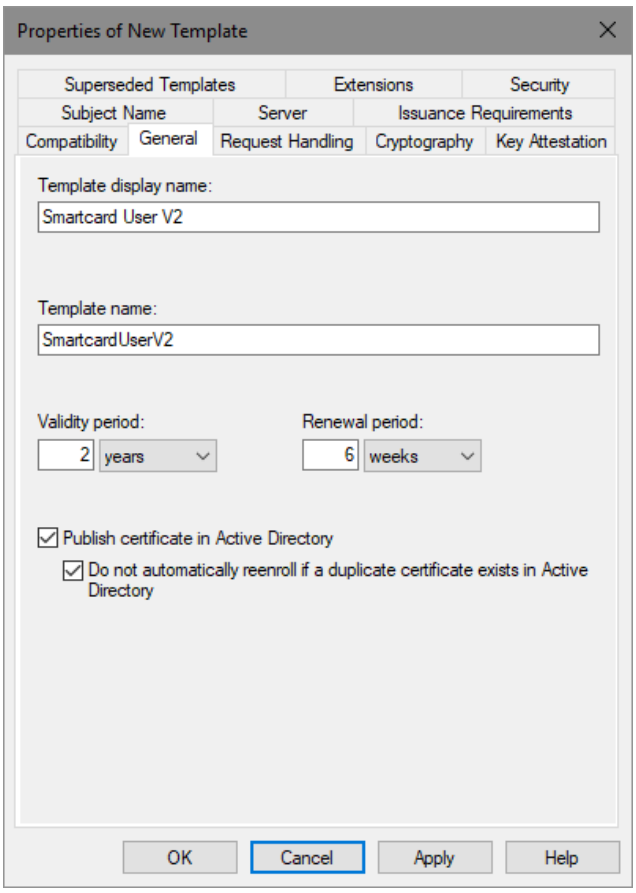

Figure 15: Configure certificate template's general tab

The "**Publish certificate in Active Directory**" checkbox should be enabled only when certificate is consumed by users and intended for Secure Email and Encrypting File System. In all other cases, this checkbox must be cleared.

If the "**Do not automatically reenroll if a duplicate certificate exists in Active Directory**" checkbox is enabled, autoenrollment will not enroll a user for the certificate template, even if a certificate does not exist in the user's **Personal** store. Active Directory is queried and determines if the user should be enrolled. This is an extremely valuable feature for users who do not have roaming profiles or when Credential Roaming feature is not enabled and log on to multiple machines. Without this setting and without roaming profiles, the user will automatically be enrolled on every machine that is logged on to (including servers).

8. Click the **Request Handling** tab (Figure 16). This tab is used to define how the certificate request should be processed. Use default settings in this tab and enable "**For automatic renewal of smart card certificates, use the existing key if a new key cannot be created**" checkbox.

   Since the certificate is supposed to be stored on a smart card, the "**Require user input**" radiobutton must be selected. If the certificate template is not going to be used for smart cards or if it is not desired for the user to be prompted to enroll for certificates, this option is not required. Machine certificates should not have this enabled or machine autoenrollment will fail.

Note that "**Delete revoked or expired certificate**" checkbox is grayed out. This is because the purpose of the certificate contains encryption (Secure Email). In order to retain access to older mails which were encrypted with expired certificate, the certificate must not be removed.

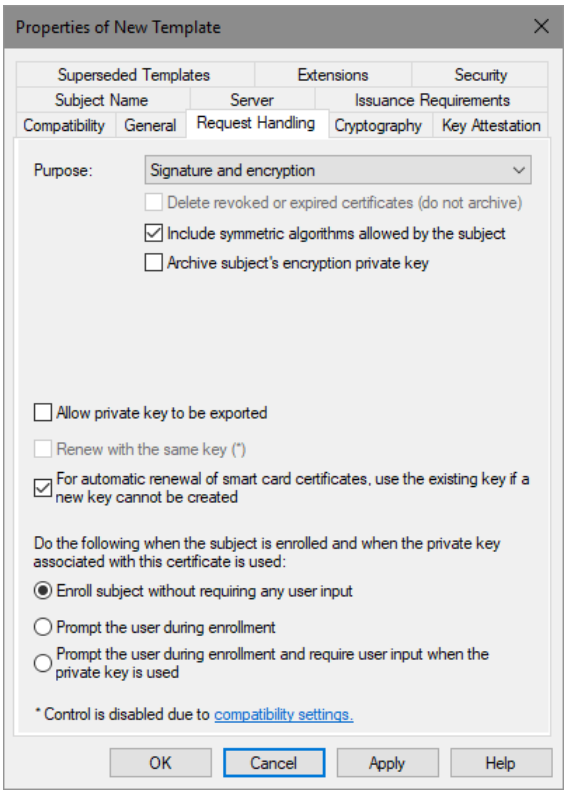

Figure 16: Configuring certificate template's Request Handling tab

9. Switch to **Cryptography** tab (Figure 17).

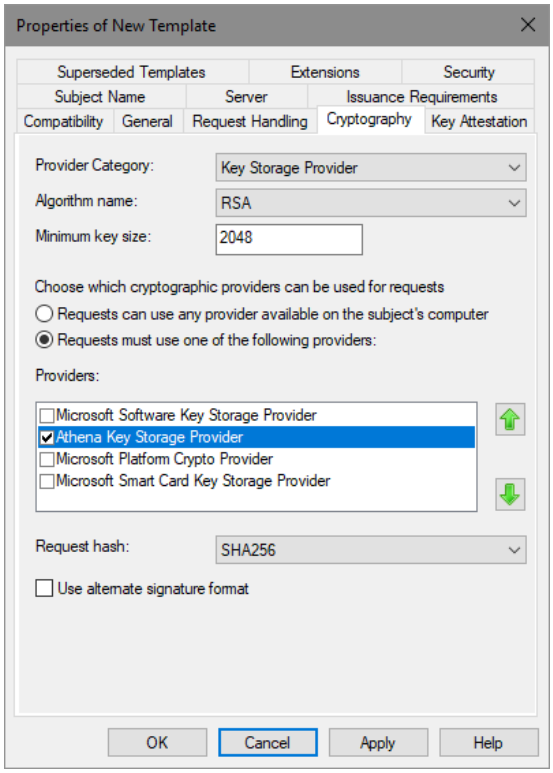

Figure 17: Configuring certificate template's Cryptography settings

In this tab, you configure provider category (Legacy CSP or Key Storage Provider). Default is Legacy CSP. If your smart card provider supports key storage provider (KSP), you should use KSP

instead. Specify the algorithm name, key length supported by smart card provider and provider name. It is recommended to explicitly specify provider

It is a common misconception when it is assumed that **Request hash** setting specifies the signature used to sign the certificate. Request hash specifies the hash used to sign the request only. Actual certificate's signature algorithm is selected by CA server.

Important: If more than one smart card CSP is made available on this tab, the user may be prompted for every CSP that is selected when enrolling for this template. The behavior may vary depending on the CSPs available on the client machine. If the user has only one smart card, the prompts for the unavailable CSPs will have to be cancelled. This behavior is by design. It is also important to select a minimum key size that is supported by the selected CSP; otherwise, enrollment will fail.

10. Switch to **Subject Name** tab. This tab is used to define how the subject name and certificate properties will be built. It is recommended to use the default selections when enrolling for a smart card template.

Starting with Windows 8 and Windows Server 2012, it is possible to supply subject along with request and use subject information in existing certificate for automatic renewal.

11. Switch to **Security** tab. This tab is used to define which users or groups may enroll or autoenroll for a certificate template. A user or group must have the **Read**, **Enroll**, and **Autoenroll** permissions to automatically be enrolled for a certificate template. For more details about certificate template permissions, refer to next section.
12. Click **OK** when finished.

The **XP Autoenrollment** tab is hidden by default in Certificate Templates MMC snap-in and is obsolete as it may not reflect the correct template's autoenrollment status for templates created with Windows 8 and Windows Server 2012 setting. However, if necessary, this tab can be added by enabling in **View** menu.

Certificate template permissions

For a user or computer to enroll for a certificate template, it must have appropriate permissions (ACEs) set on the template in Active Directory. The following list describes certificate template permissions:

- **Read** permission allows the template to be discovered by the user;
- **Write** permission allows a user to modify the contents of a certificate template. Note that only version 2 certificates with a Windows Server 2003 (or newer) schema may be modified. Version 1 certificate templates only allow ACLs to be modified;
- **Enroll** permission is enforced by the Enterprise CA when a user requests a certificate for a selected template. The Enterprise CA must also have **Read** permissions on a template to enumerate the template in the directory and issue certificates based on that template. Normally, the Enterprise CA is included in the Authenticated Users group, which has Read permissions by default on a template;
- **Autoenroll** permission is set on a template when it is desired for a user or computer to automatically enroll for a selected certificate template. The Autoenroll permission is needed in addition to the Enroll permission for a user to enroll for a given certificate template. Only version 2 templates or newly created templates may have the Autoenroll ACE set;
- **Full Control** permission is given to enterprise administrators and the primary domain administrators group by default. The Full Control permission allows a user to set or modify the permissions on a selected template.

Note that computer certificate enrollment using `certreq.exe` tool requires "`-adminforcemachine`" switch to authenticate requester as computer. Otherwise, a current user account is used to authenticate on CA server during enrollment.

A user or computer must have both **Read** and **Enroll** permissions to enroll for a selected certificate template. Use security groups when granting permissions whenever possible. Avoid permission assignment to individual accounts. Use global or universal security groups when configuring permissions on certificate templates.

Configuring an Enterprise CA

When certificate template is prepared for autoenrollment, it must be added to Enterprise CA server for issuance. This section will describe how to add certificate template to CA for issuance by using Certification Authority MMC snap-in, certutil.exe command-line tool and Windows PowerShell.

> Standalone CA does not support certificate templates

Configuring CA using MMC

The most convenient way to add certificate template to CA is to use Certification Authority MMC snap in:

1. Log on to CA server or computer with Remote Server Administration Tools installed with CA Administrator permissions;
2. Press Win+R key combination on the keyboard;
3. In the **Run…** dialog, type "*certsrv.msc*";
4. If necessary, click on root node, then press **Action** menu and select **Retarget Certification Authority** to connect to desired CA server;
5. When connected, expand CA node and select **Certificate Templates** folder. You will see certificate templates supported for issuance by this CA:

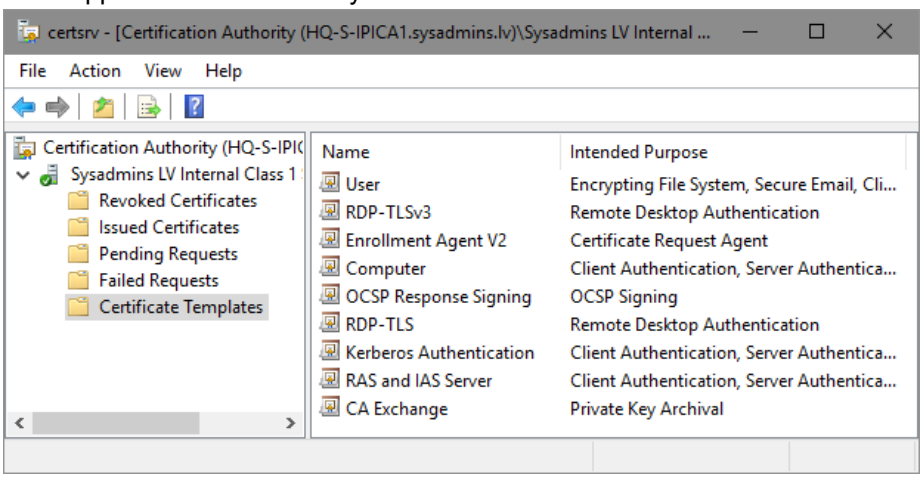

Figure 18: View certificate templates in Certification Authority MMC snap-in

6. In **Action** menu, select **New** and **Certificate Template to Issue** menu. In the opened dialog, select target template and press **Ok** to finish. Ensure that certificate template is listed in **Certification Authority** MMC console.

Configuring CA using certutil.exe

Built-in `certutil.exe` tool can be used to manage certificate templates on CA server locally or remotely:

1. Log on to CA server or computer with Remote Server Administration Tools installed with CA Administrator permissions;
2. Open elevated **Command Prompt**;

3. If you are logged on CA server, type:

```
certutil -SetCaTemplates +<TemplateCommonName>
```

Replace `<TemplateCommonName>` with actual template's common name. In a given example, it is `SmartcardUserV2`.

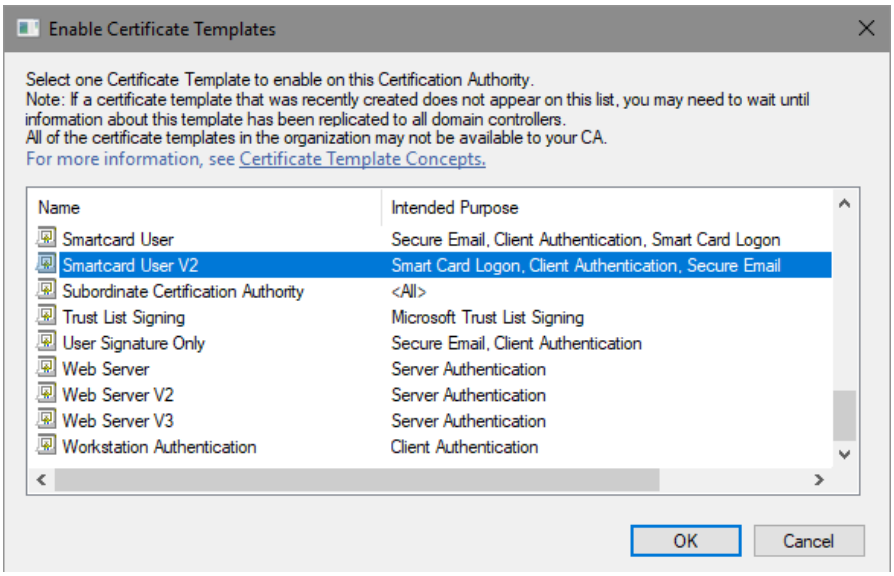

Figure 19: Enable Certificate Templates dialog

In order to add template to remote CA, specify remote CA location:

```
certutil -config <CaServerHostName>\<CaName> -SetCaTemplates
+<TemplateCommonName>
```

where `<CaServerHostName>` is DNS name of CA server and `<CaName>` is name of CA certificate. For example, "ca01.company.com\Contoso Issuing CA".

Configuring CA using Windows PowerShell

Starting with Windows 8 and Windows Server 2012, it is possible to use Windows PowerShell to manage certificate templates on CA server:

1. Log on to CA server with **CA Administrator** permissions;
2. Open elevated **Windows PowerShell** console;
3. Run the following commands:

```
Import-Module ADCSAdministration
Add-CATemplate -Name <TemplateCommonName>
```

Replace `<TemplateCommonName>` with actual template's common name. In a given example, it is `SmartcardUserV2`.

4. Confirm operation if prompted.

Unlike `certutil.exe` tool, PowerShell cmdlet does not support remote CA management and must be executed on CA server in interactive session (i.e. locally or by using PowerShell Remoting capabilities).

User Autoenrollment

This section illustrates manually pulsing autoenrollment and smart card enrollment. User autoenrollment for a smart card requires mandatory manual steps and user interaction, unlike other certificate types. Once autoenrollment has been enabled, the user will receive an informational balloon on the taskbar at the next autoenrollment trigger interval (default of eight hours) or at the next logon.

Manually pulsing autoenrollment

Autoenrollment may be pulsed manually through the Certificates MMC snap-in. Before you start, ensure that smart card is inserted in the reader and connected to computer.

To manually trigger autoenrollment:

1. Log on to the computer with the appropriate user account.
2. If **Balloon User Interface** appears in a system tray, double-click on a certificate image and proceed with next section. Otherwise, follow next steps to trigger autoenrollment feature;
3. Press Win+R key combination on the keyboard;
4. Type "*certmgr.msc*", and press ENTER;
5. Right-click the top of the tree on **Certificate\Current User**, select **All Tasks** on the context menu, and then select **Automatically Enroll and Retrieve Certificates** (Figure 20).

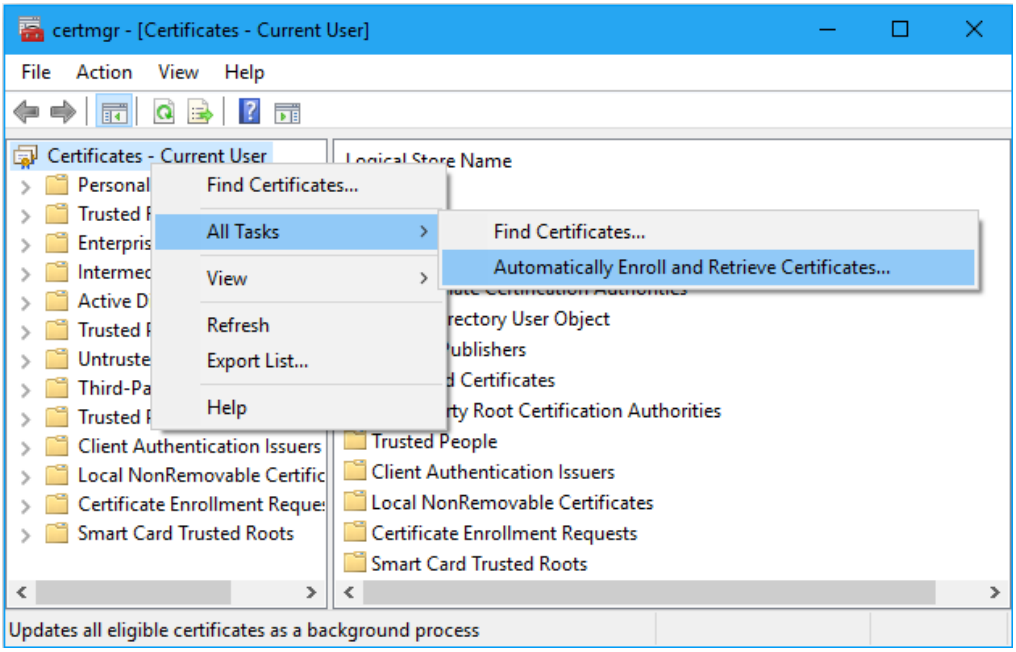

Figure 20: Automatic certificate enrollment in Certificates MMC snap-in

> It will take approximately one minute for the Certificate Enrollment balloon to be displayed, unless the registry key mentioned previously has been set. (see Balloon User Interface section.)

Smart card enrollment

1. On the **Before You Begin** page, click **Next**;

2. On the **Request Certificates** page, you will see the newly created template (Figure 21) and press **Enroll** button

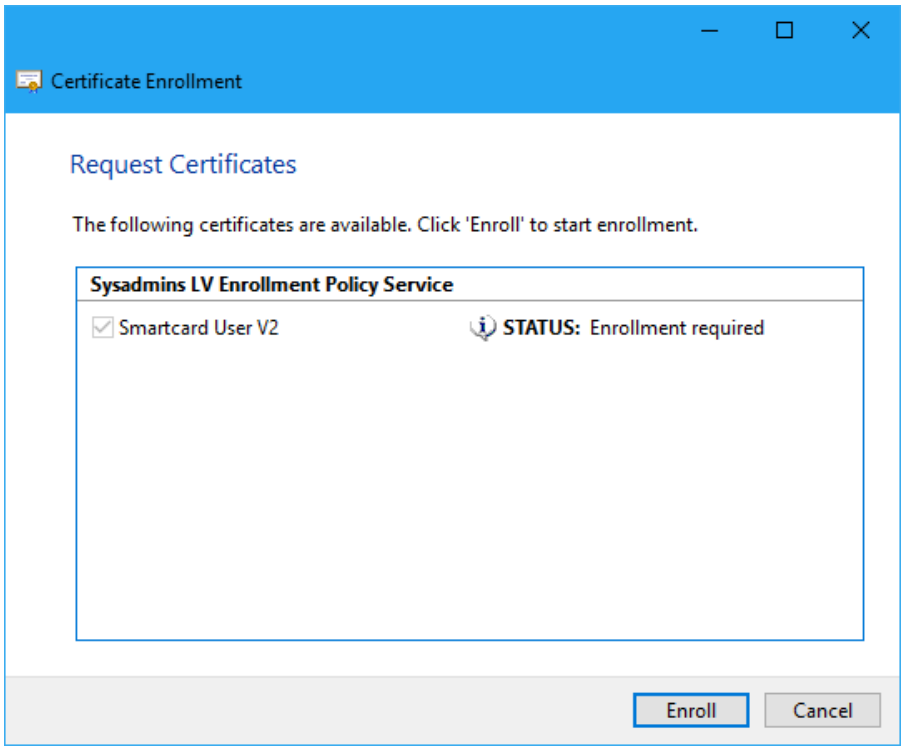

Figure 21: Certificate enrollment wizard

3. When prompted (Figure 22), enter PIN to access the smart card and generate the key pair.

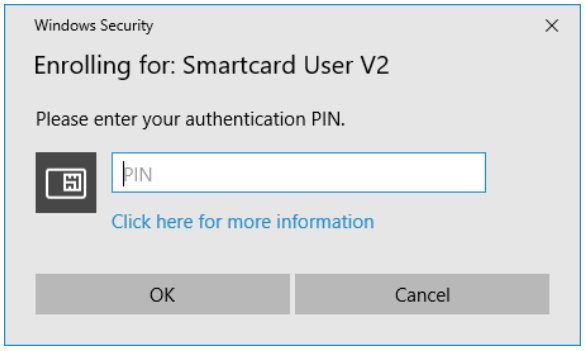

Figure 22: PIN prompt dialog

4. Follow smartcard specific dialogs (if any) provided by a smart card middleware to complete certificate enrollment.

5. Ensure that certification installation succeeded and press Finish button to finish the process.

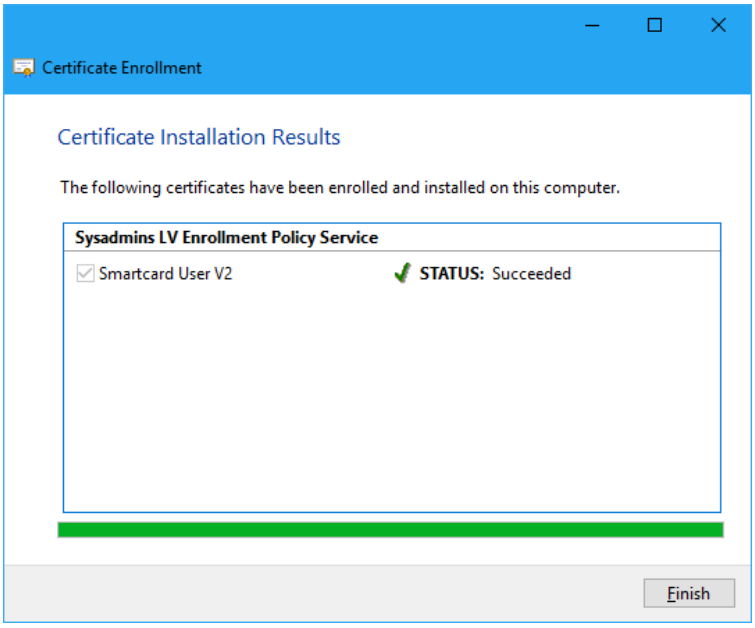

Figure 23: Certificate installation results

The success or failure of the autoenrollment process will be logged in the Application event log on the local computer. Also, a summary dialog box will appear for failed certificate requests that involved user interaction. If a failure occurs during enrollment, the user will be notified of the failure. For example, Figure 24 shows autoenrollment failure for Secure Email certificate when E-mail Active Directory attribute of the user account is empty:

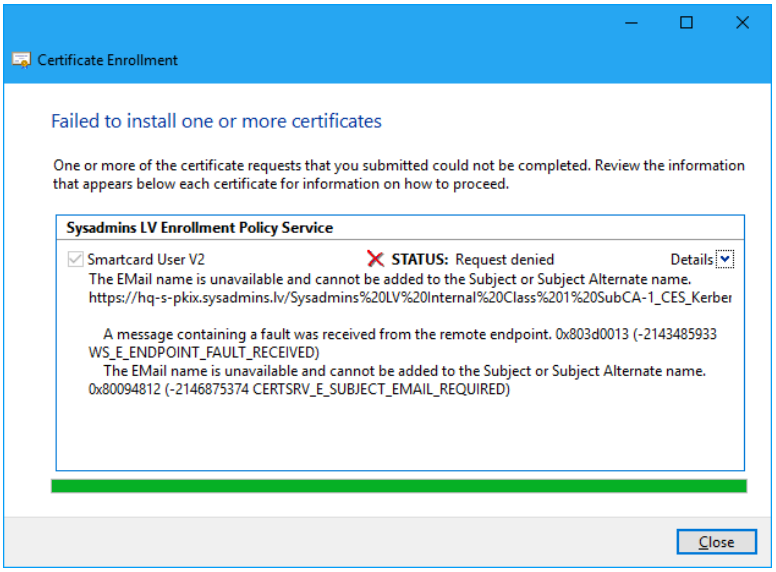

Figure 24: Notifying the user of errors while enrolling certificates

Configuring Advanced Features

This section discusses templates that require certificate manager approval, self-registration authority, and how to supersede a certificate template.

Requiring certificate manager approval

A specific certificate template can require that a certificate manager (CA officer) approve the request prior to the CA actually signing and issuing the certificate. This advanced security feature works in conjunction with autoenrollment and is enabled on the Issuance Requirements tab of a given certificate template (Figure 25). This setting overrides any pending setting on the CA itself.

Once certificate manager approval is required, all automatic enrollment requests are not issued until a certificate manager manually approves the request.

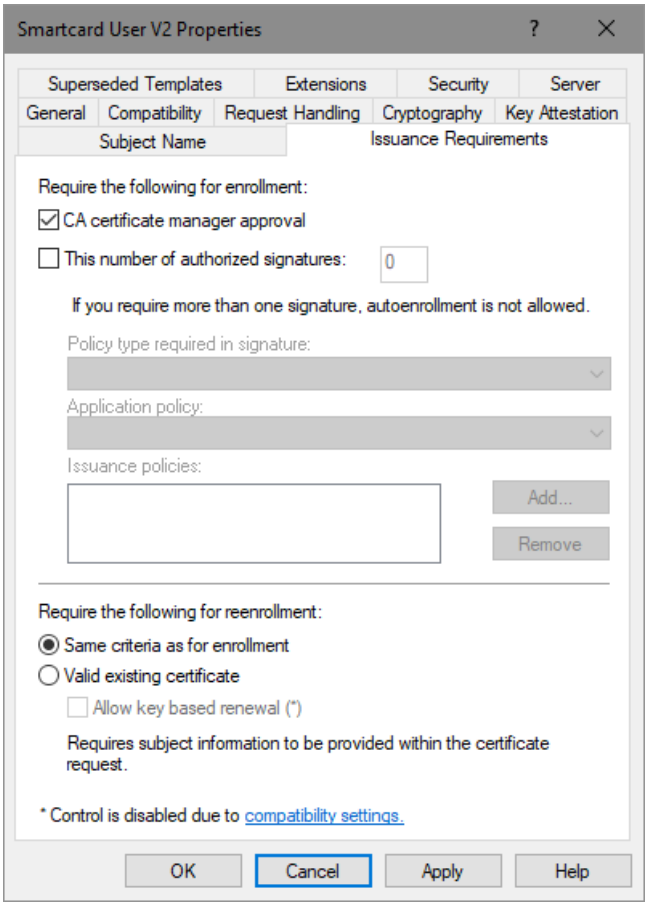

Figure 25: Setting the Requirement for Certificate Manager Approval

The autoenrollment process will periodically check the CA for approved requests and install the certificates automatically. Smart cards, user certificates, and machine certificates support pending requests. In the case of smart cards, the user will be prompted to insert the smart card when the certificate is issued so that the certificate may be written to the card.

> The autoenrollment process supports a maximum of one signature requirement on the template. This limitation exists to support the self-registration authority feature described in Self-Registration Authority. If multiple signatures are desired for a given certificate enrollment, manual enrollment should be used.

Self-registration authority

The self-registration authority (Self RA) is an advanced feature of certificate enrollment that may be combined with the autoenrollment process.

Self RA refers to certificate enrollment based on the existence of a previously enrolled certificate in which the users private key is used to sign the new certificate request. The Certificate Management Messages over CMS (CMC) protocol provides for this feature where one or more signatures may be used or required

for a given certificate enrollment. Self RA requirements are defined in a certificate template which may be managed using the Certificate Templates MMC snap-in.

To add an issuance (signature) requirement to a certificate template, open the template and click the **Issuance Requirements** tab.

To add a signature or issuance requirement, select the **This number of authorized signatures** check box and add the appropriate number in the following number field (Figure 26).

Now you may add specific requirements for the signing certificate.

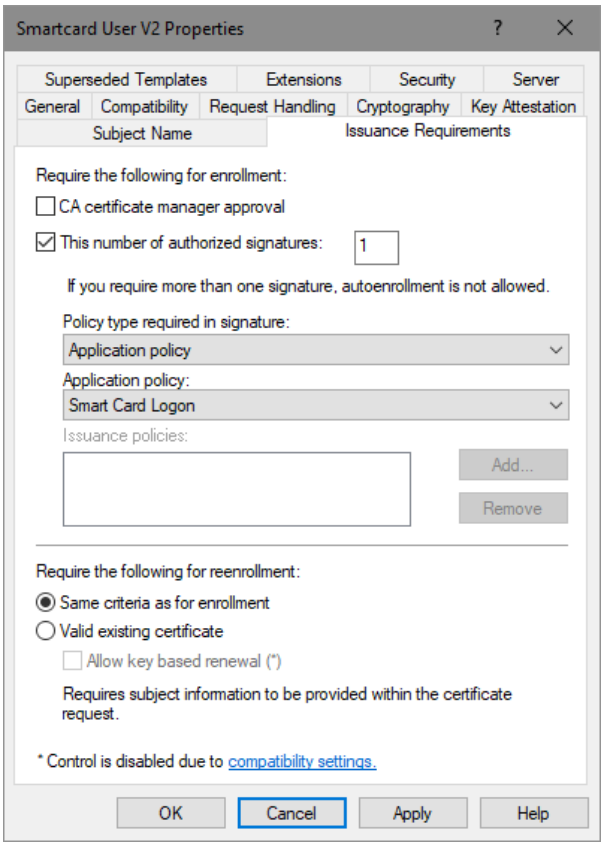

Figure 26: Setting the Number of Authorized Signatures

The previous setting is a useful configuration for customers who want to manually enroll users for smart cards with an enrollment station. Then they can supersede the original template with a new template with the previous settings to allow automatic renewal through the autoenrollment process, which will require the user to sign the renewal request with the old certificate.

Additional Self RA Example: You could add the Application Policy for a smart card logon certificate that would be used to enroll for an EFS certificate. This would mandate that users sign their request for an autoenrolled EFS certificate with a valid smart card certificate. The user would then be prompted to insert a smart card and enter a PIN when autoenrollment was activated for the EFS certificate.

Superseding certificate templates

Certificate autoenrollment also supports the concept of superseding a template or a previously enrolled certificate. Superseding a template allows an administrator to re-enroll, change, or combine previously issued certificate enrollments into a new certificate enrollment. Autoenrollment always examines existing certificates in the users store and determines if the template used in the issued certificate has been superseded. If a certificate template has been superseded, the user will automatically be enrolled with the new template, and the old certificates will be deleted or archived depending on the template setting.

Superseding certificate templates is especially useful in the following scenarios.

- Changing certificate lifetime
- Increasing key size
- Adding extended key usage or application policies
- Correcting enrollment policy errors
- Updating users from version 1 templates to version 2 templates

To create or modify a template to supersede an existing certificate

1. Open the **Properties** of the template to take precedence, click the **Superseded Templates** tab, (Figure 28) and then click **Add**.
2. Select the template you want to supersede (Figure 27), and then click **OK**.

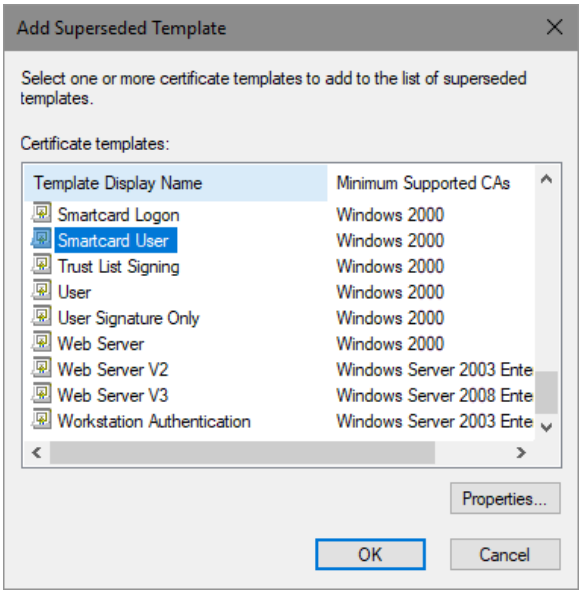

Figure 27: Selecting a Template to Supersede

3. The template will be added to the **Superseded Templates** tab (Figure 28). If you wish to add additional templates that should be superseded with this new template, click **Add** and repeat. Otherwise, click **OK**.

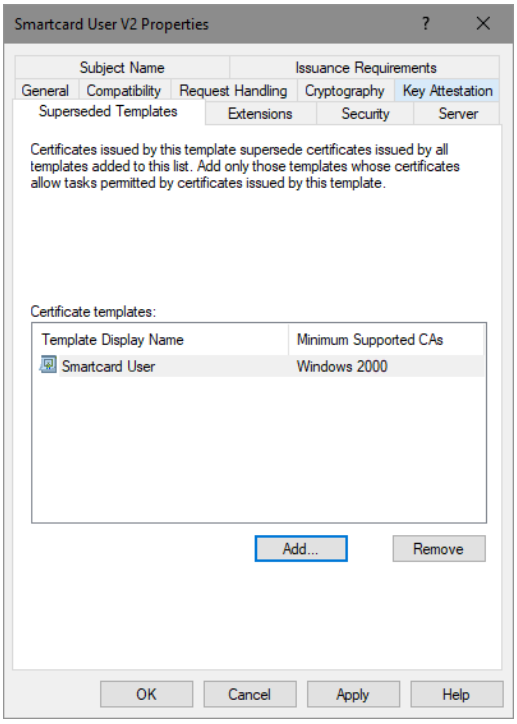

Figure 28: Listing Superseded Templates

Superseding a certificate always generates a new private key for the user or machine.

Troubleshooting

This section outlines key scenarios that need to be considered when troubleshooting autoenrollment. It also covers how to prepare for autoenrollment failures and lists event logging messages. The following key issues need to be considered when troubleshooting autoenrollment.

Infrastructure requirements

In Active Directory environment, Windows 10 clients and Windows Server 2016 CAs will always request LDAP-signed communications with domain controllers as a security function.

Root intermediate and cross-certificate download from Active Directory

Autoenrollment automatically downloads root, intermediate and cross certificates from Active Directory whenever a change is detected in the directory or when a different domain controller is contacted. If a third-party root certificate or cross-certificate is deleted from the local machine store, autoenrollment will not download the certificates again until a change occurs in Active Directory or a new domain controller is contacted.

To manually force a new download, delete the following registry key and all subordinate keys on all affected machines:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\AutoEnrollment\AEDirectoryCache
```

EFS and autoenrollment

EFS always attempts to enroll for the Basic EFS template by default. The EFS component driver generates an autoenrollment request that autoenrollment tries to fulfill. For customers who want to ensure that a specific template is used for EFS (such as to include key archival), the new template should supersede the Basic EFS template. The Basic EFS template should also be removed from any Enterprise CA. This will ensure that autoenrollment will not attempt enrollment for the Basic EFS template any more. For customers who wish to replace the Basic EFS template with a certificate and key that is archived through the Windows CA, the proper procedure is to supersede the Basic EFS template with a new version 2 certificate template.

Revoked certificates and renewal

Revoked certificates cannot be renewed and cannot be used to sign a renewal request. This scenario is explicitly blocked by autoenrollment. In this scenario, a user must perform a new manual enrollment request instead of renewal.

Smartcard renewal

The **Smartcard Logon** and **Smartcard User** version 1 templates may not be renewed through autoenrollment. To renew a version 1 **Smartcard Logon or Smartcard User** template, the proper procedure is to supersede these templates with a new version 2 template.

Autoenrollment always attempts to generate a new key when performing certificate renewal. For smart cards with limited space that do not support additional key generation, autoenrollment will attempt to reuse

the key; however, additional space will still be required to install the new certificate. If no space is available on the card for these operations, the renewal through autoenrollment may fail.

The renewal behavior of a smart card may vary depending on the type of smart card CSP being used and the state of the card at the time of renewal. In general, if the smart card being used has available space for an additional enrollment and the CSP supports multiple keys on a single card, autoenrollment will request the card to generate a new key for enrollment. If this succeeds, the certificate is written to the card and the container is marked as default.

> The default container is the only container that the Winlogon process will enumerate for a smart card logon certificate and key in Windows XP and Windows Server 2003. Starting with Windows Vista and Windows Server 2008, Winlogon process can use any smart card container for smart card logon operations.

If the smart card or CSP cannot generate a new key on the card, the existing key will be reused and a new certificate will be forced onto the card. This action will generate an event in the machines application event log.

> Autoenrollment will always use a newly generated key for all enrollment and renewal requests. The only exception to this rule is in the case of some smart card CSPs that cannot support a new key due to storage limitations on the smart card. If a key is reused, an event will be entered in the Client application log.

Autoenrollment and strong private key protection

The version 2 certificate template properties on the **Request Handling** tab support the ability to require a user password when the private key is used by applications. This is set by selecting the "**Prompt the user during enrollment**" option and requires user input when the private key is used. It is important to never use this option for smart card certificates as smart card CSPs also do not support this capability. If this option is chosen, autoenrollment may fail.

Removal of certificates on domain join/change domain

When a machine is removed from a domain or added to a new domain, all the downloaded certificates from Active Directory will be removed and refreshed if applicable. Certificates that were issued or autoenrolled from a previous forest will not be removed unless the machine is a domain controller. All client machines will automatically update certificates when the domain or machine information changes. When machines or users have certificates that are required for secure network communications, wireless communications, and so on, it may be necessary to delete the old certificates after joining a new domain or forest.

Autoenrollment failures

Autoenrollment will warn the user with a warning dialog box when an autoenrollment failure occurs. This feature is only enabled when user interaction is required on the certificate template.

To enable the warning feature for an autoenrollment failure

1. Open the specified template in the **Certificate Templates** MMC snap-in.
2. Click the Request Handling tab.
3. Click "**Prompt the user during enrollment**" on the Request Handling tab of the certificate template properties.

Re-initialized smart cards

If enrollment for a certificate is based on the existence of a smart card certificate and if the smart card has been re-initialized, the smart card Insertion dialog box will ask the user to insert a smart card matching the key container identified by the old certificate. Since the key container has been deleted, the Insertion dialog box will continue to display despite the fact that the user has removed and inserted the card. The only choice is to click **Cancel** and fail the enrollment.

Enhanced event logging

By default, autoenrollment logs errors/failures and successful enrollments in the **Application** event log on the client machine.

To enable enhanced logging of autoenrollment processes to include warning and informational messages, the following registry values must be created.

- **User Autoenrollment**

```
HKEY_CURRENT_USER\Software\Microsoft\Cryptography\Autoenrollment
```

Create a new DWORD value named `AEEventLogLevel`; set value to 0.

- **Machine Autoenrollment**

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Cryptography\Autoenrollment
```

Create a new DWORD value named `AEEventLogLevel`, set value to 0.

> All failures and errors are automatically logged. It is not necessary to enable the registry key to turn on failure logging.

Event Log Messages

The following event log messages only appear when additional event logging is enabled.

Success Event Log Messages

The following are samples of successful event log messages.

Event Type:	**Information**
Event Source:	AutoEnrollment
Event Category:	None
Event ID:	2
Date:	2/26/2001
Time:	12:52:02 PM
User:	N/A
Computer:	COMPUTER1
Description:	Automatic certificate enrollment for local system started.

Event Type:	**Information**
Event Source:	AutoEnrollment
Event Category:	None
Event ID:	3
Date:	2/26/2001

Time:	12:52:10 PM
User:	N/A
Computer:	COMPUTER1
Description:	Automatic certificate enrollment for local system completed.

Event Type:	**Information**
Event Source:	AutoEnrollment
Event Category:	None
Event ID:	27
Date:	2/26/2001
Time:	3:26:03 PM
User:	HAYBUV\USER1
Computer:	COMPUTER1
Description:	Automatic certificate enrollment for logged on user is cancelled.

Event Type:	**None**
Event Source:	AutoEnrollment
Event Category:	None
Event ID:	28
Date:	6/25/2001
Time:	7:36:16 AM
User:	HAYBUV\USER1
Computer:	COMPUTER1
Description:	Automatic certificate enrollment for HAYBUV\User1 successfully installed one AutoEnrollSmart cardEmail certificate when retrieving pending requests. User interaction was required.

Event Type:	**None**
Event Source:	AutoEnrollment
Event Category:	None
Event ID:	29
Date:	7/9/2001
Time:	6:39:29 AM
User:	HAYBUV\USER1
Computer:	COMPUTER1
Description:	Automatic certificate enrollment for HAYBUV\USER1 reused the private key when requesting one AutoEnrollSmart cardUser certificate.

Event Type:	**None**

Event Source:	AutoEnrollment
Event Category:	None
Event ID:	20
Date:	7/9/2001
Time:	6:39:29 AM
User:	HAYBUV\USER1
Computer:	COMPUTER1
Description:	Automatic certificate enrollment for HAYBUV\USER1successfully renewed one AutoEnrollSmart cardUser certificate from certificate authority TestCA on Server1.haybuv.com.

Event Type:	**None**
Event Source:	AutoEnrollment
Event Category:	None
Event ID:	29
Date:	7/17/2001
Time:	9:37:29 AM
User:	HAYBUV\user1
Computer:	TESTCA
Description:	Automatic certificate enrollment for HAYBUV\user1 reused the private key when requesting one Autoenroll Smart card User certificate.

This event signifies the fact that the private key was reused during a certificate renewal.

Failed Event Log Messages

The following are samples of failed event log messages.

Event Type:	**Error**
Event Source:	AutoEnrollment
Event Category:	None
Event ID:	15
Date:	7/8/2001
Time:	3:09:41 PM
User:	N/A
Computer:	TEST1
Description:	Automatic certificate enrollment for Haybuv\User1 failed to contact Active Directory (0x8007054b). The specified domain either does not exist or could not be contacted. Enrollment will not be performed.

This error most often occurs when a user is logged on to a machine with cached credentials and is offline. Therefore, autoenrollment cannot continue and will be attempted later.

Event Type:	**Error**
Event Source:	AutoEnrollment
Event Category:	None
Event ID:	15
Date:	2/24/2001
Time:	10:36:08 AM
User:	N/A
Computer:	TEST1
Description:	Automatic certificate enrollment for local system failed to contact a directory server (0x80072751). A socket operation was attempted to an unreachable host. Enrollment will not be performed.

This error most often occurs when a domain controller is not available or is not accessible by the client. Common causes include network errors, network connectivity, and so on.

Event Type:	**Error**
Event Source:	AutoEnrollment
Event Category:	None
Event ID:	13
Date:	7/5/2001
Time:	9:37:44 AM
User:	N/A
Computer:	TEST1
Description:	Automatic certificate enrollment for local system failed to enroll for one HAYBUV IPSEC certificate (0x800706ba). The RPC server is unavailable.

This error typically occurs when the certificate authority is not available on the network or the service is stopped.

Event Type:	**Error**
Event Source:	AutoEnrollment
Event Category:	None
Event ID:	13
Date:	7/5/2001
Time:	7:41:27 AM
User:	N/A
Computer:	TEST1
Description:	Automatic certificate enrollment for local system failed to enroll for one HAYBUV IPSEC certificate (0x8009400f). An attempt was made to open a certification authority database

	session, but there are already too many active sessions. The server may need to be configured to allow additional sessions.

This is a rare event when the certificate authority is under heavy load and cannot respond to the request in a timely manner. Autoenrollment will automatically try again at a later time.

Event Type:	**Error**
Event Source:	AutoEnrollment
Event Category:	None
Event ID:	16
Date:	7/5/2001
Time:	2:53:34 AM
User:	N/A
Computer:	TEST1
Description:	Automatic certificate enrollment for local system failed to renew one HAYBUV IPSEC certificate (0x8009400f). An attempt was made to open a Certification Authority database session, but there are already too many active sessions. The server may need to be configured to allow additional sessions.

This is the same error as the previous one, but it involves a renewal.

Event Type:	**Warning**
Event Source:	AutoEnrollment
Event Category:	None
Event ID:	7
Date:	7/24/2001
Time:	7:48:27 PM
User:	HAYBUV\USER1
Computer:	TEST1
Description:	Automatic certificate enrollment for HAYBUV\USER1 could not enroll for Key Recovery Agent certificate template due to one of the following situations. • Enrollment access is not allowed to this template. • Template subject name, signature, or hardware requirements cannot be met. • No valid certificate authority can be found to issue this template.

This is an autoenrollment error that occurs when a user has a certificate and private key installed that corresponds to a given template that is now expiring. Autoenrollment attempts to automatically renew the certificate; however, the user does not have applicable permissions for this template and therefore autoenrollment fails. Autoenrollment is based on certificates in the store as well as certificate template settings.

Event Type:	**Error**

Event Source:	AutoEnrollment
Event Category:	None
Event ID:	13
Date:	7/17/2001
Time:	9:22:10 AM
User:	HAYBUV\user1
Computer:	TESTCA
Description:	Automatic certificate enrollment for HAYBUV\user1 failed to enroll for one Autoenroll smart card user certificate (0x80094812). The e-mail name is unavailable and cannot be added to the Subject or Subject Alternate name.

This error occurs when the user account in Active Directory does not have a valid e-mail address on the user property page in Active Directory Users and Computers MMC snap-in. Enrollment for certificate templates in Active Directory requires an e-mail address to exist prior to enrollment.

Event Log Tools

With Windows 7 and Windows Server 2008 R2, there are several tools to query a local system for various events:

- Event Viewer (*eventvwr.msc*)

Event Viewer is a graphical too which is an MMC snap-in and is preinstalled in any Windows installation where graphical user interface (GUI) is enabled. Event Viewer tool is not available on Windows Server in Server Core mode installation.

- Wevtutil.exe (command-line)

The `wevtutil.exe` tool is preinstalled in any Windows installation starting with Windows Vista and Windows Server 2008.

- Get-WinEvent (PowerShell)

The `Get-WinEvent` cmdlet is shipped automatically with every PowerShell version starting with PowerShell 3.0 and above.

Summary

Windows Server 2016 through the Active Directory Certificate Services component provides user certificate autoenrollment. This allows administrators to easily deploy certificates throughout the enterprise while requiring no user interaction. User certificate autoenrollment in the Windows 10 Windows Server 2016 operating systems builds on Microsoft's long-established reputation for shipping robust PKI components that have a low TCO. Since PKI is an integral part of the Windows 10 operating system, Windows Server 2016 PKI provides some distinct advantages over third-party add-in components. These advantages include:

- No per-certificate fees or per-user PKI licenses
- Centralized user security management
- Integration with normal enterprise management tasks
- Single sign-on capabilities to networks and applications
- Managed trust capabilities
- Support for all applications through CryptoAPI

Keep in mind that almost all third-party PKIs must be purchased separately and require per-certificate license fees and increased management tasks.

Overall, certificate autoenrollment features in Windows Server 2016 should provide organizations and enterprises with the ability to effortlessly deploy digital certificates and PKI-enabled applications with little or no additional cost to a normal IT operations budget.

Reference Links

- Certificate Autoenrollment in Windows XP by David B. Cross (Microsoft) (https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-xp/bb456981(v=technet.10))
- [MS-CERSOD]: Certificate Services Protocols Overview — Open Protocol Specifications, Microsoft (https://msdn.microsoft.com/en-us/library/hh297583.aspx)
- [MS-CAESO]: Certificate Autoenrollment System Overview [ARCHIVED] — Open Protocol Specifications, Microsoft (https://msdn.microsoft.com/en-us/library/jj633107.aspx)
- [MS-WCCE]: Windows Client Certificate Enrollment Protocol — Open Protocol Specifications, Microsoft (https://msdn.microsoft.com/en-us/library/cc249879.aspx)
- [MS-XCEP]: X.509 Certificate Enrollment Policy Protocol — Open Protocol Specifications, Microsoft (https://msdn.microsoft.com/en-us/library/dd302869.aspx)
- [MS-WSTEP]: WS-Trust X.509v3 Token Enrollment Extensions — Open Protocol Specifications, Microsoft (https://msdn.microsoft.com/en-us/library/dd340609.aspx)
- [MS-CRTD]: Certificate Templates Structure — Open Protocol Specifications, Microsoft (https://msdn.microsoft.com/en-us/library/cc226517.aspx)
- RFC 5272: Certificate Management over CMS (CMC) — Internet Engineering Task Force (https://tools.ietf.org/html/rfc5272)
- Active Directory Certificate Services Longhorn Beta3 Key Archival and Recovery — Whitepaper, Microsoft (https://www.microsoft.com/en-us/download/details.aspx?id=19952)
- Implementing and Administering Certificate Templates in Windows Server 2008 — Whitepaper, Microsoft (https://www.microsoft.com/en-us/download/details.aspx?id=19169)
- Query and Manage Event Logs with the Windows Events Command Line Utility (https://technet.microsoft.com/en-us/library/dd310329.aspx)
- Certificate Rebind in IIS 8.5 — Microsoft Docs, Microsoft (https://docs.microsoft.com/iis/get-started/whats-new-in-iis-85/certificate-rebind-in-iis85)
- Superseded Certificate Templates and impact on user's AD store — Microsoft Support Knowledge Base (https://support.microsoft.com/en-us/help/2884551/superseded-certificate-templates-and-impact-on-user-s-ad-store)
- Certificate Enrollment Web Services in Active Directory Certificate Services — Whitepaper, Microsoft (https://social.technet.microsoft.com/wiki/contents/articles/7734.certificate-enrollment-web-services-in-active-directory-certificate-services.aspx)