# Symantec™ Managed PKI® Overview

v8.14

# Legal Notice



Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

# Contents

Chapter 1

# Introduction

This chapter includes the following topics:



## About Symantec Managed PKI

Symantec™ Managed PKI is a public key infrastructure (PKI) platform. PKI is the combination of software, encryption technologies, and services that enables your company to protect the security of your Internet communications and business transactions. PKI uses digital certificates, public-key cryptography, and Certification Authorities (CA) to create an enterprise-wide network security architecture that protects against intrusion. The intrusion can be from hackers who steal passwords or intercept email messages and credit card transactions.

Certificates authenticate parties and secure communications in electronic communications. Certificates are the electronic documents that identify individuals, organizations, computer servers, and computer devices, such as wireless devices. As with a driver's license or passport, a certificate provides proof of identity. For example, certificates may be used to prove one's identity in order to access sensitive

intranet and Internet information. It thereby replaces expensive and cumbersome user names and passwords.

As a PKI system, Managed PKI protects the confidentiality and integrity of electronic communications. This guide provides an overview of the Managed PKI product. Designed to orient new users, *Symantec™ Managed PKI® Overview* explains the primary concepts, and services that is involved in Managed PKI.

# About Public Key Infrastructure (PKI)

The Symantec Managed PKI service provides a flexible PKI platform to manage the complete certificate lifecycle to issue new certificates, renew existing certificates, and revoke untrustworthy certificates. Additionally, this service provides the ability to escrow and recover private keys of the certificates that are used to encrypt emails, file systems, or other data. This service offers numerous validation services to verify certificates' current status to ensure that only trustworthy certificates encrypt data, digitally sign documents, and authenticate networks.

As a managed service, Symantec Managed PKI significantly reduces the costs that are associated with an in-house PKI. For example, customers need to acquire cryptographic and application server hardware, purchase server and client licenses, and train staff before issuing the first certificate from an in-house PKI deployment. Additionally, customers have to create their own certificate policy (CP) as a principal statement of policy governing the PKI hierarchy. The customers also have to create certification practices statement (CPS), which defines certificate process and procedures as well as trusted roles and responsibilities.

Symantec Managed PKI service is designed as a multi-tenant, highly-available environment based on best-of-breed cryptographic and application server hardware. Additionally, this environment is monitored 24x7x365 by a professionally-trained staff that has passed enhanced security background checks. Further, this environment is audited on a regular basis to maintain WebTrust and SSAE16 accreditation.

In all cases, your organization acts as the enrollment and the authentication site, while Symantec processes the authenticated requests and generates certificates.

# About Symantec Managed PKI Certificates

Your organization has purchased the Managed PKI service. As a Managed PKI administrator, the Managed PKI certificates that you are able to manage are determined by the service your organization purchased. Managed PKI product allows you to issue certificates from public and private CAs and manage them from

a single, unified interface. Based on your implementation, your Managed PKI service includes one or more of the following:

# Certificate Authority (CA)

Symantec Managed PKI service creates and manages Certificate Authority (CA) hierarchies. Symantec Managed PKI service includes the following CA hierarchies:

- Symantec Trust Network (STN)
- Private Certificate Authority
- Adobe® Certified Document Services (CDS)
- Adobe Approved Trusted List (AATL)

Refer to the Symantec™ Managed Public Key Infrastructure (PKI) Service Description, available from the Symantec Authentication Services Repository at https://www.symantec.com/about/profile/policies/repository.jsp for details on these CA hierarchies.

Symantec also offers an option to create an unverified Managed PKI account. An unverified account provides full access and capabilities under private CA hierarchies but does not allow issuance of certificates under STN or Adobe CDS. Symantec populates the Organization (O) and Organizational Unit (OU) values.

Recipients of user certificates under this account meet the verification requirements that are defined as Rudimentary by the US government.

## Signing and Encryption Algorithms

Managed PKI supports the following signing and encryption algorithms:

- SHA1 with RSA encryption
- SHA256 with RSA encryption

If your account is configured for Ecliptic Curve Cryptography (ECC), or Digital Signature Algorithm (DSA), Managed PKI supports the following signing and encryption algorithms:

- ECC 224 and 384. ECC is supported for the Client authentication, Microsoft Wi-Fi, and custom certificate profile templates only. Certificate lifecycle operations for certificates with ECC-based keys are supported using Managed PKI Enterprise Gateway, PKI Web Services, and PKI Client, including native browser support.
- DSA 2048-256 and 3072-256. DSA requires custom certificate profile templates. Contact your Symantec representative for details on custom certificate profile templates.

# Managed PKI Components

Symantec Managed PKI consists of a number of components. The components you deploy (and how you deploy them) depend upon your organizational needs.

See "Choose Deployment Options" on page 23.

## PKI Manager

PKI Manager is a web portal hosted in Symantec's data centers. In this portal, Managed PKI administrator performs the tasks that are related to account, user, certificate, and key management. Managed PKI administrators authenticate themselves to this web portal using an administrator certificate that is issued to them. For increased security, these certificates can be stored on hardware tokens.

See "Token, Smart Card, and Security Device Options" on page 15.

- Account Management: PKI Manager enables a PKI administrator to view certificate authorities (CAs), number of seats, and the reports that are associated with their account. PKI Manager also allows a PKI administrator to create and assign roles and responsibilities to additional PKI administrators.
  Additionally, PKI Manager allows administrators to create and remove sub-accounts. Using sub-accounts, PKI administrators can group management tasks by many factors such as assigned administrators, available certificate types, user base, and so on.
- User Management: PKI Manager permits a PKI administrator to add and edit users, generate unique enrollment codes and links for each user, and enroll users for certificates.
  PKI Manager also lets a PKI administrator revoke the certificates that have become untrustworthy. The administrator can revoke because a user no longer needs a certificate (for example, if the user left the company). The administrator can also revoke if the user comprised a private key (for example, the user lost a laptop). Additionally, PKI Manager provides a PKI administrator with the ability to recover a private key of an encryption certificate for a user.
- Certificate Lifecycle Management: PKI Manager enables a PKI administrator to configure certificate profiles for different CAs. As part of these certificate profiles, a PKI administrator sets such parameters as key sizes, key usages, and signing algorithms. A PKI administrator also selects the certificate enrollment method and private key security protection level. Additionally, PKI Manager has the capability to customize the emails that are sent to users. PKI Manager can also provide users with document and video-based instructions to configure third-party applications to work with the newly-issued certificates. Based on your configuration settings, Managed PKI can also escrow your users' private keys and recover them in the event they are lost.

See "Certificate Profiles" on page 24.

Refer to the PKI Manager and its associated help for details on performing these tasks.

## PKI Certificate Service

PKI Certificate Service hosts the certificate enrollment web pages at Symantec that your users access to request certificates. These web pages guide users through the necessary steps to request certificates. In addition, these web pages may display instructions, provided by a PKI administrator, to configure third-party products.

## Certificate Issuance Center

The Certificate Issuance Center is the certificate engine hosted at Symantec. This certificate engine creates certificates based on certificate signing requests submitted from PKI Certificate Service. This request is received from PKI Enterprise Gateway, or sent using PKI Web Services. Additionally, this certificate engine signs these certificates with the issuing Certificate Authority.

## PKI Enterprise Gateway

You can choose to store your user and your certificate data at your enterprise location because your security policies require you to do so. You may also store data at your enterprise location if you want to leverage an existing database for this information. You implement PKI Enterprise Gateway and the optional Autoenrollment server at your enterprise site to store data. PKI Enterprise Gateway is a registration authority (RA) application that is installed in your data center, if desired. These applications tightly integrate with a Lightweight Directory Access Protocol (LDAP) user store such as Microsoft® Active Directory® (AD). It automatically approves certificate requests and publish certificate data back into the user store.

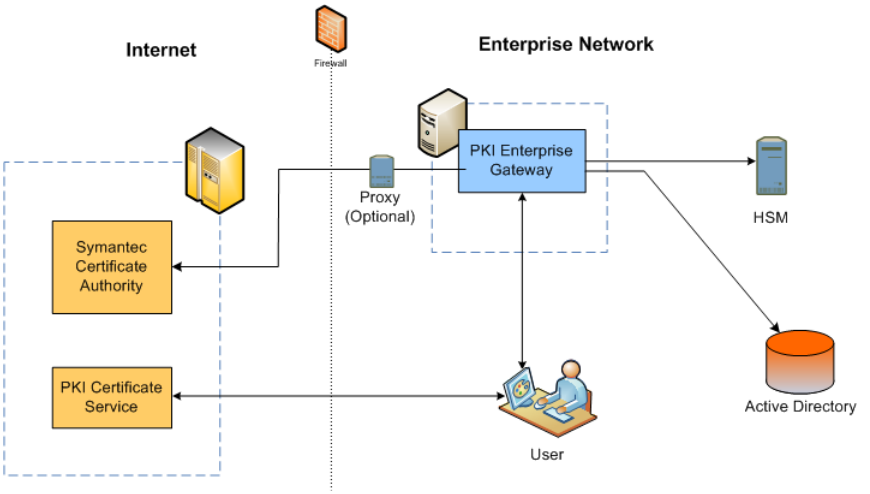
- The PKI Enterprise Gateway authenticates your user against your local user store. It authorizes the user against the policies that are set up in the certificate profiles you configured in PKI Manager. PKI Enterprise Gateway enables the user to enroll for new certificates or renew existing certificates from the PKI Certificate Service.

  Once the user has been authenticated and authorized, PKI Enterprise Gateway obtains the enrollment or the certificate data from your enterprise data store. It then enrolls for or renews the certificate on behalf of the user. If it is configured to do so in your certificate profiles, PKI Enterprise Gateway also publishes the certificate to your enterprise data store.

- The Symantec-PKI Enterprise Gateway-Autoenrollment Server (the Autoenrollment server) automates most of the certificate lifecycle operations, including requesting certificates and renewing certificates.
- The PKI Enterprise Gateway escrows your private keys in a local user store. You can recover these private keys if your user certificates are lost.

Figure 1-1 illustrates a simple PKI Enterprise Gateway deployment.

**Figure 1-1** Simple PKI Enterprise Gateway deployment




See *Symantec™ PKI Enterprise Gateway Deployment Guide* and *Symantec™ PKI Enterprise Gateway Autoenrollment Server Deployment Guide* for details about the PKI Enterprise Gateway and the Autoenrollment server.

## PKI Client

PKI Client (formerly known as Certificate Manager) is middleware designed to dramatically improve user experience with the certificate lifecycle. In the native experience, users use embedded functionality of the operating system or browser to request certificates from certificate enrollment web pages. While this native experience does not require any additional software, the native experience has known usability limitations. For example, Microsoft Internet Explorer produces numerous pop-up windows with the warning messages that often confuse users. With PKI Client, the certificate lifecycle has been streamlined to automate common functions like certificate renewal, to minimize user involvement. PKI Client also provides centralized policy management functions such as PIN management, certificate export, and smart card management, to protect certificates. Furthermore,

PKI Client has the ability to auto-configure third-party products such as wireless networks and virtual private network clients to use certificates.

You install PKI Client on any device that stores certificates or on which the smart cards that store certificates are used. Obtain the PKI Client software from the *Resources* page of PKI Manager.

See *Symantec™ PKI Client Administrator's Guide* and *Symantec™ PKI Client Writing Post-processing Scripts Guide* for more information about PKI Client.

### PKI Web Services

PKI Web Services is a Web Service hosted at Symantec that provides the capability to integrate with Symantec Managed PKI. A third-party application can use the APIs provided by PKI Web Services to programmatically:

- Obtain a certificate policy
- Search for a certificate or a user data
- Enroll for and renew a certificate
- Suspend and resume a certificate
- Revoke a certificate
- Support recovery of private keys in the event they are lost
- Delete single and multiple users
- Send enrollment email to end users

See *Symantec™ Managed PKI PKI Web Services Developer's Guide* for more information about Managed PKI PKI Web Services.

### Transaction Signing API

Symantec's Transaction Signing API allows you to integrate Symantec certificates into your client applications to enable secure transaction signing. The Transaction Signing API allows you to programmatically sign and secure user transactions (such as purchases or funds transfers), providing transaction tracking and non-repudiation.

See *Managed PKI® Transaction Signing API Developer's Guide* for more information about Symantec's Transaction Signing API.

## Seats and Seat Pools

Managed PKI certificates are issued against seats. Seats are the number of discrete users or devices available in an account. Each certificate is issued against a seat, and the seat ID (a unique identifier for a user or device) identifies the users and

devices. An organization purchase a number of seats per account, and certificates issued count against that total.

Seats can be assigned to seat types, or seat pools by account and sub-account. Managed PKI supports five seat pools:

- User seats for the certificates that are issued directly to users.
- Device seats for the certificates that are issued to machines and devices, such as Microsoft Computer certificates
- Organizational seats for the certificates that are issued to large organizations.
- Server seats for the certificates that are issued to servers such as Microsoft Domain Controller certificates
- Manufacturer seats for the certificates that are inserted into devices during the manufacturing process.
- Secure Email Gateway seats for the certificates that are used for secure email gateways
- Adobe CDS Organization seats for the certificates that are issued by the organizations that perform digital authentication of Adobe PDF documents

Seats are tracked based on the seat ID, or unique identifiers for each certificate recipient. For user seats, you can issue multiple valid certificates to the same seat ID. For all other certificates, you can issue only one valid certificate to each seat ID. If you revoke all the valid certificates that are assigned to a seat ID, the seat is credited back to the seat pool.

You can allocate seats to seat pools by sub-account. You can have the sub-account inherit any available seats from the parent account, or disable the seat pool for the sub-account (by setting the available seats to 0). If disabled, the certificate profiles that use seats from the seat pool are not visible to administrators in the sub-account. View available seats per seat pool on the PKI Manager dashboard for the main account and for each sub-account.

Work with your Symantec Client Manager to purchase seats for the appropriate seat types based on your certificate usage requirements.

## About Seat IDs

You set the attribute that populates the seat ID for a certificate recipient in the certificate profile (on the *Manage Certificate profile* page for the certificate profile, under *Customize user identification*). Select an attribute that can only be assigned to only one user or device. If you do not use a unique identifier, the user or device may not be issued the correct certificate, and the user or device may be in violation of the Subscriber Agreement (https://www.symantec.com/about/profile/policies/repository.jsp).

Symantec suggests that you assign seat IDs as follows:

Table 1-1 lists the Certificate type and the recommended or required method of assigning Seat IDs.

**Table 1-1** Seat ID assignments

| Certificate Type | Seat ID Assignment |
|---|---|
| User | Email address, employee number, or Windows Universal Principle Name (UPN). |
| Device | DNS Name |
| Server | DNS Name |
| Organization | The only allowed Organization is the approved Account name. The seat ID in this situation must be the unique common name or a serial number. |
| Manufacturer Device | The Seat ID is a unique device identifier. Recommended choices include the MAC address or serial number. IP address and DNS name are also an option if this information is known at manufacturing time. |
| Secure Email Gateway | The seat ID for this certificate type is system generated. |
| Adobe CDS Organization | The only allowed Adobe CDS Organization is the approved Account name. The seat ID for this certificate type is system generated. |

## Authentication Methods

Managed PKI requires that users be authenticated by their administrators before they can enroll for and pick up a new certificate. Managed PKI provides several methods for performing this authentication, based on your needs:

- **Enrollment code authentication** allows a PKI administrator to generate a unique enrollment code for each user in order to automatically approve certificate requests. The PKI administrator sends certificate invitations to users with a link to a certificate enrollment web page. The PKI administrator also sends the unique enrollment code for that user. Users must include their enrollment code along with any additional information in the certificate enrollment web pages when they enroll for a certificate.

**Note:** Symantec recommends that the enrollment code be sent separately from the enrollment link. Symantec also recommends that email is not used to send the enrollment code, as the enrollment code appears as plain text in the email. If you issue certificates from a private CA, the PKI administrator can configure PKI Manager to send the enrollment code as part of the enrollment link in the enrollment email. While this makes it easier for the user to pick up a certificate, it is less secure, as the enrollment code and enrollment link are delivered in the same email.

The Certificate Issuance Center compares this enrollment code to the information that is generated in PKI Manager. If there is a match, the Certificate Issuance Center issues a certificate. If the user-entered enrollment code does not match the enrollment code that is generated for that user, the Certificate Issuance Center gives an error message to the user.

- **Manual approval** allows a PKI administrator to approve individual certificate requests in PKI Manager. The PKI administrator configures the enrollment pages to request specific information from the user during certificate enrollment, such as address or contact information, or other data only available to the user. The PKI administrator reviews each certificate enrollment request, verifies the information provided, and approves or rejects the request, as appropriate. Symantec recommends that you reject any certificate request whose information is incorrect, and have the user enroll again, using the correct information.
- **AD/LDAP authentication** automatically approves authorized certificate requests based on user name and password in an AD or an LDAP source. PKI Enterprise Gateway must be installed in a customer's data center and integrated with an AD or an LDAP source.
  When users submit certificate enrollment requests, PKI Enterprise Gateway compares the data in the requests with the LDAP source. If the data matches, PKI Enterprise Gateway approves certificate requests, signs the certificate request with a Registration Authority (RA) certificate. It then sends the signed certificate request to the Certificate Issuance Center. If the data does not match, PKI Enterprise Gateway rejects the certificate request and gives an error message to the user.
- **Third-party client application for PKI Web Services** allows your client application to enroll for and approve certificates programmatically. An administrator can integrate the API provided with PKI Web Services into a client application to allow enrollment and approval.

## Certificate Validation

When a user or device authenticates using a certificate, the certificate must be validated. Symantec Managed PKI provides the following certificate validation tools:

- Certificate Revocation List (CRL): Many third-party products have the ability to use CRLs to check the current status of certificates (valid, suspended, revoked, and so on). A CRL is a black list of revoked certificates that have not yet expired. These products can be configured to download and check most recent CRL on a regular basis. If a certificate appears on the CRL, these products deny access to the online service (that is, they do not authenticate the user or device onto networks, digitally sign documents, and similar). Symantec produces a CRL at least once every 24 hours.
- Online Certificate Status Protocol (OCSP): Many third-party products verify the current status of certificates (valid, suspended, revoked, and so on) using OCSP. Although both CRLs and OCSP provide certificate status, OCSP does not experience the time delay between the certificate's revocation and when the next CRL is produced. Symantec's OCSP tool, Trusted Global Validation (TGV), is updated in near-real time if a certificate's status changes.
- PKI Web Services: If you have implemented the PKI Web Service, you can also programmatically obtain status information for a certificate using the PKI Web Services API.

## Managed PKI Service Test Drive

Managed PKI offers a free trial option that provides a full-featured Managed PKI account valid for 180 days and capable of supporting up to 100 users. You can sign up directly at http://www.symantec.com/theme.jsp?themeid=free-trial or visit the main website at http://www.symantec.com/managed-pki-service.

Use Managed PKI Service Test Drive to try out Managed PKI before you purchase it. You can also use as a sandbox to work with different configurations before rolling them out to your actual users.

## Token, Smart Card, and Security Device Options

Hardware tokens, smart cards, and similar security devices improve the security of certificates by limiting unauthorized access to them. You can use these tokens to protect your Managed PKI administrator certificates as well as your users' certificates. PKI Client and certificates issued by Managed PKI can be used with many types of hardware tokens, smart cards, and similar security devices.

Note that some security devices depend on Cryptographic Security Providers (CSPs) or other client software in addition to PKI Client.

See *Managed PKI™ v8.14 Release Notes* for a list of the supported security devices and any third-party dependencies.

### eToken from SafeNet

Symantec is an authorized reseller of the eToken from SafeNet (including PRO, NG-OTP, and NG-FLASH tokens). The Adobe CDS option requires that you store end-user certificates on tokens.

SafeNet eTokens meet Federal Information Processing Standard (FIPS) 140-2 and Common Criteria standards, and come with a three-year warranty as described in the Warranty Information Supplement.

### SafeNet Hardware Security Modules (HSMs)

If you implement PKI Enterprise Gateway or PKI Web Services, you must obtain an RA certificate to secure communications with the Certificate Issuing Center. You must also store the RA certificate in an HSM. HSMs protect the RA certificates and allow them to perform cryptographic functions such as signing end-user certificate requests. Managed PKI supports only SafeNet® Luna® HSMs. Symantec is an authorized reseller of SafeNet Luna hardware security modules (HSMs). It consists of Luna PCI cards, Luna SA network appliances, and Luna PCM tokens.

SafeNet Luna HSMs meet Federal Information Processing Standard (FIPS) 140-2 and Common Criteria standards, and come with a one-year warranty. However, Symantec resells optional SafeNet extended warranty programs for an additional charge.

### Intel® Identity Protection Technology (IPT) with PKI Tokens

Managed PKI allows you to issue certificates for Intel IPT with PKI. These Intel IPT with PKI-compliant certificates can be embedded in the firmware of the device, turning the device into an Intel IPT with PKI token. These certificates are managed through PKI Client (PKI Client treats Intel IPT with PKI as a third-party CSP).

## Specialized PKI Usage Scenarios

The Symantec Managed PKI service can offer certificates for certain specialized uses such as LTE Base Station security or Smart Meter security. In addition, the Symantec Managed PKI service can also provide support for device manufacturers ordering large numbers of certificates (asynchronously, in batches).

## LTE Base Station Security

Key network elements in a wireless operator LTE network, such as a base station (or eNodeB) or the Security Gateway (SEG) need to be secured using digital certificates as per the 3GPP standards (3GPP TS 33.310 section 9.4). The standards specify both a vendor certificate which is embedded at manufacturing time, as well as an operator certificate which an operator controls. Managed PKI's LTE base station security solution focuses on the operator certificates. Typically these certificates need to be delivered over a CMP v2 interface. In some cases, the certificates may be delivered in response to a CSR uploaded manually. In order to create an LTE base station security solution, your Managed PKI account is configured to support LTE, and a custom private CA. The LTE certificate hierarchy is loaded to your account. For further information on setting up an LTE base station security solution using the Symantec Managed PKI service, refer to *Managed PKI® Configuring an LTE Operator Base Station Solution*.

## Smart Meter Security

Smart Meters are an integral part of a growing trend of Smart Grid infrastructures being proposed and implemented around the world. These infrastructures are designed to tackle the problems of an ever-increasing need for energy while also to manage climate change and other environmental impact. The standards specify both a vendor certificate which is embedded at manufacturing time, as well as an operator certificate which an operator controls. Managed PKI's Smart Meter security solution focuses on the operator certificates. Typically these certificates need to be delivered using a programmatic interface (Web Services). They are often requested on behalf of the smart meters and then automatically pushed down onto the smart meters. In some cases, the certificates may be delivered in response to a CSR uploaded manually. In order to create a Smart Meter security solution, your account is configured with a custom private CA for the Smart Meter certificate hierarchy. For further information on setting up a Smart Meter security solution using the Symantec Managed PKI service, refer to *Managed PKI® Configuring a Smart Grid Solution*.

## Manufacturers Certificate Solution

The Machine-to-Machine (M2M) interaction space (known as the Internet of Things, or IoT) has a growing need to embed digital certificates into a variety of devices. These devices connect to each other and autonomously communicate with each other. Early examples of such devices include cable modems, digital TVs, and WiMAX-compliant devices. The market is expected to evolve into a broad range of devices in the future-including network elements and smart meters, but going far beyond that. Managed PKI provides a flexible way to configure the certificate profiles

that can be used in a batch interface to request these certificates. Device Manufacturers upload requests for certificates providing a batch of device identifiers and receive a batch of certificates and private keys. It can then be injected into devices within the secure confines of the manufacturing process. The exact CA, the base certificate template, and the certificate profile options may differ based on the nature of the device being manufactured. For further information on setting up a specific Manufacturer solution using the Symantec Managed PKI service, contact your Symantec representative.

# Hardware and Software Requirements

Your hardware and software requirements vary, based on how you deploy Managed PKI. For details on the hardware and software that Managed PKI supports, refer to *Managed PKI™ v8.13 Release Notes*.

See "Managed PKI Components" on page 8.

# Symantec Certification Practices Statement

Managed PKI allows your organization to provide certificates to your organization's employees or other constituents, while Symantec performs the back-end public key infrastructure (PKI) functions. These certificates can be either public certificates for worldwide use within the Symantec Trust Network (STN), or private certificates for use within your organization's own private domain. Using Managed PKI, your organization can create its own CA without the delay, expense, and overhead of constructing its own secure facility and performing its own PKI backbone functions. Your organization can also act as a *Local Registration Authority* for the Managed PKI Class 2 (Individual) CA within the STN.

A CA is an entity that issues, manages, revokes, and renews certificates, and assists people with performing certificate lifecycle tasks (retrieving, renewing, revoking, and so on). In some cases, the CA delegates these functions to a Local Registration Authority (LRA). Symantec owns and operates the CAs within the STN. Optionally, your organization can create its own CA through Managed PKI.

In each of these cases, the Managed PKI administrator assists people in requesting certificates, approving their certificate requests, and revoking their certificates. It also performs the other functions that are mentioned in this document on behalf of your organization. If you perform these functions for STN certificates, you act as a Local Registration Authority Administrator as described in the Symantec Certification Practice Statement (CPS), available at https://www.symantec.com/about/profile/policies/repository.jsp.

For federal agencies, Managed PKI meets all auditing requirements for FISMA (Federal Information Security Management Act) compliance.

# Related Documents

The following Symantec documents are available on the *Resources* page of PKI Manager and provide additional information about the Managed PKI service:

- *Managed PKI Release Notes* provide last-minute information about the release.
- *Symantec™ Managed PKI® Overview* (this document) describes the Managed PKI solution and outlines the process for starting with it. Managed PKI also includes the quick reference guides that describe how to configure Managed PKI to issue certificates specific to your needs.
- *Symantec™ PKI Client Administrator's Guide* describes how the PKI Client works and how to install and configure it for your users.
- *Symantec™ PKI Client Writing Post-processing Scripts Guide* describes how to write scripts to perform operations on certificates (typically to integrate them with your users' applications) once they have been issued.
- *Symantec™ PKI Enterprise Gateway Deployment Guide* describes how to install and configure PKI Enterprise Gateway to programmatically enroll and renew certificates using your enterprise user stores and certificate policies.
- *Symantec™ PKI Enterprise Gateway Autoenrollment Server Deployment Guide* describes how to install and configure the optional Autoenrollment server component of PKI Enterprise Gateway to programmatically manage issued certificates using your enterprise user stores and certificate policies.
- *Symantec™ Managed PKI PKI Web Services Developer's Guide* describes how to integrate Managed PKI Web Services with your RA applications to programmatically perform certificate lifecycle operations for your users.
- Managed PKI includes the integration guides that describe how to integrate your user certificates with common third-party applications and protocols.

# Managed PKI Contact Information

Use the following URLs and contact information to obtain additional information about Managed PKI or Symantec products in general. You can also obtain technical help with your Managed PKI service. Complete technical support contact information is available in *Symantec™ User Authentication Support and Service Overview*.

## Managed PKI Technical Support

- On the Web at http://www.symauth.com/support/contact/index.html#support4
- Call +1-520-477-3104 or 1-800-579-2848 and select the option for *Managed PKI technical support*.
- Send email to enterprise_pkisupport@symantec.com
- Obtain self-service help, including FAQs and troubleshooting tips on the Symantec Knowledge Center at https://knowledge.symantec.com/support/mpki-support/index.html.

## Symantec Repository

The Symantec Repository is a web resource that includes frequently asked question (FAQ) lists, copies of legal agreements, practices statements, and other useful information.

- Main URL: https://www.symantec.com/about/profile/policies/repository.jsp
- Symantec Certification Practices Statement (CPS): https://www.symantec.com/about/profile/policies/repository.jsp
- Managed PKI subscriber agreement: https://www.symantec.com/about/profile/policies/repository.jsp

Chapter 2

# Getting Started

This chapter includes the following topics:



## About Your Strategy for Authentication

The single most important decision that you need to make when getting started with Managed PKI is to define your strategy for authentication. This strategy is critical for determining how you configure Managed PKI.

Your strategy for authentication is:

- How you identify trusted users and devices
- What types of credentials (certificates) to issue in order to meet your security needs
- How to provide these trust credentials to your users and devices
- Where the certificates reside when issued

The effort that is required to define these vary depending upon your infrastructure and your user base.

- Simple implementations (where all of your users are in same directory), require the least effort. This implementation is not always scalable for large enterprises or complex network topologies.

- Complex implementations require more planning and configuration. It works better if you have multiple user stores (or multiple groups of users who need different types of certificates), or a complex network topology.

The following topics discuss the initial questions that you must answer to prepare for implementing Managed PKI services. You must familiarize yourself with the certificate profile configuration options that you need to set prior to issuing your first certificates.

# Identify Your Trusted Users and Devices

The most common way to identify your trusted users and devices is to prepare a user store and group users and devices into categories (or profile groups). If you have only one group of users and they all need one type of certificate (to enable secure email for all employees, for example), your group of trusted users is easily identified. However, you may need multiple groups, or multiple groups for multiple purposes.

For example, you might create one group named “Sales” in your existing employee database that contains all of your employees in the Sales division. You can create a second group named “IT” that contains all of the IT employees in your employee database. Alternatively, you might have one group of local users who access your virtual private network (VPN) from their workstation. There is another group of remote users who access your VPN with a variety of mobile devices. In these latter cases, you must define different groups for each category.

# Define What Certificates to Issue

As you defined different groups of users to receive certificates, you must also define the types of certificates each user should receive. This depends upon what you need your certificates to do. Managed PKI provides a number of certificate profile templates that you configure. The resulting certificate profiles allow you to issue the certificates that meet your PKI needs. These templates also allow you to define:

- How you will provide the certificates to your users. For example, will Managed PKI send an enrollment link? Will approval of the enrollment request be automatic?
- Where the certificates reside after they are issued. For example, will they reside in the users computer, mobile device, or on a hardware token, smart card, or similar security device? Will they be stored in a local user store?

See “Certificate Profiles” on page 24.

# Choose Deployment Options

Managed PKI allows a mixture of deployment options. You can choose which components to host in your enterprise site, and which to host in the cloud. The following sections describe two possible ways you can deploy components. However, you choose the combination of deployment configurations and tools based on your PKI needs. Additionally, you may modify your configuration at any time, as your organizational needs change.

## Cloud-based Deployment

In this deployment, the majority of the Managed PKI components (including the account, certificate, and key management tools) are hosted at Symantec. No components are installed on your end except PKI Client (which, if implemented, must always reside on the end-user computer). This solution provides the following benefits:

- Simple and most cost-efficient set-up. Simply access PKI Manager and configure your certificate profiles to begin issuing certificates.
- A single management portal (PKI Manager) to manage all aspects of the certificate lifecycle.
- Support for the most common certificate implementations, such as email signing and encryption and Wi-Fi and VPN certificates.
- When users pick up their certificates, users are authenticated using an enrollment code or by manual authentication by an administrator.

## Enterprise-based Deployment

In this deployment, some of the Managed PKI components (the account, certificate, and key management tools) reside at Symantec. However, you host your user store, directory integration tools, and RA certificates at your enterprise location. This solution provides the following benefits:

- Automation of the user's enrollment using your enterprise user store.
- The ability to manage most aspects of the certificate lifecycle from your enterprise user store to act as a local registration authority.
- Support for more advanced certificate implementations, which includes to perform certificate enrollment using the autoenrollment capabilities already present in the Windows environment.
- When users pick up their certificates, users can be authenticated using any authentication method, including against your Active Directory or LDAP directory, or using PKI Web Services.

As a more complex solution, an enterprise-based deployment requires additional set-up.

- If you implement PKI Enterprise Gateway and the optional Autoenrollment server, you need to install these components. You must also obtain an RA certificate (through PKI Manager) and store it in an HSM. You must configure PKI Manager to recognize these components.
  See *Symantec™ PKI Enterprise Gateway Deployment Guide* and *Symantec™ PKI Enterprise Gateway Autoenrollment Server Deployment Guide* for detailed procedures.
- If you implement PKI Web Services, you must obtain an RA certificate (through PKI Manager) and store it in an HSM. You must integrate PKI Web Services with your client applications to perform certificate lifecycle tasks.
  See *Symantec™ Managed PKI PKI Web Services Developer's Guide* for detailed procedures.
- If you implement the Transaction Signing API, you must obtain a signing authority certificate (through PKI Manager) and optionally store it in an HSM, and obtain an SSL server certificate. You must integrate the Transaction Signing API with your client applications to secure and sign your users' transactions.
  See *Managed PKI® Transaction Signing API Developer's Guide*.

See "About Symantec Managed PKI Certificates" on page 6.

# Certificate Profiles

Before you begin issuing certificates, you need to decide what attributes these certificates have. With Managed PKI, you configure the attributes of the certificates you issue using a certificate profile. Several certificate profiles templates are available to choose from, each with the additional configuration options that allow you to issue certificates uniquely suited for your needs. Creating multiple certificate profiles with different options allows you to issue many different types of certificates.

All certificate profiles issue certificates using seats from the user seat pool, except those created using the Computer certificate profile template. The computer certificate profile template issues certificates using seats from the device seat pool.

You can define each profile as a test or a production profile. Use the certificates that are issued using a test profile to test that the certificates that you issue work as you expect. Note that test certificates are still valid certificates, so you should take care when issuing these certificates that they are not used in production environments.

The following sections list the different certificate profiles available in PKI Manager and the options you can configure for them. Not all options are configurable for

each certificate profile template; some options are locked based on the certificate profile type.

Table 2-7 lists the options that are configurable for each template.

## Available Certificate Profile Templates

Managed PKI includes a standard set of certificate profile templates. These certificate profile templates that are listed in the following table enable you to issue the majority of the certificate types any enterprise may need.

Table 2-2 lists additional templates that are available for specialized account types and needs. These additional certificate profile templates require a custom implementation. Contact your Symantec representative for additional information about these templates.

Table 2-1 describes the standard Certificate profile templates.

**Note:** Not all templates are available for all accounts.

**Table 2-1** Standard Certificate profile templates

| Certificate Profile | Description |
|---|---|
| Adobe® CDS | Issues certificates that end users can use to digitally sign and protect Adobe PDF documents. End users must store these certificates on smart cards (certificates that are issued by Test Drive accounts can be stored in software certificate stores). |
| Domain Controller | Issues certificate that can be used to authenticate your Active Directory domains. |
| Computer | Issues certificates for the domain-joined systems that can be used by computers or other devices to authenticate themselves to your enterprise network or other devices. |
| Code Signing | Issues a limited number of certificates from a private CA that can be used to digitally sign developer code under your enterprise hierarchy.<br>For larger volumes of code signing certificates or for certificates in public hierarchies, use the public Code Signing offerings available separately from Symantec. |
| Secure Email | Issues certificates that end users can use to digitally sign and encrypt emails using S/MIME. |

**Table 2-1** Standard Certificate profile templates *(continued)*

| Certificate Profile | Description |
|---|---|
| Client Authentication | Issues certificates that end users can use to authenticate themselves to your enterprise resources (VPNs, web sites, or similar services). |
| Smart Card Logon | Issues certificates to the security devices that end users can use with the Windows smart card logon feature to authenticate themselves to your enterprise resources. These certificates must be stored on a security device such as a smart card, token, or similar security device that supports Windows smart card logon.<br>**Note:** To work properly with Windows smart card logon, the security device must use or implement a (virtual) smartcard reader. Some security devices like Intel Identity Protection (IPT) or Trusted Platform Module (TPM) may not provide support for this virtual reader on all platforms. |
| IPSec Authentication | Issues the server certificates that can be used to enable Internet Protocol Security (IPSec). |
| Offline IPSec Authentication | Issues the IPSEC Computer certificates that are used for device to device communication using the IPSec protocol |
| Windows® EFS | Issues certificates that end users can use to enable folder and file encryption using Microsoft® Windows Encrypting File System. |
| Windows® EFS Recovery | Issues certificates that EFS Recovery administrators can use to recover data previously encrypted using Microsoft® Windows Encrypting File System. |
| Secure Email Gateway | Issues certificates for secure email gateways. |
| Adobe® CDS Organization | Enables an organization to issue the certificates that perform digital authentication of Adobe PDF documents. |
| MDM | **For use by MDM vendors only:** Enables Mobile Development Management (MDM) vendors to issue device identity certificates down to the mobile devices before pushing the encrypted profile (for VPN, Wi-Fi and so on) to the user's mobile device. |
| Microsoft® Wi-Fi | Issues certificates that end users can use to authenticate themselves to a Microsoft® Wi-Fi network. |

**Table 2-1** Standard Certificate profile templates *(continued)*

| Certificate Profile | Description |
|---|---|
| OpenADR | Issues the OpenADR VTN and the VEN device certificates to manufacturers for the products that are compliant with the OpenADR Alliance specification. OpenADR certificate serves as an identity certificate for each device as it gets enrolled on the network. Each certificate binds a device MAC address to an RSA key pair, allowing the device to uniquely authenticate itself to the network using its private key. |
| OpenCable | Issues the device certificates that get embedded in the OpenCable compliant devices at the time of manufacture. OpenCable certificates provide the basis for a number of security services including data confidentiality, content integrity, and hardware authentication for the devices. |
| PacketCable | Issues the device certificates that get embedded in the PacketCable compliant devices at the time of manufacture. PacketCable certificates provide the basis for a number of security services including data confidentiality, content integrity, and hardware authentication for the devices. |
| CableHome | Issues the device certificates that get embedded in the CableHome compliant devices at the time of manufacture. CableHome certificates provide the basis for a number of security services including data confidentiality, content integrity, and hardware authentication for the devices. |
| Adobe® Individual | Issues certificates that end users can use to digitally sign and protect Adobe PDF documents. |
| Adobe® Organization | Enables an organization to issue certificates that perform digital authentication of Adobe PDF documents. |
| Generic Server | Enables an organization to issue customized server certificates commonly needed to enable Internet Protocol Security (IPSec), authenticate computers or other devices to your Active Directory domains, or to issue private server certificates. |
| Private Server | Issues a limited numbers of private Server certificates to facilitate authentication for server entities under your private enterprise CA hierarchy, to provide the verification that the server entity is internally trusted.<br>**Note:** For larger volumes of SSL certificates or for certificates in public hierarchies, use the public SSL offerings available separately from Symantec. |

**Table 2-1** Standard Certificate profile templates *(continued)*

| Certificate Profile | Description |
|---|---|
| Generic Device Authentication | Enables an organization to issue customized device certificates commonly needed for computer client to server, server to server, and device to server authentication. |

Table 2-2 describes the custom Certificate profile templates.

**Table 2-2** Custom Certificate profile templates

| Certificate Profile | Description |
|---|---|
| LTE Operator Base Station | Issues certificates that are compliant with Long Term Evolution (LTE) operator certificates. |
| Smart Grid | Issues operator device, Server, and Push certificates compatible with Smart Grid technology. |

# Primary Certificate Options

Table 2-3 describes the primary certificate options that you can configure.

**Table 2-3** Primary certificate options

| Option | Description |
|---|---|
| Enrollment method | Enrollment method is the methods and tools for users to install and manage their certificates:<br>■ PKI Client<br>■ OS/browseriOS Enrollment method<br>■ Android<br>■ iOS<br>■ Microsoft® Autoenrollment<br>■ CSR<br>■ SCEP<br>■ PKI Web Services<br>The enrollment method also defines how the certificates are renewed.<br>See "Renewal Method" on page 33. |

**Table 2-3** Primary certificate options *(continued)*

| Option | Description |
|---|---|
| Authentication method | The authentication method is how a certificate enrollment request gets user information, and how the enrollment request is authenticated when the certificate is generated:<br>■ Enrollment code<br>■ Active Directory<br>■ LDAP<br>■ Manual approval<br>■ 3rd party application (for PKI Web Services) |
| Certificate store | The certificate store is where the certificate is installed when a user gets a new certificate:<br>■ Security device (the certificate is installed on a smart card, token, or similar security device)<br>■ Computer (the certificate is installed on the computer on which the user enrolls)<br>This option may also allow you to select the cryptographic security provider (CSP) used to perform cryptographic operations. If a CSP requires additional hardware or software, make sure that it is installed on the user's device before issuing certificates. |
| Private key security level | Private key security level sets certain certificate management requirements around the private key that help prevent tampering, theft, or other certificate compromise:<br>■ High<br>■ Medium<br>■ Low |

# Certificate Fields

Table 2-4 describes the certificate fields that you can configure for your certificates. You can also add more certificate fields, as needed.

**Table 2-4** Certificate fields

| Certificate Fields | Description |
|---|---|
| Subject DN | Configure the contents and appearance of Subject Domain Name fields that appear in the certificate:<br>■ Common Name (CN)<br>■ Email<br>■ Organizational Unit (OU)<br>■ Country<br>■ Organization (O)<br>**Note:** Not all fields appear in all certificate profile templates.<br>You can also include additional Subject Domain Name fields, as needed. You need to define where PKI Manager gets the information to populate this field for the enrollment request. For example, from an LDAP/AD or entered by the user during enrollment.<br>The exact values you can configure for each of these fields depends upon the certificate profile type. |
| Subject Alt Name | You can include Subject Alt Name fields, as needed. You need to define where PKI Manager gets the information to populate this field for the enrollment request. For example, from an LDAP/AD or entered by the user during enrollment.<br>The exact values you can configure for each of these fields depends upon the certificate profile type. |
| Key Usage (KU) and Extended Key Usage (EKU) | You can define key usage and extended key usage values to include in the certificate. You need to define whether the value must appear in the certificate (Criticality).<br>Some of the KU and the EKU values are selected by default. Additionally, if a value is required for a specific profile, you cannot deselect it. |

# Additional Certificate Options

Table 2-5 describes the additional certificate options you can configure for your certificates. Not all options appear in all certificate profile templates.

**Table 2-5** Additional certificate options

| Certificate Option | Description |
|---|---|
| Validity period | Sets the active life span for an issued certificate. |

**Table 2-5** Additional certificate options *(continued)*

| Certificate Option | Description |
|---|---|
| Key escrow | Set whether to automatically back up the certificate' private key and where the private key is stored (at Symantec or in a local user store). If set to **No** and the private key is damaged or no longer available, a new certificate needs to be issued.<br><br>For the certificate profiles that issue S/MIME certificates (such as Secure Email), also determine whether multiple certificates can be issued to a single user. If enabled, the user can enroll for multiple certificates for multiple devices, against the same certificate profile. Managed PKI returns the same certificate for each enrollment request. Additionally, Managed PKI returns this certificate for all key recovery requests. |
| Publish to public directory | Set whether to publish the certificate's public key to the Symantec™ PKI directory.<br><br>If set to **Yes**, partners, customers, and others outside your company can download the public key to quickly enable secure communication. Otherwise, they need to send an email to, and receive an email from, a user before communications can be secured. |
| Publish to company directory | Set whether to publish the certificate's public key to your company's user directory.<br><br>If set to **Yes**, users within your company can download the public key to quickly enable secure communication. Otherwise, they need to send an email to, and receive an email from, a user before communications can be secured |
| Renewal window | The time period before a certificate's expiration date during which a certificate can be renewed.<br><br>A renewed certificate is valid through the remaining renewal window, plus the new validity period, so your user won't lose any time on the certificate. |
| Delete inactive certificates | Sets whether PKI Client automatically deletes expired and revoked certificates.<br><br>If expired and revoked certificates are deleted, users cannot read emails encrypted with those certificates. |

**Table 2-5** Additional certificate options *(continued)*

| Certificate Option | Description |
|---|---|
| Make space for new certificate | Sets whether PKI Client will automatically delete older versions of a certificate when installing a newer version. Certificate renewal requires the older certificate, so this setting does not apply to certificates being renewed. This option is available only when the profile is configured to install the certificate in Adobe tokens or smart cards.<br>If set to **No** and there is insufficient space to install a new certificate, certificate installation will fail.<br>If set to **Yes**, users will not be able to read emails encrypted with a deleted certificate. |
| Signing algorithm | The algorithm that is used to sign the newly generated certificate key pair. Managed PKI supports the following signing and encryption algorithms:<br>■ SHA1 with RSA encryption<br>■ SHA256 with RSA encryption<br>If your account is configured for Ecliptic Curve Cryptography (ECC) or Digital Signature Algorithm (DSA), Managed PKI supports the following signing and encryption algorithms:<br>■ ECC 224 and 384. ECC is supported for the Client authentication and Microsoft Wi-Fi certificate profiles only. Certificate lifecycle operations are supported for certificates with ECC-based keys using Managed PKI Web Services.<br>■ DSA 2048-256 and 3072-256. DSA requires custom certificate profile templates. |
| Key size | The size of the cryptographic key that is used to generate the certificate key pair. |

## Authentication Field for Enrollment

If you configured Manual approval as your Authentication method, you can configure the additional authentication fields that appear on the enrollment page for your users. Use these fields to request information to uniquely identify the user (such as employee number or telephone number). The values your users enter in these fields appear in the enrollment request, and you can use these values to authenticate the user. This information does not appear in the certificate.

### Renewal Method

The manner by which a certificate is renewed depends upon the enrollment method.

Table 2-6 describes the method for certificate renewal, based on the enrollment method.

**Table 2-6** Certificate renewal methods

| Enrollment Method | How Certificates are Renewed |
|---|---|
| PKI Client | PKI Client prompts the user to renew the certificates that are PIN-protected. For the certificates that are not PIN-protected, PKI Client performs the renewal and installs the new certificate transparently. |
| OS/browser | Internet Explorer users receive an email containing a renewal link. Clicking the link takes the user to the PKI Certificate Services page for a new certificate. The user follows a renewal process similar to the enrollment process. FireFox users must enroll for a new certificate. |
| Android | Managed PKI supports only enrollment for Android certificates. |
| iOS | The user receives an email containing a renewal link. Clicking the link prompts the user to select a credential to authenticate the renewal. The user is then taken to the PKI Certificate Services page and the renewed certificate is installed. |
| Microsoft® Autoenrollment | The certificate is renewed transparently. Unless the PKI administrator configured the certificate profile to do so, the user is not notified of the renewal. |
| CSR | The user who obtained the original certificate receives an email containing a renewal link. Clicking the renewal link takes the user to the PKI Certificate Services page where the user enrolls for a replacement certificate. The user must generate a new CSR for enrollment. |
| SCEP | The third-party vendor manages the renewal process. |
| PKI Web Services | Your client application must track certificate renewals. Before the certificate expires, the user must enroll for a replacement certificate using the same procedures as the original enrollment. |

## Certificate Profile Configuration Matrix

Table 2-7 lists the different configuration options available to each certificate profile template.

If an option is marked as locked, the option cannot be configured for that certificate profile template.

**Table 2-7** Certificate profile templates

| Profile Name | Customizable options | Configurable/Locked |
|---|---|---|
| Adobe® CDS | Enrollment method | Locked on **PKI Client** |
| | Authentication method | Configurable |
| | Certificate store | Locked on **Security device** |
| | Private key security level | Locked on **High** |
| | Subject DN | All fields locked; can add fields. |
| | Subject Alt Name | Configurable |
| | Key Usage and Extended Key Usage | All fields locked. |
| | Additional certificate options | All options configurable except:<br>■ **Key escrow** (locked on **No**)<br>■ **Publish to company directory** (Locked on **No**) |
| Code Signing | Enrollment method | Locked on **CSR** |
| | Authentication method | Locked on **Manual Approval** |
| | Certificate store | Not applicable |
| | Private key security level | Not applicable |
| | Subject DN | Configurable |
| | Subject Alt Name | Not configurable |
| | Key Usage and Extended Key Usage | Locked to **Digital Signature** and **Code Signing** |
| | Additional certificate options | All options configurable except **Key escrow** (locked on **No**) |
| Computer | Enrollment method | Configurable |
| | Authentication method | Locked on **Active Directory** |
| | Certificate store | Locked on **Computer** |

**Table 2-7** Certificate profile templates *(continued)*

| Profile Name | Customizable options | Configurable/Locked |
|---|---|---|
| | Private key security level | Configurable |
| | Subject DN | All fields configurable except **Organization (O)**; can add fields. |
| | Subject Alt Name | Configurable; **DNS Name** is configured by default. |
| | Key Usage and Extended Key Usage | All fields that are locked except Extended Key Usage Criticality. |
| | Additional certificate options | All options configurable except:<br>■ **Key escrow** (locked on **No**)<br>■ **Publish to company directory** (Locked on **No**) |
| Domain Controller | Enrollment method | Configurable |
| | Authentication method | Locked on **Manual Approval** |
| | Certificate store | Not applicable |
| | Private key security level | Not applicable |
| | Subject DN | Only **Organizational Unit (OU)** field is editable: can add fields. |
| | Subject Alt Name | All fields locked; cannot add fields. |
| | Key Usage and Extended Key Usage | Configurable except Key Usage (KU) values cannot be deselected. |
| | Additional certificate options | All options configurable except **Key escrow** (locked on **No**) |
| Secure Email | Enrollment method | Configurable |
| | Authentication method | Configurable |
| | Certificate store | Configurable |
| | Private key security level | Configurable |
| | Subject DN | All fields configurable except **Organization (O)**; can add fields. |

**Table 2-7** Certificate profile templates *(continued)*

| Profile Name | Customizable options | Configurable/Locked |
|---|---|---|
| | Subject Alt Name | Configurable; **RFC822 Name** is configured by default. |
| | Key Usage and Extended Key Usage | Configurable except **Key Usage (KU)** values cannot be deselected. |
| | Additional certificate options | All options configurable except:<br>■ **Key escrow** (locked on **Yes**) |
| Client Authentication | Enrollment method | Configurable |
| | Authentication method | Configurable |
| | Certificate store | Configurable |
| | Private key security level | Configurable |
| | Subject DN | All fields configurable except:<br>■ Organization (O) (Locked to a fixed value)<br>■ Organizational Unit (OU) (Locked to a fixed value)<br>Can add fields |
| | Subject Alt Name | Configurable; **Other Name (UPN)** is configured by default. |
| | Key Usage and Extended Key Usage | Configurable except Extended Key Usage (EKU) values cannot be deselected. |
| | Additional certificate options | All options configurable except:<br>■ **Key escrow** (locked on **No**) |
| IPSec Authentication | Enrollment method | Configurable |
| | Authentication method | Locked on **Manual Approval** |
| | Certificate store | Not applicable |
| | Private key security level | Not applicable |

**Table 2-7** Certificate profile templates *(continued)*

| Profile Name | Customizable options | Configurable/Locked |
|---|---|---|
| | Subject DN | Only **Organizational Unit (OU)** field is editable: can add fields. |
| | Subject Alt Name | All fields locked; cannot add fields. |
| | Key Usage and Extended Key Usage | Configurable except Key Usage (KU) values cannot be deselected. |
| | Additional certificate options | All options configurable except **Key escrow** (locked on **No**) |
| Microsoft Wi-Fi | Enrollment method | Configurable |
| | Authentication method | Configurable. If it is set to OS/browser, the user must enroll for certificates using Internet Explorer on Windows XP or 7. |
| | Certificate store | Locked on **Computer** |
| | Private key security level | Locked on **Low** |
| | Subject DN | All fields configurable except:<br>■ Organization (O) (Locked to a fixed value)<br>■ Organizational Unit (OU) (Locked to a fixed value)<br>Can add fields |
| | Subject Alt Name | Configurable; **Other Name (UPN)** is configured by default. |
| | Key Usage and Extended Key Usage | Configurable except Extended Key Usage (EKU) values cannot be deselected. |
| | Additional certificate options | All options configurable except:<br>■ **Key escrow** (locked on **No**) |
| Smart Card Logon | Enrollment method | Locked on **PKI Client** |
| | Authentication method | Configurable |
| | Certificate store | Locked on **Security device** |

**Table 2-7** Certificate profile templates *(continued)*

| Profile Name | Customizable options | Configurable/Locked |
|---|---|---|
| | Private key security level | Locked on **High** |
| | Subject DN | All fields configurable except **Organization (O)**; can add fields. |
| | Subject Alt Name | Configurable; **Other Name (UPN)** is configured by default. |
| | Key Usage and Extended Key Usage | Configurable except Extended Key Usage (EKU) values cannot be deselected. |
| | Additional certificate options | All options configurable except:<br>■ **Key escrow** (locked on **No**)<br>■ **Publish to public directory** (Locked on **No**)<br>■ **Publish to company directory** (Locked on **No**) |
| Windows® EFS | Enrollment method | Configurable |
| | Authentication method | Configurable. If it is set to OS/browser, the user must enroll for certificates using Internet Explorer on Windows XP or 7. |
| | Certificate store | Locked on **Computer** |
| | Private key security level | Locked on **Low** |
| | Subject DN | All fields configurable except:<br>■ Organization (O) (Locked to a fixed value)<br>■ Organizational Unit (OU) (Locked to a fixed value)<br>Can add fields |
| | Subject Alt Name | Configurable |
| | Key Usage and Extended Key Usage | Configurable except:<br>■ Key Usage Criticality is locked on **False**. Extended Key Usage (EKU) values cannot be deselected. |

**Table 2-7** Certificate profile templates *(continued)*

| Profile Name | Customizable options | Configurable/Locked |
|---|---|---|
| | Additional certificate options | All options configurable except:<br>■ **Publish to public directory** (Locked on **No**)<br>■ **Publish to company directory** (Locked on **No**)<br>■ **Delete inactive certificates** (Locked on **No**) |
| Windows® EFS Recovery | Enrollment method | Configurable |
| | Authentication method | Configurable<br>If it is set to OS/browser, the user must enroll for certificates using Internet Explorer on Windows XP or 7. |
| | Certificate store | Locked on **Computer** |
| | Private key security level | Locked on **Low** |
| | Subject DN | All fields configurable except **Organization (O)**; can add fields. |
| | Subject Alt Name | Configurable |
| | Key Usage and Extended Key Usage | Configurable except:<br>■ Key Usage Criticality is locked on **False**. Extended Key Usage (EKU) values cannot be deselected. |
| | Additional certificate options | All options configurable except:<br>■ **Key escrow** (locked on **Yes**)<br>■ **Publish to public directory** (Locked on **No**)<br>■ **Publish to company directory** (Locked on **No**)<br>■ **Delete inactive certificates** (Locked on **No**) |
| Secure Email Gateway | Enrollment method | CSR |

**Table 2-7** Certificate profile templates *(continued)*

| Profile Name | Customizable options | Configurable/Locked |
|---|---|---|
| | Authentication method | Manual approval |
| | Certificate store | Not applicable |
| | Private key security level | Not applicable |
| | Subject DN | All fields configurable except:<br>■ Organization (O) (Locked to a fixed value)<br>■ Organizational Unit (OU) (Locked to a fixed value)<br>■ S/MIME GW<br>Can add fields |
| | Subject Alt Name | Configurable |
| | Key Usage and Extended Key Usage | Configurable |
| | Additional certificate options | All options configurable except:<br>■ Key escrow (locked on **None**) |
| Adobe® CDS Organization | Enrollment method | CSR |
| | Authentication method | Manual approval |
| | Certificate store | Not applicable |
| | Private key security level | Not applicable |
| | Subject DN | Subject DN has a DN qualifier as an optional field. |
| | Subject Alt Name | Configurable |
| | Key Usage and Extended Key Usage | Configurable except:<br>■ Key Usage Criticality is locked on **False**. Extended Key Usage (EKU) values cannot be deselected. |
| | Additional certificate options | All options configurable except:<br>■ Key escrow (locked on **None**) |

**Table 2-7** Certificate profile templates *(continued)*

| Profile Name | Customizable options | Configurable/Locked |
|---|---|---|
| MDM | Enrollment method | Locked on **SCEP** |
| | Authentication method | Locked on **Enrollment Code** |
| | Certificate store | Not applicable |
| | Private key security level | Not applicable |
| | Subject DN | All fields configurable except:<br>■ Common Name (CN) (Locked to a fixed value)<br>■ Organization (O) (Locked to a fixed value)<br>■ Organizational Unit (OU) (Locked to a fixed value)<br>Additional Organizational Unit (OU) field that is locked to fixed value (iOS SESSION) is included by default. Otherwise, can add fields. |
| | Subject Alt Name | Configurable |
| | Key Usage and Extended Key Usage | Configurable |
| | Additional certificate options | All options configurable except:<br>■ **Key escrow** (locked on **None**) |
| Private Server | Enrollment method | Configurable |
| | Authentication method | Locked on **Manual Approval** |
| | Certificate store | Not applicable |
| | Private key security level | Not applicable |
| | Subject DN | Only **Organizational Unit (OU)** field is editable: can add fields. |
| | Subject Alt Name | All fields locked; cannot add fields. |
| | Key Usage and Extended Key Usage | Configurable except Key Usage (KU) values cannot be deselected. |

**Table 2-7** Certificate profile templates *(continued)*

| Profile Name | Customizable options | Configurable/Locked |
|---|---|---|
| | Additional certificate options | All options configurable except **Key escrow** (locked on **No**) |
| LTE Operator Base Station | Enrollment method | Locked on **LTE** |
| | Authentication method | Locked on **LTE**. Any IP addresses or trusted CAs that you have configured for the account is displayed here. |
| | Certificate store | Not applicable |
| | Private key security level | Not applicable |
| | Subject DN | Configurable. |
| | Subject Alt Name | All fields locked; cannot add fields. |
| | Key Usage and Extended Key Usage | Configurable. |
| | Additional certificate options | All options configurable except **Key escrow** (locked on **No**) |
| Smart Grid | Enrollment method | Configurable |
| | Authentication method | Configurable. If it is set to OS/browser, the user must enroll for certificates using Internet Explorer on Windows XP or 7. |
| | Certificate store | Locked on **Computer** |
| | Private key security level | Locked on **Low** |
| | Subject DN | All fields configurable except:<br>■ Organization (O) (Locked to a fixed value)<br>■ Organizational Unit (OU) (Locked to a fixed value)<br>Can add fields |
| | Subject Alt Name | Configurable; **Other Name (UPN)** is configured by default. |

**Table 2-7** Certificate profile templates *(continued)*

| Profile Name | Customizable options | Configurable/Locked |
|---|---|---|
| | Key Usage and Extended Key Usage | Configurable except Extended Key Usage (EKU) values cannot be deselected. |
| | Additional certificate options | All options configurable except:<br>■ **Key escrow** (locked on **No**) |
| OpenADR | Enrollment method | Locked on **Batch** |
| | Authentication method | Locked on **Batch** |
| | Certificate store | Locked on **Computer** |
| | Subject DN | All fields configurable except:<br>■ Organization (O) (Locked to a fixed value from account)<br>■ Organizational Unit (OU)<br>Can add fields |
| | Key Usage and Extended Key Usage | Locked |
| | Additional certificate options | Duplicate certificates allowed |
| OpenCable | Enrollment method | Locked on **Batch** |
| | Authentication method | Locked on **Batch** |
| | Subject DN | All fields configurable except:<br>■ Organization (O) (Locked to a fixed value from account)<br>■ Organizational Unit (OU)<br>Can add fields |
| | Key Usage and Extended Key Usage | Locked |
| | Additional certificate options | Duplicate certificates allowed |
| PacketCable | Enrollment method | Locked on **Batch** |
| | Authentication method | Locked on **Batch** |

**Table 2-7** Certificate profile templates *(continued)*

| Profile Name | Customizable options | Configurable/Locked |
|---|---|---|
| | Subject DN | All fields configurable except:<br>■ Organization (O) (Locked to a fixed value from account)<br>■ Organizational Unit (OU)<br>Can add fields |
| | Key Usage and Extended Key Usage | Configurable |
| | Additional certificate options | Duplicate certificates allowed |
| CableHome | Enrollment method | Locked on **Batch** |
| | Authentication method | Locked on **Batch** |
| | Subject DN | All fields configurable except:<br>■ Organization (O) (Locked to a fixed value from account)<br>■ Organizational Unit (OU)<br>Can add fields |
| | Key Usage and Extended Key Usage | Locked |
| | Additional certificate options | Duplicate certificates allowed |
| Adobe® Individual | Enrollment method | Configurable |
| | Authentication method | Configurable |
| | Certificate store | Configurable |
| | Private key security level | Configurable |
| | Subject DN | Configurable. All fields locked expect **Organizational Unit** |
| | Subject Alt Name | Configurable |
| | Key Usage and Extended Key Usage | All fields locked except Extended Key Usage Criticality. |
| | Additional Extensions | Two more additional extension can be added, but cannot modify default additional extension. |

**Table 2-7** Certificate profile templates *(continued)*

| Profile Name | Customizable options | Configurable/Locked |
|---|---|---|
| | Additional certificate options | All options configurable except:<br>■ **Key escrow** (locked on **No**)<br>■ **Publish to company directory** (Locked on **No**) |
| Adobe® Organization | Enrollment method | CSR |
| | Authentication method | Manual approval |
| | Certificate store | Not applicable |
| | Private key security level | Not applicable |
| | Subject DN | Subject DN has a DN qualifier as an optional field. |
| | Subject Alt Name | Configurable |
| | Key Usage and Extended Key Usage | All fields locked except Extended Key Usage Criticality. |
| | Additional Extensions | Two more additional extension can be added, but cannot modify default additional extension. |
| | Additional certificate options | All options configurable except:<br>■ Key escrow (locked on **None**) |
| Generic | Enrollment method | Configurable |
| | Authentication method | Locked on**Manual approval** |
| | Certificate store | Not applicable |
| | Private key security level | Not applicable |
| | Subject DN | Configurable |
| | Subject Alt Name | Configurable |
| | Key Usage and Extended Key Usage | Configurable except Key Usage (KU) values cannot be deselected. |
| | Additional certificate options | All options configurable except **Key escrow**(locked on **No**) |

# Using PKI Manager

Once you have defined your trust strategy and configured your initial certificate profiles, you are ready to begin issuing certificates to your users. Log into PKI Manager at to begin your administrative tasks. From PKI Manager, you can:

- Further refine your certificate profiles, for example, to:
  - Customize enrollment field labels
  - Upload user instructions or post-processing scripts
  - Select user identifiers for certificate enrollment
  - Customize email templates
  - Change administrator contact information
- Add, edit, and remove administrators and users
- Add sub-accounts to group management tasks by assigned administrators, available certificate types, user base, and other criteria
- Enroll users for certificates or assist them to enroll for their own certificates
- Revoke, recover, and renew certificates for users
- Revoke certificates in bulk by using a .cvs template
- Migrate certificate profiles when your CAs are ready to expire or when you need to rekey
- Migrate certificate profiles when your CAs are ready to expire and you need to rekey
- Delete certificate profiles when you have accumulated the old profiles that are no longer in use
- Run reports of administrator, user, and certificate activity
- Invite administrators from other PKI Manager accounts to become administrators of other accounts
- Configure advanced options such as PKI Enterprise Gateway or PKI Web Services
- Manage accounts for SSL by clicking the MPKI for SSL link (for Managed PKI users who use SSL)

For additional information about using PKI Manager to manage users and certificates, refer to its associated help. Symantec also provides a series of quick reference guides to assist you in determining how to configure your certificate profiles to best fit your specific needs.

# Index

## Symbols



## A

## C

## D



## E

## F



## H



## I



## K



## L



## M

## N



## O



## P

## R



## S

## T



## U



## V



## W