WHITE PAPER:
SYMANTEC MANAGED PKI SERVICE
DEPLOYMENT OPTIONS

Symantec™ Managed PKI Service Deployment Options

Who should read this paper

This whitepaper explains some of the Symantec™ Managed PKI Service enterprise deployment options based on an organization's current enterprise identity management methods, application requirements, and staff capabilities; that are available to simplify or scale an enterprise's certificate lifecycle management process. It also covers the key features of the Symantec™ PKI Client, which when deployed provides an improved user experience for end-user applications.

Content

Introduction 1

Symantec Managed PKI Service 1

1.1 Key Features 1

1.2 Enterprise Deployment Modes 2

Symantec Managed PKI Enrollment Options 2

2.1 Enrollment Options 3

2.2 How to Choose an Enrollment Method 4

2.3 Symantec PKI Client Software 5

Selecting a the Right Certificate Enrollment Method and Lifecycle 8

Want to Try Before you Buy? 9

Introduction

Public Key Infrastructure (PKI) is a combination of hardware, software, facilities, people, policies, and processes. It can be leveraged to create, manage, store, distribute, and revoke digital certificates. Digital certificates provide a simple, stable, scalable, and highly secure method of authenticating devices and users.

Symantec™ Managed PKI Service is a managed service offering that allows organizations to outsource their infrastructure for managing digital certificates and leverage the best-practices and high availability of an expertly run certificate lifecycle platform.

This whitepaper explains some of the Managed PKI Service enterprise deployment options that are available to simplify or scale your enterprise's certificate lifecycle management process. This paper also covers the key features of Symantec™ PKI Client, which can be deployed to provide an improved user experience for end-user applications.

Symantec Managed PKI Service

Managed PKI provides a full-featured solution equivalent to any on-premise PKI system with additional features and benefits, including a global validation, twenty-four hours a day, seven days a week, 365 days a year monitoring, high availability operations, and full disaster recovery.

Built on Symantec's proven, globally managed, highly reliable infrastructure, Symantec Managed PKI Service reduces the cost and complexity associated with in-house PKI and focuses enterprises on delivering solutions, instead of infrastructure. It alleviates the burden of planning, building, and maintaining a PKI, while allowing enterprises to maintain internal control over digital certificate issuance, suspension, and revocation.

Depending on your current enterprise identity management methods, application requirements, and the capabilities of your staff, you may opt to manage all certificate related user information entirely in the Symantec PKI service, or integrate Managed PKI with your existing Active Directory® and Domain services. The following information will guide you through your options to help you make these decisions.

1.1 Key Features

- Broad, cross-platform client support for certificate-based applications including Windows®, Mac®, iOS®, Android, or any standards-based browser client
- Supports authentication, encryption, digital signing, access control, and non-repudiation certificates out-of-the-box with flexible settings
- Public root of trust and certificate validation services
- Templatized certificate format provisioning for common applications such as VPNs, 802.11x WiFi, Web applications, Secure S/MIME email, and Adobe® CDS
- Web-based dashboard with on-demand and scheduled reports
- Simplified and automated certificate lifecycle management capabilities
- Flexible identity management options, either 100 percent in the cloud, or through an on-premise gateway to Active Directory
- Auto-configuration capabilities for iOS clients or through Symantec PKI Client for Windows, Mac, or Android devices

1.2 Enterprise Deployment Modes

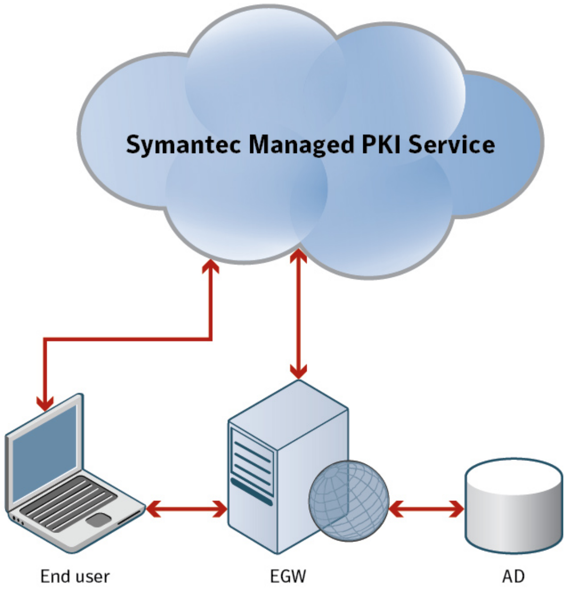
Organizations deploying a Symantec Managed PKI solution can choose a solely cloud-based identity management solution for simplicity, or deploy on-premise components to enable enterprise directory integration and automation. The available options are as follows:

1.2.1. Cloud deployment

In the cloud scenario, an enterprise can manage users directly in the cloud through Symantec® PKI Manager. Users can be managed through bulk operations as well as individually. The cloud service has a pass code distribution mechanism for authenticating the users before issuing certificates.

1.2.2. Hybrid enterprise deployment through Symantec™ PKI Enterprise Gateway

The hybrid enterprise mode takes advantage of a PKI Enterprise Gateway (EGW) to provide corporate directory integration, where the EGW effectively acts as a proxy for the cloud-based service. This allows certificate metadata to be automatically populated, and certificates can be directly published in the corporate directory. The PKI EGW also acts as local Registration Authority and integrates with Hardware Security Modules to protect key material. The diagram below illustrates the hybrid deployment mode:

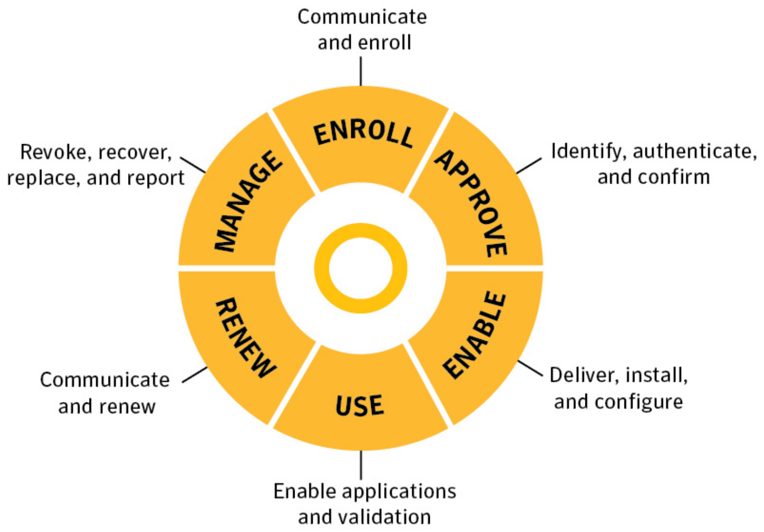


Symantec Managed PKI Enrollment Options

Certificate lifecycle management is a policy-based process. Each organization using Symantec Managed PKI Service has its own management objectives and therefore defines its own policies, such as the type of certificates they issues, the method of distributing certificates, and so on.

Typically, as a best practice, certificates are issued with a finite lifespan as defined by policy. When a certificate expires, if the choice is made to renew, a new certificate will be issued. Thus, the certificate management process is a lifecycle process.

The figure below illustrates the various processes within the certificate management lifecycle:


Communicate and enroll
ENROLL
Identify, authenticate, and confirm
APPROVE
ENABLE
Deliver, install, and configure
USE
Enable applications and validation
RENEW
Communicate and renew
MANAGE
Revoke, recover, replace, and report

2.1 Enrollment Options

After global account policies have been defined, the *enroll* and *approve* processes are the first steps toward defining certificate policies and issuing certificates. Symantec Managed PKI provides three distinct options for the *enroll* category. Within the provisioning for the chosen enrollment option are policies that will affect the *enable, use, and renew* options of the certificate's lifecycle.

At a high level the three enrollment options are:

2.1.1 Native browser enrollment

The native browser enrollment requires no software to be installed on the end user's computer, and works in both cloud and hybrid scenarios. Enrollment is performed through a Web interface available in either Firefox® or Internet Explorer® (IE); Web interfaces are continuously being added.

2.1.2 Microsoft auto-enroll client

Auto-enrollment using Microsoft auto-enroll client requires an Enterprise Gateway to be installed on-premise, and therefore works only for hybrid scenarios. Enrollment is performed through the Microsoft® auto-enrollment client distributed with the various versions of Windows; users will be automatically enrolled through their domain credentials.

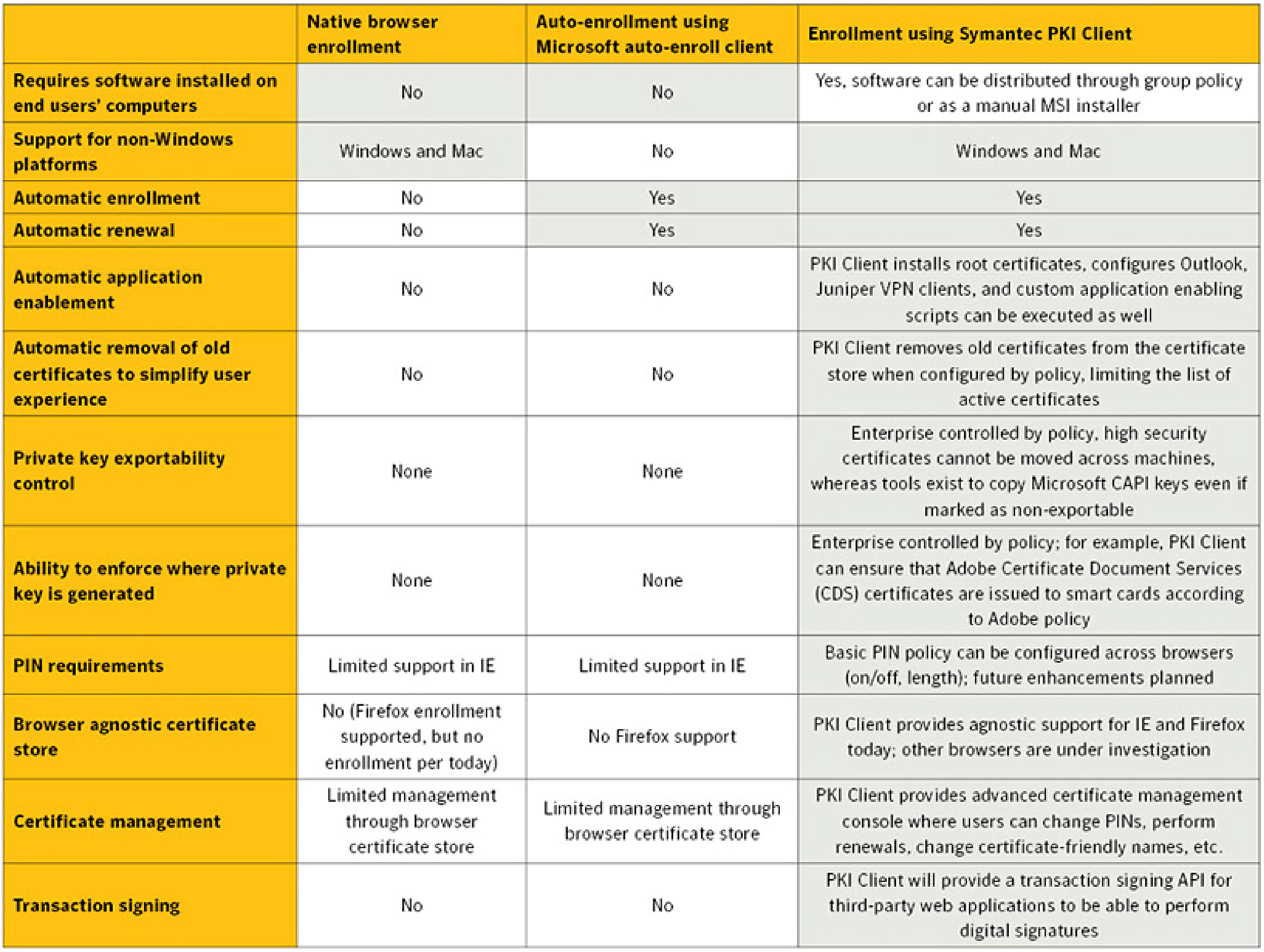
2.1.3 Enrollment using Symantec PKI Client

PKI Client is available for both cloud and hybrid scenarios, supports both Windows and Mac operating systems, and provides several lifecycle management functions as well as security policies that are not available with the other enrollment options. This does come at the cost of having to initially distribute software. However, once software is installed on an end user's computer the software automatically keeps itself current through Symantec's Live Update™ technology. Auto-enrollment is also supported by PKI Client. Auto-enrollment requires an Enterprise Gateway be installed on-premise so therefore works only for the hybrid scenario. Manual enrollment is performed through a Web interface available in either Firefox or IE; browsers are continuously being added. Once enrolled, the certificate lifecycle is managed by the client through automatic renewals.

2.2 How to Choose an Enrollment Method

When choosing an enrollment method, an organization must balance their requirements for security, usability, and scale. The method which is the most broadly supported across client platforms is browser-based enrollment. However, this method puts some of the enrollment processes in the hands of the end user. The most automated enrollment method makes the enrollment and client configuration process all but invisible to the end user. This is accomplished by utilizing either Symantec PKI Client software, or specialized built-in client capabilities such as iOS Simple Certificate Enrollment Protocol (SCEP)-based enrollment.

A feature comparison of the three Managed PKI enrollment options is provided below to help select the best enrollment method for users. In each row, the enrollment option that best supports that particular feature is highlighted.



	Native browser enrollment	Auto-enrollment using Microsoft auto-enroll client	Enrollment using Symantec PKI Client
Requires software installed on end users' computers	No	No	Yes, software can be distributed through group policy or as a manual MSI installer
Support for non-Windows platforms	Windows and Mac	No	Windows and Mac
Automatic enrollment	No	Yes	Yes
Automatic renewal	No	Yes	Yes
Automatic application enablement	No	No	PKI Client installs root certificates, configures Outlook, Juniper VPN clients, and custom application enabling scripts can be executed as well
Automatic removal of old certificates to simplify user experience	No	No	PKI Client removes old certificates from the certificate store when configured by policy, limiting the list of active certificates
Private key exportability control	None	None	Enterprise controlled by policy, high security certificates cannot be moved across machines, whereas tools exist to copy Microsoft CAPI keys even if marked as non-exportable
Ability to enforce where private key is generated	None	None	Enterprise controlled by policy; for example, PKI Client can ensure that Adobe Certificate Document Services (CDS) certificates are issued to smart cards according to Adobe policy
PIN requirements	Limited support in IE	Limited support in IE	Basic PIN policy can be configured across browsers (on/off, length); future enhancements planned
Browser agnostic certificate store	No (Firefox enrollment supported, but no enrollment per today)	No Firefox support	PKI Client provides agnostic support for IE and Firefox today; other browsers are under investigation
Certificate management	Limited management through browser certificate store	Limited management through browser certificate store	PKI Client provides advanced certificate management console where users can change PINs, perform renewals, change certificate-friendly names, etc.
Transaction signing	No	No	PKI Client will provide a transaction signing API for third-party web applications to be able to perform digital signatures

As the highlights in the table illustrate, the PKI Client is the preferred option for most categories. This resonates well with the vision behind Managed PKI, which in short is to revolutionize the digital certificate experience with dramatic enhancements in flexibility and usability; PKI Client is an integral part of this vision. The next section will look at some of the PKI Client differentiating features in detail.

2.3 Symantec PKI Client Software

PKI Client can issue and automatically renew Symantec Managed PKI software and hardware certificates for a simplified user experience that works across various Web browsers. This section describes some of the key features of PKI Client.

2.3.1 Streamlined PKI lifecycle management

PKI Client offers a uniform enrollment experience regardless of the browser that is used for enrollment. The certificate store is also browser agnostic, meaning the user can enroll in Firefox and have the certificate available for usage in IE. PKI Client supports auto-enrollment, where end users automatically have certificates installed based on their domain credentials.

One of the main issues facing enterprises is renewal of certificates before they expire. Symantec PKI Client automatically renews certificates that are not PIN-protected, and will ask the user to renew PIN-protected certificates well before they expiration date.

2.3.2 Centralized policy management for security and convenience

Policies dictating how credentials are secured on the client, such as user PIN and export policies, can be configured for PKI Client through PKI Manager. Policy also allows the enterprise to control which physical store to use for the certificates that are enrolled. This option is important in terms of ensuring that high security certificates, such as a smart card or USB token, end up in the appropriate store.

Friendly names for certificates can also be set through policy (as well as customized by the user), and provide the user a more recognizable credential for authentication. Furthermore, policy can dictate whether to remove certificates from the user's certificate store on renewal. This feature ensures that in scenarios where users do have to select between certificates, only relevant certificates show up in the list presented to the user.

2.3.3 Post-processing framework

After a certificate is enrolled on an end user's computer, it is still necessary for the user to configure the certificate for usage with their applications. To simplify the end user experience, PKI Client offers a post-processing framework that automatically takes care of the application configuration. The framework can also be extended to perform custom configurations. The following applications are supported by the post-processing framework out of the box:

- Juniper® VPN Client
- Cisco® VPN client
- Check Point® VPN client
- Outlook® 2007 and 2010
- Installation of root/intermediate certificates for IE and Firefox
- Install PKCS#11 module in Firefox (basically exposing the enrolled certificate in Firefox)
- Publish S/MIME encryption certificate to the user attribute in Active Directory for cloud scenarios
- Configure WiFi connections for Microsoft® WiFi client

2.3.4 PKI Client use cases

Studies have shown that PKI deployments are most successful when the certificates are made transparent to the user; so that end users are not required to make technical choices regarding certificates. Through the PKI Client integration with the Symantec Managed PKI Service and the post-processing framework, the certificate experience can largely be hidden from the end user.

Example use cases supported by the Symantec PKI Client include:

- WiFi PKI certificates for enterprise users authenticated through Active Directory credentials:
  - One simple PKI enrollment flow with very few clicks for ENROLL, APPROVE, and ENABLE:
    - Enroll the certificate using a Web interface
    - Authenticate the user with active directory credentials through Enterprise Gateway
    - The certificate is enabled for WiFi automatically by PKI Client
  - USE: no action required from user to authenticate to a WiFi network
  - RENEW: no action required from user, PKI Client will automatically renew the certificate and delete the expired certificate from the client computer
- SSL client authentication for enterprise Web site using Active Directory:
  - One simple PKI enrollment flow with very few clicks for ENROLL, APPROVE, and ENABLE:
    - Enroll the certificate using a Web interface
    - Authenticate the user with Active Directory credentials through Enterprise Gateway
    - Enable the certificate for client authentication in both Firefox and IE
  - USE: one click to choose the certificate identified by a friendly name
  - RENEW: no action required from user, PKI Client will automatically renew the certificate and delete the expired certificate from the client computer

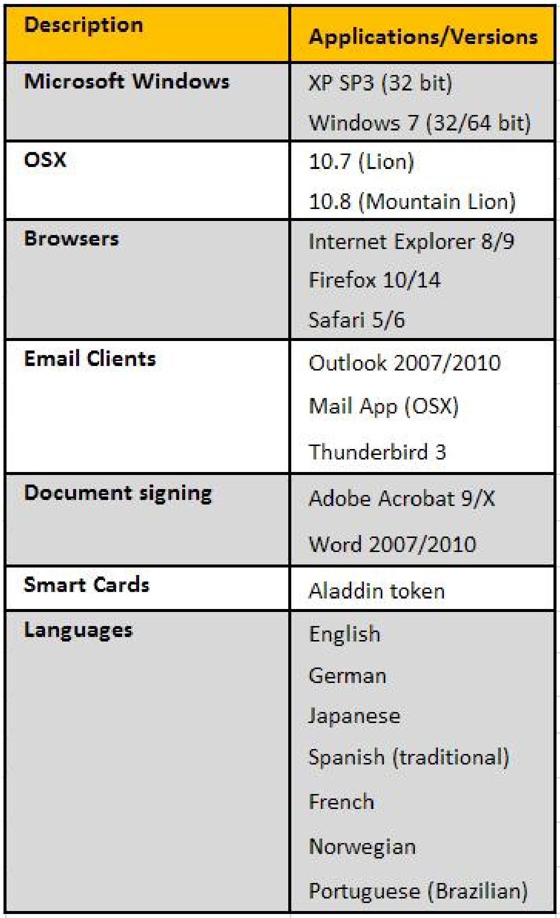
2.3.5 Certificate management console

The end user will be able to perform the following operations using the certificate management console provided by PKI Client console:

- Change PIN for a device
- Manually renew certificates
- Export certificates
- Import certificates
- View diagnostics information to help troubleshooting
- See a list of certificates on their system
- Be able to view certificate details of individual certificates
- Delete individual certificates
- Erase all certificates from a device

2.3.6 PKI Client support matrix

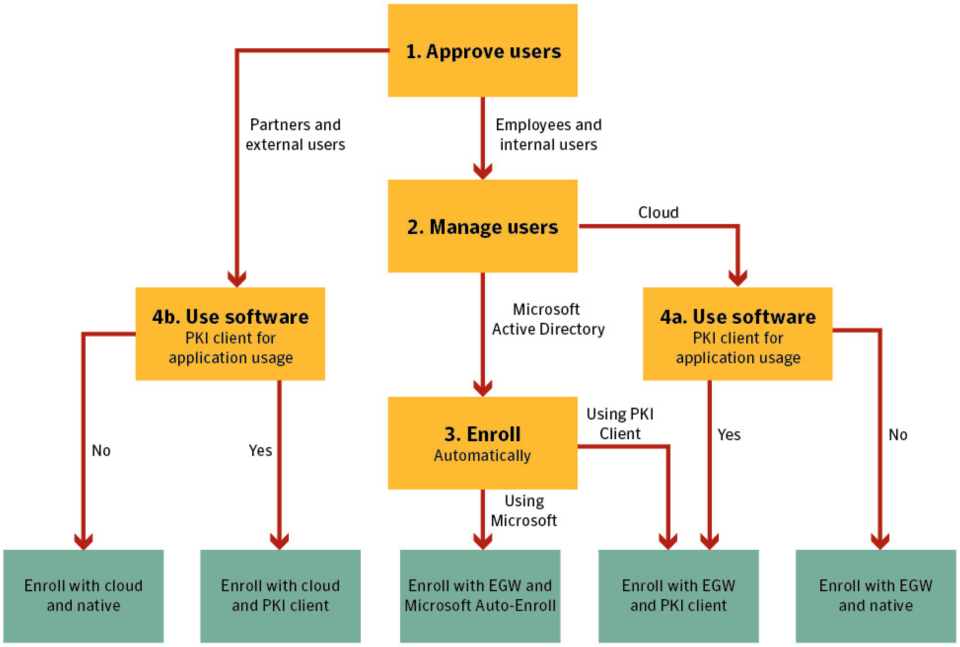
The table below provides the support matrix for PKI Client:



Description	Applications/Versions
Microsoft Windows	XP SP3 (32 bit) Windows 7 (32/64 bit)
OSX	10.7 (Lion) 10.8 (Mountain Lion)
Browsers	Internet Explorer 8/9 Firefox 10/14 Safari 5/6
Email Clients	Outlook 2007/2010 Mail App (OSX) Thunderbird 3
Document signing	Adobe Acrobat 9/X Word 2007/2010
Smart Cards	Aladdin token
Languages	English German Japanese Spanish (traditional) French Norwegian Portuguese (Brazilian)

Selecting a the Right Certificate Enrollment Method and Lifecycle

The decision tree below highlights a few common questions an administrator should ask regarding their PKI deployment, along with the recommended enrollment methods:


1. Approve users
Partners and external users
Employees and internal users
2. Manage users
Cloud
Microsoft Active Directory
4b. Use software PKI client for application usage
4a. Use software PKI client for application usage
3. Enroll Automatically
Using PKI Client
Using Microsoft
No
Yes
Yes
No
Enroll with cloud and native
Enroll with cloud and PKI client
Enroll with EGW and Microsoft Auto-Enroll
Enroll with EGW and PKI client
Enroll with EGW and native

1. Approve Users - The first path concerns whether the end user base is internal or external. If the end users are external (for example, partners), they are most likely not in an Active Directory infrastructure within the organization, and would need to be managed through the Symantec cloud infrastructure.
2. Manage Users - Assuming the end-user base is internal, the enterprise has a choice of whether to manage users through the cloud, or install an Enterprise Gateway, which can perform authentication directly against an Active Directory infrastructure.
3. Enroll - If the enterprise has chosen to deploy an Enterprise Gateway, the next question is whether to automatically enroll users. If automatic enrollment is desired to simplify the enrollment experience, the administrator can configure the auto-enrollment service that is installed as part of the Enterprise Gateway. This will take advantage of the Microsoft auto-enrollment client.
4. Use Software
    - 4a) Assuming auto-enrollment is not a requirement, the next question is whether to deploy PKI Client. The client can easily be pushed out to end user's computers through standard Microsoft group policy installation.
    - 4b) Similar to 4a) above, but for cloud deployments, the enterprise must decide whether to deploy PKI Client. The difference in this scenario is that since the external customer's computers may not be available in a domain, the software distribution would be more complicated and Native enrollment may be preferred.

Want to Try Before you Buy?

More information can be found about Symantec Managed PKI Service on the web:

http://www.symantec.com/managed-pki-service

A free trial of Symantec Managed PKI Service is also available:

http://www.symantec.com/business/theme.jsp?themeid=free-trial

The trial is full featured and includes all the Symantec Manager PKI deployment options, ranging from a fully cloud-based deployment to a hybrid Enterprise Gateway deployment. The trial is limited to 90 days and up to 100 users.

About Symantec

Symantec protects the world's information, and is a global leader in security, backup, and availability solutions. Our innovative products and services protect people and information in any environment – from the smallest mobile device, to the enterprise data center, to cloud-based systems. Our world-renowned expertise in protecting data, identities, and interactions gives our customers confidence in a connected world. More information is available at www.symantec.com or by connecting with Symantec at go.symantec.com/socialmedia.

For specific country offices and contact numbers, please visit our website.

Symantec World Headquarters
350 Ellis St.<br/>Mountain View,
CA 94043 USA<br/>+1 (650) 527
8000<br/>1 (800) 721
3934<br/>www.symantec.com