Managed PKI™ v8.7 Release Notes

Symantec

Managed PKI™ v8.7 Release Notes

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Last updated January 16, 2013

Legal Notice

Symantec Corporation

350 Ellis Street Mountain View, CA 94043

http://www.symantec.com

http://www.symauth.com/support/contact/index.html#support4

Contents

Managed PKI v8.7 Release Notes

Managed PKI v8.7 Release Notes

These release notes accompany the delivery of the Symantec Managed PKI v8.7 release. Managed PKI v8.7 is an automatic upgrade of Managed PKI v8.6, except where described in these release notes.

What's New in Managed PKI v8.7

This release of Managed PKI provides the following updates:

Updated Component Support

Table 1-1 lists the optional components supported by Managed PKI v8.7. All components are available from the *Resources* page of PKI Manager.

Table 1-1 Supported components

Component	Version Supported
PKI Client	v2.7 [a]
PKI Enterprise Gateway (including Autoenrollment Server and Transaction Signing API)	v1.7
PKI Web Services	v1.7

a.Previous versions of PKI Client will work with Managed PKI v8.7; however, you must be running v2.7 or higher to benefit from the features described in these release notes.

Updated Platform Support

Managed PKI v8.7 supports the following platforms and operating systems (OS).

It is not possible for Symantec to test every combination of third-party client, server, operating system, service pack, and so on. As a result, Managed PKI and its components may work on other platforms or operating systems; however, Symantec is unable to provide support for platform and operating systems not listed here.

PKI Manager

PKI Manager is a web portal hosted in Symantec's data centers that allow a Managed PKI administrator to perform tasks related to account, user, certificate, and key management.

Table 1-2 PKI Manager operating system/browser support

OS	Browser
Windows® XP SP3	IE 8 (32-bit) Firefox 17
Windows 7 Enterprise edition (32-bit)	IE 8 (32-bit), 9 (32-bit) Firefox 17
Windows 7 Enterprise edition (64-bit)	IE 8 (32-bit and 64-bit), 9 (32-bit and 64-bit) Firefox 17

PKI Certificate Services

PKI Certificate Services are the web pages that enable users to request, install, renew, and recover their certificates.

Table 1-3 PKI Certificate Services operating system/browser support

OS	Browser
Windows XP SP3	IE 8 (32-bit) Firefox 17 Chrome 23[a]
Windows 7 Enterprise edition (32-bit)	IE 8 (32-bit), 9 (32-bit) Firefox 17 Chrome 23[a]
Windows 7 Enterprise edition (64-bit)	IE 8 (32-bit and 64-bit), 9 (32-bit and 64-bit) Firefox 17 Chrome 23[a]
Mac OS X v10.7	Safari 5.1 Firefox 17
Mac OS X v10.8	Safari 6 Firefox 17

a.The Chrome browser is supported for certificate lifecycle operations using PKI Client only.

PKI Client

PKI Client is middleware for digital signing, authentication, and data protection with desktop-based applications using digital certificates, stored on a smart card, security device, or end-user computer.

Table 1-4 PKI Client operating system/browser support

OS	Browser
Windows XP SP3	IE 8 (32-bit) Firefox 17 Chrome 23
Windows Vista SP 2 (32-bit)	IE 8 (32-bit), 9 (32-bit) Firefox 17 Chrome 23
Windows® 7 Enterprise edition (32-bit)	IE 8 (32-bit), 9 (32-bit) Firefox 17 Chrome 23
Windows® 7 Enterprise edition (64-bit)	IE 8 (32-bit and 64-bit), 9 (32-bit and 64-bit) Firefox 17
Mac OS X v10.7	Safari 5.1 Firefox 17
Mac OS X v10.8	Safari 6 Firefox 17

PKI Client also supports the following applications:

- Outlook Client 2007, 2010 (32-bit and 64-bit)
- Thunderbird 3
- Adobe Reader 9 and X (Windows XP) and Adobe X and XI (all other platforms)
- Word 2007, 2010 (32-bit and 64-bit)

PKI Enterprise Gateway

PKI Enterprise Gateway is software installed at the enterprise site that, in conjunction with the enterprises' LDAP directory service, allows an enterprise to programmatically approve certificate requests and publish certificate information back to the enterprises' user store.

For PKI Enterprise Gateway installations:

- Memory: 4 GB RAM and 100 GB hard disk space
- OS: Windows 2008 R2 Server Enterprise/Standard (64-bit) or Windows 2008 R2 SP1 Server Enterprise/Standard (64-bit)

- Web Server: IIS 7.5, NET Framework 4.0
- User Stores: Microsoft Active Directory or Novell eDirectory 8.8.5
- HSMs

Table 1-5 PKI Enterprise Gateway HSMs

Type	Luna SA	Luna PCI Express	Luna SA Hybrid (PED Auth)
Driver	4.4.3-1	3.0	4.4.3-1
Firmware	4.8.1	4.7.1	4.8.1

For Autoenrollment Server installations:

- Memory: 4 GB RAM and 100 GB hard disk space
- Server OS: Windows 2008 R2 Server Enterprise (64-bit) or Windows 2008 R2 SP1 Server Enterprise (64-bit)
- HSMs:

Table 1-6 Autoenrollment Server HSMs

Type	Luna SA	Luna PCI Express	Luna SA Hybrid (PED Auth)
Driver	4.4.3-1	3.0	4.4.3-1
Firmware	4.8.1	4.7.1	4.8.1

For Microsoft Autoenrollment Client OS:

- OS: Windows XP SP3, Windows 2008 Server (64-bit), or Windows 7 Enterprise (32- and 64-bit)

iOS Devices

Managed PKI supports issuing digital certificates on iOS 4, 5, and 6.

Android Mobile Devices

Managed PKI supports issuing digital certificates on many Android devices. New Android mobile devices are constantly being qualified. Refer to the PKI Client download page on Google play for the most up-to-date list of supported devices.

General Improvements

Managed PKI v8.7 includes the following general improvements. It:

- Provides a mechanism for Symantec to update certificate profile templates and CAs if necessary (for example, if Symantec needs to add new signing algorithms to a profile template or needs to re-key an expiring CA). If a change will have an impact on your certificate profiles, you will be notified in advance, and you will have an opportunity to test the changes before it goes live. You also will have the opportunity to accept the changes manually before the scheduled update.

Once the update has been scheduled, you will not be able to modify the affected certificate profile until the change has been made. However, the certificate profile will be able to issue the certificate as usual.

- Includes a new security feature where all URLs are generated so that no identifying information (such as an enrollment code) is visible in the URL. The old URLs will continue to work.
  - Example of an original URL:

    https://pki.symauth.com/certificate-service?ac=115623&pf=2.16.890.1.113733.1.86.1.2.3.1.1.10676951&id=10febuser1%40yopmail.com&pc=510992443
  - Example of a shortened URL:

    https://pki.symauth.com/certificate-service?p=OC36yX7oABlNInNi

PKI Manager Updates

PKI Manager is the portal you use to configure your Managed PKI account and perform the daily certificate lifecycle tasks. This release of Managed PKI includes the following updates to PKI Manager. Refer to PKI Manager and the online help for more information about these new features.

Improvements to Email Templates

This release of Managed PKI improves the process of creating custom email notifications from the templates provided with each certificate profile.

- Only the templates that are applicable to the certificate profile will be available for that profile. For example, the certificate pick-up email template will not be available for certificate profiles that issue autoenrollment certificates.
- Only the system variables that are applicable to the email template will be available for that template. For example, the variable that inserts the certificate renewal URL will not be available for the certificate enrollment email template.
- Email notification templates are now available to certificate profiles that issue certificates to iOS and Android devices.

Certificate Profile Template Changes

The following changes were made to certificate profile templates for Managed PKI 8.7:

Wi-Fi Certificate Profile Templates Consolidated

With Managed PKI 8.7, the Client Authentication certificate profile template replaces the Wi-Fi certificate profile template. Users can use this template to issue certificates that enable standard Wi-Fi, VPN, or website access for any device (including iOS and Android mobile devices). Microsoft Wi-Fi is used to issue certificates that enable Wi-Fi access to Windows wireless access points and clients.

All existing profiles created using the Wi-Fi template will continue to work, but this template will no longer be available to create new profiles.

Restricted Attributes

In Managed PKI 8.7, restrictions were added to certain certificate profile templates. Previously, the certificate profiles created from these templates that had allowed combinations of Subject DN attributes which could break other functions of the Managed PKI product. For example, when Microsoft® Autoenrollment is chosen as the Enrollment method, all data must come from the enterprise's Active Directory, and must also map to specific fields in the Microsoft templates that are pushed to all clients.

Additionally, restrictions on content were added where the Certificate Type and the available attribute clashed.

New certificate profiles created with these templates will not show the restricted attributes. All existing profiles will continue to work as expected. If any restricted attributes are being used, they will continue to work. Care should be taken in removing existing SDN attributes from existing profiles, because those that are restricted cannot be added back.

Smart Grid Support

PKI Manager now includes optional functionality that allows an enterprise to issue certificates that are compliant with recent Smart Grid technology. Smart Grid certificates can be issued to operational devices (such as a smart appliance) and other Smart Grid-compliant devices (such as Push and Server devices). These devices use the strong public key authentication of certificates to establish trust between these components of the Smart Grid network.

Smart Grid-compliant certificates are lightweight certificates, and so do not include all of the certificate extensions of standard certificates.

Contact your Symantec representative for more information on implementing this option.

Support for Private Server Certificates

This release of Managed PKI allows you to issue low volumes of private Server certificates for specific complementary use cases. With private Server certificates, users within your organization or hierarchy can facilitate authentication for server entities under your private enterprise CA hierarchy, providing verification that the server entity is internally trusted. For larger volumes of these certificates or for public trust, use the public SSL offerings available separately from Symantec.

Contact your Symantec representative for more information on implementing this option.

Support for Private Code Signing Certificates

This release of Managed PKI allows you to issue low volumes of private Code Signing certificates for limited use. With private Code Signing certificates, users within your organization or hierarchy can digitally sign code under your private enterprise CA hierarchy, providing verification that the code has come from an internally trusted

source. For larger volumes of these certificates and for public trust, use the public Code Signing offerings available separately from Symantec.

Contact your Symantec representative for more information on implementing this option.

Support for Manufacturer Certificates

This release of Managed PKI allows you to request for Manufacturer certificates (and private keys) in bulk through a batch interface. With the batch interface, administrators have an ability to request up to 50,000 certificates at a time by uploading .csv or .txt files. Once the certificates are created, administrators will also be able to retrieve and download all the certificates and private keys. Batch Interface provides both online and email notifications in case of success or failure.

Contact your Symantec representative for more information on implementing this option.

Uploading Non-Managed PKI Issued Keys

In Managed PKI 8.7, you can upload certificates issued by other PKI solutions into Managed PKI. This allows you to store and manage all of your certificates in one central interface.

Once the certificates are uploaded to Managed PKI, you can download the certificates, view details about them, and configure the certificate policy for them (such as whether the certificates can be exported, and how they can be accessed if they are exported).

Note: Symantec does not support ECC-based keys while importing non-Managed PKI issued certificates.

Signing Algorithms

Managed PKI 8.7 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 256, 384, and 521. ECC is supported for the Client authentication and Microsoft® Wi-Fi certificate profiles only. Certificate lifecycle operations for certificates with ECC-based keys are only supported using Managed PKI Web Services.
- DSA 2048 (prime)-256 (subprime) and 3072 (prime)-256 (subprime). DSA requires custom certificate profile templates. Contact your Symantec representative for details on custom certificate profile templates.

Multiple S/MIME Certificates with one Identity

This release of PKI Manager allows the enrollment of S/MIME (Secure/Multipurpose Internet Mail Extensions) certificates for the same user from multiple devices.

PKI Web Services will allow enrollment of certificates during the first enrollment and also during the renewal period.

During the non-renewal period, an enrollment request will return the same S/MIME certificate from PKI Web Services. PKI Web Services will do a key recovery and return the S/MIME certificate with the latest issuing date.

Web Services Renewal for RA Certificates

This release of PKI Manager allows renewal for RA certificate in PKI Web Services. Authentication is based on the RA certificate, and only the same RA certificate can be renewed. The renewal can be performed only once as the certificates are valid for 5 years. For the second renewal, you will have to enroll for a new RA certificate as a security precaution.

Administrator RA Renewal Notification

In Managed PKI 8.7, when an Registration Authority (RA) or signing authority certificate is about to expire, Symantec will send a renewal notice. You can now modify the recipient's email address. Symantec recommends that you use an email alias.

Web Client Authentication for iOS and Android

This release provides web client authentication by default in both iOS and Android profiles.

Removing High Security Settings for Native Browser Enrollment

In previous releases, when you enrolled a certificate with the "High Security" setting using native browser enrollment, users would receive a Microsoft pop-up window giving them the option to modify the security level of the private key to be medium or low, conflicting with the original setting.

In this release, when configuring a certificate profile with native enrollment, you can configure a private key to be non-exportable and you will not have a security pop-up window show up for users later.

Assigning Seats to Sub-accounts

In this release, you can set the number of seats available to sub-accounts for each seat pool. You do this by switching to the sub-account and setting the number of seats available in the dashboard. You can:

- Set the seat pool to inherit (share) available seats from the main account. This is the default.

- Allocate seats to the seat pool. This will reduce the number of seats available to the main account accordingly.
- Disable the seat pool. This sets the seat count to 0 and makes any certificate profiles that issue certificates from that seat pool type unavailable.

Note: You cannot assign seats from one seat pool type to another.

Seat pool utilization is displayed in the dashboard for the account and for the sub-account. In *Reports*, you can generate reports for seat usage for each pool for the primary account and sub-account.

Certificate Information Report Type

This release has added a new report that can be created from the *Manage Reports* pages, called Certificate information. The Certificate information report provides information about each certificate issued from a given date to the date the report was generated, including to whom it was issued, the serial number, the validity end date, and its status.

Delete Users (Singly and in Bulk)

In this release, administrators can now delete users, both singly and in bulk. Deleting a user revokes all certificates and deletes any pending enrollments for the user. After deleting a user, you cannot search for that user. You can still search the certificates from **Manage Certificates**.

Revoke Certificates for Multiple Users

In this release, administrators can revoke multiple certificates on the **Manage Certificates** page. Revoking a certificate does not delete the user. If you want to delete the user, you would also need to **Delete User**. After revoking a certificate, you can still search and find that certificate.

PKI Enterprise Gateway Updates

The 1.7 version of PKI Enterprise Gateway includes some minor updates. However, there are no new functionality changes since the previous release and you do not need to update it.

PKI Client Updates

PKI Client has been updated to support many of the features described in these release notes. To obtain the benefits of these updates, your users must upgrade to PKI Client 2.7. For most users, this will happen automatically, unless you have disabled Live Update. Refer to *Symantec™ PKI Client Administrator's Guide* for instructions on how to disable Live Update.

Symantec™ PKI Client Administrator's Guide and *Symantec™ PKI Client Writing Post-processing Scripts Guide* have been updated to reflect theses new features.

Additionally, PKI Client has been updated for the following new features:

Support for Security Devices using Third-party CSPs

PKI Client supports the following security devices using third-party Cryptographic Service Providers (CSPs). These CSPs may support other devices; however, Symantec has only qualified these devices with Managed PKI:.

Table 1-7 Supported security devices

Security Device	CSP
Gemalto SA .NET Dual	Microsoft Base Smart Card CSP
SafeNet iKey 2032	eToken Base Cryptographic Service Provider (requires the SafeNet Authentication Client)[a]
SafeNet iKey 4000	

a.If you purchase eTokens from Symantec, you can use either PKI Client or the SafeNet eToken Base Cryptographic Provider as the CSP. You set this when you configure the Certificate store in the certificate profile.

The third-party CSP will manage PIN operations (such as PIN set and change), and provide the prompts when a PIN-based transaction is performed. However, PKI Client will otherwise manage the token and certificate (import certificates to, view details of, and renew certificates).

Note: Managed PKI v8.7 provides limited support for Aladdin tokens initiated using third-party certificate management software, as long as the tokens already have certificates stored on them. If you remove these certificates, Managed PKI will no longer be able to support the tokens.

You will need to enable the CSP in PKI Client for your users. Refer to *Symantec™ PKI Client Administrator's Guide* for instructions on enabling this setting through a GPO push.

Support for VPN Post-processing on Mac

In this release, PKI Client supports post-processing for VPN on Mac-based devices. If the VPN post-processing script is enabled for a certificate profile in PKI Manager, the PKI Client will configure the Managed PKI certificate to work with Juniper VPN servers during enrollment. Refer to *Symantec™ PKI Client Writing Post-processing Scripts Guide*.

Updated Language Support

Managed PKI v8.7 includes support for the following languages:

- PKI Manager supports English, French, and Japanese
- PKI Certificate Services supports English, French, German, Japanese, Portuguese, Norwegian, Spanish, and simplified Chinese

- PKI Client supports English, French, German, Japanese, Portuguese, Norwegian, Spanish, and simplified Chinese.

These components will auto-detect the languages set in the browser and display the correct language. The browser must have the appropriate language packs installed.

Documentation

The following documents have been revised to incorporate Managed PKI v8.7-specific material:

- *Managed PKI™ v8.7 Release Notes* (this document)
- *Symantec™ PKI Client Administrator's Guide*
- *Symantec™ PKI Client Writing Post-processing Scripts Guide*
- *Symantec™ PKI Enterprise Gateway Deployment Guide*
- *Symantec™ PKI Enterprise Gateway Autoenrollment Server Deployment Guide*
- *Symantec™ Managed PKI® Overview*
- *Managed PKI® Transaction Signing API Developer's Guide*

The following new documents have been added to the Managed PKI documentation set:

- *Managed PKI® Getting Started with Android Mobile Devices* is a quick reference for integrating Managed PKI certificates with your users' iOS mobile devices.
- *Managed PKI® Configuring an LTE Operator Base Station Solution* (available from your Symantec representative or the Symantec Knowledge Center for Managed PKI)
- *Managed PKI® Configuring a Smart Grid Solution* (available from your Symantec representative or the Symantec Knowledge Center for Managed PKI)
- *Managed PKI® Configuring a Manufacturer Certificate Solution for ZigBee* available from your Symantec representative or the Symantec Knowledge Center for Managed PKI)

Unless otherwise noted, all other Managed PKI documents are available from the *Resources* page of PKI Manager.

Issues Addressed and Known Issues and Workarounds

For information about issues that were fixed in this release, and workarounds related to known issues in this release, access the Symantec Knowledge Center for Managed PKI at the following URL. Enter **Managed PKI v8.7** as the Knowledge Center Search text.

https://knowledge.verisign.com/support/mpki-support/index.html