Symantec™ PKI Client
For Symantec™ Managed PKI Services

Additional Information Supplement

This *Additional Information Supplement* describes the additional information, as well as the terms and conditions, applicable to the *Symantec™ PKI Client* software component that may be added, at the customer's option, to supplement the following Symantec™ Managed PKI Services:

- Managed PKI Co-Branded Certificate Service
- Managed PKI Private-Label Certificate Service
- Managed PKI Service for CertiPath
- Managed PKI Service for Windows® (Co-Branded Certificates)
- Managed PKI Service for Windows® (Private Label Certificates)
- Federal Shared Service Provider (SSP) PKI
- Non-Federal Shared Service Provider (SSP) PKI

Symantec™ PKI Client simplifies the certificate lifecycle process by providing easy PKI issuance, renewal, and application integration. *Symantec PKI Client* is a client middleware used in conjunction with a Symantec™ Managed PKI (MPKI) Service add-on package for authentication, data protection, and digital signing using PKI credentials. *Symantec™ PKI Client* uses a unique software PKI credential known as a virtual token, or "vToken," and can be used with a variety of standard desktop and online applications. vTokens provide unique capabilities that are unavailable using standard browser/OS based PKI, including a streamlined user experience, which simplifies the entire PKI lifecycle. Additionally, vTokens can have server based policies, which dictate how they are used, secured, and how their users are authenticated.

Capabilities

PKI Client provides the following key capabilities:

- **Streamlined PKI Lifecycle Management**

  When used with Symantec Managed PKI Service, it can issue and automatically renew PKI credentials into vTokens through simplified user experience that works across various web browsers and platforms.

- **Centralized Policy Management**

  Control policies on how vTokens are secured such as user PIN policies and export policies. Determine how PKI credentials are renewed, even automatically in the client. Custom naming of the vToken can provide an easier to use and more recognizable credential for authentication.

- **Email Signing and Encryption**

  Encrypt email and insert digital signatures into email for data protection and non-repudiation. Automatic configuration of Outlook® simplifies the usage of PKI credentials for email signing and encryption.

- **Securely Login to Websites**

  Authenticate to websites using vToken and a PIN over SSL, providing extra security.

- **Sign and Encrypt Files, Documents, and PDF's**

  Enables native encryption functionality (if any) of Microsoft® Word documents, Adobe® PDF's, and other files while inserting digital signatures into them for data protection and non-repudiation.

- **Standard CSP and PKCS#11 functionality**

  Supports standard applications and algorithms including: RSA 1024/2048, MD5, SHA1, DES, 3DES, and RC2 through standard application interfaces

Clients Supported:

- Microsoft® Windows®
  - XP SP3 (32 bit), Vista SP2 (32 bit), 2003 SP2 (32 bit), 7 (32/64 bit), 2008 (64 bit)
- Pentium® III or higher with 256 MB RAM, 25 MB free hard disk
- Email Clients: Outlook 2003/2007, Thunderbird® 3
- Browsers: Internet Explorer® 7/8, Firefox® 3
- Office: 2003/2007
- Adobe Acrobat® 9

Server Requisites:

- Windows Server® 2003 R2
- IIS 6.0 and ASP.net 2.0
- .NET Framework 2.0
- Java Runtime Environment™ 6
- Java™ Cryptography Policy Files
- MPKI 7.2 or 7.3 Site Kit
- 2GB RAM, 256 MB free hard disk

This *Additional Information Supplement* does not provide details of the Managed PKI Services, which are described in the applicable service descriptions.

* * *

***Symantec™ PKI Client* For Symantec™ Managed PKI Services**
ADDITIONAL TERMS AND CONDITIONS

1. DEFINITION

"Agreement" means the Master Services Agreement or such other master agreement entered into between Symantec and Customer under which the underling Services set forth in the applicable Service Description are provided by Symantec to Customer. Service Descriptions are available on Symantec's website.
"Services" mean Symantec™ Managed PKI Services with which the Software is bundled.
"Software" means any software component provided by Symantec to Customer in connection with the provision of the Services, including without limitation, the *Symantec™PKI Client*.

2. CUSTOMER'S OBLIGATIONS

(a) Customer Obligations. Customer is solely responsible for acquiring and maintains requisite hardware requirements on its premises for the Services and Software, and maintaining the security of its network and computer systems.

(b) Customer's Warranties. In addition to the express limited warranties set forth in the Agreement, Customer warrants to Symantec that Customer: (i) will not monitor, interfere with, reverse engineer the technical implementation of, or otherwise knowingly compromise the security of any Symantec system, Software or Services; and (ii) will comply with its obligations under HSPD-12 and the processes and obligations set forth in the Federal Information Processing Standards Publication 201-1.

(c) Audit. Not more than twice a year, Symantec may audit and inspect, at its own expense, Customer's utilization of the Services and Software in order to ensure compliance with the terms of this Additional Information Supplement, the applicable Service Description, the Services Order and the Agreement. Any such audit will be conducted during normal business hours of Customer upon reasonable written notice to Customer and will not unreasonably interfere with Customer's business activities. Customer shall reasonably cooperate with Symantec in connection with any such audit. If the audit reveals that Customer has underpaid fees to Symantec, such underpaid fees shall be immediately due and payable by Customer.

(d) Compliance with Local Laws. Customer is responsible for ensuring that Customer's acquisition, use, or acceptance of public and private key pairs generated by Symantec in accordance with this Service Description complies with applicable local laws, rules and regulations – including but not limited to export and import laws, rules, and regulations – in the jurisdiction in which Customer acquires, uses, accepts or otherwise receives such key pairs.

3. SYMANTEC'S OBLIGATIONS

(a) Installation. Unless expressly provided in the applicable Order Document, Services do not include Software installation and/or system configuration services. In the event that any installation work is required due to unusual or particularly complex Customer systems or requirements, such additional work may be purchased separately from Symantec.

(b) Support and Maintenance. Customer is responsible for setting up first-level support to customer's individual users. Symantec shall provide Customer with second-level and third-level support and maintenance for the Software in connection with the Services. The support and maintenance commitments of Symantec are described in the applicable Service Level Agreement available on Symantec's website.

(c) Disclaimers. EXCEPT AS SET FORTH IN THIS ADDITIONAL INFORMATION SUPPLEMENT, THE APPLICABLE SERVICE DESCRIPTION OR THE AGREEMENT, THE SERVICES AND THE SOFTWARE ARE PROVIDED "AS IS" AND WITHOUT ANY WARRANTIES WHATSOEVER, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE (ALL OF WHICH ARE HEREBY DISCLAIMED). SYMANTEC MAKES NOT WARRANTY THAT THE SERVICES OR SOFTWARE WILL BE UNINTERRUPTED OR ERROR-FREE.

4. EFFECT OF TERMINATION OF SERVICES FOR ANY REASON

In the event of a termination of the Services for any reason: (a) Customer will immediately cease use of the Services and Software; (b) the rights to use the Services and Software will immediately terminate; (c) Customer will permanently delete the Software related to the provision of the Services from any storage media upon which such Software is stored; and (d) neither party shall be relieved of obligations or liabilities which accrued prior to the date of termination.