Symantec *Managed PKI Service for Windows*® Service Description

Introduction

Symantec *Managed PKI Service for Windows*® provides a flexible PKI platform to manage complete lifecycle of certificates, which includes: the ability to issue, renew, and revoke certificates; escrow and recover private keys; and validate the status of certificates. As a managed service, *Managed PKI Service for Windows* significantly reduces the costs associated with an in-house PKI such as acquiring hardware systems, purchasing software licenses, and training staff. Additionally, *Managed PKI Service for Windows* is tightly integrated with Microsoft® *Active Directory*®, *Windows Server*® *2003* and *2008*, as well as *Windows*® *XP*, *Windows Vista*®, and *Windows 7* operating systems to provide a consistent experience for both administrators and users.

Capabilities

Managed PKI Service for Windows provides the following key capabilities:

- **Certificate Auto-Enrollment**

  Certificate Auto-Enrollment feature leverages Microsoft PKI protocols and *Windows XP*, *Windows Vista*, and *Windows 7* desktop clients to issue and renew certificates for end users and devices. Administrators create and push a group policy to users and/or groups in Microsoft *Active Directory* to enroll for certificates via two (2) methods: silent or balloon pop-up. Silent auto-enrollment issues the certificates to users without their action during a *Windows* operation (*e.g.*, log-in, re-boot, etc.). Balloon pop-up auto-enrollment prompts users to click an acknowledgement to install the certificates. In addition, this feature enables certificates to be automatically renewed within 30 days of expiration through either method.

- **Provisioning Proxy**

  Provisioning Proxy is an in-premise enterprise software module that consists of various services to manage interactions among various service components such as Microsoft *Active Directory*, *Windows* desktop clients, *Microsoft*® *Management Console* (MMC), and Symantec™ *Issuing Center*. The proxy is designed for tight integration with Microsoft *Active Directory* to enable seamless administration and user experience during certificate lifecycle management.

- **Management Console**

  Management Console is a custom version of MMC to provide a similar look and feel for administrators to manage certificate templates and PKI tokens. Administrators can also perform certificate lifecycle functions (*e.g.*, issue, renew, etc.) in this console.

Additional Options

Managed PKI Service for Windows also provides the following additional options:

- **Key Management Service**

  Administrators can centralize generation of public/private key pairs, back-up private keys, and distribute key recovery through the Key Management Service (KMS). KMS ensures maximum security and protection of private keys. Additionally, KMS support dual-key pair which allows for separate issuance and back-up of encryption and signature key pairs.

- **Premium Certificate Revocation List (CRL)**

  Administrators can configure applications (*e.g.*, Microsoft Outlook®) to validate current status of certificates (*e.g.*, active, revoked, etc.) via Premium Certificate Revocation List (CRL). A CRL is a black list of all *revoked* certificates. If a certificate appears on a CRL, the application can take an appropriate action such as denying access or refusing to use certificate for encryption or digitally signing. As part of standard service, Symantec produces a CRL every 24 hours. With Premium CRL, Symantec generates a CRL every hour.

- **Online Certificate Status Protocol (OCSP)**

Administrators can also configure applications to validate the current status of certificates (*e.g.*, active, revoked, etc.) via On-line Certificate Status Protocol (OCSP) service. While all *revoked* certificates will appear on a CRL, there is a time delay between the certificate's revocation and the next CRL run which can be up to 1 hour for Premium CRL and 24 hours for standard CRL. Administrators may have polices that require applications to check certificate's status in real-time to take appropriate action. Symantec immediately updates the certificates' status to OCSP service upon any status changing action (*e.g.* revocation, suspension, etc.). Administrators can configure applications to send OCSP requests and receive OCSP responses to check certificate's status in real-time.

- **Professional Services**

Symantec offers a wide range of professional services to help customers install *Managed PKI Service for Windows*® in the customer's data centers and train administrators. If required, customers can also leverage Symantec's extensive experience with Certificate Policy (CP) and Certification Practice Statements (CPS) to help draft custom CP and CPS.

Public CA Certification

Public (co-branded) certificates reside in the Symantec™ Trust Network ("STN"), a globally-interoperable digital certificate infrastructure based on a trusted network of Certification Authorities throughout the world. The roots of the Symantec™ Trust Network are embedded in most popular browsers, servers, and email applications. Therefore, public certificates generally can be used across organizations without any special preparation on the part of the certificate users. .

Note: Users of the *Managed PKI Service for Windows* (Co-Branded Certificates) must adhere to the Symantec Certification Practice Statement (CPS).

Private CA Certification

When your organization enrolls for the *Managed PKI Service for Windows* (Private Label Certificates), Symantec will perform a key ceremony for you: a formal, secure procedure for creating the private/public key pair for your CA with your own private root at the top of the CA hierarchy. Generally, private certificates are used within your organization for applications such as intranets, virtual private networks (VPNs), and, occasionally, for Web access. Although private certificates may be used externally in private domains, you must first distribute your organization's root and certificates to those with whom you wish to communicate. Organizations running a private CA are responsible for defining and following their own certificate rules and practices.

Note: IPSec implementations for VPNs require use of private certification.

* * *

APPENDIX A - *MPKI SERVICE FOR WINDOWS*® (CO-BRANDED CERTIFICATES) SERVICE TERMS AND CONDITIONS:

1. DEFINITIONS

"Affiliated Individual" means a person that is affiliated to Customer: (a) as an officer, director, employee, partner, contractor, intern, or other person within Customer's organization, or (b) as a person maintaining a contractual relationship with Customer's organization where Customer has business records providing strong assurances of the identity of such person.

"Agreement" means the Master Services Agreement or such other master agreement entered into between Symantec and Customer under which the Services Order applicable to this Service Description is issued.

"Certificate" or **"Digital Certificate"** means a message that, at least, states a name or identifies the issuing CA, identifies the Subscriber, contains the Subscriber's Public Key, identifies the Certificate's Operational Period, contains a Certificate serial number, and contains a digital signature of the issuing CA.

"Certificate Applicant" means a person or authorized agent that requests the issuance of a Certificate by a CA.

"Certificate Signing Unit" or **"CSU"** means a hardware unit or software designed for use in signing Certificates and key storage.

"Certification Authority" or **"CA"** means a person or entity authorized to issue, suspend, or revoke Certificates.

"Certification Practices Statement" or **"CPS"** means a document, as revised from time to time, representing a statement of the practices a CA or RA employs in issuing Certificates. The Symantec CPS is published on Symantec's website.

"Erroneous Issuance" means: (a) issuance of a Certificate in a manner not materially in accordance with the procedures required by the Symantec CPS, (b) issuance of a Certificate to a person other than the one named as the subject of the Certificate, or (c) issuance of a Certificate without the authorization of the person named as the subject of the Certificate.

"Key Generation" means the Symantec procedures for proper generation of Customer CA Public Key and Private Key via a trustworthy process and for storage of the Private Key and documentation thereof.

"Operational Period" means a period starting with the date and time a Certificate is issued (or on a later date and time certain if stated in the Certificate) and ending with a date and time at which the Certificate expires or is earlier revoked.

"Private Key" means a mathematical key (kept secret by the holder) used to create digital signatures and, depending upon the algorithm, decrypt messages or files encrypted (for confidentiality) with the corresponding Public Key.

"Public Key" means a mathematical key that can be made publicly available and which is used to verify signatures created with its corresponding Private Key. Depending on the algorithm, Public Keys are also used to encrypt messages or files which can then be decrypted with the corresponding Private Key.

"Registration Authority" or **"RA"** is an entity approved by a CA to validate Subscribers for application and receipt of Certificates and/or revoke Certificates, in connection with the Managed PKI Service for Windows (Co-Branded Certificate) Service. An RA is not the agent of a Certificate Applicant. An RA may not delegate the authority to approve Certificate Applications other than to authorized RAAs of the RA.

"Registration Authority Administrator" or **"RAA"** is an employee or such other Trusted Person of an RA that is responsible for carrying out the functions of an RA.

"Seat" means a single individual that is an authorized end user of the service, without regard to the number of Certificates actually issued to that individual.

"Subscriber" means a person who is the subject of, and has been issued, a Certificate, and is capable of using, and is authorized to use, the Private Key that corresponds to the Public Key listed in the Certificate at issue.

"Subscriber Agreement" is the agreement executed between a Subscriber and the CA or Symantec relating to the provision of designated Certificate-related services governing the Subscriber's rights and obligations relating to the Certificate.

"Trusted Person" has the meaning given in the Symantec™ CPS.

"Symantec™ Trust Network" or **"STN"** means the Certificate-based Public Key Infrastructure governed by the Symantec Trust Network certificate policies, which enables the worldwide deployment and use of Certificates by Symantec and its affiliates, and their respective customers, subscribers, and relying parties.

2. APPOINTMENT

(a) Appointment. Symantec hereby appoints Customer as a non-Symantec CA within the STN pursuant to the Symantec CPS, and Customer accepts such appointment.

(b) Symantec CPS. Except for the functions outsourced to Symantec under this Service Description, Customer shall meet all requirements and perform all obligations imposed upon a CA and/or RA within the STN including but not limited to: (i) the Symantec CPS, as periodically amended; and (ii) the duties in Section 3 of these Service Terms and Conditions.

3. CUSTOMER'S OBLIGATION

(a) Appointment. Customer shall appoint one or more authorized Customer employees or Trusted Persons as RAA(s). Such RAA(s) shall be entitled to appoint additional RAAs on Customer's behalf.

(b) Administrator Functions. Customer shall comply with the requirements stated in the Symantec CPS, as periodically amended, including without limitation, requirements for validating the identity and enrollment information of Certificate Applicants, and issuing and revoking Certificates. Customer shall perform such tasks in a competent, professional, and workmanlike manner. Customer shall allow the issuance of Certificates only when

the Certificate Applicant is an Affiliated Individual as to Customer. If a Subscriber who had been issued a Certificate by Customer ceases to be affiliated with Customer as an Affiliated Individual, then Customer shall promptly revoke such Subscriber's Certificate. If an RAA ceases to have the authority to act as RAA on behalf of Customer, then Customer shall promptly prevent such person from further issuance of Certificates.

(c) Customer's Subscribers. Customer shall cause Subscribers receiving Certificates hereunder to abide by the terms of the appropriate Subscriber Agreement, to which they shall assent as a condition of enrolling for their Certificates. Customer will ensure that the terms of such Subscriber Agreement shall be no less protective of CAs than those in the Symantec™ CPS.

(d) Survival. In addition to the termination provisions set forth in the Agreement, the revocation and security requirements in this Service Description and the Symantec CPS shall survive termination of the Agreement until the end of the Operational Period of all Certificates issued hereunder.

(e) Customer's Warranties. In addition to the express limited warranties set forth in the Agreement, Customer warrants to Symantec that (i) all information material to the issuance of a Certificate and validated by or on behalf of Customer is true and correct in all material respects; (ii) Customer's performance hereunder will not result in Erroneous Issuance; (iii) Customer has substantially complied with the Symantec CPS and the RA requirements; (iv) Customer's RAA has been and will remain the only person authorized or enabled to effect the issuance of Certificates on Customer's behalf hereunder; and (v) Customer will not monitor, interfere with, reverse engineer the technical implementation of, or otherwise knowingly compromise the security of any Symantec system, software or the STN.

(f) Audit Rights. Symantec may conduct an audit of Customer's records and procedures not more than once per year to ensure compliance with the terms of this Service Description. Any such audit will be conducted during business hours 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 breached any term of these Service Description Terms and Conditions, then (i) Customer will pay Symantec's reasonable costs of conducting the audit, and (ii) notwithstanding the one audit per year limitation stated above, Symantec may conduct such further audits as it deems reasonably necessary to ensure compliance with the terms herein. Routine annual audits may only cover the activities of the immediately preceding year.

(g) 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.

4. SYMANTEC'S OBLIGATIONS

(a) Services. Following completion of the requisite installation, Symantec shall provide Customer with the services specified in this Service Description in accordance with these terms and conditions throughout the term of the service. Symantec shall issue and/or post revocation status information, for client Certificates in accordance with the instructions provided by Customer and its RAA(s). Symantec shall also register Public Keys, provide Public Keys to relying parties, and revoke the registration of Public Keys under XKMS in response to properly-structured XKMS requests submitted by Customer. Upon Customer's initiation of Certificate issuance, Symantec shall be entitled to (i) rely upon the accuracy of the Certificate Applicant information subject to validation by Customer's RAA, and (ii) issue a Certificate for the corresponding Certificate Applicant. Certificates issued or licensed under this Agreement will have a maximum validity period of twelve (12) months from the date each Certificate was issued.

(b) CA Key Generation. During a single Key Generation event, Symantec shall generate for Customer pairs of CA keys for use in signing Certificates issued by Symantec on behalf of Customer for use in the STN. Customer's CA Private Key of each key pair shall be stored in one or more Certificate Signing Units.

(c) Symantec's Warranties. Symantec warrants that: (i) there are no errors introduced by Symantec in the Certificate(s) as a result of Symantec's failure to use reasonable care in creating the Certificate(s); and (ii) its issuance of the Certificate(s), revocation information services, and use of a repository conform to the Symantec CPS in all material aspects.

5. ADDITIONAL TERMS

Each service account includes at least one CA Certificate. Additional CA Certificates for a given volume may be purchased later. Automated Administration hardware components become the property of Customer, but upon termination of the service any Certificates stored in the hardware will be revoked. Administrator Kits consist of a smart card, software and one (1) Administrator Certificate. CA Certificates and/or corresponding key pairs may not be extracted from Symantec's systems upon termination of service.

APPENDIX B - MPKI SERVICE FOR WINDOWS® (PRIVATE LABEL CERTIFICATES) SERVICE TERMS AND CONDITIONS

1. DEFINITIONS

"**Agreement**" means the Master Services Agreement or such other agreement entered into between Symantec and Customer under which the Services Order applicable to this Service Description is issued.

"Certificate" or **"Digital Certificate"** means a message that, at least, states a name or identifies the issuing CA, identifies the Subscriber, contains the Subscriber's Public Key, identifies the Certificate's Operational Period, contains a Certificate serial number, and contains a digital signature of the issuing CA.

"Certificate Applicant" means a person or authorized agent that requests the issuance of a Certificate by a CA.

"Certificate Signing Unit" or **"CSU"** means a hardware unit or software designed for use in signing Certificates and key storage.

"Certification Authority" or **"CA"** means a person authorized to issue, suspend, or revoke Certificates.

"Erroneous Issuance" means: (a) issuance of a Certificate in a manner not materially in accordance with the procedures required by the applicable CPS; (b) issuance of a Certificate to a person other than the one named as the subject of the Certificate; or (c) issuance of a Certificate without the authorization of the person named as the subject of the Certificate.

"Key Generation" means the Symantec procedures for proper generation of Customer's Public Key and Private Key via a trustworthy process and for storage of Customer's Private Key and documentation thereof.

"Operational Period" means a period starting with the date and time a Certificate is issued (or on a later date and time certain if stated in the Certificate) and ending with a date and time at which the Certificate expires or is earlier revoked.

"Private Hierarchy" means a domain consisting of a system of CAs that issue Certificates in a chain leading from Customer's root CA through one or more Certification Authorities to Subscribers in accordance with Customer's practices. Certificates issued in a Private Hierarchy are intended to meet the needs of organizations authorizing their issuance and are not intended for interactions between organizations and/or individuals through public channels.

"Private Key" means a mathematical key (kept secret by the holder) used to create digital signatures and, depending upon the algorithm, to decrypt messages or files encrypted (for confidentiality) with the corresponding Public Key.

"Public Key" means a mathematical key that can be made publicly available and which is used to verify signatures created with its corresponding Private Key. Depending on the algorithm, Public Keys are also used to encrypt messages or files which can then be decrypted with the corresponding Private Key.

"Registration Authority" or **"RA"** is an entity approved by a CA to validate Subscribers for application and receipt of Certificates and/or revoke Certificates, in connection with the Co-Branded Certificate Services. An RA is not the agent of a Certificate Applicant. An RA may not delegate the authority to approve Certificate Applications other than to authorized RAAs of the RA.

"Registration Authority Administrator" or **"RAA"** is an employee or such other Trusted Person of an RA that is responsible for carrying out the functions of an RA.

"Seat" means a single individual that is an authorized end user of the service, without regard to the number of Certificates actually issued to that individual.

"Subscriber" means a person who is the subject of, and has been issued, a Certificate, and is capable of using, and is authorized to use, the Private Key that corresponds to the Public Key listed in the Certificate at issue.

"Subscriber Agreement" is the agreement executed between a Subscriber and the CA or Symantec relating to the provision of designated Certificate-related services and governing the Subscriber's rights and obligations relating to the Certificate.

"Trusted Person" means an employee, contractor, or consultant of Customer who is responsible for managing infrastructural trustworthiness of Customer, its products, its services, its facilities, and/or its practices.

2. CUSTOMER'S OBLIGATIONS

(a) Appointment. Customer shall appoint one or more authorized Customer employees or Trusted Persons as RAA(s). Such RAA(s) shall be entitled to appoint additional RAAs on Customer's behalf. Customer shall cause RAAs receiving Certificates hereunder to abide by the terms of the applicable CPS.

(b) Administrator Functions. Customer shall, through its RAA(s), be responsible for validating identity and enrollment information of Certificate Applicants, and issuing and revoking Certificates. If an RAA ceases to have the authority to act as RAA on behalf of Customer, then Customer shall promptly prevent such person from further issuance of Certificates.

(c) Survival. In addition to the termination provisions set forth in the Agreement, the revocation and security requirements herein shall survive termination of this Agreement until the end of the Operational Period of all Certificates issued hereunder.

(d) Customer's Warranties. In addition to the express limited warranties set forth in the Agreement, Customer warrants that: (i) all information material to the issuance of a Certificate and validated by or on behalf of Customer is true and correct in all material respects; (ii) Customer's performance hereunder will not result in Erroneous Issuance; (iii) Customer has substantially complied with the applicable CPS and the RA requirements; (iv) Customer's RAA has been and will remain the only person authorized or enabled to effect the issuance of Certificates on Customer's behalf hereunder; and (v) Customer will not monitor, interfere with, reverse engineer the technical implementation of, or otherwise knowingly compromise the security of any Symantec system, software or the STN.

(e) 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) Services. Following completion of the requisite installation, Symantec shall provide Customer with the services indicated in this Service Description throughout the term of the service. Symantec shall issue and/or post revocation status information, for client Certificates in accordance with the instructions provided by Customer and its RAAs. Symantec shall also register Public Keys, provide Public Keys to relying parties, and revoke the registration of Public Keys under XKMS in response to properly-structured XKMS requests submitted by Customer. Upon Customer's initiation of Certificate issuance, Symantec shall be entitled to: (i) rely upon the accuracy of the Certificate Applicant information subject to validation by Customer's RAA; and (ii) issue a Certificate for the corresponding Certificate Applicant. Certificates issued or licensed under this Agreement will have a maximum validity period of twelve (12) months from the date each Certificate was issued.

(b) CA Key Generation. During a single CA Key Generation event, Symantec shall generate for Customer pairs of CA keys for use in signing Certificates issued by Symantec on behalf of Customer for use in Customer's Private Hierarchy. Customer's Private Key of each pair shall be stored in one or more Certificate Signing Units.

(c) Symantec's Warranty. Symantec warrants that there are no errors introduced by Symantec in the Certificate(s) as a result of Symantec's failure to use reasonable care in creating the Certificate(s).

4. ADDITIONAL TERMS

Each service account includes at least one CA Certificate. Additional CA Certificates for a given volume may be purchased later. Automated Administration hardware components become the property of Customer, but upon termination of the service any Certificates stored in the hardware will be revoked. Administrator Kits consist of a smart card, software and one (1) Administrator Certificate. CA Certificates and/or corresponding key pairs may not be extracted from Symantec's systems upon termination of service.

APPENDIX C - MICROSOFT REQUIRED SUPPLEMENTAL OBLIGATIONS

(1) Disclaimer of Warranties. MICROSOFT AND ITS AFFILIATES MAKE NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY AS TO THE SERVER SOFTWARE PROVIDED HEREUNDER ("**SERVER SOFTWARE**"), AND HAVE NO RESPONSIBILITY FOR ITS PERFORMANCE OR FAILURE TO PERFORM. AS TO MICROSOFT, THE SERVER SOFTWARE IS PROVIDED **AS IS** AND WITH ALL FAULTS, AND MICROSOFT AND ITS AFFILIATES HEREBY DISCLAIM ALL OTHER WARRANTIES, DUTIES AND CONDITIONS, EITHER EXPRESS, IMPLIED OR STATUTORY, INCLUDING, BUT NOT LIMITED TO, ANY (IF ANY) IMPLIED WARRANTIES, CONDITIONS OF MERCHANTABILITY, OF FITNESS FOR A PARTICULAR PURPOSE, OF RELIABILITY OR AVAILABILITY, ALL WITH REGARD TO THE SERVER SOFTWARE. ALSO, MICROSOFT AND ITS AFFILIATES MAKE NO WARRANTY OR CONDITION OF TITLE, QUIET ENJOYMENT, CORRESPONDENCE TO DESCRIPTION OR NON-INFRINGEMENT WITH REGARD TO THE SERVER SOFTWARE.

(2) Exclusion of Certain Damages. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL MICROSOFT BE LIABLE FOR ANY SPECIAL, INCIDENTAL, PUNITIVE, INDIRECT, OR CONSEQUENTIAL DAMAGES WHATSOEVER (INCLUDING, BUT NOT LIMITED TO, DAMAGES FOR LOSS OF PROFITS OR CONFIDENTIAL OR OTHER INFORMATION, FOR BUSINESS INTERRUPTION, FOR PERSONAL INJURY, FOR LOSS OF PRIVACY, FOR FAILURE TO MEET ANY DUTY INCLUDING OF GOOD FAITH OR OF REASONABLE CARE, FOR NEGLIGENCE, AND FOR ANY OTHER PECUNIARY OR OTHER LOSS WHATSOEVER) ARISING OUT OF OR IN ANY WAY RELATED TO THE USE OF OR INABILITY TO USE THE SERVER SOFTWARE, THE PROVISION OF OR FAILURE TO PROVIDE SUPPORT OR OTHER SERVICES, INFORMATION, SOFTWARE, AND RELATED CONTENT THROUGH THE SERVER SOFTWARE OR OTHERWISE ARISING OUT OF THE USE OF THE SERVER SOFTWARE, OR OTHERWISE UNDER OR IN CONNECTION WITH ANY OF THESE SERVICE DESCRIPTION TERMS AND CONDITIONS, EVEN IN THE EVENT OF THE FAULT, TORT (INCLUDING NEGLIGENCE), STRICT LIABILITY, BREACH OF CONTRACT OR BREACH OF WARRANTY OF MICROSOFT, AND EVEN IF MICROSOFT HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

(3) Server Software Requirements. Customer may use only one (1) copy (unless otherwise specified in the applicable Services Order or Statement of Work**)** of the Server Software provided hereunder as specified in the documentation accompanying this software, and only to interoperate or communicate with native Microsoft Windows 2000 Professional , Windows XP Home or Professional, or Vista client operating systems (or any successors thereto). Customer may not use the Server Software on a Personal Computer under any circumstances. For purposes of the foregoing, a "**Personal Computer**" means any computer configured so that its primary purpose is for use by one person at a time and that uses a video display and keyboard.

(4) Third Party Beneficiary. Notwithstanding any inconsistent terms of the Agreement, Customer hereby agrees that Microsoft Corporation, as a licensor of intellectual property included in the Server Software, is intended to be a third party beneficiary of these Service Description terms and conditions with rights to enforce any terms herein that affect any included Microsoft intellectual property or other Microsoft interest related to the terms hereof.

(5) Server Class 2. If Customer has elected the Server Class 2, Customer may use the Server Software on a server that (a) contains not more than four (4) processors, where each such processor has a maximum of thirty-two (32) bits and four (4) gigabytes of RAM, and (b) is not capable of having memory added, changed or removed without the requirement that the server on which it is running be rebooted ("**Hot Swapping Capabilities**"). Customer may not use the Server Software in conjunction with any software that supports Hot Swapping Capabilities or Clustering Capabilities, where "**Clustering Capabilities**" means the ability to allow a group of servers to function as a single high-availability platform for running applications using application failover between Server nodes in the group.

(6) Audit Rights. Symantec may audit Customer and inspect Customer's facilities and procedures during regular business hours at Customer premises upon not less than fourteen (14) days' notice to verify Customer's compliance with all terms and conditions hereof. Notwithstanding any inconsistent terms of the Agreement (including without limitation any confidentiality provisions), should Customer refuse to undergo such audit and Symantec has reason to believe Customer may not be in compliance with the Service Description terms and conditions, Customer agrees that Symantec may disclose to Microsoft Customer's identity and the basis for Symantec's belief of non-compliance.

(7) Multiplexing Devices. Hardware or software that reduces the number of users directly accessing or using services provided by the Server Software does not reduce the number of users deemed to be accessing or using services provided by the Server Software. The number of users accessing or using the Server Software is equal to the number of users who access or use, either directly or through a Multiplexing Device, services provided by (a) the Server Software or (b) any other software or system where the authentication or authorization for such software or system is provided by the Server Software (an "**Other Authenticated System**"). As used here, a "**Multiplexing Device**" means any hardware or software that provides or obtains access, directly or indirectly, to services provided by the Server Software or any Other Authenticated System to or on behalf of multiple other users through a reduced number of connections.

(8) Windows CAL Requirement. Customer must acquire and dedicate a separate Windows CAL for each user that is accessing or using, either directly or through or from a Multiplexing Device, services provided by the Server

Software or any Other Authenticated System. A "**Windows CAL**" means (a) a Windows Device Client Access License ("**CAL**"), or a Windows User CAL, in either case for a Microsoft Windows Server 2003 (Standard Edition, Enterprise Edition, or Datacenter Edition) server operating system product (or any successors thereto) ("**Windows Server**"); or (b) a Microsoft Core CAL that provides an individual person or electronic device with rights to access and use Windows Server, in either of (a) or (b) above that Customer has acquired for use with one or more such Microsoft Windows Server operating system products or electronic device and that is used on a per user or per device basis.

APPENDIX D – KEY MANAGEMENT SERVICE TERMS AND CONDITIONS:

KMS.1. DEFINITIONS

"Erroneous Key Recovery" means: (a) recovery and transmission of a Private Key in a manner not materially in accordance with the procedures required in the applicable CPS; (b) recovery and transmission of a Private Key to a person other than the Subscriber who is the rightful holder of the Private Key; or (c) recovery and transmission of a Private Key without the authorization of the Subscriber who is the rightful holder of the Private Key. Notwithstanding the foregoing, Erroneous Key Recovery does not include: (d) Customer's recovery of a Subscriber's Private Key and transmission to law enforcement officials in response to a search warrant or subpoena; (e) Customer's recovery of a Subscriber's Private Key and transmission in response to judicial or administrative process; or (f) Customer's recovery of a Subscriber's Private Key to obtain access to messages that are intended to be decrypted by use of such Private Key, even without Subscriber's authorization, for Customer's legitimate and lawful business purposes.

"Key Manager Administrator" means a person designated by Customer that shall use trustworthy systems to generate key pairs, send Public Keys and Private Key recovery information to Symantec, store Private Keys, and transmit Private Keys to Subscribers.

"Key Recovery Impersonation" means a request and receipt from Customer of a Subscriber's Private Key by submitting false or falsified information relating to naming or identity indicating that such Person is such Subscriber.

KMS.2. CUSTOMER'S OBLIGATIONS

(a) Appointment. Customer shall appoint one or more authorized Customer employees or such other Trusted Persons as Key Manager Administrators ("KMAs"). KMAs may have different roles, such as a security administrator role or a key recovery role. Only KMAs with a security administrator role shall be entitled to appoint additional KMAs on Customer's behalf. If any KMA is no longer authorized to recover keys, Customer shall use the Managed PKI Control Center to revoke such authority. Customer must comply with the applicable requirements of the Key Management Service Administrator's Guide published at the Managed PKI Control Center, as periodically amended. Symantec shall notify the Customer-appointed KMA of any such amendments by posting the information to the Managed PKI Control Center.

(b) Administrator Functions. Customer shall comply with the requirements of the Key Management Service Administrator's Guide including, without limitation, requirements for generating key pairs on behalf of Certificate Applicants, transmitting Public Keys to Symantec for inclusion in Certificates to be issued to such Certificate Applicants, transmitting key recovery information to Symantec, validating requests from Subscribers who wish to recover their Private Keys to ensure that they are in fact from such Subscribers, approving or rejecting such requests, using hardware and software designated by Symantec, using the Unified Authentication Managed PKI Key Management Service to request the information needed to recover Private Keys, and (where appropriate) transmitting recovered Private Keys to the requesting Subscribers. Customer shall use trustworthy systems to generate key pairs, send Public Keys and Private Key recovery information to Symantec, store Private Keys, and transmit Private Keys to Subscribers.

(c) Manner of Performance. Customer shall perform the tasks in Section KMS.2(b) above in a competent, professional, and workmanlike manner. Customer shall utilize Symantec's software and services provided under this Service Description exclusively for lawful purposes and for purposes consistent with the Key Management Service Administrator's Guide.

(d) Customer's Warranties. In addition to the express limited warranties contained in each applicable Service Description under this Agreement, Customer warrants that (i) each request by Customer to recover a Subscriber's Private Key has in fact been submitted to Customer and authorized by such Subscriber; (ii) requests by Customer to recover a Subscriber's Private Key without the Subscriber's permission are authorized by Customer for its legitimate and lawful business purposes; (iii) without limiting the generality of the foregoing, a request by Customer to recover a Subscriber's Private Key will not result in an Erroneous Key Recovery regardless of whether it results from Key Recovery Impersonation; and (iv) Customer has substantially complied with the Key Management Service Administrator's Guide.

(e) 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.

KMS.3. SYMANTEC'S OBLIGATIONS

Symantec shall provide the Key Management Service as set forth herein, to be used concurrently with the Symantec Managed PKI Service for Windows.

(a) KMA Certificate. Upon approval of a Certificate Application of the KMA(s), if any, Symantec shall issue a KMA Certificate or Administrator Certificate to each such KMA as appropriate to gain access to the services provided under this Service Description.

(b) Placement of Public Keys in Certificates. After Customer generates a key pair on behalf of a Certificate Applicant (upon approval of a Certificate Application) and transmits the Public Key to Symantec, Symantec shall place such Public Key in a Certificate and issue the Certificate pursuant to the applicable Symantec Managed PKI Service for Windows service terms.

(c) Symantec Centralized Key Management Service. Symantec shall authenticate requests received from Customer's KMA for a Subscriber's Private Key that Customer generated or approved in accordance with the Key Management Service Administrator's Guide. If Symantec authenticates the request, it shall provide Customer with Key Recovery information needed to recover such Subscriber's Private Key.

KMS.4. LIABILITY RELATING TO REQUESTS FOR PRIVATE KEYS

CUSTOMER SHALL BE SOLELY RESPONSIBLE FOR THE GENERATION OR AUTHENTICATION OF ALL RECOVERY REQUESTS FOR PRIVATE KEYS THAT CUSTOMER SUBMITS TO SYMANTEC AND FOR THE CONDUCT OF CUSTOMER'S KMAs. SYMANTEC DISCLAIMS ANY AND ALL LIABILITY ASSOCIATED THEREWITH.