Symantec Managed PKI for SSL Certificate

Service Description

April 2016

Service Overview

The Symantec Managed PKI for SSL Certificate Service ("**Service**") is a hosted, Web-based solution that allows Customer to centralize issuing, renewing, revoking, and managing access privileges for its SSL and code signing certificates within its own organization.

This Service Description, with any attachments included by reference, is part of any agreement which incorporates this Service Description by reference (collectively, the "Agreement"), for those Services which are described in this Service Description and are provided by Symantec. If terms and conditions accompany this Service Description, such terms and conditions apply to Customer unless Customer has an applicable signed Agreement.

Table of Contents

Symantec Managed PKI for SSL Certificate

Service Description

April 2016

TECHNICAL/BUSINESS FUNCTIONALITY AND CAPABILITIES

Service Features

- Symantec offers the following certificates through the Service:
  - *MPKI for SSL Premium with Extended Validation*: Secure and high performing certificates for website security, with strong visual trust indicators and added assurance for business continuity including ECC, DSA and RSA algorithm support, vulnerability assessment and malware scanning.
  - *MPKI for SSL Standard with Extended Validation*: Secure and high performing certificates for website security, with strong visual trust indicators and added assurance for business continuity including DSA and RSA algorithm support and malware scanning.
  - *MPKI for SSL Premium SSL*: Secure and high performing certificates for website security including ECC, DSA and RSA algorithm support, vulnerability assessment and malware scanning.
  - *MPKI for SSL Standard SSL*: Secure and high performing certificates for website security including DSA and RSA algorithm support and malware scanning.
  - *MPKI for SSL Premium Intranet SSL*: Designed specifically for intranets and private networks including ECC, DSA and RSA algorithm support.
  - *MPKI for SSL Standard Intranet SSL*: Designed specifically for intranets and private networks including DSA and RSA algorithm support.
  - *MPKI for SSL Wildcard SSL*: Protect the transfer of sensitive data on multiple subdomains under one domain on the server using a single certificate.
  - *MPKI for SSL Rapid SSL Enterprise*: The GeoTrust brand certificates including DSA and RSA algorithm support.
  - *MPKI for Private SSL*: The root is not chained to the Symantec Trust Network, or governed by the Symantec Trust Network CPS. Customer is responsible for defining the rules and practices for the Customer private root and intermediate certificates. For *MPKI for Private SSL*, Licensed Certificate Option is included, and use of a single SSL certificate is permitted for any number of physical servers or devices within private hierarchies.
    - (*Symantec's Private Root*) SSL certificates signed off Symantec's private root and designed specifically for intranets and private networks. Customer must distribute the Symantec private root to those with whom customer wishes to communicate.
    - (*Customer's Own Dedicated Private Root*) SSL certificates signed off Customer's private root and designed specifically for intranets and private networks. Symantec will perform a key ceremony for Customer: a formal, secure procedure for creating and hosting the private/public key pair for Customer CA with the private root at the top of the CA hierarchy. Customer must distribute the Customer private root to those with whom customer wishes to communicate. The OCSP and CRL services for the Customer private root will be removed after the Service is expired or terminated.
  - *Open Financial Exchange (OFX) SSL Certificates*: For financial and other eligible banking institutions (please contact your Symantec sales representative for more information); compatible with the most popular servers to enable SSL on Web sites and are accepted by all browsers that support SSL.
  - *Authenticode Code Signing Certificates*: Provide content integrity and publisher identity in conjunction with Microsoft's Authenticode technology by enabling Developers to digitally sign executables, .cab, .dll and .ocx files for trusted download. Authenticode code signing certificates support various Windows logo certification programs.

- *Java Code Signing Certificates*: For Java applications for desktop, digitally sign .jar files and Netscape Object Signing. Recognized by Java Runtime Environment (JRE).
- *Extended Validation Code Signing:* The EV Code Signing process can provide reputation service within browsers, operating systems, and security software an additional source of confidence in applications signed with EV Code Signing certificates.

- Administrators use the MPKI Control Center to manage and control SSL Certificate enrollment, approval, issuance, rejection, revocation, and renewal.
  - *Enterprise Certificate Manager (ECM): Allows centralized administration and control of SSL, OFX SSL, and Code Signing Certificates across the various divisions or sub-organizations of Customer's entire organization through the account.*
  - *Full PKI management.*
  - *Reporting to track Certificate details.*
  - *Audit log of Certificates issued and Administrator actions.*
  - *Email alerts.*
  - *Download CRL.*
  - *Interactive online help.*
- Subscriber Tools feature, permitting role-based task delegation for distributed administration. Certificate Subscribers interact with the system via customizable screens. All data is automatically processed in the Symantec-hosted, carrier-class data center, relay hub between the Administrator, users, and the CA.
- For an additional fee, depending on the applicable support level package, Customer can add multiple organizations and domain names to the Service account.
- For an additional fee, Customer can add Administrator kits. Each account includes one (1) Administrator kit. The kit includes a client Certificate for authentication to the MPKI Control Center and an optional, security hardware token for storage.
- For an additional fee, the *SSL Certificate Licensing Option* permits the use of a Certificate on one physical device with additional Certificate licenses for each physical server that each device manages, or where replicated Certificates may otherwise reside. Even though Symantec recommends following best practices by not copying or sharing Certificates (and private keys) from server to server, due to redundancy, load balancing and other performance and availability considerations, some Customers have unique Web infrastructure configurations that require sharing Certificates between multiple servers or other devices.

Customer Responsibilities

Symantec can only perform the Service if Customer provides required information or performs required actions. If Customer does not provide/perform per the following responsibilities, Symantec's performance of the Service may be delayed, impaired or prevented, as noted below.

- Setup Enablement: Customer must provide information required for Symantec to begin providing the Service.
- Adequate Customer Personnel: Customer must provide adequate personnel to assist Symantec in delivery of the Service, upon reasonable request by Symantec.
- Customer accepts the appointment as a non-Symantec RA.
- Customer must meet all requirements and perform all obligations imposed upon an RA within the STN, which shall include, but are not limited to: (i) the Symantec Trust Network CPS, as periodically amended; (ii) the Handbook; and (iii) the obligations set forth in this Section V. In addition to the termination, revocation, and security provisions set forth in this Service Description, the Symantec Trust Network CPS and the Handbook shall survive termination of the term of the Service until the end of the Operational Period of all Certificates issued hereunder.

- Customer must appoint one or more authorized employees or agents as RAA(s). All such employees or agents must meet the minimum personnel qualifications set forth in the Handbook. Such RAA(s) will be entitled to appoint additional RAAs on Customer's behalf. Customer must cause your RAAs receiving Certificates hereunder to abide by the terms of the applicable Subscriber Agreement, which can be found in the Handbook.
- Administrator Functions. Customer must comply with the requirements set forth in the Symantec Trust Network CPS and the Handbook for validating the information in Certificate Applications, approving or rejecting such Certificate Applications, using hardware and software designated by Symantec, and revoking Certificates. Customer must perform such tasks in a competent, professional, and workmanlike manner. Customer can approve a Certificate Application only if (i) the application was made on behalf of a device or internet domain (for purposes of approving SSL Certificates) or a software publisher (for purposes of approving Code Signing certificates) within Customer's organization; and (ii) Customer's RA has authorized the use of Customer's organizational name in the Certificate. If Customer's RAA ceases to have the authority to act as RAA on Customer's behalf, then Customer must promptly revoke such authority. If Customer's organizational name and/or domain registration changes, then Customer's RAA must promptly request revocation of all Certificates issued therein. Customer must not disclose any challenge phrase, PIN, software, or hardware mechanism protecting the RAA Certificate private key to a third party.
- Certificates under the Licensed Certificate Option may be used on one (1) physical device with additional Certificate licenses for each physical server that each device manages, or where replicated Certificates may otherwise reside. Each Certificate under the Licensed Certificate Option has the value of one Unit per device per year. Each Certificate under the Subject Alternative Name Option may be used to secure multiple domains. There is a limit of one hundred (100) domains or "SubAltNames" per Certificate. Each Certificate under the Subject Alternative Name Option has the value of one Unit, per domain, per year.
- The RAA must review the information in it before using it and promptly notify Symantec of any errors. Upon receipt of such notice, Symantec will revoke the RAA Certificate and issue a corrected RAA Certificate, subject to the requirements set forth herein.
- Customer must keep the "Technical Contact" information in the account up to date at all times to ensure that Customer receives provisioning emails and other time sensitive information from Symantec that affect the account.
- Customer must maintain accurate email addresses for each administrative user of the Service.
- Customer's Indemnification Related to Appointment as RA. To the extent any third party claim, suit, proceeding or judgment arises from your failure to strictly comply with the obligations set forth above, Customer must defend, hold harmless, and indemnify Symantec and its directors, officers, agents, employees, successors and assigns from such claim.

Assistance and Technical Support

Support plans are available in connection with *Symantec Managed PKI for SSL Certificate Services*. See under "*Support Plan*" for more details at: https://certmanager.websecurity.symantec.com/contents_en_US/HTML/ecm_onlineguide.htm.

SERVICE-SPECIFIC TERMS

Subscription Service

- Customer's minimum yearly commit ("Minimum Commitment") is as outlined in Symantec's quote, accepted by Customer.
- Symantec shall populate Customer's MPKI Control Center initially with 9,999 Certificate Units. During the Service term, Symantec will top up the Certificate Units on request.
- Sixty days (60) days prior to the end of any given year during the Service term, the parties will meet and review Customer's usage.

- In addition to the Minimum Commitment, Customer will also be responsible to pay any additional fees should Customer's usage grow beyond the pricing tier level corresponding to the Minimum Commitment in any given year during the Service term. Such increase in fees, where applicable, shall be guided by the total number of active and renewable Certificates issued from Customer's MPKI Control Center and calculated in accordance with the pricing range table ("Pricing Range Table") as outlined in Symantec's quote, accepted by Customer. At the end of each year during the Service term, Symantec will review Customer's usage and the Certificates issued from Customer's MPKI Control Center to determine whether any increase in pricing applies. The unit equivalency table ("Unit Equivalency Table"), as outlined in Symantec's quote, accepted by Customer, will be used to convert the number of Certificates issued from Customer's MPKI Control Center into the number of Certificate Units for the purposes of fee calculation.
- Within 30 days of termination or expiration of the Service, all Certificates issued during the Service term will be deactivated and/or revoked.
- Before the final year in the Service term is over, any use in excess of the Minimum Commitment will be charged on a pro-rata basis as follows:
  - The applicable tier level for usage including any overage shall be based on good faith estimate, guided by the total number of active and renewable Certificates issued from Customer's account during the Service term, and according to the Pricing Range Table. The Unit Equivalency Table will be used to convert the number of Certificates into the number of Certificate Units for the purposes of calculation.
  - The overage fee shall be calculated by subtracting the fee stated in the final year's Minimum Commitment from the higher fee associated with the higher tier level according to the Pricing Range Table, then dividing the balance by two (mid-year convention). Customer shall issue a purchase order, and Symantec shall submit an invoice for such overage fee.

Symantec Responsibilities

- Symantec appoints Customer as a non-Symantec RA within the Symantec Trust Network pursuant to the Symantec Trust Network CPS.
- Symantec will notify the individual that Customer appoints as the RAA of any amendments to the Service by posting the information to the MPKI Control Center.
- Symantec grants Customer a limited, non-exclusive, non-transferable, non-sublicenseable license during the term of the Service to access and use the Service, any console, software or other tools which Symantec makes available through the Service. Customer may use the MPKI Control Center and such software and tools solely in accordance with the applicable instructions or documentation and any end-user license terms and/or restrictions provided therewith.
- Symantec will provide the Service until the term of the Service purchased hereunder expires.
- Symantec will provide the infrastructure required to provide the Service.
- Symantec will issue, manage, revoke, and/or renew Certificates in accordance with the instructions that Customer provides through the RAA(s). Upon the approval of a Certificate Application, Symantec will (i) be entitled to rely upon the accuracy of the information in each such approved Certificate Application; and (ii) issue a Certificate to the Certificate Applicant submitting such Certificate Application. Notwithstanding the terms of the "Basic" Service Level Agreement, no service level commitments will apply with respect to the Service provided herein unless a Gold or Platinum Service Fee obligation is then in effect.
- Symantec will notify Customer whether the RAA Certificate Application is approved or rejected. If the RAA Certificate Application is approved, Symantec will issue an RAA Certificate for use in accordance with this Service Description.

- Symantec warrants that (i) there are no errors introduced by Symantec in the Certificate information as a result of Symantec's failure to use reasonable care in creating the Certificate; (ii) its issuance of Certificates shall comply in all material respects with its CPS; and (iii) its revocation services and use of a repository conform to its CPS in all material aspects.

Service Conditions

- You may not disclose the results of any benchmark tests or other tests connected with the Service to any third party without Symantec's prior written consent.
- The use of any Service Component in the form of software shall be governed by the EULA accompanying the software. If no license agreement accompanies the Service Component, it shall be governed by the terms and conditions located at (http://www.symantec.com/content/en/us/enterprise/eulas/b-hosted-service-component-eula-eng.pdf).Any additional rights and obligations with respect to the use of such Service Component shall be as set forth in this Service Description.
- Except as otherwise specified in the Service Description, the Service (including any Hosted Service Software Component provided therewith) may use open source and other third party materials that are subject to a separate license. Please see the applicable Third Party Notice, if applicable, at http://www.symantec.com/about/profile/policies/eulas/.
- Restrictions for Code Signing Certificates. Customer must not use a Code Signing Certificate: (i) for or on behalf of any organization other than Customer's organization; (ii) to perform private or public key operations in connection with any domain and/or organization name other than the one Customer submitted on the Certificate Application; (iii) to distribute malicious or harmful content of any kind including, but not limited to, content that would otherwise have the effect of inconveniencing the recipient of such content; or (iv) in a manner that transfers control or permits access for the private key corresponding to the public key of the Certificate to anyone other than an employee that Customer has authorized (any such transfer to be in a secure manner so as to protect the private key).
- Restrictions for MPKI for Intranet SSL and MPKI for Intranet SSL Premium Certificates. Intranet SSL Certificates must be used only with intranet domains and may not be assigned to devices that are publicly accessible from the Internet. Symantec reserves the right to monitor publicly-facing Internet servers and/or devices to ensure that Intranet SSL Certificates comply with this clause. If Symantec discovers any use of Intranet SSL Certificate(s) not in compliance with this clause, then Symantec will immediately notify Customer's RAA of non-compliance. The RAA must, within twenty (24) hours, either (i) immediately move the Intranet SSL Certificate to an intranet domain; or (ii) remove and revoke the Intranet SSL Certificate from Customer's servers. If the RAA does not revoke or remove the non-compliant Certificate, then Symantec may revoke the RAA Certificate.
- Restrictions for SSL Certificates. Customer must not use a SSL Certificate (i) for or on behalf of any organization other than Customer's own; (ii) to perform private or public key operations in connection with any domain name and/or organization name other than the one(s) submitted by Customer's RAA during enrollment; or (iii) on more than one physical server or device at a time, unless Customer has selected the Licensed Certificate Option. Customer acknowledges that the Licensed Certificate Option can result in increased security risks to Customer's network and Symantec expressly disclaims any liability for breaches of security that result from the distribution of a single key across multiple devices. SYMANTEC CONSIDERS THE UNLICENSED USE OF A SSL CERTIFICATE ON A DEVICE THAT RESIDES ABOVE A SERVER OR SERVER FARM SOFTWARE PIRACY AND WILL PURSUE VIOLATORS TO THE FULLEST EXTENT OF THE LAW.
- Customer agrees that (i) all information material to the issuance of a Certificate and validated by Customer or on its behalf is true and correct in all material respects; (ii) approval of Certificate Applications will not result in Erroneous Issuance; (iii) Customer has substantially complied with the Symantec Trust Network CPS, the Handbook, and Customer's obligations set forth herein; (iv) no Certificate information provided to Symantec infringes the intellectual property rights of any third party;

(v) the information Customer provides in the Certificate Application(s) (including email address(es)) has not been and will not be used for any unlawful purpose; (vi) the RAA has been (since the time of the RAA Certificate's creation) and will remain the only person possessing the RAA Certificate private key, or any challenge phrase, PIN, software, or hardware mechanism protecting the private key, and no unauthorized person has had or will have access to such materials or information; (vii) Customer will use the RAA Certificate exclusively for authorized and legal purposes consistent with this Agreement; and (viii) Customer will not monitor, interfere with or reverse engineer the technical implementation of the Symantec systems or software or the STN, except with the prior written approval from Symantec, and will not otherwise intentionally compromise the security of the Symantec systems or software or the STN.

- Each Service license may support multiple organizations and multiple domain names, as long as each organization and related domain name(s) is owned and registered to the organization that owns the Service account. This Service is not intended for service providers that issue Certificates to unrelated organizations and may not be used for such purpose.
- If Customer displays a Web site trust seal supplied by Symantec, then Customer must install and display such seal only in accordance with the Symantec Seal License Agreement published on the Repository.
- Symantec may update the Service at any time in order to maintain the effectiveness of the Service.
- The Service may be accessed and used globally, subject to applicable export compliance limitations and technical limitations in accordance with the then-current Symantec standards.

DEFINITIONS

Capitalized terms used in this Service Description, and not otherwise defined in the Agreement or this Services Description, have the meaning given below:

"**Administrator**" means any person authorized and responsible for carrying out the trusted functions within the Service.

"Application" means a set of files or a computer program in object code format.

"**Certificate**" or "**Digital Certificate**" means a message that, at least, states a name or identifies the CA, identifies the Subscriber, contains the Subscriber's public key, identifies the Certificate's Operational Period, contains a Certificate serial number, and is digitally signed by the CA.

"**Certificate Applicant**" means an individual or organization that requests the issuance of a Certificate by a CA.

"**Certificate Application**" means a request from a Certificate Applicant (or authorized agent of the Certificate Applicant) to a CA for the issuance of a Certificate.

"**Certification Authority**" or "**CA**" means an entity authorized to issue, manage, revoke and renew Certificates in the STN. For purposes of this Service Description, CA shall mean Symantec and its affiliates, as applicable.

"**Certification Practice Statement**" or "**CPS**" means a statement of the practices that a CA or RA employs in approving or rejecting Certificate Applications and issuing, managing, and revoking Certificates. The CPS is published on the Repository.

"**Code Signing Certificate**" means a Certificate used to electronically sign an Application verifying the identity of and affirming the integrity of code supplied by Publishers and/or Developers.

"Developer" means an individual who is enrolled for an administrator Certificate and accesses the Service on behalf of a Publisher who has developed an Application.

"**Erroneous Issuance**" means (a) issuance of a Certificate not materially in accordance with the procedures required by the CPS; (b) issuance of a Certificate to a Subscriber other than the one named as the subject of the Certificate; or (c) issuance of a Certificate without the authorization of the Subscriber that is the subject of such Certificate.

"**Handbook**" means the *Managed PKI for SSL* Administrator's Handbook published at the Managed PKI Control Center.

"**Licensed Certificate Option**" means the service option that grants a Subscriber the right to use a Certificate on one physical device (the "Initial Physical Device") and obtain additional Certificate licenses for (i) additional physical servers or physical devices that are secured by the Initial Physical Device, including, but not limited to, servers that are secured with a load balancer on which the Certificate is installed; or (ii) additional physical servers on which replicated Certificates are installed. This option may not be available to you.

"**Managed PKI Control Center**" or "**MPKI Control Center**" means the Web console used by Administrators to access the Service.

"**NetSure Protection Plan**" shall mean the extended warranty program offered by Symantec.

"**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.

"Publisher" means the individual, the company, or the legal entity utilizing Code Signing Certificates.

"**Registration Authority**" or "**RA**" means an entity approved by a CA to assist Certificate Applicants in applying for Certificates, and to approve or reject Certificate Applications, revoke Certificates, or renew Certificates.

"**Registration Authority Administrator**" or "**RAA**" means any person appointed by an RA and responsible for carrying out the functions of an RA.

"Repository" means the collection of documents located at www.symantec.com maintained for the purpose of compliance with any applicable CPS.

"**Service Component**" means certain enabling software, hardware peripherals and associated documentation which may be separately provided by Symantec as an incidental part of a Service.

"**SSL Certificate**" means a Certificate used to support SSL sessions between a Web browser (or another client) and a Web server that uses encryption.

"**Subject Alternative Name Option**" means a licensing option that permits the use of a Certificate to secure multiple domains.

"**Subscriber**" means in the case of an individual Certificate, a person who is the Subject of, and has been issued, a Certificate. In the case of an organization Certificate, an organization that owns the equipment or device that is the Subject of, and that has been issued, a Certificate. A Subscriber is capable of using, and is authorized to use, the private key that corresponds to the public key

listed in the Certificate.

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

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

"**Unit**" or "**Certificate Unit**" means the number of Certificates multiplied and duration of Certificates purchased measured by years. Use of additional features may increase the number of Units required for issuance of a Certificate.

END OF SERVICE DESCRIPTION

SYMANTEC SERVICES AGREEMENT

SYMANTEC CORPORATION AND/OR ITS SUBSIDIARIES ("SYMANTEC") IS WILLING TO PROVIDE THE SERVICES TO YOU AS THE INDIVIDUAL, THE COMPANY, OR THE LEGAL ENTITY THAT WILL BE UTILIZING THE SERVICES (REFERENCED BELOW AS "YOU" OR "YOUR") ONLY ON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS OF THIS AGREEMENT ("AGREEMENT"). READ THE TERMS AND CONDITIONS OF THIS AGREEMENT CAREFULLY BEFORE USING THE SERVICES. THIS IS A LEGAL AND ENFORCEABLE CONTRACT BETWEEN YOU AND SYMANTEC. BY CLICKING THE 'ACCEPT', "I AGREE" OR "YES" BUTTON, OR USING THE SERVICES, YOU AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THESE TERMS AND CONDITIONS, CLICK THE "I DO NOT AGREE" OR "NO" BUTTON OR OTHERWISE INDICATE REFUSAL AND MAKE NO FURTHER USE OF THE SERVICES. UNLESS OTHERWISE DEFINED HEREIN, CAPITALIZED TERMS WILL HAVE THE MEANING GIVEN IN THE "DEFINITIONS" SECTION OF THIS AGREEMENT AND SUCH CAPITALIZED TERMS MAY BE USED IN THE SINGULAR OR IN THE PLURAL, AS THE CONTEXT REQUIRES.

IF CUSTOMER PURCHASES THROUGH A RESELLER, CUSTOMER REPRESENTS AND WARRANTS THAT CUSTOMER AUTHORIZES THE RESELLER TO APPLY FOR, ACCEPT, INSTALL, MAINTAIN AND, IF NECESSARY, CANCEL THE SERVICE ON CUSTOMER'S BEHALF. BY AUTHORIZING THE RESELLER AS SUCH, CUSTOMER AGREES TO BE BOUND BY THE TERMS OF THIS AGREEMENT. IF CUSTOMER DOES NOT AGREE TO THESE TERMS, DO NOT USE THE SERVICE.

IF A RESELLER IS ACTING AS THE AUTHORIZED REPRESENTATIVE OF AN END USER IN APPLYING FOR THE SERVICE, RESELLER AGREES TO THE TERMS AND CONDITIONS OF THIS AGREEMENT ON BEHALF OF SUCH END USER CUSTOMER. IF RESELLER IS OBTAINING SERVICES FOR RESELLER'S OWN USE, THIS AGREEMENT APPLIES IN ITS ENTIRETY, EXCEPT FOR YOUR OBLIGATION AS A RESELLER.

1. TERM AND TERMINATION

(a) Term and Termination. Unless earlier terminated in accordance with the terms hereof, this Agreement shall continue until the term of the Service purchased hereunder expires. In the event of a material breach of this Agreement (excluding any breaches for which an exclusive remedy is expressly provided), the non-breaching party may terminate this Agreement if such breach is not cured within thirty (30) days after written notice thereof.

(b) Customer shall cease using the Service upon termination for any reason. Further, any termination of this Agreement shall not relieve either party of any obligations that accrued prior to the date of such termination. The terms that by their nature are intended to survive beyond the termination, cancellation, or expiration shall survive.

2. FEES, PAYMENTS, AND TAXES

Applicable fees will be as set forth on the console at the time of purchase or in the applicable invoice ("**Service Fees"**). All Service Fees are due immediately and are non-refundable, except as otherwise may be stated in the Agreement. All sums due and payable that remain unpaid after any applicable cure period herein will accrue interest as a late charge of 1.5% per month or the maximum allowed by law. The Service Fees stated are exclusive of tax. All taxes, duties, fees and other governmental charges of any kind (including sales, services, use, and value-added taxes, but excluding taxes based on the net income of Symantec) which are imposed by or under the authority of any government on the Service Fees shall be borne by Customer and shall not be considered a part of, a deduction from or an offset against such Service Fees. All payments due to Symantec shall be made without any deduction or withholding on account of any tax, duty, charge, penalty, or otherwise except as required by law in which case the sum payable by Customer in respect of which such deduction or withholding is to be made shall be increased to the extent necessary to ensure that, after making such deduction or withholding, Symantec receives and retains (free from any liability in respect thereof) a net sum

equal to the sum it would have received but for such deduction or withholding being required. This Section does not apply to you if you purchased the Service from a Reseller.

3. PROPRIETARY RIGHTS

"Intellectual Property Rights" means any and all now known or hereafter existing rights associated with intangible property, including, but not limited to, registered and unregistered, United States and foreign copyrights, trade dress, trade names, corporate names, logos, inventions, patents, patent applications, software, know-how and all other intellectual property and proprietary rights. Customer acknowledges that Symantec and its licensors retain all Intellectual Property Rights and title in and to all of their Confidential Information or other proprietary information, products, services, and the ideas, concepts, techniques, inventions, processes, software or works of authorship developed, embodied in, or practiced in connection with the Service provided by Symantec hereunder, including without limitation all modifications, enhancements, derivative works, configurations, translations, upgrades, and interfaces thereto (all of the foregoing "**Symantec Works**"). Symantec Works do not include Customer pre-existing hardware, software, or networks. Nothing in this Agreement shall create any right of ownership or license in and to the other party's Intellectual Property Rights and each party shall continue to independently own and maintain its Intellectual Property Rights.

4. CONFIDENTIAL INFORMATION

"Confidential Information" means material, data, systems and other information concerning the operation, business, projections, market goals, financial affairs, products, services, customers and Intellectual Property Rights of the other party that may not be accessible or known to the general public. Confidential Information shall include, but not be limited to, the terms of this Agreement, and any information that concerns technical details of operation of any of Symantec's services, software or hardware offered or provided hereunder. The parties acknowledge that by reason of their relationship under this Agreement, they may have access to and acquire Confidential Information of the other party. Each party receiving Confidential Information (the "**Receiving Party**") agrees to maintain all such Confidential Information received from the other party (the "**Disclosing Party**"), both orally and in writing, in confidence and agrees not to disclose or otherwise make available such Confidential Information to any third party without the prior written consent of the Disclosing Party; provided, however, that the Receiving Party may disclose the terms of this Agreement to its legal and business advisors if such third parties agree to maintain the confidentiality of such Confidential Information under terms no less restrictive than those set forth herein. The Receiving Party further agrees to use the Confidential Information only for the purpose of performing this Agreement. Notwithstanding the foregoing, the obligations set forth herein shall not apply to Confidential Information which: (i) is or becomes a matter of public knowledge through no fault of or action by the Receiving Party; (ii) was lawfully in the Receiving Party's possession prior to disclosure by the Disclosing Party; (iii) subsequent to disclosure, is rightfully obtained by the Receiving Party from a third party who is lawfully in possession of such Confidential Information without restriction; (iv) is independently developed by the Receiving Party without resort to the Confidential Information; or (v) is required by law or judicial order, provided that the Receiving Party shall give the Disclosing Party prompt written notice of such required disclosure in order to afford the Disclosing Party an opportunity to seek a protective order or other legal remedy to prevent the disclosure, and shall reasonably cooperate with the Disclosing Party's efforts to secure such a protective order or other legal remedy to prevent the disclosure.

5. PRIVACY

By providing Personal Information, as defined below, Customer consents, for itself, its users and contacts, to the following: Customer may be required to provide certain personal information of individuals ("**Personal Information**"), which will be processed and accessible on a global basis by Symantec, its affiliates, agents and subcontractors for the purposes of providing the Service, to generate statistical information about the Service, for internal research and development, including in countries that may have less

protective data protection laws than the country in which You or Your users are located. Symantec may disclose the collected Personal Information as required or permitted by law or in response to a subpoena or other legal process. The Personal Information which Customer may be required to provide, and which is necessary to provide the Service, may include, but is not limited to, names, email address, IP address and contact details of designated users and contacts for the Service, Personal Information provided during configuration of the Service or any subsequent service call and other Personal Information as described herein. Contact the following for any questions or to access Customer's Personal Information: Symantec Corporation – Privacy Program Office, 350 Ellis Street, PO Box 7011, Mountain View, CA 94043, U.S.A. Email: privacyteam@symantec.com

6. INTELLECTUAL PROPERTY INFRINGEMENT INDEMNIFICATION

(a) Symantec's Intellectual Property Indemnification Obligation. To the extent any third party claim, suit, proceeding or judgment is based on a claim that the Services infringe any United States patent, copyright or trade secret (an **"Infringement Claim**"), Symantec shall defend and hold harmless Customer and its directors, officers, agents, employees, successors and assigns from such Infringement Claim, and indemnify Customer for damages finally awarded against Customer to the extent such damages are attributable to direct infringement by the Services or agreed to in settlement by Symantec, plus costs (including reasonable attorneys' fees and expenses).

In the event of any Infringement Claim, Symantec shall have the right, at its sole option, to obtain the right to continue use of the affected Service or to replace or modify the affected Service so that they may be provided by Symantec and used by Customer without infringement of third party United States patent, copyright or trade secret rights. If neither of the foregoing options is available to Symantec on a commercially reasonable basis, Symantec may terminate the Service immediately upon written notice to Customer, and within thirty (30) days after such termination Symantec shall pay a termination fee equal to the prorated portion of any Service Fees (excluding installation and any other non-recurring fees) paid in advance commensurate with the remaining portion of the Service period for which such Service Fees were assessed and paid.

The foregoing indemnity shall not apply to any infringement resulting from: (i) any open source or third party components or products; (ii) any use of the Service not in accordance with the Agreement; (iii) any use of the Services in combination with other services, software or hardware not supplied by Symantec if the alleged infringement would not have occurred but for such combination; (iv) any modification of the Services not performed by Symantec if the alleged infringement would not have occurred but for such modification; or (v) use of an allegedly infringing version of the Service if the alleged infringement could be avoided by the use of a more current version of the Service made available to Customer.

NOTWITHSTANDING ANY OTHER PROVISION OF THE AGREEMENT, THE RIGHTS AND REMEDIES SET FORTH IN SECTION 6 CONSTITUTE THE ENTIRE OBLIGATION OF SYMANTEC AND YOUR EXCLUSIVE REMEDIES WITH RESPECT TO THE SUBJECT MATTER THEREOF.

(b) Customer shall promptly notify Symantec of any claim for indemnity by providing written notice pursuant to Section 9 of this Agreement. When notifying an Infringement Claim, any such notice shall: (i) identify the United States patent, copyright or trade secret asserted by a third party and the Service potentially impacted by the third party claim; and (ii) identify, initially and on an ongoing basis, any other potential indemnitor to whom Customer have provided notice of the third party claim and the Service supplied to Customer by such other potential indemnitor.

After receipt of such notice, Symantec shall have a reasonable time to investigate whether the third party claim might fall within the scope of the indemnification prior to assuming the defense of such claim. With respect to any claim for which such notification is provided or otherwise within the scope of the indemnity, Symantec shall have the right to control and bear full responsibility for the defense of such claim (including any settlements); provided however, that: (i) Symantec shall keep Customer informed of, and consult with Customer in connection with the progress of such litigation or settlement; (ii) Symantec shall not have any right, without Customer's written consent, which consent shall not be unreasonably withheld, to settle any such claim if such settlement arises from or is part of any criminal action, suit or proceeding or contains a stipulation to or admission or acknowledgment of, any liability or wrongdoing (whether in contract, tort or otherwise) on Customer's part, or requires any specific performance or non-pecuniary remedy by Customer; and (iii) You shall have the right to participate in the defense of a claim with counsel of Customer's choice at Customer's own expense.

7. LIMITATION OF LIABILITY

NEITHER PARTY WILL BE LIABLE UNDER ANY CIRCUMSTANCES WHATSOEVER FOR ANY CONSEQUENTIAL, INDIRECT, SPECIAL, PUNITIVE, INCIDENTAL OR EXEMPLARY DAMAGES, INCLUDING WITHOUT LIMITATION LOST PROFITS OR REVENUES, WHETHER FORESEEABLE OR UNFORESEEABLE, EVEN IF SUCH PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. EXCEPT FOR LIABILITY ARISING UNDER: (I) SECTION 4 (CONFIDENTIAL INFORMATION); (II) SECTION 6(A) (SYMANTEC'S INTELLECTUAL PROPERTY INDEMNIFICATION OBLIGATION); OR (III) DEATH OR SERIOUS BODILY INJURY, EACH PARTY'S AGGREGATE LIABILITY FOR ANY AND ALL CLAIMS UNDER THE AGREEMENT SHALL NOT EXCEED TWO (2) TIMES THE AMOUNTS PAID OR PAYABLE BY CUSTOMER TO SYMANTEC DURING THE TWELVE (12) MONTH PERIOD IMMEDIATELY PRECEDING THE EVENTS GIVING RISE TO SUCH CLAIMS, UP TO A MAXIMUM OF ONE MILLION DOLLARS ($1,000,000).

EXCEPT FOR THE EXPRESS LIMITED WARRANTY AS MAY BE SET FORTH IN THE SERVICE DESCRIPTION ABOVE, SYMANTEC DISCLAIMS ALL OTHER WARRANTIES, EXPRESS, IMPLIED, OR STATUTORY, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, SATISFACTION OF CUSTOMER REQUIREMENTS, NON-INFRINGEMENT, AND ANY WARRANTY ARISING OUT OF A COURSE OF PERFORMANCE, DEALING OR TRADE USAGE. SYMANTEC DOES NOT WARRANT THAT THE SERVICES WILL BE UNINTERRUPTED OR ERROR FREE. TO THE EXTENT JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF CERTAIN REPRESENTATIONS, WARRANTIES OR GUARANTEES, SOME OF THE ABOVE EXCLUSIONS MAY NOT APPLY.

8. EVALUATION LICENSE. The terms and conditions of this Section apply if Customer is accessing the Service for evaluation purposes.

(a) ***Use Rights*.** The licenses granted to Customer under the Agreement are for restricted use in a non-production, test environment solely for the purpose of internal, non-commercial evaluation and interoperability testing of the Service. Customer may not use the Service for any other purposes.

(b) ***Evaluation Period.*** The licenses granted to Customer are time limited, and continue through the trial end date as specified upon Customer's enrollment for evaluation license (the "Evaluation Period"). Unless Customer purchases a commercial license for the Service, the licenses granted to Customer under the Agreement are terminated upon expiration of the Evaluation Period, and Customer must follow the requirements specified in "*Term and Termination*" of the Agreement.

(c) ***LIMITATION OF LIABILITY.*** IN NO EVENT WILL SYMANTEC BE LIABLE FOR ANY DAMAGES UNDER THE AGREEMENT, INCLUDING WITHOUT LIMITATION, ANY LOST REVENUE, LOST PROFITS, OR CONSEQUENTIAL DAMAGES EVEN IF ADVISED OF THEIR POSSIBILITY.

(d) ***DISCLAIMERS.*** THE PARTIES ACKNOWLEDGE THAT THE SERVICE OR SOFTWARE PROVIDED TO CUSTOMER PURSUANT TO AND FOR THE PURPOSES OF THIS EVALUATION ARE PROVIDED "AS IS" AND WITHOUT ANY WARRANTY WHATSOEVER. SYMANTEC DISCLAIMS ANY AND ALL WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT OF THIRD-PARTY RIGHTS. THE PARTIES FURTHER ACKNOWLEDGE THAT THE SERVICE DESCRIPTION IN THE AGREEMENT IS SOLELY FOR THE PURPOSE OF DESCRIBING THE SERVICE AND THAT ANY REPRESENTATIONS, WARRANTIES, SERVICE LEVEL COMMITMENTS OR OTHER SYMANTEC COMMITMENTS, OBLIGATIONS OR LIABILITIES THEREIN ARE HEREBY DISCLAIMED BY SYMANTEC. NO SYMANTEC AGENT OR EMPLOYEE IS AUTHORIZED TO MAKE ANY MODIFICATIONS, EXTENSIONS, OR ADDITIONS TO THIS WARRANTY.

(e) ***Order of Precedence.*** In the event of any conflict between this Section and any provision of the Agreement, this Section will prevail and supersede such other provisions with respect to the Service while provide for evaluation purposes.

9. GENERAL PROVISIONS

(a) Notices. Customer shall make all notices, demands or requests to Symantec with respect to this Agreement in writing (excluding email) to the "Contact" address listed on the website from which Customer purchased the Services, with a copy to the General Counsel – Legal Department, Symantec Corporation, 350 Ellis Street, Mountain View, CA 94043, USA.

(b) Entire Agreement. This Agreement (including any applicable Service Description)(if you are a Reseller, also including Reseller agreement with Symantec) constitutes the entire understanding and agreement between Symantec and Customer with respect to the Services purchased hereunder, and supersedes any and all prior or contemporaneous oral or written representation, understanding, agreement or communication relating thereto. Terms and conditions in any purchase orders that are not included in or that conflict with this Agreement are null and void.

(c) Amendments and Waiver. Except as provided below, any term or provision of this Agreement may be amended, and the observance of any term of this Agreement may be waived, only by a writing in the form of a non-electronic record referencing this Agreement and signed by the parties to be bound thereby, and this Agreement may not be modified or extended solely by submission of a purchase order or similar instrument referencing this Agreement. Notwithstanding the foregoing, Symantec may revise the terms of this Agreement at any time. Any such change will be binding and effective thirty (30) days after publication of the change on Symantec's website, or upon notification to Customer by email. If Customer does not agree with the change, it may terminate this Agreement at any time by notifying Symantec and requesting a partial refund of fees paid, prorated from the date of termination to the end of the Service term. By continuing to use the Service after such change, Customer agrees to abide by and be bound thereby.

(d) Force Majeure. Neither party shall be deemed in default hereunder, nor shall it hold the other party responsible for, any cessation, interruption or delay in the performance of its obligations hereunder (excluding payment obligations) due to earthquake, flood, fire, storm, natural disaster, act of God, war, terrorism, armed conflict, labor strike, lockout, boycott or other similar events beyond the reasonable control of such party, provided that the party relying upon this provision: (i) gives prompt written notice thereof, and (ii) takes all steps reasonably necessary to mitigate the effects of the force majeure event; provided further, that in the event a force majeure event extends for a period in excess of thirty (30) days in the aggregate, either party may immediately terminate this Agreement upon written notice.

(e) Severability. In the event that any provision of this Agreement should be found by a court of competent jurisdiction to be invalid, illegal or unenforceable in any respect, the validity, legality and enforceability of the remaining provisions contained shall not, in any way, be affected or impaired thereby.

(f) Compliance with Law. Each party shall comply with all applicable federal, state and local laws and regulations in connection with its performance under this Agreement. Customer hereby acknowledges and agrees that the Services and any related download or technology ("Controlled Technology") may be subject to applicable export control, trade sanction, and physical or electronic import laws, regulations, rules and licenses, and that Customer is hereby notified of the information published by Symantec on http://www.symantec.com/about/profile/policies/legal.jsp, or successor website, and will comply with the foregoing, and with such further export restrictions that may govern individual Services, as specified in the relevant Service Descriptions. Symantec shall have the right to suspend performance of any of its obligations under this Agreement, without any prior notice being required and without any liability to Customer, if You fail to comply with this provision.

(g) Assignment. Customer may not assign the rights granted hereunder or this Agreement, in whole or in part and whether by operation of contract, law or otherwise, without Symantec's prior express written consent. Such consent shall not be unreasonably withheld or delayed.

(h) Independent Contractors. The parties to this Agreement are independent contractors. Neither party is an agent, representative, joint venturer, or partner of the other party. Neither party shall have any right, power or authority to enter into any Agreement for or on behalf of, or incur any obligation or liability of, or to otherwise bind, the other party. Each party shall bear its own costs and expenses in performing this Agreement.

(i) Governing Law. This Agreement and any disputes relating to the Services provided hereunder shall be governed and interpreted according to each of the following laws, respectively, without regard to its conflicts of law provisions: (i) the laws of the State of California, if Customer is located in North America or Latin America; or (ii) the law of England, if Customer is located in Europe, Middle East or Africa; or (iii) the laws of Singapore, if Customer is located in Asia Pacific including Japan. The United Nations Convention on Contracts for the International Sale of Goods shall not apply to this Agreement.

(j) Dispute Resolution. To the extent permitted by law, before Customer files suit or initiates an administrative claim with respect to a dispute involving any aspect of this Agreement, Customer shall notify Symantec, and any other party to the dispute for the purpose of seeking business resolution. Both Customer and Symantec shall make good faith efforts to resolve such dispute via business discussions. If the dispute is not resolved within sixty (60) days after the initial notice, then a party may proceed as permitted under applicable law as specified under this Agreement.

(k) English Version. If this Agreement is translated in any language other than the English language, and in the event of a conflict between the English language version and the translated version, the English language version shall prevail in all respects.