Secure App Service

Service Description

February 2017

Service Overview

The Symantec Secure App ("SAS") Service is available through a web-based portal (the Symantec Code Signing Portal), which enables Publishers and their Developers to ensure authenticity and integrity of their Applications to third parties.

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. Customer acknowledges and agrees that modifications to this Service Description may be necessary to comply with any changes in the Minimum Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates (the "Code Signing Minimum Requirements"), as may be updated from time to time, and/or the CA/Browser Forum Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates (the "CABF Baseline Requirements"), as may be updated from time to time. Customer's continued use of the Service after a change or update has been made will constitute acceptance to the revised terms. For more information, a current copy of the Code Signing Minimum Requirements can be found at: https://casecurity.org/wp-content/uploads/2016/09/Minimum-requirements-for-the-Issuance-and-Management-of-code-signing.pdf, and a current copy of the CABF Baseline Requirements can be found at: https://cabforum.org/wp-content/uploads/CA-Browser-Forum-BR-1.4.2.pdf.

Table of Contents

TECHNICAL/BUSINESS FUNCTIONALITY AND CAPABILITIES

Service Features

- Upon registration for a Publisher account, Symantec will take action to validate Customer's identity and issue a Publisher ID when the Customer identity is validated. The Publisher ID may require installation on a USB token.
- Customer may designate one or more Developers, each of which shall be entitled to designate additional Developers on Customer's behalf.
- Each Developer is eligible to enroll for an administrator Certificate under this Service. Administrator Certificate may require installation on a USB token.
- Applications may be submitted for signing via a browser or a SOAP-based API.
- Signing Events can be purchased and account information is available within the Symantec Code Signing Portal.
- For each Signing Event, a new Key Pair is generated, a Code Signing Certificate issued, and Customer's Application digitally signed with a Code Signing Certificate.
- The private key associated with the Code Signing Certificate will be destroyed.
- The digitally-signed Application is stored until Customer downloads it.
- Certain features of this Service permit Providers to download, review, and/or approve Applications prior to signing. Customer will be notified via email following the Provider's review, if applicable.
- Symantec will not knowingly introduce errors in the process of performing the Service, will comply with its CPS in the performance of the Service, and any use of a Repository and revocation services will conform to its CPS.
- The Service offers key protection as follows:
    - Standard Certificates – Signing Service keys for Standard End Entity Certificates are stored in a PKCS12 format encrypted with a secure system-generated long passphrase. The passphrase is further encrypted using 128 bit AES using a key derived from information that is not stored in the database.
    - Extended Validation Keys – Signing Service keys are stored in FIPS 140-2 level 2 HSMs.
    - All CA Root and Intermediate keys are stored in FIPS 140-2 level 3 HSM.
    - All keys and cryptographic devices are hosted in a military-grade data center.
- The Service operates a Timestamp Authority in compliance with the RFC-3161 standard and the minimum requirements of the Microsoft Trusted Root Certificate Program. Symantec recommends that all customers of the Service use the CA's Timestamping Authority to time-stamp signed code.

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 must maintain Signing Event credits in its account to redeem for the applicable Signing Event. An account without Signing Event credit will become inactive, and reactivation may require additional fees.
- Customer must use Signing Events within one (1) calendar year from the date of purchase, otherwise they will automatically expire.
- Customer must provide the complete Application, or a unique representation of the Application.

- Customer must not knowingly sign any Application that contains suspect code and must use the Code Signing Certificate solely for authorized company business and in compliance with this Service Description and all applicable laws and guidelines.
- Customer must not use a Certificate: (i) for or on behalf of any other individual or entity; (ii) to perform private or public key operations in connection with any individual or entity name other than the one Customer named in its Certificate; or (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.
- If Customer discovers or has reason to believe there has been a Compromise of its private key, or the information within its Certificate is, or has become, incorrect or inaccurate, or if Customer's organization name has changed, or if there is evidence that the Certificate was used to sign suspect code, Customer must immediately notify Symantec to revoke the Certificate.

Customer Service-Specific Warranties

Customer represents and warrants to Symantec and Relying Parties that:

- It has provided accurate and complete information material to the issuance of a Certificate;
- It will inform Symantec if the representations it has made have changed or are no longer valid;
- It will not knowingly submit software for signature that contains suspect code;
- It will immediately inform Symantec if it is discovered (by whatever means) that code submitted to Symantec for signature contained suspect code;
- Any Certificate information it provided (including any email address) does not infringe the Intellectual Property Rights of any third party;
- The Certificate information provided (including any email address) has not been and will not be used for any unlawful purpose;
- Customer or its delegates have been (since the time of its creation) and will remain the only person possessing your 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;
- It will use a Certificate and the Services exclusively for authorized and lawful purposes consistent with this Service Description, the applicable Subscriber Agreement, and the Minimum Requirements;
- It assents to this Service Description as a condition of obtaining a Certificate; and
- It will not monitor, interfere with, or reverse engineer (save to the extent that Customer cannot be prohibited from so doing under applicable law) the technical implementation of or otherwise knowingly compromise the security of the public key infrastructure system or software system.
- Customer further represents and warrants that it has sufficient information to make an informed decision to the extent to which it chooses to rely on a digital certificate, that Customer is solely responsible for deciding whether or not to rely on such information, and that Customer shall bear the legal consequences of its failure to perform any obligation that it might have as a Relying Party under the applicable Relying Party Agreement.
- Customer further represents and warrants that, in the case of third party integration where authentication occurs via Customer's network or systems, (i) it is Customer's responsibility to make any changes required for two-factor authentication on Customer's network or systems with a method of Customer's choice, at all times in compliance with the Minimum Requirements, and (ii) Customer will securely store all tokens and/or key credentials required for two-factor access.

SERVICE-SPECIFIC TERMS

Reporting and Revocation

If an Application Software Supplier requests that Symantec revoke because the Application Software Supplier believes that a Certificate attribute is deceptive, or that the Certificate is being used for malware, bundle ware, unwanted software, or some other illicit purpose, then the Application Software Supplier may request that Symantec revoke a Certificate. Within two (2) business days of receipt of the request, Symantec will either revoke the Certificate or inform the Application Software Supplier that it is conducting an investigation. If Symantec decides to conduct an investigation, it will inform the Application Software Supplier whether or not it will revoke the Certificate, within two (2) business days.

If Symantec decides that the revocation will have an unreasonable impact on Customer, then Symantec will propose an alternative course of action to the Application Software Supplier based on its investigation.

For all incidents involving malware, Symantec is obligated to revoke the Code Signing Certificate in accordance with the following timeframes:

(i) Symantec will contact the software publisher within one (1) business day after Symantec is made aware of the incident;
(ii) Symantec will determine the volume of Relying Parties that are impacted (e.g., based on OCSP logs) within 72 hours after being made aware of the incident.
(iii) Symantec will request the software publisher send an acknowledgement to Symantec within 72 hours of receipt of the request.
(iv) If the publisher responds within 72 hours, then Symantec and publisher will determine a "reasonable date" to revoke the Certificate.
(v) If Symantec does not receive a response, then Symantec will notify the publisher that Symantec will revoke in 7 days if no further response is received.
(vi) If the publisher responds within 7 days, Symantec and the publisher will determine a "reasonable date" to revoke the Certificate.
(vii) If no response is received after 7 days, then Symantec will revoke the Certificate except if Symantec has documented proof (e.g., OCSP logs) that this will cause significant impact to the general public.

Additionally, if (a) the Certificate or the Certificate Applicant is identified as a source of suspect code, (b) the authority to request the Certificate cannot be verified, or (c) the Certificate is revoked for reasons other than Subscriber request (e.g. as a result of private key compromise, discovery of malware, etc.), then Symantec is authorized to share information about the Certificate Applicant, signed application, Certificate, and surrounding circumstances with other CAs or industry groups, including the CA/Browser Forum.

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 license agreement accompanying the software. If no EULA 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/.
- 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.
- Certain features of this Service made available through the Symantec Code Signing Portal enable Providers to access Applications submitted to the Service, so that Providers may test and/or approve such Applications before they are digitally signed. By virtue of the collaborative nature of the Services, Customer acknowledges and agrees that any Confidential Information contained in any Application uploaded to the Symantec Code Signing Portal may be disclosed to Providers, and such disclosure shall not violate the terms of this Service Description.
- Symantec retains the right to revoke a Certificate at any time without notice if: (i) Symantec discovers that the information within a Certificate is no longer valid; (ii) Customer fails to perform its obligations under the terms of this Service Description; or (iii) in Symantec's sole discretion, Customer has engaged in activities which Symantec determines are harmful to its public key infrastructure system.
- 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:

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

"Application Software Supplier" means a supplier of software or other relying-party application software that displays or uses code signing Certificates, incorporates root Certificates, and adopts the Minimum Requirements as all or part of its requirements for participation in a root store program.

"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 the purpose 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. The Code Signing Certificate will not be delivered to Customer and can only be used in the hosted environment of the Service.

"Compromise" means a violation (or suspended violation) of a security policy, in which an unauthorized disclosure of, or loss of control over, sensitive information may have occurred. With respect to private keys, a Compromise is a loss, theft, disclosure, modification, unauthorized use, or other compromise of the security of such private key.

"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.

"**End User License Agreement (EULA)**" means the terms and conditions accompanying Software (defined below).

"Key Pair" means two mathematically related keys, having the following properties: (i) one key can be used to encrypt a message that can only be decrypted using the other key, and (ii) even knowing one key, it is computationally infeasible to discover the other key.

"Operational Period" means the 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 the date and time on which the Certificate expires or is earlier revoked.

"Provider" means a third-party entity that has an interest in ensuring that Applications signed using the Service meet certain quality-control requirements.

"Publisher" means the individual, the company, or the legal entity utilizing the Service (also referenced as "Customer").

"Publisher ID" means an administrator Certificate that is issued to the individual, the company, or the legal entity registered as Publisher for the Service, and used to access the Service and to submit an Application to the Service. The current CPS applicable to the Publisher ID is located at http://www.geotrust.com/resources/cps/pdfs/GeoTrustCPS-Version1.1.12.pdf.

"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.

"Relying Party" means an individual or organization that acts in reliance on a Certificate and/or a digital signature.

"Relying Party Agreement" means an agreement used by a CA setting forth the terms and conditions under which an individual or organization acts as a Relying Party, such as the Symantec Relying Party Agreement published in the Repository.

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

"Signing Event" means the digital signing of an Application.

"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.

"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.

"Timestamp Authority" means a service operated by the CA or a delegated third party for its own Code Signing Certificate users that timestamps data using a Certificate chained to a public root, thereby asserting that the data (or the data from which the data were derived via a secure hashing algorithm) existed at the specified time.

END OF SERVICE DESCRIPTION

SYMANTEC SERVICES AGREEMENT

SYMANTEC CORPORATION AND/OR ITS AFFILIATES ("SYMANTEC") IS WILLING TO PROVIDE THE SERVICES TO CUSTOMER AS THE INDIVIDUAL, THE COMPANY, OR THE LEGAL ENTITY THAT WILL BE UTILIZING THE SERVICES (REFERENCED BELOW AS "CUSTOMER") ONLY ON THE CONDITION THAT CUSTOMER ACCEPTS 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 CUSTOMER AND SYMANTEC. BY CLICKING THE "ACCEPT", "I AGREE" OR "YES" BUTTON, OR USING THE SERVICES, CUSTOMER AGREES TO THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF CUSTOMER DOES 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 THE SERVICE DESCRIPTION ABOVE 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 Symantec Code Signing Portal 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 amount 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: privacy@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 8 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.