

## **CODE SIGNING CERTIFICATE SUBSCRIBER AGREEMENT**

THIS CODE SIGNING CERTIFICATE SUBSCRIBER AGREEMENT ("AGREEMENT") IS ENTERED INTO BETWEEN SYMANTEC AND ITS AFFILIATES ("COMPANY") AND THE ENTITY YOU REPRESENT IN EXECUTING THIS AGREEMENT ("SUBSCRIBER" OR "YOU"). THIS AGREEMENT SETS FORTH THE TERMS AND CONDITIONS APPLICABLE TO SUBSCRIBER IN USING THE SERVICE. BY CLICKING "ACCEPT" OR BY USING THE SERVICE, SUBSCRIBER REPRESENTS AND WARRANTS THAT IT HAS FULL AUTHORITY TO ENTER INTO THIS AGREEMENT AND FULLY PERFORM ITS OBLIGATIONS HEREUNDER, AND SUBSCRIBER AGREES TO BECOME A PARTY TO, AND BE BOUND BY, THESE TERMS. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, DO NOT APPLY FOR, ACCEPT, OR USE ANY CODE SIGNING CERTIFICATE ISSUED UNDER THIS AGREEMENT.

IF YOU ARE A CUSTOMER OF A RESELLER (AS DEFINED HEREIN), SUBSCRIBER REPRESENTS AND WARRANTS THAT IT AUTHORIZES SUCH RESELLER TO APPLY FOR, ACCEPT, INSTALL, MAINTAIN, RENEW, AND, IF NECESSARY, REVOKE THE CERTIFICATE ON SUBSCRIBER'S BEHALF. BY AUTHORIZING THE RESELLER TO USE YOUR CERTIFICATE, SUBSCRIBER AGREES TO BE BOUND BY THE TERMS OF THIS AGREEMENT.

IF YOU ARE A RESELLER AND ARE ACTING AS THE AUTHORIZED REPRESENTATIVE OF A SUBSCRIBER IN APPLYING FOR A CERTIFICATE, RESELLER AGREES TO THE REPRESENTATIONS AND WARRANTIES AS SET FORTH IN THIS AGREEMENT. IF YOU ARE A RESELLER, BUT ARE SOLELY APPLYING FOR YOUR OWN CERTIFICATE, THIS AGREEMENT APPLIES TO YOU AS A SUBSCRIBER IN ITS ENTIRETY, EXCLUDING THE RESELLER-SPECIFIC OBLIGATIONS.

### **Part I – SERVICE-SPECIFIC TERMS AND CONDITIONS**

#### **1. Processing the Certificate Application.**

- a) Company will perform the authentication procedures for the Certificate that You have requested, upon receipt of the applicable payment, and subsequently process any Certificate Application.
- b) Upon approval of the Certificate Application, Company will issue a Class 3 Certificate, which is issued to to provide authentication; message, software, and content integrity signing. The Certificate is intended to provide assurances of the identity of the Subscriber based on a confirmation that the Subscriber organization exists, has authorized the Certificate Application, and that the person submitting the Certificate Application, on behalf of Subscriber, was authorized to do so.
- c) Subscriber must review the information in the Certificate and promptly notify Company of any errors. Upon receipt of such notice, Company may revoke the Certificate and issue a corrected Certificate.

#### **2. Use and Restrictions.**

- a) Subscriber must not knowingly sign software that contains suspect code and must use the Code Signing Certificate solely for the authorized company business and in compliance with this Agreement and all applicable laws and guidelines.
- b) A Certificate may not be used: (i) for or on behalf of any other organization; (ii) to perform private or public key operations in connection with any organization name other than the one

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; nor (iv) for use as control equipment in hazardous circumstances or for uses requiring fail-safe performance such as the operation of nuclear facilities, aircraft navigation or communication systems, air traffic control systems, or weapons control systems, where failure could lead directly to death, personal injury, or severe environmental damage.

c) Subscriber may not use the OCSP or the time stamping services in a manner that is not reasonable with respect to the services it has purchased. Company reserves the right to charge additional fees for excessive usage of these services. d) Company may modify this Agreement when necessary to comply with any changes in the Minimum Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates and/or the CA/Browser Forum Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates.

**3. Reporting and Revocation.** Upon discovery of, or if there is reason to believe that there has been, a compromise of the private key provided under this Agreement, or the information within a Certificate is, or has become, incorrect or inaccurate, or if Subscriber's organization name has changed, or if there is evidence that the Certificate was used to sign suspect code, Subscriber must immediately cease using the Certificate and its associated private key, and must promptly request that Company revoke the subject Certificate(s). If Company discovers or has reason to believe that there has been a compromise of the private key or misuse of a Certificate, Subscriber must respond to Company's instructions within the time specified by Company. Company retains the right to revoke a Certificate at any time without notice if: (i) Company discovers that the information within the Certificate is no longer valid; (ii) Company discovers unauthorized access to the private keys; (iii) Subscriber violates or fails to perform its obligations under the terms of this Agreement; or (iv) Company determines in its sole discretion that the continued use of the Certificate may compromise the security or integrity of the PKI or the Company. Company may also revoke a Certificate for non-payment.

If the Application Software Supplier requests that Company 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 Company revoke the Certificate. Within two (2) business days of receipt of the request, Company will either revoke the Certificate or inform the Application Software Supplier that it is conducting an investigation. If Company 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 Company decides that the revocation will have an unreasonable impact on the customer, then Company will propose an alternative course of action to the Application Software Supplier based on its investigation.

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

- (i) Company will contact the software publisher within one (1) business day after Company is made aware of the incident;
- (ii) Company 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) Company will request the software publisher send an acknowledgement to Company within 72 hours of receipt of the request.

- (iv) If the publisher responds within 72 hours, then Company and publisher will determine a “reasonable date” to revoke the Certificate.
- (v) If Company does not receive a response, then Company will notify the publisher that Company will revoke in 7 days if no further response is received.
- (vi) If the publisher responds within 7 days, Company and the publisher will determine a “reasonable date” to revoke the Certificate.
- (vii) If no response is received after 7 days, then Company will revoke the Certificate except if Company 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 Company 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.

**4. Obligations Upon Revocation or Expiration.** Upon expiration or notice of revocation of a Certificate, Subscriber shall promptly remove all installations of the Certificate and shall not use it for any purpose thereafter.

**5. Company Representations and Warranties.** Company represents and warrants that (i) there are no errors introduced by Company in the Certificate information as a result of Company's failure to use reasonable care in creating the Certificate; (ii) its issuance of Certificates shall comply in all material respects with its Certification Practices Statement (CPS); it is compliant with Code Signing Minimum Requirements outlined by the Certificate Authority Security Council (iii) its revocation services and use of a Repository conform to its CPS in all material aspects; (iv) it has provided the Subscriber with documentation on how to protect a private key; (v) it has provided the Subscriber with a document of code signing best practices during the ordering process.

**6. Subscriber Representations and Warranties.** Subscriber represents and warrants to Company and Relying Parties that:

- (i) All information material to the issuance of a Certificate You provide to Company in each Certificate Application is accurate and complete;
- (ii) Subscriber will inform Company if the representations made to Company in a Certificate Application changed or are no longer valid;
- (iii) The Certificate information that Subscriber provided (including any email address) does not infringe the Intellectual Property Rights of any third party;
- (iv) The Certificate information that Subscriber provided (including any email address) has not been and will not be used for any unlawful purpose;
- (v) Subscriber, or someone explicitly authorized by Subscriber, has been (since the time of its creation) and will remain the only person(s) possessing the 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;
- (vi) Subscriber will use passwords that are randomly generated with at least sixteen (16) characters containing uppercase letters, lowercase letters, numbers, and symbols to transport private keys.
- (vii) Subscriber will generate and operate any device storing private keys in a secure manner, as described in a document of code signing best practices.

- (viii) Subscriber will not apply for a Code Signing Certificate if the Public Key in the Certificate is or will be used with a non-Code Signing Certificate.
- (ix) Subscriber will use the Certificate exclusively for authorized and lawful purposes, including, but not limited to, not using the Certificate to sign Suspect Code and to use the Certificate and private key solely in compliance with applicable laws and solely in accordance with this Agreement.
- (x) Subscriber will provide adequate network and other security controls to protect against misuse of the private key.
- (xi) Subscriber will use each Certificate as an end user and not as a Certification Authority to issue Certificates, certification revocation lists, or otherwise;
- (xii) Subscriber will not use the Certificate until after the Certificate Applicant, or an agent of Certificate Applicant, has reviewed and verified the Certificate contents for accuracy.
- (xiii) Subscriber will promptly cease using a Certificate and its associated private key and promptly request that the Company revoke the Certificate if the Subscriber believes that (a) any information in the Certificate is, or becomes, incorrect or inaccurate, (b) the private key associated with the public key contained in the Certificate was misused or compromised, or (c) there is evidence that the Certificate was used to sign Suspect Code.
- (xiv) Subscriber will promptly cease using the private key corresponding to the public key listed in the Certificate upon expiration or revocation of the Certificate.
- (xv) Each digital signature created using the private key is the Subscriber's digital signature, and the Certificate has been accepted and is operational (not expired or revoked) at the time the digital signature is created;
- (xvi) Subscriber enters into this Agreement as a condition of obtaining a Certificate; and
- (xvii) Subscriber will not monitor, interfere with, or reverse engineer (save to the extent that it cannot be prohibited from so doing under applicable law) the technical implementation of Company's system. Subscriber further represents and warrants that it has sufficient information to make an informed decision as to the extent to which it chooses to rely on a digital certificate, that Subscriber is solely responsible for deciding whether or not to rely on such information, and that Subscriber shall bear the legal consequences of any failure to perform any obligation Subscriber might have as a Relying Party under the applicable Relying Party Agreement.
- (xviii) Subscriber will use one of the following options to generate and protect their Code Signing Certificate private keys: (1) A Trusted Platform Module ("TPM") that generates and secures a key pair and that can document the Subscriber's private key protection through a TPM key attestation; (2) A hardware crypto module with a unit design form factor certified as conforming to at least FIPS 140 Level 2, Common Criteria EAL 4+, or equivalent; (3) Another type of hardware storage token with a unit design form factor of SD Card or USB token (not necessarily certified as conformant with FIPS 140 Level 2 or Common Criteria EAL 4+).
- (xix) If the Services received include malware and/or vulnerability assessment, Subscriber further represents and warrants to Company that it has the corporate power and authority to give Company consent to proceed with the assessment; if the subject web site is managed and/or hosted by a third-party service provider, Subscriber warrants that it has obtained the consent and authorization from the service provider necessary for Company to perform the assessment.
- (xx) Subscriber will keep the token physically separate from the device that hosts the code signing function until a signing session is begun.

**7. Reseller Representations and Warranties.** Reseller represents and warrants to Company and Relying Parties that (i) it has obtained the authority of its customer to enter into this Agreement on behalf of its customer and/or to bind its customer to this Agreement; and (ii) it shall comply with and procure its customer's compliance with this Agreement.

**8. Refund Policy.** If You are not completely satisfied with the Certificate or with the Services for any reason, You may request, within thirty (30) days of Certificate Application approval, that Company revoke the Certificate (if issued), terminate the Services, and provide You with a refund. Following the initial 30-day period, You are entitled to a refund only if Company has breached a warranty or other material obligation under this Agreement. This entire Section does not apply to You if You have purchased Your Certificate from a Reseller.

**9. Indemnity.** You agree to indemnify, defend and hold harmless Company, its directors, shareholders, officers, agents, employees, successors and assigns from any and all third party claims, suits, proceedings, judgments, damages, and costs (including reasonable attorney's fees and expenses) arising from (i) the breach of any of Your warranties, representations and obligations under this Agreement, (ii) any falsehoods or misrepresentations of fact You make on the Certificate Application, (iii) any infringement of an Intellectual Property Right of any person or entity in information or content provided by you, (iv) failure to disclose a material fact on the Certificate Application if the misrepresentation or omission was made negligently or with intent to deceive any party, or (v) failure to protect the private key, or use a trustworthy system, or to take the precautions necessary to prevent the compromise, loss, disclosure, modification or unauthorized use of the private key under the terms of this Agreement. Company shall promptly notify you of any such claim, and You shall bear full responsibility for the defense of such claim (including any settlements); provided however, that (a) You keep Company informed of, and consult with Company in connection with the progress of such litigation or settlement; (b) You shall not have any right, without Company'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 acknowledgement of, any liability or wrongdoing (whether in contract, tort, or otherwise) on the part of Company, or requires any specific performance or non-pecuniary remedy by Company; and (c) Company shall have the right to participate in the defense of a claim with counsel of its choice at its own expense. The terms of this Section 15 will survive any termination of this Agreement. As a Relying Party, You agree to indemnify, defend and hold harmless Company, its directors, shareholders, officers, agents, employees, successors and assigns from any and all third party claims, suits, proceedings, judgments, damages, and costs (including reasonable attorney's fees and expenses) arising from (i) Your failure to perform the obligations of a Relying Party as set forth in the applicable Relying Party Agreement; (ii) Your reliance on a Certificate is not reasonable under the circumstances; or (iii) Your failure to check the status of such Certificate to determine whether the certificate is expired or revoked.

**10. Protection Plan.** Subscriber may be covered by the most current version of the Protection Plan, the details of which are published in the Repository. Under this Protection Plan, Company will pay Subscriber for certain damages arising from the breach by Company of one or more of the limited warranties in the Protection Plan, up to the limits set forth therein. Certificates provided free of charge or in connection with a Company trial offer are not covered by the Protection Plan.

## **11. Limitations of Liability.**

IF THE CERTIFICATE YOU PURCHASED IS COVERED UNDER THE PROTECTION PLAN, THE MOST THAT COMPANY MUST PAY YOU UNDER THE PROTECTION PLAN IS THE AMOUNT DETERMINED BY THE PROTECTION PLAN. ADDITIONALLY, THE LIMITATIONS ON DAMAGES AND PAYMENTS IN THIS SECTION DO NOT APPLY TO REFUND PAYMENTS.

THE LIABILITY LIMITATIONS PROVIDED IN THE AGREEMENT SHALL BE THE SAME REGARDLESS OF THE NUMBER OF DIGITAL SIGNATURES, TRANSACTIONS, OR CLAIMS RELATED TO THIS AGREEMENT. **THIS SECTION DOES NOT LIMIT REFUND PAYMENTS OR PAYMENTS UNDER THE PROTECTION PLAN.**

**12.** Symantec may update the Service at any time in order to maintain the effectiveness of the Service.

**13.** 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.

## **Part II – GENERAL TERMS AND CONDITIONS**

### **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) Subscriber 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 web site at the time of purchase or in the applicable invoice ("**Service Fees**"). All Service Fees are due immediately and are non-refundable, except as may otherwise 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 Subscriber 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 Subscriber 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. Subscriber 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 Subscriber 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, Subscriber consents, for itself, its users and contacts, to the following: Subscriber 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 Subscriber 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 Subscriber'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](mailto: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 Subscriber and its directors, officers, agents, employees, successors and assigns from such Infringement Claim, and indemnify Subscriber for damages finally awarded against Subscriber 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 Subscriber 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 Subscriber, 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 Subscriber.

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

(b) Subscriber shall promptly notify Symantec of any claim for indemnity by providing written notice pursuant to 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 Subscriber has provided notice of the third party claim and the Service supplied to Subscriber 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 Subscriber informed of, and consult with Subscriber in connection with the progress of such litigation or settlement; (ii) Symantec shall not have any right, without Subscriber'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 Subscriber's part, or requires any specific performance or non-pecuniary remedy by Subscriber; and (iii) Subscriber shall have the right to participate in the defense of a claim with counsel of its choice at its 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 2.4 (CONFIDENTIAL INFORMATION); (II) SECTION 2.6(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 SUBSCRIBER 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-SPECIFIC TERMS AND CONDITIONS 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 SUBSCRIBER 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. General Provisions**

(a) Notices. Subscriber 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 Subscriber 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 the Reseller agreement with Symantec) constitutes the entire understanding and agreement between Company and Subscriber 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, Company may revise the terms of this Agreement at any time for the following reasons: (i) it becomes necessary due to applicable laws or industry standards, including, without limitation, any change of the foregoing; (ii) it becomes necessary for technological reasons when any changes is made without materially degrading the Service functionality; (iii) it becomes necessary to maintain the operation of the Service when any change is made without materially degrading the Service functionality; or (iv) changes are in favor of the Subscriber. Any such change will be binding and effective thirty (30) days after publication of the change on Symantec's website, or upon notification to Subscriber by email. If Subscriber 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, Subscriber 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. Subscriber 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 Subscriber is hereby notified of the information published by Company 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. Company 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 Subscriber, if You fail to comply with this provision.

(g) Assignment. Subscriber 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 Company'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: (a) the laws of the State of California, if Subscriber is located in North America or Latin America; or (b) the law of England, if Subscriber is located in Europe, Middle East or Africa; or (c) the laws of Singapore, if Subscriber 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 Subscriber files suit or initiates an administrative claim with respect to a dispute involving any aspect of this Agreement, Subscriber shall notify Company, and any other party to the dispute for the purpose of seeking business resolution. Both Subscriber and Company 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.

## 9. Additional Provisions

The Section entitled *Limitation of Liability* reflects the general limitation of Symantec's liability, which is supplemented by further details that are unique to the provision of the Service. See *Section entitled Protection Plan* in **Part I – SERVICE-SPECIFIC TERMS AND CONDITIONS** for more information.

Except as otherwise specified in the Service Description, the Service, and any software 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 at <http://www.symantec.com/about/profile/policies/eulas/>.

## Part III – DEFINITIONS

“**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 these 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 PKI. For purposes of this Agreement, 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 in the Repository.

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

**"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.

**"Protection Plan"** means the extended warranty program offered by Company and as detailed in the Repository. Symantec's Protection Plan is entitled "NetSure Protection Plan" and Thawte's Protection Plan is entitled "Thawte Protection Plan".

**"Public Key Infrastructure"** or **"PKI"** means the Certificate-based public key infrastructure governed by the Company's certificate policies, which enables the worldwide deployment and use of Certificates by Company, its affiliates, their respective customers, Subscribers, and Relying Parties. Symantec's PKI is entitled "Symantec Trust Network" or "STN"; and Thawte's PKI is entitled "Thawte PKI".

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

**"Relying Party Agreement"** means the agreement under which the CA sets forth the terms and conditions under which an individual or organization acts as a Relying Party, specifically the Relying Party Agreement published in the Repository.

**"Repository"** means the collection of documents located at the link for the repository, which may be accessed from the website of Company from which You applied for Your Certificate, such as [www.symantec.com](http://www.symantec.com), or [www.thawte.com](http://www.thawte.com), .

**"Reseller"** means An entity authorized by Company to resell the Certificates or Services governed by this Agreement.

**"Services"** mean, collectively, the digital certificate service and any related product, benefit, or utility that Company makes available to You through Your purchase of the Certificate.

**"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.

**Code Signing Certificate Subscriber Agreement Version 11.0 (December 2016)**