SYMANTEC ECA SUBSCRIBER AGREEMENT
External Certification Authority Subscriber Agreement

YOU MUST READ THIS EXTERNAL CERTIFICATION AUTHORITY SUBSCRIBER AGREEMENT ("SUBSCRIBER AGREEMENT") BEFORE APPLYING FOR, ACCEPTING, OR USING THE ECA ENCRYPTION AND ECA IDENTITY CERTIFICATE (COLLECTIVELY, "CERTIFICATE"). THIS AGREEMENT BECOMES EFFECTIVE WHEN YOU DOWNLOAD AND ACCEPT AN ECA CERTIFICATE.

This Subscriber Agreement details the terms and conditions regarding your application for a Certificate and, if Symantec accepts your Certificate application, the terms and conditions regarding your use of the Certificate to be issued by Symantec to you as a "Subscriber" of that Certificate. A Certificate is an electronic credential that uses public key cryptography. Each holder of a Certificate has a public/private key pair. The private key, which is held securely by the holder, is used for creating digital signatures. The public key, which may be widely distributed, is used to enable other users to verify digital signatures created by the holder of the private key. In order to rely on a public key, it is necessary that it be certified by an entity called a Certification Authority ("CA"). The CA binds a Subscriber's public key to his or her identity, certifies the public key and creates an electronic credential called the Certificate. The Certificate to be issued to you is part of the Symantec External Certification Authority ("ECA") public key infrastructure in support of the ECA initiative of the United States Department of Defense ("DOD"). The Certificate is intended for use by entities such as US Government contractors and external organizations to enable secure, interoperable communications with the DOD, federal, state and local government agencies. Selected portions of the Symantec ECA Certification Practice Statement ("CPS") and the Symantec ECA Key Recovery Practice Statement ("KRPS"), as amended from time to time, are available publicly at Symantec's website, *www.symantec.com/about/profile/policies/repository.jsp*.

Definitions.

The ***ECA Identity Certificate*** is used for authenticating the user and/or to verify the user's digital signature in electronic applications. There is just one (1) copy of the private key associated with the ECA Identity Certificate and it is controlled exclusively by you.

The ***ECA Encryption Certificate*** is intended to be used for encryption of communication and data. A copy of the private key associated with the ECA Encryption Certificate will be held securely in escrow with Symantec. In the event that you lose access to the private key associated with your ECA Encryption Certificate, or if there is an authorized order to recover this private key, Symantec will provide services to recover it. Symantec will charge a fee, as set forth on Symantec's website and updated from time to time, to recover the subscriber's ECA Encryption Certificate private key.

A ***Registration Authority*** ("RA") is a person or entity approved by Symantec to authenticate Certificate applicants per the requirements in the Symantec ECA CPS and to approve or reject Certificate, revoke Certificates, and renew Certificates.

A ***Key Recovery Agent*** ("KRA") is a person or entity approved by Symantec to authenticate key recovery Requestors, per the requirements in the Symantec ECA CPS and KRPS, and to approve or reject key recovery applications, and recover ECA Encryption Certificate private keys.

A ***Requestor*** means you or anyone authorized (e.g., supervisor, corporate officer, or law enforcement officer) to recover your ECA Encryption Certificate private key.

A ***Trusted Agent*** is a person appointed by a company or organization that is responsible for authenticating Subscribers, revocation requests, and Requestors per the requirements of the Symantec ECA CPS and KRPS.

1. Certificate Application and Issuance. You must provide accurate information on your Certificate application. Upon completion of validation procedures required for your Certificate, Symantec, an authorized Trusted Agent, or RA will process your Certificate application. Symantec will notify you when your Certificate application is approved or rejected. If approved, Symantec will issue you a Certificate for your use in accordance with this Subscriber Agreement. Some of the information you provide in your Certificate application will be contained in your Certificate and will be published in the Symantec ECA repository. When you pick up your Certificate, you are deemed to have accepted the Certificate and agree to be bound to the terms of this Subscriber Agreement. You must review the information in your Certificate before using it and promptly notify Symantec, the Trusted Agent, or RA of any errors. Upon receipt of such notice, Symantec, the authorized Trusted Agent, or RA shall revoke your Certificate and issue a corrected Certificate. Symantec has the right to refuse to issue a Certificate for any reason, in its sole discretion, without incurring any liability for any loss or expenses from such refusal. By accepting a Certificate, you acknowledge that you agree to the terms and conditions contained in the ECA CP, the Symantec ECA CPS, and this Subscriber Agreement.

2. Subscriber Obligations and Use Limits. In addition to the terms of this Subscriber Agreement, you agree to use the private key and Certificate only in accordance with the Symantec ECA Certificate Policy ("CP"), the Symantec ECA Key Recovery Policy ("KRP"), and the Symantec ECA CPS and Symantec KRPS. Certificates issued within the ECA PKI are not designed, intended, or authorized 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. Therefore, you agree not to use your Certificate in any such situation.

3. Security Requirements and Revocation. You must protect your private key at all times in accordance with the Symantec ECA CPS and this Subscriber Agreement. You must use a FIPS 140-1/2 Level 1or higher crypto module to generate and protect your private key. Your workstation must be protected using appropriate physical, procedural, operating system and boundary protection (e.g., firewall) security. In addition, you must select strong passwords and PINs and not allow others to access your private key, crypto module, password, or any other security mechanisms protecting your private key. You must establish strong passwords to dissuade brute force attack by applying the following password rules:

- passwords must be between 6 and 8 characters long, and contain at least one uppercase character and at least two interspersed digits,
- passwords must not be repeated sequences, numbers or letters, and
- passwords must not contain personal names, logins or dictionary words. Select passwords that are easily remembered by you, but not easily guessed by someone else.

The private key of the ECA Encryption Certificate will be securely escrowed with Symantec. If you know or suspect that a compromise of your private key has occurred, you must promptly notify Symantec or, if applicable, the Trusted Agent or RA and request that the Certificate be revoked. The Certificate will be revoked after your request is authenticated by Symantec or, if applicable, the Trusted Agent or RA. Revocation shall result in listing the certificate information on a publicly available CRL as identified by the distribution point identified in the certificate.

You agree that Symantec is entitled to investigate all actual or suspected compromises of your private key or breach in the security of the Symantec ECA PKI as permitted by law and you must reasonably cooperate with Symantec in any such investigation. You agree that Symantec, an authorized Trusted Agent, or the RA is entitled to revoke your Certificate upon an actual or suspected compromise of your private key if you

materially breach this Agreement (including not paying the required Certificate fee, if applicable), or if Symantec, in its sole discretion, determines that your Certificate was issued in a manner that materially differed from what is required under the Symantec ECA CPS and KRPS. You further agree that Symantec is entitled to revoke your Certificate for other reasons, provided that Symantec either: (i) promptly replaces your Certificate with a comparable Certificate; or (ii) provides reasonable compensation. Upon expiration or notice of revocation of your ECA Identity Certificate, you shall no longer use this certificate and the associated private key for any purpose. In the event that your private key is compromised, you shall destroy the private key as specified in CPS section 6.2.10. For software cryptographic modules, you are advised to overwrite the private key data by running an erasure program on the drive and overwriting the drive at least 3 times.

4. Ownership. Except as otherwise set forth herein, all right, title and interest in and to all Symantec (i) registered and unregistered trademarks, service marks and logos; (ii) patents, patent applications, and patentable ideas, inventions, and/or improvements; (iii) trade secrets, proprietary information, and know-how; (iv) all divisions, continuations, reissues, renewals, and extensions thereof now existing or hereafter filed, issued, or acquired; (v) registered and unregistered copyrights including, without limitation, any forms, images, audiovisual displays, text, software; and (vi) all other intellectual property, proprietary rights or other rights related to intangible property which are used, developed, comprising, embodied in, or practiced in connection with any of the Symantec services identified herein ("Symantec Intellectual Property") are owned by Symantec or its licensors, and you agree to make no claim of interest in or ownership of any such Symantec Intellectual Property. You acknowledge that no title to the Symantec Intellectual Property is transferred to you, and that you do not obtain any rights, express or implied, in the Symantec or its licensors' service, other than the rights expressly granted in this Subscriber Agreement. To the extent that you create any Derivative Work (any work that is based upon one or more preexisting versions of a Symantec owned or licensed work provided to you, such as an enhancement or modification, revision, translation, abridgement, condensation, expansion, collection, compilation or any other form in which such preexisting works may be recast, transformed or adapted) such Derivative Work shall be owned by Symantec or its licensors and all right, title and interest in and to each such Derivative Work shall automatically vest in Symantec or its licensors. Symantec shall have no obligation to grant you any right in any such Derivative Work. You may not reverse engineer, disassemble or decompile the Symantec Intellectual Property or make any attempt to obtain source code to the Symantec Intellectual Property. You have the right to use the Certificate under the terms and conditions of this Subscriber Agreement.

5. Modifications. This Subscriber Agreement may not be modified, and no amendment shall be binding, unless made in writing and signed by you and Symantec.

6. Warranties.

6.1 Symantec Warranty.

Symantec warrants to you that:
(i)There are no misrepresentations of fact in such Certificate known to or originating from Symantec;

(ii)Any Certificate issued that assert the policy OIDs identified in the Symantec ECA CPS § 1.2 is issued in accordance with the ECA CP and the Symantec ECA CPS;

(iii)There are no errors in the information in the Certificate that were introduced by Symantec as a result of its failure to exercise reasonable care in creating the Certificate;

(iv)Such Certificates meet all requirements of the Symantec ECA CPS;

(v)Revocation services and use of a repository conform to the Symantec ECA CPS in all respects; and

(vi)Any RA or its Trusted Agent will operate in accordance with the applicable sections of the ECA CP and the Symantec ECA CPS.

6.2 Your Warranty.

By accepting an ECA Certificate issued by Symantec, you certify to and agree with Symantec and to all who rely on the information contained in your Certificate that at the time of acceptance and throughout the operational period of the Certificate, until notified otherwise by you:
(i) Each digital signature created using the private key corresponding to the public key listed in the Certificate is your digital signature and the Certificate has been accepted by you and is operational (not expired, suspended or revoked) at the time the digital signature is created;

(ii) You have no knowledge of any unauthorized access to your private key;

(iii) All representations made by you to Symantec regarding the information contained in the Certificate are correct;

(iv) All information contained in the Certificate is correct to the extent that you had knowledge or notice of such information and you shall promptly notify Symantec of any material inaccuracies in such information provided through the Subscriber enrollment process;

(v) The certificate is being used exclusively for authorized and legal purposes, consistent with the CPS;

(vi) You are an end-user and will not use or authorize anyone to use the private key associated with the ECA certificate for signing any Certificate or CRL;

(vii) Generate PINs, passwords, and pass-phrases used to protect the private keys and used in registration and revocation process in accordance with the requirements of the ECA CP and the Symantec ECA CPS;

(viii) Protect PINs, passwords, and pass-phrases used to protect the private keys and used in registration and revocation process from disclosure to anyone; and

(ix) Install the ECA Root CA trust anchor in accordance with the requirements of the ECA CP and Symantec ECA CPS.

7. DISCLAIMERS OF WARRANTY AND LIABILITY.

7.1 SPECIFIC DISCLAIMERS

EXCEPT AS OTHERWISE SET FORTH IN THE ECA CP AND THE CPS, SYMANTEC:

(I) SHALL NOT INCUR LIABILITY TO ANY PERSON OR ENTITY FOR REPRESENTATIONS CONTAINED IN A CERTIFICATE, PROVIDED THE CERTIFICATE WAS PREPARED IN COMPLIANCE WITH THE CPS, AND PROVIDED FURTHER THAT THE FOREGOING DISCLAIMER SHALL NOT APPLY TO SYMANTEC'S LIABILITY IN TORT FOR NEGLIGENT, RECKLESS, OR FRAUDULENT CONDUCT OR WILLFUL MISCONDUCT, AND

(II) DOES NOT WARRANT THE STANDARDS OR PERFORMANCE OF ANY HARDWARE OR SOFTWARE NOT UNDER EXCLUSIVE OWNERSHIP OF, EXCLUSIVE CONTROL OF, OR LICENSED TO SYMANTEC.

7.2 GENERAL WARRANTY DISCLAIMER

EXCEPT AS SET FORTH IN THE ECA CP AND THE CPS AND THIS SUBSCRIBER AGREEMENT, AND TO THE EXTENT PERMITTED BY APPLICABLE LAW, SYMANTEC DISCLAIMS ANY AND ALL OTHER EXPRESS OR IMPLIED WARRANTIES OF ANY TYPE TO ANY PERSON OR ENTITY, INCLUDING ANY WARRANTY OF MERCHANTABILITY, ANY WARRANTY OF FITNESS FOR A PARTICULAR PURPOSE, AND ANY WARRANTY OF THE ACCURACY OF INFORMATION PROVIDED BY CERTIFICATE APPLICANTS, SUBSCRIBERS, AND THIRD PARTIES.

8. LIMITATIONS OF LIABILITY.

8.1 LIMITATIONS ON AMOUNT OF DAMAGES

IN THE EVENT YOU INITIATE ANY CLAIM, ACTION, SUIT, ARBITRATION, OR OTHER PROCEEDING SEPARATE FROM A REQUEST FOR PAYMENT UNDER THE ECA CPS AND TO THE EXTENT PERMITTED BY APPLICABLE LAW, SYMANTEC'S LIABILITY SHALL BE LIMITED AS FOLLOWS:

THE TOTAL LIABILITY OF SYMANTEC TO ANY PARTY FOR GENERAL CONTRACT, TORT OR ANY OTHER DAMAGES FOR NEGLIGENT, RECKLESS, OR FRAUDULENT CONDUCT BY THE SYMANTEC ECA, ITS RA'S OR TRUSTED AGENTS IN CONNECTION WITH A SINGLE TRANSACTION INVOLVING THE USE OR RELIANCE ON A CERTIFICATE SHALL BE LIMITED TO ONE THOUSAND DOLLARS ($1,000 USD). FURTHERMORE, SYMANTEC'S TOTAL LIABILITY FOR ANY INCIDENT (AGGREGATE OF ALL TRANSACTIONS) INVOLVING THE USE OR RELIANCE ON A CERTIFICATE SHALL BE LIMITED TO ONE MILLION DOLLARS ($1,000,000 USD). THESE LIABILITY CAPS SHALL BE THE SAME REGARDLESS OF THE NUMBER OF DIGITAL SIGNATURES, ACTS OF AUTHENTICATION, OR ENCRYPTED MESSAGES RELATED TO, OR CLAIMS ARISING OUT OF, SUCH TRANSACTION.

8.2 EXCLUSION OF CERTAIN ELEMENTS OF DAMAGES

EXCEPT AS EXPRESSLY PROVIDED IN THE ECA CPS, AND TO THE EXTENT PERMITTED BY APPLICABLE LAW, SYMANTEC SHALL NOT BE LIABLE IN CONTRACT TO ANY PERSON OR ENTITY FOR ANY INDIRECT, SPECIAL, RELIANCE, INCIDENTAL, OR CONSEQUENTIAL DAMAGES (INCLUDING BUT NOT LIMITED TO ANY LOSS OF PROFITS OR LOSS OF DATA), ARISING FROM OR IN CONNECTION WITH THE USE, DELIVERY, LICENSE, PERFORMANCE, OR NONPERFORMANCE OF CERTIFICATES, DIGITAL SIGNATURES, OR ANY OTHER TRANSACTIONS, PRODUCTS, OR SERVICES OFFERED OR CONTEMPLATED BY THE ECA CPS, EVEN IF SYMANTEC HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

TO THE EXTENT PERMITTED BY APPLICABLE LAW, SYMANTEC SHALL NOT BE LIABLE TO ANY PERSON OR ENTITY FOR ANY PUNITIVE DAMAGES ARISING FROM OR IN CONNECTION WITH THE USE, DELIVERY, LICENSE, PERFORMANCE, OR NONPERFORMANCE OF CERTIFICATES, DIGITAL SIGNATURES, OR ANY OTHER TRANSACTIONS OR SERVICES OFFERED OR CONTEMPLATED BY THE ECA CPS.

8.3 U.S. FEDERAL GOVERNMENT LIABILITY

YOU SHALL HAVE NO CLAIM AGAINST THE UNITED STATES FEDERAL GOVERNMENT ARISING FROM USE OF YOUR CERTIFICATE OR A CERTIFICATE MANAGEMENT AUTHORITY'S DETERMINATION TO TERMINATE A CERTIFICATE. IN NO EVENT WILL THE GOVERNMENT BE LIABLE FOR ANY LOSSES, INCLUDING DIRECT OR INDIRECT, INCIDENTAL, CONSEQUENTIAL, SPECIAL, OR PUNITIVE DAMAGES, ARISING OUT OF OR RELATING TO ANY CERTIFICATE ISSUED OR REVOKED BY THE SYMANTEC ECA.

YOU SHALL HAVE NO CLAIM AGAINST THE U.S. FEDERAL GOVERNMENT ARISING FROM ERRONEOUS CERTIFICATE STATUS INFORMATION PROVIDED BY THE SERVERS AND SERVICES OPERATED BY THE ECA AND BY THE U.S. FEDERAL GOVERNMENT.

9. Force Majeure. Except for payment and indemnity obligations hereunder, neither party shall be deemed in default hereunder, nor shall it hold the other party responsible for, any delay or failure in the performance of its obligations hereunder from events beyond its control including, but not limited to, acts of God, acts of war, epidemics, power outages, fire, earthquakes, and other disasters, provided that the party relying upon this section (i) shall have given the other party written notice thereof promptly and, in any event, within five (5) business days of discovery thereof; and (ii) shall take all reasonable steps reasonably necessary under the circumstances to mitigate the effects of the force majeure event upon which such notice is based; provided further, that in the event of a force majeure event described in this section extends for a period in excess of thirty (30) days in the aggregate, the other party may immediately terminate this Subscriber Agreement.

10. Export Control. You agree to conform to applicable export laws and regulations.

11. Severability. You agree that the terms of this Subscriber Agreement are severable. If any term or provision is declared invalid or unenforceable, in whole or in part, that term or provision will not affect the remainder of this Subscriber Agreement; this Subscriber Agreement will be deemed amended to the extent necessary to make this Subscriber Agreement enforceable, valid and, to the maximum extent possible consistent with applicable law, consistent with the original intentions of the parties; and the remaining terms and conditions will remain in full force and effect.

12. Governing Law. **.** If You are located in North America or Latin America, this License Agreement will be governed by the laws of the State of California, United States of America. If You are located in China, this License Agreement will be governed by the laws of the Peoples Republic of China. Otherwise, this License Agreement will be governed by the laws of England. Such governing laws are exclusive of any provisions of the United Nations Convention on Contracts for Sale of Goods, including any amendments thereto, and without regard to principles of conflicts of law. If any provision of this License Agreement is found partly or wholly illegal or unenforceable, such provision shall be enforced to the maximum extent permissible, and remaining provisions of this License Agreement shall remain in full force and effect. A waiver of any breach or default under this License Agreement shall not constitute a waiver of any other subsequent breach or default.

13. Non-Assignment. Except as otherwise set forth herein, your rights under this Subscriber Agreement are not assignable or transferable. Any attempt by your creditors to obtain an interest in your rights under this Subscriber Agreement, whether by attachment, levy, garnishment or otherwise, renders this Subscriber Agreement voidable at Symantec's option.

14. Notices. You shall make all notices, demands, or requests to Symantec with respect to this Subscriber Agreement in writing to: Symantec Corporation, 350 Ellis Street, Mountain View, CA 94043, USA.

15. Survival. This Subscriber Agreement shall be applicable for as long as the Certificate remains valid.

16. Privacy. You agree that Symantec may place in your Certificate certain information that you provide for inclusion in your Certificate. You also agree that Symantec may publish your Certificate and information about its status in the Symantec ECA repository and make this information available to relying parties.

17. Conflict of Provisions. In the event of a conflict between this Subscriber Agreement, the Symantec ECA CPS and other rules, guidelines, or contracts, the Subscriber shall be bound by the provisions of the ECA CP and the Symantec ECA CPS except to the extent that the provisions of the ECA CP and the Symantec CPS are prohibited by law. In the event of a conflict between the ECA CP and the Symantec CPS, the ECA CP shall take precedence over the Symantec ECA CPS.

18. Entire Agreement. This Subscriber Agreement, together with the ECA CP and KRP, and the Symantec ECA CPS and KRPS, constitutes the entire understanding and agreement between Symantec and you with respect to the transactions contemplated, and supersedes any and all prior or contemporaneous oral or written representation, understanding, agreement or communication between Symantec and you concerning the subject matter hereof. Neither party is relying upon any warranties, representations, assurances or inducements not expressly set forth herein.

19. **Effect of a Certificate.** You acknowledge and understand that your ECA Identity Certificate may be used to digitally sign certain instruments that can be signed using a handwritten signature and doing so may lead to enforceable obligations.