AFFIRMTRUST

CERTIFICATION PRACTICE STATEMENT

for the following root certificates:

AffirmTrust Commercial

AffirmTrust Networking

AffirmTrust Premium

AffirmTrust Premium ECC

AFFIRMTRUST
CERTIFICATION PRACTICE STATEMENT

FOR THE FOLLOWING ROOT CERTIFICATES:

AFFIRMTRUST COMMERCIAL
AFFIRMTRUST NETWORKING
AFFIRMTRUST PREMIUM
AFFIRMTRUST PREMIUM ECC

TABLE of CONTENTS

I. INTRODUCTION

A. Overview

This AffirmTrust Certification Practice Statement (the "CPS") dated January 7, 2010 presents the principles and procedures AffirmTrust employs in the issuance and life cycle management of AffirmTrust Extended Validation Server Certificates from the following trusted roots: AffirmTrust Commercial, AffirmTrust Networking, AffirmTrust Premium, and AffirmTrust Premium ECC. This CPS and any and all amendments thereto are incorporated by reference into all of the above-listed AffirmTrust Certificates. AffirmTrust's CPS is available at www.affirmtrust.com/resources/cps.

AffirmTrust is established to provide certificate services for a variety of external customers. The organization operates three CAs, which issues user certificates to various CA customers. Subscribers include all parties who contract with the CA for digital certificate services. All parties who may rely upon the certificates issued by the CA are considered relying parties.

This certification policy statement (CPS) and other AffirmTrust business practices disclosures are applicable to all certificates issued by AffirmTrust.

B. Definitions

For the purposes of this CPS, all capitalized terms used herein shall have the meaning given to them in Section VIII, Definitions, or elsewhere in this CPS.

C. Description and Use of Certificates

1. AffirmTrust Extended Validation Server Certificates

AffirmTrust Extended Validation Server Certificates are X.509 Certificates with SSL Extensions that chain to the following AffirmTrust's Certificate Authority trusted roots: AffirmTrust Commercial, AffirmTrust Networking, AffirmTrust Premium, and AffirmTrust Premium ECC, and which facilitate secure electronic commerce by providing limited authentication of a Subscriber's server and permitting SSL encrypted transactions between a Relying Party's browser and the Subscriber's server. AffirmTrust conforms to the current version of the CA/Browser Forum Guidelines for Issuance and Management of Extended Validation Certificates ("Guidelines") published at http://www.cabforum.org, and implements the EV Guidelines through this CPS and AffirmTrust’s other EV Policies. In the event of any inconsistency between AffirmTrust’s EV Policies and the EV Guidelines, the EV Guidelines take precedence.

AffirmTrust does not issue wildcard certificates, or issue certificates referencing hostnames or private IP addresses.

2. Operational Period of Certificates

At the present time, AffirmTrust issues only Extended Validation Server Certificates. AffirmTrust Extended Validation Server Certificates have an Operational Period of 379 days from the date of issuance unless the Certificate is revoked prior to the expiration of the Certificate's Operational Period.

In the event this CPS is amended and AffirmTrust issues Organization Validated (OV) Certificates, Domain Validated (DV) Certificates, or other Certificate types, the operational period for such certificates will be specified at that time, and will comply with all applicable CA/Browser Forum guidelines.

3. Installation of Certificates

Certificates may not be installed on more than a single server at a time unless Subscriber has requested to do so during the enrollment process and has paid the corresponding fees for installation on multiple servers.

4. Technical Requirements of Certificates

In order to use a Certificate, the appropriate server software must support SSL.

II. GENERAL PROVISIONS

A. Obligations

1. AffirmTrust Obligations

AffirmTrust will: (i) issue Certificates in accordance with this CPS; (ii) perform Extended Validation authentication of Subscribers as described in this CPS; (iii) revoke Certificates as described in this CPS; and (iv) perform any other functions which are described within this CPS.

2. Subscriber Obligations

Subscribers are required to (a) submit truthful information about itself and its business entity, domain ownership and contacts, as applicable, (b) at all times abide by this CPS and the terms and conditions of the Subscriber Agreement, (c) safeguard their private key from compromise, (d) use Certificates only for legal purposes, and (e) immediately request revocation of a Certificate if the related Private Key is Compromised. The Subscriber will only use the AffirmTrust Extended Validation Server Certificate for purposes of negotiating SSL sessions. The Subscriber is solely responsible for the protection of its Private Key and for notifying AffirmTrust immediately in the event that its Private Key has been Compromised.

3. Relying Party Obligations

Relying parties are obligated to: (a) Restrict reliance on certificates issued by the CA to the purposes for those certificates, in accordance with the relevant certificate policy and with this CPS, (b) Verify the status of certificates at the time of reliance by examining the Certificate Revocation List before initiating a transaction involving such Certificate, and (c) Agree to be bound by the provisions of limitations of liability as described in the CPS (or other CA business practices disclosure) upon reliance on a certificate issued by the CA. AffirmTrust does not accept responsibility for reliance on a fraudulently obtained Certificate or a Certificate that is on the CRL.

B. Fees

1. Issuance, Management, and Renewal Fees

AffirmTrust is entitled to charge Subscribers for the issuance, management, and renewal of Certificates. The fees charged will be as stated on AffirmTrust's Web site or in any applicable contract at the time the Certificate is issued or renewed, and may change from time to time without prior notice.

2. Certificate Access Fees

AffirmTrust does not charge a fee as a condition of making Certificates available to Relying Parties.

3. Revocation or Status Information Fees

AffirmTrust does not charge a fee as a condition of making the CRL required by CPS Section II.I available in a repository or otherwise available to Relying Parties. AffirmTrust does not permit access to revocation information, Certificate status information, or time stamping in its repository by third parties that provide products or services that utilize such Certificate status information without AffirmTrust's prior express written consent.

4. Fees for Other Services Such as Policy Information

AffirmTrust does not charge a fee for access to this CPS.

5. Refund and Reissue Policy

A Subscriber may apply a refund toward the issuance of a substitute Certificate. To obtain a substitute Certificate, the Subscriber must provide a new Certificate Signing Request to AffirmTrust or request reissue of a Certificate based upon a prior Certificate Signing Request previously provided to AffirmTrust by the Subscriber.

AffirmTrust will not revoke a Certificate previously issued following a refund or reissue request. A request for a refund or reissue of a Certificate will not be treated as a request by the Subscriber for revocation of a Certificate previously issued by AffirmTrust unless the Subscriber follows the procedures for requesting revocation as stated at Section III.I. of this CPS.

C. Compliance Audit

An annual WebTrust for Certification Authorities examination and Extended Validation WebTrust for Certification Authorities examination will be performed for the Certificates issued under this CPS. AffirmTrust's compliance audits are performed by a public accounting firm that (1) is independent of AffirmTrust and demonstrates proficiency in public key infrastructure technology, information security tools and techniques, security auditing, and the third-party attestation function, and (2) is accredited by the American Institute of Certified Public Accountants (AICPA), which requires the possession of certain skill sets, quality assurance measures such as peer review, competency testing, standards with respect to proper assignment of staff to engagements, and requirements for continuing professional education. The scope of AffirmTrust's annual WebTrust for Certification Authorities examination will include certificate life cycle management and CA business practices disclosure.

With respect to WebTrust audits of AffirmTrust's operations, significant exceptions or deficiencies identified during the WebTrust audit will result in a determination of actions to be taken. This determination is made by AffirmTrust’s PKI Policy Authority with input from the auditor. AffirmTrust’s PKI Policy Authority is responsible for developing and implementing a corrective action plan. If AffirmTrust determines that such exceptions or deficiencies pose an immediate threat to the security or integrity of the Certificates issued under this CPS, a corrective action plan will be developed within 30 days and implemented within a commercially reasonable period of time. For less serious exceptions or deficiencies, AffirmTrust’s PKI Policy Authority will evaluate the significance of such issues and determine the appropriate course of action. Results of the WebTrust audit of AffirmTrust's operations may be released at the discretion of AffirmTrust’s PKI Policy Authority.

AffirmTrust also performs periodic internal audits performed by AffirmTrust personnel according to AffirmTrust's policies and procedures and the EV Guidelines. Results of the periodic audits are presented to AffirmTrust's PKI Policy Authority with a description of any deficiencies noted and corrective actions taken.

D. Limited Warranty/Disclaimer

When AffirmTrust issues an EV Certificate, AffirmTrust represents and warrants to the EV Certificate Beneficiaries, during the period when the EV Certificate is Valid, that AffirmTrust has followed the requirements of the EV Guidelines and its EV Policies in issuing the EV Certificate and in verifying the accuracy of the information contained in the EV Certificate ("EV Certificate Warranties"). The EV Certificate Warranties specifically include, but are not limited to, the following:

(1) Legal Existence. AffirmTrust has confirmed with the incorporating or registration agency in the Subject's jurisdiction of incorporation or registration that, as of the date the EV Certificate was issued, the Subject named in the EV Certificate legally exists as a valid organization or entity in the jurisdiction of incorporation or registration;

(2) Identity. In accordance with the procedures stated in the EV Guidelines, AffirmTrust has confirmed that, as of the date the EV Certificate was issued, the legal name of the Subject named in the EV Certificate matches the name on the official government records of the incorporating or registration agency in the Subject's jurisdiction of incorporation or registration, and if an assumed name is also included, that the assumed name is properly registered by the Subject in the jurisdiction of its place of business;

(3) Right to Use Domain Name. AffirmTrust has taken all steps reasonably necessary to verify that, as of the date the EV Certificate was issued, the Subject named in the EV Certificate has the exclusive right to use the domain name(s) listed in the EV Certificate;

(4) Authorization for EV Certificate. AffirmTrust has taken all steps reasonably necessary to verify that the Subject named in the EV Certificate has authorized the issuance of the EV Certificate;

(5) Accuracy of Information. AffirmTrust has taken all steps reasonably necessary to verify that all of the other information in the EV Certificate is accurate, as of the date the EV Certificate was issued;

(6) Subscriber Agreement. The Subject named in the EV Certificate has entered into a legally valid and enforceable Subscriber Agreement with AffirmTrust that satisfies the requirements of the EV Guidelines;

(7) Status. AffirmTrust will follow the requirements of these Guidelines and maintain a 24 x 7 online-accessible repository with current information regarding the status of the EV Certificate as valid or revoked; and

(8) Revocation. AffirmTrust will follow the requirements of the EV Guidelines and revoke the EV Certificate upon the occurrence of any revocation event as specified in the EV Guidelines.

See the EV Guidelines for definition of defined terms above.

EV Certificates focus only on the identity of the Subject named in the Certificate, and not on the behavior of the Subject. As such, when issuing an EV Certificate, AffirmTrust does not provide any assurances, or otherwise represent or warrant:

- That the Subject named in the EV Certificate is actively engaged in doing business;
- That the Subject named in the EV Certificate complies with applicable laws;
- That the Subject named in the EV Certificate is trustworthy, honest, or reputable in its business dealings; or
- That it is “safe” to do business with the Subject named in the EV Certificate.

EXCEPT FOR THE LIMITED WARRANTY DESCRIBED ABOVE, AFFIRMTRUST EXPRESSLY DISCLAIMS AND MAKES NO REPRESENTATION, WARRANTY OR COVENANT OF ANY KIND, WHETHER EXPRESS OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, WITH RESPECT TO THIS CPS OR ANY CERTIFICATE ISSUED HEREUNDER, INCLUDING WITHOUT LIMITATION, ALL WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE OR USE OF A CERTIFICATE OR ANY SERVICE (INCLUDING, WITHOUT LIMITATION, ANY SUPPORT SERVICES) PROVIDED BY AFFIRMTRUST AS DESCRIBED HEREIN, AND ALL WARRANTIES, REPRESENTATIONS, CONDITIONS, UNDERTAKINGS, TERMS AND OBLIGATIONS IMPLIED BY STATUTE OR COMMON LAW, TRADE USAGE, COURSE OF DEALING OR OTHERWISE ARE HEREBY EXCLUDED TO THE FULLEST EXTENT PERMITTED BY LAW. EXCEPT FOR THE LIMITED WARRANTY DESCRIBED ABOVE, AFFIRMTRUST FURTHER DISCLAIMS AND MAKES NO REPRESENTATION, WARRANTY OR COVENANT OF ANY KIND, WHETHER EXPRESS OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, TO ANY APPLICANT, SUBSCRIBER OR ANY RELYING PARTY THAT (A) THE SUBSCRIBER TO WHICH IT HAS ISSUED A CERTIFICATE IS IN THE FACT THE PERSON, ENTITY OR ORGANIZATION IT CLAIMS TO HAVE BEEN (B) A SUBSCRIBER IS IN FACT THE PERSON, ENTITY OR ORGANIZATION LISTED IN THE CERTIFICATE, OR (C) THAT THE INFORMATION CONTAINED IN THE CERTIFICATES OR IN ANY CERTIFICATE STATUS MECHANISM COMPILED, PUBLISHED OR OTHERWISE DISSEMINATED BY AFFIRMTRUST, OR THE RESULTS OF ANY CRYPTOGRAPHIC METHOD IMPLEMENTED IN CONNECTION WITH THE CERTIFICATES IS ACCURATE, AUTHENTIC, COMPLETE OR RELIABLE.

IT IS AGREED AND ACKNOWLEDGED THAT APPLICANTS AND SUBSCRIBERS ARE LIABLE FOR ANY MISREPRESENTATIONS MADE TO AFFIRMTRUST AND RELIED UPON BY A RELYING PARTY. AFFIRMTRUST DOES NOT WARRANT OR GUARANTEE UNDER ANY CIRCUMSTANCES THE "NON-REPUDIATION" BY A SUBSCRIBER AND/OR RELYING PARTY OF ANY TRANSACTION ENTERED INTO BY THE SUBSCRIBER AND/OR RELYING PARTY INVOLVING THE USE OF OR RELIANCE UPON A CERTIFICATE.

IT IS UNDERSTOOD AND AGREED UPON BY SUBSCRIBERS AND RELYING PARTIES THAT IN USING AND/OR RELYING UPON A CERTIFICATE THEY ARE SOLELY RESPONSIBLE FOR THEIR RELIANCE UPON THAT CERTIFICATE AND THAT SUCH PARTIES MUST CONSIDER THE FACTS, CIRCUMSTANCES AND CONTEXT SURROUNDING THE TRANSACTION IN WHICH THE CERTIFICATE IS USED IN DETERMINING SUCH RELIANCE.

THE SUBSCRIBERS AND RELYING PARTIES AGREE AND ACKNOWLEDGE THAT CERTIFICATES HAVE A LIMITED OPERATIONAL PERIOD AND MAY BE REVOKED AT ANY TIME. SUBSCRIBERS AND RELYING PARTIES ARE UNDER AN OBLIGATION TO VERIFY WHETHER A CERTIFICATE IS EXPIRED OR HAS BEEN REVOKED. AFFIRMTRUST HEREBY DISCLAIMS ANY AND ALL LIABILITY TO SUBSCRIBERS AND RELYING PARTIES WHO DO NOT FOLLOW SUCH PROCEDURES. MORE INFORMATION ABOUT THE SITUATIONS IN WHICH A CERTIFICATE MAY BE REVOKED CAN BE FOUND IN SECTION III.I. OF THIS CPS.

AffirmTrust provides no warranties with respect to another party's software, hardware or telecommunications or networking equipment utilized in connection with the use, issuance, revocation or management of Certificates or providing other services (including, without limitation, any support services) with respect to this CPS. Applicants, Subscribers and Relying Parties agree and acknowledge that AffirmTrust is not responsible or liable for any misrepresentations or incomplete representations of Certificates or any information contained therein caused by another party's application software or graphical user interfaces. The cryptographic key-generation technology used by Applicants, Subscribers and Relying Parties in conjunction with the Certificates may or may not be subject to the intellectual property rights of third parties. It is the responsibility of Applicants, Subscribers and Relying Parties to ensure that they are using technology that is properly licensed or to otherwise obtain the right to use such technology

E. Limitation on Liability

EXCEPT TO THE EXTENT CAUSED BY AFFIRMTRUST'S WILLFUL MISCONDUCT, IN NO EVENT SHALL THE CUMULATIVE LIABILITY OF AFFIRMTRUST TO APPLICANTS, SUBSCRIBER AND/OR ANY RELYING PARTY FOR ALL CLAIMS RELATED TO THE INSTALLATION OF, USE OF OR RELIANCE UPON A CERTIFICATE OR FOR THE SERVICES PROVIDED HEREUNDER INCLUDING WITHOUT LIMITATION ANY CAUSE OF ACTION SOUNDING IN CONTRACT, TORT (INCLUDING NEGLIGENCE), STRICT LIABILITY, FOR BREACH OF A STATUTORY DUTY OR IN ANY OTHER WAY EXCEED (A) FOR SUBSCRIBERS AND RELYING PARTIES, TWO THOUSAND U.S. DOLLARS ($2,000.00) PER SUBSCRIBER OR RELYING PARTY PER EV CERTIFICATE, OR (B) FOR ALL OTHERS, TEN THOUSAND U.S. DOLLARS ($10,000.00) IN THE AGGREGATE ALL CLAIMS AND ALL CLAIMANTS PER EV CERTIFICATE.

AFFIRMTRUST SHALL NOT BE LIABLE IN CONTRACT, TORT (INCLUDING NEGLIGENCE), STRICT LIABILITY, FOR BREACH OF A STATUTORY DUTY OR IN ANY OTHER WAY (EVEN IF AFFIRMTRUST HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES) FOR:

(I) ANY ECONOMIC LOSS (INCLUDING, WITHOUT LIMITATION, LOSS OF REVENUES, PROFITS, CONTRACTS, BUSINESS OR ANTICIPATED SAVINGS);

(II) TO THE EXTENT ALLOWED BY APPLICABLE LAW, ANY LOSS OR DAMAGE RESULTING FROM DEATH OR INJURY OF SUBSCRIBER AND/OR ANY RELYING PARTY OR ANYONE ELSE;

(III) ANY LOSS OF GOODWILL OR REPUTATION; OR

(IV) ANY OTHER INDIRECT, CONSEQUENTIAL, INCIDENTAL, MULTIPLE, SPECIAL, PUNITIVE, EXEMPLARY DAMAGES

IN ANY CASE WHETHER OR NOT SUCH LOSSES OR DAMAGES WERE WITHIN THE CONTEMPLATION OF THE PARTIES AT THE TIME OF THE APPLICATION FOR, INSTALLATION OF, USE OF OR RELIANCE ON THE CERTIFICATE, OR AROSE OUT OF ANY OTHER MATTER OR SERVICES (INCLUDING, WITHOUT LIMITATION, ANY SUPPORT SERVICES) UNDER THIS CPS OR WITH REGARD TO THE USE OF OR RELIANCE ON THE CERTIFICATE.

BECAUSE SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, THE ABOVE EXCLUSIONS OF INCIDENTAL AND CONSEQUENTIAL DAMAGES MAY NOT

APPLY TO AN APPLICANT, SUBSCRIBER AND/OR A RELYING PARTY BUT SHALL BE GIVEN EFFECT TO THE FULL EXTENT PERMITTED BY LAW.

THE FOREGOING LIMITATIONS OF LIABILITY SHALL APPLY ON A CERTIFICATE-BY-CERTIFICATE BASIS, REGARDLESS OF THE NUMBER OF TRANSACTIONS OR CLAIMS RELATED TO EACH CERTIFICATE, AND SHALL BE APPORTIONED FIRST TO THE EARLIER CLAIMS TO ACHIEVE FINAL RESOLUTION.

In no event will AffirmTrust be liable for any damages to Applicants, Subscribers, Relying Parties or any other party arising out of or related to the use or misuse of, or reliance on any Certificate issued under this CPS that: (i) has expired or been revoked; (ii) has been used for any purpose other than as set forth in the CPS (See Section l.C. for more detail); (iii) has been tampered with; (iv) with respect to which the Key Pair underlying such Certificate or the cryptography algorithm used to generate such Certificate's Key Pair, has been Compromised by the action of any party other than AffirmTrust (including without limitation the Subscriber or Relying Party); or (v) is the subject of misrepresentations or other misleading acts or omissions of any other party, including but not limited to Applicants, Subscribers and Relying Parties.

In no event shall AffirmTrust be liable to the Applicant, Subscriber, Relying Party or other party for damages arising out of any claim that a Certificate infringes any patent, trademark, copyright, trade secret or other intellectual property right of any party.

F. Force Majeure

AffirmTrust shall not be liable for any default or delay in the performance of its obligations hereunder to the extent and while such default or delay is caused, directly or indirectly, by fire, flood, earthquake, elements of nature or acts of God, acts of war, terrorism, riots, civil disorders, rebellions or revolutions in the United States, strikes, lockouts, or labor difficulties or any other similar cause beyond the reasonable control of AffirmTrust.

G. Financial Responsibility

1. Fiduciary Relationships

AffirmTrust is not an agent, fiduciary, trustee, or other representative of the Applicant or Subscriber and the relationship between AffirmTrust and the Applicant and the Subscriber is not that of an agent and a principal. AffirmTrust makes no representation to the contrary, either explicitly, implicitly, by appearance or otherwise. Neither the Applicant nor the Subscriber has any authority to bind AffirmTrust by contract or otherwise, to any obligation.

2. Indemnification by Applicant and Subscriber

Unless otherwise set forth in this CPS and/or Subscriber Agreement, Applicant and

Subscriber, as applicable, hereby agrees to indemnify and hold AffirmTrust (including, but not limited to, its officers, directors, employees, agents, successors and assigns) harmless from any claims, actions, or demands that are caused by the use or publication of a Certificate and that arises from (a) any false or misleading statement of fact by the Applicant (or any person acting on the behalf of the Applicant) (b) any failure by the Applicant or the Subscriber to disclose a material fact, if such omission was made negligibly or with the intent to deceive; (c) any failure on the part of the Subscriber to protect its Private Key and Certificate or to take the precautions necessary to prevent the Compromise, disclosure, loss, modification or unauthorized use of the Private Key or Certificate; or (d) any failure on the part of the Subscriber to promptly notify AffirmTrust, as the case may be, of the Compromise, disclosure, loss, modification or unauthorized use of the Private Key or Certificate once the Subscriber has constructive or actual notice of such event.

3. Insurance for EV Certificates

AffirmTrust will maintain the insurance coverages for issuance of EV Certificates as required by the EV Guidelines.

H. Interpretation & Enforcement

1. Governing Law

The enforceability, construction, interpretation, and validity of this CPS and any Certificates issued by AffirmTrust shall be governed by the substantive laws of the State of Oregon, United States of America, excluding (i) the conflicts of law provisions thereof and (ii) the United Nations Convention on Contracts for the International Sale of Goods.

2. Dispute Resolution Procedures

Any dispute, controversy or claim arising under, in connection with or relating to this CPS or any Certificate issued by AffirmTrust shall be subject to and settled finally by binding arbitration in accordance with the Arbitration Rules of the American Arbitration Association (AAA). All arbitration proceedings shall be held in Portland, Oregon. There shall be one arbitrator appointed by the AAA who shall exhibit a reasonable familiarity with the issues involved or presented in such dispute, controversy or claim. The award of the arbitrator shall be binding and final upon all parties, and judgment on the award may be entered by any court having proper jurisdiction thereof. This CPS and the rights and obligations of the parties hereunder and under any Certificate issued by AffirmTrust shall remain in full force and effect pending the outcome and award in any arbitration proceeding hereunder. In any arbitration arising hereunder, each party to the preceding shall be responsible for its own costs incurred in connection with the arbitration proceedings, unless the arbitrator determines that the prevailing party is entitled to an award of all or a portion of such costs, including reasonable attorneys fees actually incurred.

3. Conflict of Provisions

This CPS represents the entire agreement between any Subscriber (including the Subscriber Agreement, if any) or Relying Party and AffirmTrust and supersedes any and all prior understandings and representations pertaining to its subject matter. In the event, however, of a conflict between this CPS and any other express agreement a Subscriber has with AffirmTrust with respect to a Certificate, including but not limited to a Subscriber Agreement, such other agreement shall take precedence.

4. Severability

If any provision of this CPS shall be held to be invalid, illegal, or unenforceable, the validity, legality, or enforceability of the remainder of this CPS shall not in any way be affected or impaired hereby.

I. Repository and CRL

With regard to AffirmTrust Extended Validation Server Certificates, AffirmTrust shall operate one or more CRLs that will be available to both Subscribers and Relying Parties. End-entity certificate CRLs will be updated and reissued at least every seven days, and the nextUpdate field value will not be more than ten days, except as otherwise provided in AffirmTrust's Business Continuity Plan. AffirmTrust shall post the CRLs online at http://www.affirmtrust.com/resources/ at the interval stated in the previous sentence (but also within 24 hours of a Certificate revocation) in a DER format. Each CRL is signed by the issuing AffirmTrust. The procedures for revocation are as stated elsewhere in this CPS. Revoked Certificates will not be removed from the CRL until after the expiration date of the revoked Certificate.

With regard to AffirmTrust’s subordinate CA Certificates issued off of AffirmTrust’s trusted roots, AffirmTrust will post a CRL at least every 12 months that will be available to both Subscribers and Relying Parties.

AffirmTrust retains copies of all Certificates for the life of the CA, but does not archive or retain expired or superseded CRLs. AffirmTrust does not provide other online status mechanisms (e.g., OCSP) for checking certificate status requests or revocation advertisements or provide a Repository or directory making end-entity Certificates available to Relying Parties.

J. Confidentiality Policy

1. Individual Subscriber Information

Except as provided herein, information regarding Subscribers that is submitted on enrollment forms for Certificates will be kept confidential by AffirmTrust (such as contact information for individuals and credit card information) and AffirmTrust shall not release such information without the prior consent of the Subscriber. Notwithstanding the foregoing, AffirmTrust may make such information available (a) to courts, law enforcement agencies or other third parties (including release in response to civil discovery) upon receipt of a court order or subpoena or upon the advice of AffirmTrust's legal counsel, (b) to law enforcement officials and others for the purpose of investigating suspected fraud, misrepresentation, unauthorized access, or potential illegal activity by the Subscriber in the opinion of AffirmTrust and (c) to third parties as may be necessary for AffirmTrust to perform its responsibilities under this Agreement. The foregoing confidentiality obligation shall not apply, however, to information appearing on Certificates, information relating to Certificate revocation, or to information regarding Subscribers that is already in the possession of or separately acquired by AffirmTrust.

2. Aggregate Subscriber Information

Notwithstanding the previous Section, AffirmTrust may disclose Subscriber information on an aggregate basis, and the Subscriber hereby grants to AffirmTrust a license to do so, including the right to modify the aggregated Subscriber information and to permit third parties to perform such functions on its behalf. AffirmTrust shall not disclose to any third party any personally identifiable information about any Subscriber that AffirmTrust obtains in its performance of services hereunder.

K. Waiver

A failure or delay in exercising any right or remedy hereunder shall not operate as a waiver of that right or remedy, nor shall any single or partial exercise of any right or remedy preclude any other or further exercise thereof or the exercise of any other right or remedy.

L. Survival

The following sections shall survive, along with all definitions required thereby: Sections I, II, and VIII.

M. Export

Subscribers and Relying Parties acknowledge and agree to use Certificates in compliance with all applicable laws and regulations, including without limitation U.S. export laws and regulations. AffirmTrust may refuse to issue or may revoke Certificates if in the reasonable opinion of AffirmTrust such issuance or the continued use of such Certificates would violate applicable laws and regulations.

N. Intellectual Property Rights

AffirmTrust’s Public Key Certificates, this CPS, and CRLs issued by AffirmTrust are the property of AffirmTrust.

III. OPERATIONAL REQUIREMENTS

A. Application Requirements

An Applicant for an AffirmTrust Extended Validation Server Certificate shall complete an AffirmTrust enrollment form in a form prescribed by AffirmTrust. All enrollment forms are subject to review, approval and acceptance by AffirmTrust. AffirmTrust performs the authentication steps listed below and checks generally for errors and omissions relevant to the authentication steps taken, but does not otherwise verify the accuracy of the information contained in the Subscriber's Certificate request or otherwise check for errors and omissions.

B. Authentication Process

At the present time, AffirmTrust issues only Extended Validation Server Certificates and only to Private Organizations created in the United States as defined in the EV Guidelines.

AffirmTrust does not presently issue Domain Validated (DV) Certificates (SSL/TLS), Organization Validated (OV) Certificates (SSL/TLS), Email (S/MIME) Certificates, or Code Signing Certificates. In the event AffirmTrust decides to issue one or more of these other Certificate types, it will amend its CPS at that time to include generally the authentication and issuing procedures listed in Appendix A, as applicable for each Certificate type, as well as all applicable CA/Browser Forum guidelines.

Authentication of Subscribers for Extended Validation Server Certificates will follow the Extended Validation Guidelines as published by the CA-Browser Forum, as such Guidelines may be updated from time to time. In the event AffirmTrust decides to issue certificates for any of the following usages, it will authenticate Subscribers using the authentication processes for each as specified in its then-applicable Certification Practices Statement: client authentication, extended validation, secure email, code signing, time stamping, encrypting file system, IP security tunnel, IP security user, and OCSP signing. AffirmTrust does not utilize external Registration Authorities.

Test Certificates may be issued to test applicants, browsers, and other applications as required from AffirmTrust roots or sub-roots (including the generation of a certificate signing request and installation of the test certificate on AffirmTrust test servers) with or without following the EV Guidelines for authentication of Subscribers, but such test Certificates will be restricted in their use solely to the test environment.

AffirmTrust does not delegate any of its Extended Validation authentication functions to subordinate CAs, RAs, Enterprise RAs, and subcontractors at the present time. In the event AffirmTrust decides to delegate any of its Extended Validation authentication functions to such parties in the future, AffirmTrust intends to amend its CPS to follow all relevant rules as stated in the EV Guidelines concerning authentication by such parties (as such rules may be amended from time to time in the Guidelines), including but not limited to EV Guidelines 12.2, 14.1.2, and 14.1.3, and to disclose its requirements concerning appropriate attestations and/or audits to confirm compliance by such parties. In the event AffirmTrust decides to delegate any of its authentication functions for non-EV Certificates to such parties in the future, AffirmTrust intends to amend its CPS to disclose its requirements concerning appropriate attestations and/or audits from the parties to confirm compliance by such parties.

C. Procedure for Processing Certificate Applications

Subscribers submit their Public Key to AffirmTrust for certification electronically through the use of a PKCS#10 Certificate Signing Request (CSR) or other package digitally signed by the Subscriber's Private Key. At a minimum, the Subscriber must provide the data in or with the CSR required by the CA-Browser Forum Extended Validation Guidelines and the AffirmTrust Subscriber Agreement. Subscribers are not required to prove possession of the Private Key corresponding to the Public Key submitted to AffirmTrust. AffirmTrust verifies the accuracy of the information included in the Subscriber's certificate request and performs a limited check for errors and omissions by following the validation procedures outlined in the EV Guidelines.

D. Application Issues

At certain times during the application process in which AffirmTrust is not able to verify information in an enrollment form, a customer service representative may be assigned to the applicant to facilitate the completion of the application process. Otherwise, the applicant may be required to correct its associated information with third parties and re-submit its enrollment form for a Certificate.

E. Certificate Delivery

If AffirmTrust finds that the applicant's enrollment form was sufficiently verified, then the applicant's Certificate will be signed by AffirmTrust. Certificates format, validity period, extension field, and key usage extension field requirements are specified in accordance with AffirmTrust's disclosed certificate profile. Upon signing the applicant's Certificate, AffirmTrust will attach such Certificate to an e-mail and send such e-mail to the appropriate contacts. The e-mail will typically be sent to the administrative contact, technical contact and billing contact designated by the Subscriber. Notification will not be sent to others than the subject of the Certificate and the subject's designated contacts. In certain circumstances the e-mail may include an AffirmTrust customer service representative telephone number and e-mail address for any technical or customer service problems. AffirmTrust, in its sole discretion, may provide such technical or customer support to the applicants/Subscribers. AffirmTrust does not distribute Certificates via Integrated Circuit Cards (ICC) to Subscribers.

F. Certificate Acceptance

The applicant expressly indicates acceptance of a Certificate by using such Certificate.

G. Certificate Renewal and Rekey

Prior to the expiration of an existing Subscriber's Certificate, it is necessary for the Subscriber to obtain a new Certificate to maintain continuity of Certificate usage. Subscribers have the option of generating a new Key Pair to replace the expiring Key Pair (technically defined as "rekey") or of creating a new Certificate Signing Request for an existing Key Pair (technically defined as "renewal"), depending on their preferences and the capabilities and restrictions of the Subscriber's web server and web server key generation tools. For purposes of this CPS, both a "rekey" and "renewal" as defined above will be treated as a renewal Certificate. Rekey after revocation or expiration is not supported.

Renewal Certificates are subject to the authentication processes specified in the EV Guidelines. Expiring Certificates are not revoked by AffirmTrust upon issuance of the renewal Certificate.

The Subscriber must pay the fees and comply with the other terms and conditions for renewal, if any, as presented on AffirmTrust's Web site.

H. Certificate Expiration

AffirmTrust will attempt to notify all Subscribers of the expiration date of their Certificate. Notifications will generally be by e-mail message to the administrative, technical, and/or billing contacts listed in the enrollment form submitted by Subscriber, and will likely occur periodically during the 90 day period prior to the expiration date and the 14 day period following the expiration date. Subscribers may then follow the Certificate renewal procedures.

I. Certificate Revocation and Suspension

1. Circumstances For Revocation

Certificate revocation is the process by which AffirmTrust prematurely ends the Operational Period of a Certificate by posting the serial number of the Certificate to a Certificate Revocation List. AffirmTrust will maintain a continuous 24x7 ability to accept and respond to revocation requests and related inquiries.

A Subscriber shall inform AffirmTrust and promptly request revocation of a Certificate:

- whenever any of the information on the Certificate changes or becomes obsolete; or

- whenever the Private Key, or the media holding the Private Key, associated with the Certificate is Compromised; or

- upon a change in the ownership of a Subscriber's web server.

The Subscriber shall state the reason(s) for requesting revocation upon submitting the request.

AffirmTrust shall revoke a Certificate if:

- The Subscriber requests revocation of its EV Certificate;

- The Subscriber indicates that the original EV Certificate Request was not authorized and does not retroactively grant authorization;

- AffirmTrust obtains reasonable evidence that the Subscriber's Private Key (corresponding to the Public Key in the EV Certificate) has been compromised or is suspected of compromise (e.g. Debian known weak keys), or that the EV Certificate has otherwise been misused;

- AffirmTrust receives notice or otherwise becomes aware that a Subscriber has violated one or more of its material obligations under the Subscriber Agreement;

- AffirmTrust receives notice or otherwise becomes aware that a court or arbitrator has revoked a Subscriber's right to use the domain name listed in the EV Certificate, or that the Subscriber has failed to renew its domain name;

- AffirmTrust receives notice or otherwise becomes aware of a material change in the information contained in the EV Certificate;

- A determination, in AffirmTrust's sole discretion, that the EV Certificate was not issued in accordance with the terms and conditions of the EV Guidelines or AffirmTrust's EV Policies;

- AffirmTrust determines that any of the information appearing in the EV Certificate is not accurate.

- AffirmTrust ceases operations for any reason and has not arranged for another EV Certificate Authority to provide revocation support for the EV Certificate;

- AffirmTrust's right to issue EV Certificates under the EV Guidelines expires or is revoked or terminated, unless AffirmTrust makes arrangements to continue maintaining the CRL Repository;

- The Private Key of AffirmTrust's Root Certificate used for issuing that EV Certificate is suspected to have been compromised;

- Such additional revocation events as AffirmTrust publishes in its EV Policies; or

- AffirmTrust receives notice or otherwise becomes aware that a Subscriber has been added as a denied party or prohibited person to a blacklist, or is operating from a prohibited destination under the laws of AffirmTrust's jurisdiction of operation as described in Section 10.11.2 of the EV Guidelines.

If AffirmTrust initiates revocation of a Certificate, AffirmTrust shall notify the administrative and technical contact provided by Subscriber by e-mail message of the revocation and the reasons why. In the event that AffirmTrust ceases operations, all Certificates issued by AffirmTrust shall be revoked prior to the date that AffirmTrust ceases operations, and AffirmTrust shall notify the administrative and technical contact provided by Subscriber by e-mail message of the revocation and the reasons why.

A refund and/or reissue request by a Subscriber pursuant to Section II.B.5 will not be treated as a request for revocation of a Certificate under this subsection unless the Subscriber specifically requests revocation of the Certificate.

2. Who Can Request Revocation

The only persons permitted to request revocation of a Certificate issued by AffirmTrust are the Subscriber (including designated representatives) and the administrative or technical contact for the Subscriber.

3. Procedure For Revocation Request

To request revocation, a Subscriber must contact AffirmTrust, either by e-mail message, a national/regional postal service, facsimile, or overnight courier, and specifically request "revocation" (using that term) of a particular Certificate identified by the Subscriber. Upon receipt of a revocation request, AffirmTrust will seek confirmation of the request by e-mail message to the person requesting revocation (as defined in Section lll.I.2 above). The message will state that, upon confirmation of the revocation request, AffirmTrust will revoke the Certificate and that posting the revocation to the appropriate CRL will constitute notice to the Subscriber that the Certificate has been revoked. AffirmTrust will require a confirming e-mail message back from either the administrative or technical contact authorizing revocation (or by other means of confirmation acceptable to AffirmTrust). Upon receipt of the confirming e-mail message, AffirmTrust will revoke the Certificate and the revocation will be posted to the appropriate CRL. Notification will be sent to the subject of the Certificate and the subject's designated contacts. There is no grace period available to the Subscriber prior to revocation, and AffirmTrust shall respond to the revocation request within the next business day and post the revocation to the next published CRL.

In the event of Compromise of AffirmTrust's Private Key used to sign a Certificate; AffirmTrust will send an e-mail message as soon as practicable to all Subscribers with Certificates issued off the Private Key stating that the Certificates will be revoked by the next business day and that posting the revocation to the appropriate CRL will constitute notice to the Subscriber that the Certificate has been revoked.

4. Certificate Suspension

AffirmTrust does not support Certificate suspension for the Certificates.

J. Problem Reporting and Response

Subscribers, Relying Parties, Application Software Vendors, and other third parties may report complaints or suspected Private Key compromise, EV Certificate misuse, or other types of fraud, compromise, misuse, or inappropriate conduct related to EV Certificates ("Certificate Problem Reports") at any time.

AffirmTrust will post instructions for how to send Certificate Problem Reports on its website, and will maintain 24x7 capability to accept and acknowledge such Reports. In addition, AffirmTrust will begin investigation of all Certificate Problem Reports within twenty-four hours and decide whether revocation or other appropriate action is warranted based on at least the following criteria:

- The nature of the alleged problem;
- The number of Certificate Problem Reports received about a particular EV Certificate or website;
- The identity of the complainants (for example, complaints from a law enforcement official that a Web site is engaged in illegal activities will carry more weight than a complaint from consumers alleging that they didn't receive the goods they ordered); and
- Relevant legislation.

AffirmTrust will also maintain a continuous 24x7 ability to internally respond to any high-priority Certificate Problem Report, and where appropriate, forward such complaints to law enforcement and/or revoke an EV Certificate that is the subject of such a complaint.

K. Key Management

AffirmTrust does not provide Subscriber Private Key protection or other Subscriber key management services in connection with its Certificates.

L. Subscriber Key Pair Generation

AffirmTrust does not provide Subscriber Key Pair generation or Subscriber Private Key protection for the Certificates.

M. Records Archival

AffirmTrust shall maintain and archive records relating to the issuance of the Certificates for seven (7) years after the date the applicable Certificate ceases to be valid.

N. CA Termination

In the event that it is necessary for AffirmTrust or its CAs to cease operation, AffirmTrust will make a commercially reasonable effort to notify Subscribers, Relying Parties, and other affected entities of such termination in advance of the CA termination. Where CA termination is required, AffirmTrust will develop a termination plan to minimize disruption to Subscribers and Relying Parties. Such termination plans may address the following, as applicable:

- Provision of notice to parties affected by the termination, such as Subscribers and Relying Parties, informing them of the status of the CA,
- Handling the cost of such notice,
- The revocation of the Certificate issued to the CA by AffirmTrust,
- The preservation of the CA's archives and records for the time periods required in this CPS,
- The continuation of Subscriber and customer support services,
- The continuation of revocation services, such as the issuance of CRLs,
- The revocation of unexpired unrevoked Certificates of Subscribers and subordinate CAs, if necessary,
- The payment of compensation (if necessary) to Subscribers whose unexpired unrevoked Certificates are revoked under the termination plan or provision, or alternatively, the issuance of replacement Certificates by a successor CA,
- Disposition of the CA's Private Key and the hardware tokens containing such Private Key,
- Provisions needed for the transition of the CA's services to a successor CA, and
- The identity of the custodian of AffirmTrust’s CA and RA archival records. Unless a different custodian is indicated through notice to Subscribers and Relying Parties, the Registered Agent for AffirmTrust LLC, an Oregon limited liability company, shall be the custodian.

IV. PHYSICAL SECURITY CONTROLS

The AffirmTrust operates a tightly controlled and restricted PKI infrastructure at its secure facility in the greater metropolitan area of a major US city which has been evaluated and approved by formal action of the PKI Policy Authority. The infrastructure is comprised of physical boundaries, computer hardware, software and procedures that provide an acceptable resilience against security risks and provide a reasonable level of availability, reliability and correct operation and the enforcing of a security policy.

The hardware is located in a dedicated, resistant server enclosure. Access to the facility by individuals (personnel and others) is strictly controlled and restricted to authorized and trusted personnel only. Maintenance and other services applied to the cryptographic devices and server systems are limited to authorized AffirmTrust representatives. Physical access to the server infrastructure and facilities is logged and signed by at least one other authorized witness on the four-eyes principal. Otherwise physical access to the systems shall be avoided.

Maintenance operations, changes, modifications or removal of devices or hardware components of the CA server systems are strictly restricted and must be authorized by a member of the AffirmTrust PKI Policy Authority. Any removed device which may contain data (like hard drives) must be wiped out of any data before disposal.

The facility is fully air conditioned and maintains electrical power as well as electrical power backup (UPS), and is supported by an external, independent electricity power source for cases of prolonged power outages.

The facility has taken reasonable precautions to minimize the impact of water exposure. Fire alarm and prevention equipment are installed and available at the premise.

The server room is monitored by a closed-circuit camera and television monitoring system with recording capabilities and records are archived in a rolling and increasing mode. Data is backed up upon the occurrence of all certificate life cycle events.

All waste (paper, media, or any other waste) is disposed of in a secure manner in order to prevent the unauthorized use of, or access to, or disclosure of, waste containing confidential information.

V. TECHNICAL SECURITY CONTROLS

A. CA Key Pair, Sub-CAs

CA Key Pair generation is performed by multiple trained and trusted individuals using secure systems and processes that provide for the security and required cryptographic strength for the keys that are generated and using the RSA algorithm. All CA Key Pairs are generated in pre-planned key generation ceremonies witnessed by independent auditors in accordance with the requirements of the EV Guidelines. The activities performed in each key generation ceremony are recorded, dated and signed by all individuals involved. These records are kept for audit and tracking purposes for a length of time deemed appropriate by AffirmTrust's PKI Policy Authority, but not less than the Key Pair validity period plus the archive period.

The cryptographic modules used for key generation and storage meet the requirements of FIPS 140-2 level 3. The CA Root Keys for each CA Certificate were generated and are stored in hardware. The Root Keys for each CA Certificate are maintained under multi-person control. The CA private key is backed up (but not escrowed), stored, and recovered by authorized personnel using dual control in a physically secured environment. Backup copies of the CA private keys are subject to the same or greater level of security controls as keys currently in use. If required, recovery of the CA private key is conducted in the same secure schema used in the backup process, using dual control.

The Root Keys for each CA Certificate may be used for Certificate signing (Extended Validation server authentication), CRL signing, and off-line CRL signing.

AffirmTrust makes the CA Certificates available to Subscribers and Relying Parties through their inclusion in web browser software. For specific applications, AffirmTrust's Public Keys are provided by the application vendors through the applications root stores.

AffirmTrust has not authorized any external sub-CAs to be operated by third parties at the present time. In the event AffirmTrust decides to authorize any external sub-CAs to be operated by third parties in the future, AffirmTrust intends to amend this CPS to impose legal, technical, attestation and audit, and other requirements on the sub-CAs substantially equivalent to those followed by AffirmTrust for similar certificates. In the event an external sub-CA is authorized to issue EV Certificates, AffirmTrust intends to state in its CPS AffirmTrust's practices following all relevant rules as stated in the EV Guidelines concerning external sub-CAs operated by third parties (as such rules may be amended from time to time in the Guidelines), including but not limited to EV Guidelines 7.1.2(3), 8.2.2, 10.12, 11.1.1(1), 12.2.2, and 15.2.2.

End-entity certificates are not issued off AffirmTrust's root certificates, but are issued off intermediate certificates that have been issued off the following Sub-CA root certificates:

For AffirmTrust Commercial Root:

- End-entity certificates using Extended Validation authentication will be issued off the sub-CA root certificates: AffirmTrust Commercial Extended Validation. Key length is 2048 bits. Each end-entity Extended Validation (EV) Certificate issued by AffirmTrust to a Subscriber will include AffirmTrust's EV OID for the AffirmTrust Commercial Root in the certificate's certificatePolicies extension. AffirmTrust's EV OID used for this purpose is 1.3.6.1.4.1.34697.2.1.

- End-entity certificates using Organization Validated authentication will be issued off the sub-CA root certificates: AffirmTrust Commercial OV Sub-CA. Key length is 2048 bits.

- End-entity certificates using Domain Validated authentication will be issued off the sub-CA root certificates: AffirmTrust Commercial DV Sub-CA. Key length is 2048 bits.

- End-entity certificates issued by any future external sub-CA will be issued off a sub-CA root certificate identified by sub-CA identity and authentication method with the following naming scheme: AffirmTrust Commercial *[additional identity information re sub-CA and authentication method].* Key length will be 2048 bits.

For AffirmTrust Networking Root:

- End-entity certificates using Extended Validation authentication will be issued off the sub-CA root certificates: AffirmTrust Networking Extended Validation. Key length is 2048 bits. Each end-entity Extended Validation (EV) Certificate issued by AffirmTrust to a Subscriber will include AffirmTrust's EV OID for the AffirmTrust Networking Root in the certificate's certificatePolicies extension. AffirmTrust's EV OID used for this purpose is 1.3.6.1.4.1.34697.2.2.

- End-entity certificates using Organization Validated authentication will be issued off the sub-CA root certificates: AffirmTrust Networking OV Sub-CA. Key length is 2048 bits.

- End-entity certificates using Domain Validated authentication will be issued off the sub-CA root certificates: AffirmTrust Networking DV Sub-CA. Key length is 2048 bits.

- End-entity certificates issued by any future external sub-CA will be issued off a sub-CA root certificate identified by sub-CA identity and authentication method with the following naming scheme: AffirmTrust Networking *[additional identity information re sub-CA and authentication method].* Key length will be 2048 bits.

For AffirmTrust Premium Root:

- End-entity certificates using Extended Validation authentication will be issued off the sub-CA root certificates: AffirmTrust Premium Extended Validation. Key length is 4096 bits. Each end-entity Extended Validation (EV) Certificate issued by AffirmTrust to a Subscriber will include AffirmTrust's EV OID for the AffirmTrust Commercial Root in the certificate's certificatePolicies extension. AffirmTrust's EV OID used for this purpose is 1.3.6.1.4.1.34697.2.3.

- End-entity certificates using Organization Validated authentication will be issued off the sub-CA root certificates: AffirmTrust Premium OV Sub-CA. Key length is 4096 bits.

- End-entity certificates using Domain Validated authentication will be issued off the sub-CA root certificates: AffirmTrust Premium DV Sub-CA. Key length is 4096 bits.

- End-entity certificates issued by any future external sub-CA will be issued off a sub-CA root certificate identified by sub-CA identity and authentication method with the following naming scheme: AffirmTrust Premium *[additional identity information re sub-CA and authentication method.]* Key length will be 4096 bits.

For AffirmTrust Premium ECC Root:

- End-entity certificates using Extended Validation authentication will be issued off the sub-CA root certificates: AffirmTrust Premium ECC Extended Validation. Key length is 384 bits. Each end-entity Extended Validation (EV) Certificate issued by AffirmTrust to a Subscriber will include AffirmTrust's EV OID for the AffirmTrust Commercial Root in the certificate's certificatePolicies extension. AffirmTrust's EV OID used for this purpose is 1.3.6.1.4.1.34697.2.4.

- End-entity certificates using Organization Validated authentication will be issued off the sub-CA root certificates: AffirmTrust Premium ECC OV Sub-CA. Key length is 384 bits.

- End-entity certificates using Domain Validated authentication will be issued off the sub-CA root certificates: AffirmTrust Premium ECC DV Sub-CA. Key length is 384 bits.

- End-entity certificates issued by any future external sub-CA will be issued off a sub-CA root certificate identified by sub-CA identity and authentication method with the following naming scheme: AffirmTrust Premium ECC *[additional identity information re sub-CA and authentication method.]* Key length will be 384 bits.

Both AffirmTrust's root certificates and any AffirmTrust intermediate certificates are referred to as the "CA Certificates".

AffirmTrust generally provides the full certificate chain (including the issuing CA Certificate and any CA Certificates in the chain) to the Subscriber upon Certificate issuance. AffirmTrust CA Certificates may also be downloaded from the AffirmTrust Resource Web site at www.affirmtrust.com/resources.

There are no restrictions on the purposes for which the CA Key Pair may be used. The usage period or active lifetime for the AffirmTrust Commercial and AffirmTrust Networking Public and Private Keys is through December 31, 2030, and the usage period or active lifetime for the AffirmTrust Premium and AffirmTrust Premium ECC

Public and Private Keys is through December 31, 2040. The CA Certificate for each is generally available in the Root Key Store of the applicable browser or application software.

In the event of the Compromise of one or more of the AffirmTrust Root Key(s) (including the CA Certificates), AffirmTrust shall promptly notify all Subscribers via e-mail and notify Relying Parties and others via the CRL and additional notice posted at www.affirmtrust.com/resources, and shall revoke all Certificates issued with such AffirmTrust Root Key(s).

When AffirmTrust CA Key Pairs reach the end of their validity period, such CA Key Pairs will be archived for a period of at least 5 years. Archived CA Key Pairs will be securely stored using offline media. Procedural controls will prevent archived CA Key Pairs from being returned to production use. Upon the end of the archive period, all copies of the archived CA Private Keys will be securely destroyed.

AffirmTrust CA Key Pairs are retired from service at the end of their respective maximum lifetimes as defined above, and so there is no key changeover. Certificates may be renewed as long as the cumulative certified lifetime of the Certificate Key Pair does not exceed the maximum CA Key Pair lifetime. AffirmTrust Key Pairs will be generated as necessary, for example to replace CA Key Pairs that are being retired, to supplement existing, active Key Pairs and to support new services in accordance with this CPS. AffirmTrust will cease to use the CA Key Pair at the end of the cryptoperiod or when the compromise of the CA Private Key is known our suspected.

B. Subscriber Key Pairs

AffirmTrust recommends that Subscribers select the highest encryption strength option when generating their certificate requests. All AffirmTrust certificates will accommodate the use of domestic and international 256-, 128-, 56-, and 40-bit strength browsers and web servers.

Generation of Subscriber Key Pairs is generally performed by the Subscriber, and may be generated in either hardware or software. For server Certificates, the Subscriber typically uses the key generation utility provided with the web server software. AffirmTrust does not require any particular standard for the module used to generate the Keys. Key pairs generated by the Subscriber for Certificates may be used for server authentication. There are no purposes for which AffirmTrust restricts the use of the Subscriber key or Certificate.

For X.509 Version 3 Certificates, AffirmTrust generally populates the KeyUsage extension of Certificates in accordance with RFC 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, May 2008.

C. Business Continuity Management Controls

AffirmTrust has a business continuity plan (BCP) to maintain or restore the AffirmTrust CAs business operations in a reasonably timely manner following interruption to or failure of critical business processes. The BCP defines the following time periods for acceptable system outage and recovery time:

(1) Restore ability to receive and respond to Subscriber and Public communications – 3 business days

(2) Post an existing CRL – 3 business days

(3) Restore existing root keys – 7 days

(4) Publish a new CRL - 7 days

(5) Vet a Subscriber -2 weeks

(6) Issue a Certificate - 2 weeks

(7) Audit Security Policy – 1 month

(8) Audit Vetting Procedures - 2 months

(9) Create new root keys – 2 months

Backup copies of essential business and CA information are made routinely. Backup root keys are maintained several miles from the AffirmTrust facility's main site.

D. Event Logging, Documentation, and Audit Trail Requirements

AffirmTrust’s event journal data is archived at least monthly (or more frequently depending on data changes). Daily and monthly event journals are reviewed at least monthly by the PKI Policy Authority or its designee. Event logs will be retained for at least seven years and will be available to independent auditors upon request.

AffirmTrust will record in detail every action taken to process an EV Certificate Request and to issue an EV Certificate, including all information generated or received in connection with an EV Certificate Request, and every action taken to process the Request, including time, date, and personnel involved in the action. These records will be available as auditable proof of the CA's practices.

The foregoing record requirements include, but are not limited to, an obligation to record the following events:

- CA key lifecycle management events, including:

  - Key generation, backup, storage, recovery, archival, and destruction; and
  - Cryptographic device lifecycle management events.

- CA and Subscriber EV Certificate lifecycle management events, including:
  - EV Certificate Requests, renewal and re-key requests, and revocation;
  - All verification activities required by these Guidelines;
  - Date, time, phone number used, persons spoken to, and end results of verification telephone calls;
  - Acceptance and rejection of EV Certificate Requests;
  - Issuance of EV Certificates; and
  - Generation of EV Certificate Revocation Lists (CRLs).
- Security events, including:
  - Successful and unsuccessful PKI system access attempts;
  - PKI and security system actions performed;
  - Security profile changes;
  - System crashes, hardware failures, and other anomalies;
  - Firewall and router activities; and
  - Entries to and exits from the CA facility.
- Log entries MUST include the following elements:
  - Date and time of entry;
  - Identity of the person making the journal entry; and
  - Description of entry.

AffirmTrust will retain all documentation relating to all EV Certificate Requests and verification thereof, and all EV Certificates and revocation thereof, for at least seven years after any EV Certificate based on that documentation ceases to be valid. In connection therewith, AffirmTrust will maintain current an internal database of all previously revoked EV Certificates and previously rejected EV Certificate Requests due to suspected phishing or other fraudulent usage or concerns. Such information will be used to flag suspicious EV Certificate Requests.

VI. CERTIFICATE AND CRL PROFILE

A. Certificate Profile

AffirmTrust Certificates conform to (a) ITU-T Recommendation X.509 Version 3 (1997): Information Technology - Open Systems Interconnection - The Directory: Authentication Framework, June 1997, and (b) RFC 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, May 2008 ("RFC 5280"). Certificate extensions and their criticality, as well as cryptographic algorithm object identifiers, are populated according to the IETF RFC 5280 standards and recommendations.

The name forms for Subscribers are enforced through AffirmTrust's internal policies and the authentication steps described elsewhere in this CPS and the EV Guidelines. Name constraint enforcement is not through the name constraint extension, but through the authentication steps followed and contractual limitations with each Subscriber. Names must be meaningful as required by the EV Guidelines, but do not have to be unique. Once a Subscriber has established its right to use a name under the EV Guidelines AffirmTrust will issue a Certificate in that name. Any name claim disputes between a Subscriber and any other party (including disputes involving trademarks) must be resolved separately by the parties, and AffirmTrust will abide by any final and binding judicial or arbitration result between the parties. The policy constraints extensions and policy qualifiers syntax and semantics, when used, conform to the RFC 5280 standards.

AffirmTrust does not apply any specific Certificate Policy Object Identifiers, but instead refers to the applicable CPS.

B. CRL Profile

AffirmTrust issued CRLs conform to all RFC 5280 standards and recommendations.

VII. CPS ADMINISTRATION

A. CPS Authority

The authority administering this CPS is the AffirmTrust PKI Policy Authority. The Authority shall be responsible for establishing and maintaining all AffirmTrust security, information, and other critical policies as well as change control procedures. The Authority shall also establish and maintain appropriate personnel security policies as well as physical, operational, system access, and environmental security policies and compliance with legal requirements in order to enhance and support the trustworthiness of AffirmTrust’s operations and Certificates and help protect them from compromise or interruption. Inquiries to AffirmTrust's PKI Policy Authority should be addressed as follows:

PKI Policy Authority
AffirmTrust LLC
838 SW First Avenue, Suite 210
Portland, OR 97204 USA
pkipolicv@affirmtrust.com

AffirmTrust does not support a Certificate Policy (CP) for AffirmTrust Commercial, AffirmTrust Networking, AffirmTrust Premium, and AffirmTrust Premium ECC Extended Validation server certificates.

B. Contact Person

Address inquiries about the CPS to pkipolicv@affirmtrust.com or to the following address:

PKI Policy Authority
AffirmTrust LLC
838 SW First Avenue, Suite 210
Portland, OR 97204 USA

C. CPS Change Procedures

This CPS (and all amendments to this CPS) is subject to approval by the PKI Policy Authority. AffirmTrust may change this CPS at any time without prior notice. The CPS and any amendments thereto are available through www.affirmtrust.com/resources/cps. Amendments to this CPS will be evidenced by a new version number and date posted online (except where the amendments are purely clerical), and shall apply as of the stated effective date.

VIII. DEFINITIONS

AffirmTrust. AffirmTrust LLC, an Oregon, USA limited liability company.

CA. Certification Authority.

Certificate. A record that, at a minimum: (a) identifies the CA issuing it; (b) names or otherwise identifies its Subscriber; (c) contains a Public Key that corresponds to a Private Key under the control of the Subscriber; (d) identifies its Operational Period; and (e) contains a Certificate serial number and is digitally signed by the CA. The term Certificate, as referred to in this CPS, means a Certificate issued by AffirmTrust pursuant to this CPS.

Certificate Administrator. An individual designated by the Organization to approve the issuance of Certificates for the vetted domain names on behalf of the Organization as part of AffirmTrust's Extended Validation server certificate service.

Certificate Revocation List. A time-stamped list of revoked Certificates that has been digitally signed by the CA Certification Authority. An entity that issues Certificates and performs all of the functions associated with issuing such Certificates.

Compromise. Suspected or actual unauthorized disclosure, loss, loss of control over, or use of a Private Key associated with Certificate.

CRL. See Certificate Revocation List.

Domain Validated (DV) Certificate. A certificate that contains the domain name of the Subscriber that has been validated according to the issuer's disclosed practices, but that does not contain any information about any organization or person associated with the Subscriber.

EV Certificate: A certificate that contains information specified in the EV Guidelines and that has been validated in accordance with those Guidelines.

EV Certificate Beneficiaries. (a) The Subscriber entering into the Subscriber Agreement for the EV Certificate; (b) the Subject named in the EV Certificate; (c) all application software vendors with whom the AffirmTrust has entered into a contract for inclusion of its Root Certificate in software distributed by such application software vendors; and (d) all Relying Parties that actually rely on such EV Certificate during the period when it is valid.

EV Guidelines. The CA/Browser Forum Guidelines for Issuance and Management of Extended Validation Certificates published at http://www.cabforum.org, as such Guidelines may be amended from time to time. All references to the EV Guidelines herein is to version 1.2.

EV Policies. AffirmTrust's EV Certificate practices, policies, and procedures governing the issuance of EV Certificates, including this CPS.

Extension, means to place additional information about a Certificate within a Certificate. The X.509 standard defines a set of Extensions that may be used in Certificates.

Key Pair. 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 impractical to discover the other key.

Operational Period. A Certificate's period of validity. It would typically begin on the date the Certificate is issued (or such later date as specified in the Certificate), and ends on the date and time it expires as noted in the Certificate or is earlier revoked unless it is suspended.

Organization. The entity named or identified in a Certificate in the Organizational Name field that has purchased a Certificate.

Organization Validated (OV) Certificate. A certificate that contains information about the organization named in the certificate that has been validated according to the issuer's disclosed practices, but which has not been validated according to the EV Guidelines.

Private Key. The key of a Key Pair used to create a digital signature. This key must be kept a secret.

Public Key. The key of a Key Pair used to verify a digital signature. The Public Key is made freely available to anyone who will receive digitally signed messages from the holder of the Key Pair. The Public Key is usually provided via a Certificate issued by AffirmTrust. A Public Key is used to verify the digital signature of a message purportedly sent by the holder of the corresponding Private Key.

Relying Party. A recipient of a digitally signed message who relies on a Certificate to verify the digital signature on the message. Also, a recipient of a Certificate who relies on the information contained in the Certificate.

Root Key(s). The Private Key used by AffirmTrust to sign the Certificates.

SSL An industry standard protocol that uses public key cryptography for Internet security.

Subscriber. A person or entity who (1) is the subject named or identified in a Certificate issued to such person or entity, (2) holds a Private Key that corresponds to a Public Key listed in that Certificate, and (3) the person or entity to whom digitally signed messages verified by reference to such Certificate are to be attributed. For the purpose of this CPS, a person or entity who applies for a Certificate (an “Applicant”) by the submission of an enrollment form is also referred to as a Subscriber.

APPENDIX A TO AFFIRMTRUST CPS
Authentication and Certificate Issuance Procedures for Non-EV Certificates

As noted at CPS Section III.B, AffirmTrust presently issues only Extended Validation Certificates, and does not issue Domain Validated (DV) Certificates (SSL/TLS), Organization Validated (OV) Certificates (SSL/TLS), Email (S/MIME) or Code Signing Certificates.

In the event AffirmTrust decides to issue one or more of these other Certificate types, it will amend its CPS at that time to include generally the following procedures for authentication and issuance, as applicable for each Certificate type.

1. Certificate Application Processing

1.1 People Who May Submit a Certificate Application

Below is a list of people who may submit certificate applications:

- Any individual who is the subject of the certificate,
- Any authorized representative of an Organization or entity,

1.2 Enrollment Process

All end-user Certificate Subscribers shall manifest assent to the relevant Subscriber Agreement and undergo an enrollment process consisting of:

- Completing a Certificate Application and providing true and correct information,
- Generating, or arranging to have generated, a key pair,
- Delivering his, her, or its public key to AffirmTrust, and
- Demonstrating possession of the private key corresponding to the public key delivered to AffirmTrust.

1.3 Performing Identification and Authentication Functions

AffirmTrust shall perform identification and authentication of all required Subscriber information in terms of Section 3.

At certain times during the enrollment process in which AffirmTrust is not able to verify information in an enrollment form, a customer service representative may be assigned to the Applicant to facilitate the completion of the application process. Otherwise, the Applicant may be required to correct its associated information with third parties and re-submit its enrollment form for a Certificate.

1.4 Approval or Rejection of Certificate Applications

AffirmTrust will approve an application for a certificate if the following criteria are met:

- Successful identification and authentication of all required Subscriber information in terms of Section 3 , and

- Payment has been received

AffirmTrust or an RA will reject a certificate application if:

Identification and authentication of all required Subscriber information in terms of Section 3 cannot be completed, or

The Subscriber fails to furnish supporting documentation upon request

The Subscriber fails to respond to notices within a specified time, or

Payment has not been received, or

AffirmTrust believes that issuing a certificate to the Subscriber may bring the AffirmTrust PKI into disrepute.

1.5 Time to Process Certificate Applications

AffirmTrust begins processing certificate applications within a reasonable time of receipt. There is no time stipulation to complete the processing of an application unless otherwise indicated in the relevant Subscriber Agreement, CPS or other Agreement between AffirmTrust PKI participants.

A certificate application remains active until rejected or issued.

1.6 CA Actions during Certificate Issuance

A Certificate is created and issued following the approval of a Certificate Application by AffirmTrust. AffirmTrust creates and issues to a Certificate Applicant a Certificate based on the information in a Certificate Application following approval of such Certificate Application.

1.7 Notifications to Subscriber by the CA of Issuance of Certificates

AffirmTrust shall notify Subscribers that it has created such Certificates, and provide Subscribers with access to the Certificates by notifying them that their Certificates are available. Certificates shall be made available to end-user Subscribers, either by allowing them to download them from a web site, an application programming interface

(API) or via a message sent to the Subscriber containing the Certificate.

1.8 Conduct Constituting Certificate Acceptance

The applicant expressly indicates acceptance of a Certificate by downloading and/or using such Certificate.

2. Naming

2.1 Types of Names

Certificates contain an X.501 distinguished name in the Subject name field and consist of the components specified in the table below (as applicable for each Certificate type).

Attribute	**Value**
Country (C) =	2 letter ISO country code or not used for certain Certificates.
Organization (O) =	The Organization attribute is used as follows: • Subscriber organizational name for web server Certificates and individual Certificates that have an organization affiliation, or • A domain name, or “AffirmTrust Verified Site” or similar language in the Organization field (for web server certificates that have domain control validation only and no organization verification), or • When applicable, wording to the effect that the organization has not been authenticated.
Organizational Unit (OU) =	AffirmTrust Certificates may contain multiple OU attributes. Such attributes may contain one or more of the following: • Subscriber organizational unit (for organizational Certificates and individual Certificates that have an organization affiliation) • Text to describe the type of Certificate. • Text to describe the entity that performed the verification • “Domain Control Validated”, where appropriate • The address of the customer
State or Province (ST) =	When used, indicates the Subscriber’s State or Province
Locality (L) =	When used, indicates the Subscriber’s Locality
Common Name (CN) =	This attribute may include: • Domain name (for web server Certificates) • Organization name (for code/object signing Certificates) • Name of individual (for certificates issued to individuals).
E-Mail Address (E) =	When used, the e-mail address associated with the certificate

2.2 Need for Names to be Meaningful

Domain names do not have to be meaningful or unique, but must match a second level domain name as posted by InterNIC.

2.3 Anonymity or Pseudonymity of Subscribers

Subscribers are not permitted to use pseudonyms (names other than a Subscriber's true personal or organizational name).

2.4 Recognition, Authentication, and Role of Trademarks

Certificate Applicants are prohibited from using names in their Certificate Applications that infringe upon the Intellectual Property Rights of others. Trademark disputes will be handled as provided in Section VI.A of this CPS. AffirmTrust does not verify whether a Certificate Applicant has Intellectual Property Rights in the name appearing in a Certificate Application or arbitrate, mediate, or otherwise resolve any dispute concerning the ownership of any domain name, trade name, trademark, or service mark. AffirmTrust is entitled, without liability to any Certificate Applicant, to reject or suspend any Certificate Application because of such dispute.

3. Initial Identity Validation

3.1 Method to Prove Possession of Private Key

The certificate applicant must demonstrate that it rightfully holds the private key corresponding to the public key to be listed in the Certificate. The method to prove possession of a private key shall be PKCS #10, another cryptographically equivalent demonstration, or another AffirmTrust approved method. This requirement does not apply where a key pair is generated by a CA on behalf of a Subscriber, for example where pregenerated keys are placed on smart cards.

3.2 Authentication of Organization Identity

Whenever an organization name is included in the Certificate (e.g., for OV Certificates), AffirmTrust will take reasonable steps to establish that a Certificate request made on behalf of that Organization is legitimate and properly authorized. AffirmTrust will ensure the following: (a) the Organizational Name appears in conjunction with a country and possibly a state or province of other locality to sufficiently identify its place of registration or a place where it is currently doing business; and (b) in the case of an Organization that could reasonably be expected to be registered with a local, state or national authority, in certain circumstances AffirmTrust will obtain, view and verify copies of the registration documents. For instance, AffirmTrust may (a) verify the validity of the registration through the authority that issued it, or (b) verify the validity of the registration through a reputable third party database or other resource, or (c) verify the validity of the Organization through a trusted third party data source, or (d) confirm that the

Organization exists if such Organization is not the type that is typically registered or is capable of being verified under clause (b).

3.3 Authentication of Domain Name

When a domain name is included in a Certificate together with an organization name (e.g., for OV Certificates), AffirmTrust will verify that the Subscriber had the right to use the domain name submitted by the Subscriber at the time it submitted its application. For instance, AffirmTrust may perform this verification by confirming that the Subscriber is the same person or entity that holds the domain name registration from the relevant domain name registrar or that the Subscriber is otherwise authorized to use such domain name.

When a domain name is included in a Certificate without authentication of the entity owning the domain name (e.g., for DV Certificates), AffirmTrust will verify that the Subscriber has control over such domain name at the time it submitted its enrollment form by accessing a third party database of domain names and their owners. To do this, AffirmTrust will send an e-mail message to one of the following e-mail addresses requesting confirmation of the Certificate order and authorization to issue the Certificate in the domain name: (a) an e-mail address listed as the administrative or technical contact for the domain name in an official InterNIC domain name registry that includes the domain name, (b) a limited list of the most commonly used generic e-mail addresses for authorized persons at domain names (e.g., "*admin@domain.com*,“ or "*hostmaster@domain.com*" for the domain name domain.com), or (c) using a manual process conducted by AffirmTrust, to another e-mail address containing the domain name that is listed as the Common Name in the enrollment form. Upon receipt of a confirming e-mail message authorizing issuance of the Certificate, AffirmTrust will issue the Certificate as described below. Additionally, a confirmatory phone call to the applicant may be performed for Domain Control Certificate applications.

3.4 Authentication of Individual Identity (S/MIME Certificate)

An Applicant for an email (S/MIME) Certificate shall complete an AffirmTrust enrollment application on behalf of Subscriber in a form prescribed by AffirmTrust. All applications are subject to review, approval and acceptance by AffirmTrust. All Applicants are required to include a name, e-mail contact address ("Contact Address") and telephone number ("Telephone Number") within the enrollment application and prove control over the Contact Address and Telephone Number. AffirmTrust does not otherwise verify the accuracy of the information contained in the Applicant's enrollment form or otherwise check for errors and omissions.

3.5 Non-Verified Subscriber Information

Non-verified subscriber information for all products includes:

- Organization Unit (OU)

- Any other information designated as non-verified in the certificate.

3.6 Validation of Authority

Whenever an organization name is included in the Certificate (e.g., for OV Certificates), AffirmTrust will take reasonable steps to establish that a Certificate request made on behalf of that Organization is legitimate and properly authorized. To prove that a Certificate is duly authorized by the Organization, AffirmTrust will typically request the name of a contact person who is employed by or is an officer of the Organization. AffirmTrust will also typically require a form of authorization from the Organization confirming its intent to obtain a Certificate and will usually document the Organization's contact person. AffirmTrust normally confirms the contents of this authorization with the listed contact person.

3.7 Additional Requirements for Code Signing Certificates

AffirmTrust may impose additional authentication requirements for Code Signing Certificates as required by certain browsers or applications. The additional requirements, if any, will be outlined to Applicants at the time of application.

4. Identification and Authentication for Re-key Requests

Prior to the expiration of an existing Certificate, it is necessary for the Subscriber to obtain a new Certificate to maintain continuity of Certificate usage. Subscribers have the option of generating a new Key Pair to replace the expiring Key Pair (technically defined as “rekey”) or of creating a new CSR for an existing Key Pair (technically defined as “renewal”), depending on their preferences and the capabilities and restrictions of the Subscriber’s key generation tools. For purposes of this CPS, both a “rekey” and “renewal” as defined above will be treated as a renewal Certificate.

Renewal Certificates are subject to the same authentication steps outlined in this Appendix as apply to initial issuance of a Certificate.

5. Identification and Authentication for Revocation Request

The only persons permitted to request revocation of a Certificate issued by AffirmTrust are the Subscriber (including designated representatives), the administrative contact or the technical contact, as applicable.

To request revocation, a Subscriber or Authorized requester must contact AffirmTrust, either by e-mail message, a national/regional postal service, facsimile, or overnight courier, and specifically request “revocation” (using that term) of a particular Certificate identified by the Subscriber.

Upon receipt of a revocation request, AffirmTrust will seek confirmation of the request by e-mail message to the person requesting revocation. The message will state that, upon confirmation of the revocation request, AffirmTrust will revoke the Certificate and that posting the revocation to the appropriate CRL will constitute notice to the Subscriber that the Certificate has been revoked. AffirmTrust will require a confirming e-mail message back from either the administrative or technical contact authorizing revocation (or by other means of confirmation acceptable to AffirmTrust). Upon receipt of the confirming e-mail message, AffirmTrust will revoke the Certificate and the revocation will be posted to the appropriate CRL. Notification will be sent to the subject of the Certificate and the subject's designated contacts. There is no grace period available to the Subscriber prior to revocation, and AffirmTrust shall respond to the revocation request within the next business day and post the revocation to the next published CRL.