AFFIRMTRUST™

CERTIFICATION PRACTICE STATEMENT

Version 3.1

Effective Date: 6 March 2017

TABLE OF CONTENTS

1. INTRODUCTION

1.1 Overview

This AffirmTrust Certification Practice Statement (the "CPS"), Version 3.1, effective date: 6 March 2017, presents the principles and procedures AffirmTrust employs in the issuance and life cycle management of the roots, sub-roots, and certificates listed on Appendix A.

This CPS and any and all amendments thereto are incorporated by reference into all of the Certificates listed on Appendix A. The CPS is available on AffirmTrust's website. In the event of any differences between the Japanese and English versions of this document, the English version will prevail.

AffirmTrust is established to provide certificate services for a variety of external customers. The organization operates from the sub-CA roots listed on Appendix A, which issue certificates to various AffirmTrust customers. Subscribers include all parties who contract with AffirmTrust for AffirmTrust digital certificate services. All parties who may rely upon the AffirmTrust certificates are considered relying parties. This CPS and other AffirmTrust business practices disclosures are applicable to all AffirmTrust certificates issued by AffirmTrust.

This CPS follows the format of RFC 3647. For the purposes of this CPS, all capitalized terms used herein shall have the meaning given to them in Section 1.6, Definitions and Acronyms, or elsewhere in this CPS.

1.2 Document Name and Identification

This document is the AffirmTrust Certification Practices Statement and was approved for publication as of 6 March 2017 by the AffirmTrust PKI Policy Authority. IANA has assigned the following OID to AffirmTrust: 1.3.6.1.4.1.34697. The OID for this CPS is 1.3.6.1.4.1.34697.1.1, which is also the OID that AffirmTrust uses to indicate its adherence to and compliance with the Baseline Requirements of the CA/Browser Forum.

The following table shows the OID arc for AffirmTrust:

OID	Meaning
1.3.6.1.4.1.34697	AffirmTrust OID
1.3.6.1.4.1.34697.1	[Reserved]
1.3.6.1.4.1.34697.1.1	CPS
1.3.6.1.4.1.34697.2	Certificate Policy
1.3.6.1.4.1.34697.2.1	AFT EV commercial
1.3.6.1.4.1.34697.2.2	AFT EV networking
1.3.6.1.4.1.34697.2.3	AFT EV Premium
1.3.6.1.4.1.34697.2.4	AFT EV Premium ECC
1.3.6.1.4.1.34697.2.5	Organization Validation
1.3.6.1.4.1.34697.2.6	Domain Validation

1.3 PKI Participants

1.3.1 Certification Authorities

AffirmTrust is a certification authority (CA) that issues SSL digital certificates in accordance with

this CPS. As a CA, AffirmTrust performs functions associated with Public Key operations, including receiving certificate requests, issuing, revoking and renewing a digital certificate, and maintaining, issuing, and publishing CRLs and OCSP responses.

AffirmTrust's self-signed, offline Root CAs create online subordinate CAs in accordance with this CPS and applicable cross-certification policies and memoranda of agreement with other CAs. For ease of reference herein, all AffirmTrust Root CAs and cross-signed or subordinate CAs that issue certificates are referred to as "CAs."

AffirmTrust operations are managed by the AffirmTrust PKI Policy Authority (PKIPA) which is composed of members of the AffirmTrust Group management. The PKIPA is responsible for the approval of this CPS and overseeing the conformance of the AffirmTrust practices with applicable requirements.

AffirmTrust Server Certificates are X.509 Certificates with SSL Extensions issued from sub-roots that chain and may be cross-signed to the trusted roots listed on Appendix A, 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 Baseline Requirements ("Baseline Requirements") and Guidelines for Issuance and Management of Extended Validation Certificates ("EV Guidelines") and implements the Baseline Requirements and EV Guidelines through this CPS and AffirmTrust's other policies. In the event of any inconsistency between AffirmTrust's other policies and the Baseline Requirements or EV Guidelines, the Baseline Requirements and EV Guidelines take precedence.

1.3.2 Registration Authorities

AffirmTrust does not use external Registration Authorities.

1.3.3 Subscribers

Subscribers use AffirmTrust's SSL services and PKI to support transactions and communications. The Subject of a Certificate is the party named in the Certificate. A Subscriber, as used herein, refers to both the Subject of the Certificate and the entity that contracted with AffirmTrust for the Certificate's issuance. Prior to verification of identity and issuance of a Certificate, a Subscriber is an Applicant.

1.3.4 Relying Parties

Relying Parties are entities that act in reliance on a Certificate and/or digital signature issued by AffirmTrust. Relying parties must check the appropriate CRL or OCSP response prior to relying on information featured in a Certificate. The location of the CRL distribution point is detailed within the Certificate.

Relying Parties are also obligated to: (a) Restrict reliance on Certificates issued by the CA to the purposes for those Certificates, in accordance with this CPS, (b) 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, and (c) agree to be bound by the Relying Party Agreement as published at the AffirmTrust website. AffirmTrust does not accept responsibility for reliance on a fraudulently obtained Certificate or a Certificate that is on the CRL or OCSP.

1.3.5 Other Participants

No provision.

1.4 Certificate Usage

A digital certificate (or certificate) is formatted data that cryptographically binds an identified subscriber with a Public Key. A digital certificate allows an entity taking part in an electronic transaction to prove its identity to other participants in such transaction. Digital certificates are used in commercial environments as a digital equivalent of an identification card.

1.4.1 Appropriate Certificate Uses

Certificates issued pursuant to this CPS may be used for all legal authentication, encryption, access control, and digital signature purposes, as designated by the key usage and extended key usage fields found within the Certificate. However, the sensitivity of the information processed or protected by a Certificate varies greatly, and each Relying Party must evaluate the application environment and associated risks before deciding on whether to use a Certificate issued under this CPS.

1.4.2 Prohibited certificate uses

Certificates do not guarantee that the Subject is trustworthy, honest, reputable in its business dealings, compliant with any laws, or safe to do business with. A Certificate only establishes that the information in the Certificate was verified as reasonably correct when the Certificate issued.

Certificates issued under this CPS may not be used (i) for any application requiring fail-safe performance such as (a) the operation of nuclear power facilities, (b) air traffic control systems, (c) aircraft navigation systems, (d) weapons control systems, or (e) any other system whose failure could lead to injury, death or environmental damage; or (ii) where prohibited by law.

1.5 Policy Administration

1.5.1 Organization administering the document

The authority administering this CPS is the AffirmTrust PKI Policy Authority, which can be contacted at:

AffirmTrust PKI Policy Authority
Entrust Limited dba AffirmTrust
1000 Innovation Drive
Ottawa K2K 3E7 ON Canada

legal@affirmtrust.com

1.5.2 Contact person

Legal Counsel
Entrust Limited dba AffirmTrust
1000 Innovation Drive
Ottawa K2K 3E7 ON Canada

legal@affirmtrust.com

1.5.3 Person Determining CPS Suitability for the Policy

AffirmTrust does not support a Certificate Policy, but instead enforces its PKI policies through this CPS and other documents. The PKI Policy Authority determines the suitability and applicability of this CPS for its policies.

1.5.4 CPS Approval Procedures

The PKI Policy Authority approves the CPS and any amendments. Amendments may be made by either updating the entire CPS or by publishing an addendum. The PKI Policy Authority determines whether an amendment to this CPS requires notice or an OID change. See also Section 9.10 and Section 9.12 below.

1.6 Definitions and Acronyms

Affiliate. An organization which is directly or indirectly controlled by one entity, which directly or indirectly controls such entity or which is under common control with such entity; "control" means the direct or indirect ownership of more than fifty percent (50%) of the shares or interests entitled to vote for the directors of such entity or the equivalent, for so long as such entitlement exists, or equivalent power over management.

AffirmTrust. Entrust Limited, an Ontario, Canada corporation doing business as AffirmTrust.

AffirmTrust Group. Collectively Entrust Holdings, Inc., its subsidiaries, its licensors (including for the avoidance of any doubt Microsoft), its resellers, its suppliers, and the directors, officers, employees, agents and independent contractors of any of them.

AffirmTrust Group Affiliates. Collectively, Entrust Datacard Corporation and its Affiliates.

Applicant. All parties who apply for AffirmTrust digital certificate services with AffirmTrust to be a Subscriber.

Baseline Requirements. The CA/Browser Forum Baseline Requirements published at http://www.cabforum.org, as such Baseline Requirements may be amended from time to time.

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 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 a Certificate.

CRL. See Certificate Revocation List.

DV (Domain Validated) 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 suppliers with whom AffirmTrust has entered into a contract for inclusion of its Root Certificate in software distributed by such application software suppliers; 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.

EV Policies. AffirmTrust 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.

OCSP. Online Certificate Status Protocol as used by AffirmTrust to report the revocation status of Certificates.

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.

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 (a) is the subject named or identified in a Certificate issued to such person or entity, (b) holds a Private Key that corresponds to a Public Key listed in that Certificate, and (c) 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.

Subscriber Agreement (also known as Terms of Service). The agreement between a Subscriber and AffirmTrust.

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

AffirmTrust publishes its root certificates, revocation data for issued digital certificates, CPSs, Relying Party Agreements, and Subscriber Agreements (Terms of Service) in AffirmTrust's publicly-available online repositories.

AffirmTrust operates its PKI infrastructure to ensure that its root certificates and CRLs are available through an online repository 24 hours a day, 7 days a week, with minimal interruption. AffirmTrust does not provide a Repository or directory making end-entity Certificates available to Relying Parties.

2.2 Publication of Certification Information

AffirmTrust certificate services and the AffirmTrust repository are accessible through several means of communication:

1. By email using any email link listed at the AffirmTrust website, or such successor website as AffirmTrust may use.
2. By mail addressed to: Legal Counsel, AffirmTrust PKI Policy Authority, c/o Entrust Limited doing business as AffirmTrust, 1000 Innovation Drive, Ottawa K2K 3E7 ON Canada

AffirmTrust publishes its CPS, CA certificates, cross-certificates, Subscriber Agreements (Terms of Service), Relying Party Agreements, and CRLs for all revoked un-expired certificates in online repositories.

2.3 Time or Frequency of Publication

AffirmTrust CA certificates are published in a repository as soon as possible after issuance. CRLs for end-user certificates are issued at least as frequently as required by the Baseline Requirements. CRLs for CA certificates are issued at least every 12 months. AffirmTrust may publish new CRLs prior to the expiration of the current CRL.

New or modified versions of this CPS, Subscriber Agreements (Terms of Service), or Relying Party Agreements are published within seven days after their approval.

2.4 Access Controls on Repositories

Information published on repositories is public information. Read only access is unrestricted. AffirmTrust has implemented logical and physical controls to prevent unauthorized write access to its repositories.

3. IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of Names

Certificates are issued with a non-null subject Distinguished Name (DN) that complies with ITU X.500 standards.

Non-wildcard SSL Certificates and Unified Communications Certificates are issued using the Fully Qualified Domain Name (FQDN) name or IP address of the servers, services, or applications. Wildcard SSL Certificates have a wildcard asterisk character for the server name in the subject field. The FQDN or authenticated domain name is placed in the Common Name (CN) attribute of the Subject field and, when applicable, the Subject Alternative Name extension contains the FQDNs or authenticated domain names of the servers that are owned or under the control of the Subscriber. Subject Alternative Names are marked non-critical. When DNs are used, common names must respect name space uniqueness and must not be misleading.

3.1.2 Need for Names to Be Meaningful

AffirmTrust uses distinguished names that identify both the subject and issuer of the Certificate.

3.1.3 Anonymity or Pseudonymity of Subscribers

Generally, AffirmTrust does not issue anonymous or pseudonymous certificates; however, for IDNs, AffirmTrust may include the Punycode version of the IDN as the subject name.

3.1.4 Rules for Interpreting Various Name Forms

Distinguished Names in certificates are interpreted using X.500 standards and ASN.1 syntax. *See* RFC 2253 and RFC 2616 for further information on how X.500 distinguished names in certificates are interpreted as Uniform Resource Identifiers and HTTP references.

3.1.5 Uniqueness of Names

The uniqueness of each subject name in a certificate is enforced by entering the domain name in the Common Name attribute of the subject field or the Subject Alternative Name field. Domain name uniqueness is controlled by the Internet Corporation for Assigned Names and Numbers (ICANN).

3.1.6 Recognition, Authentication, and Role of Trademarks

Subscribers should not request certificates with any content that infringes on the intellectual property rights of another entity. Unless otherwise specifically stated in this CPS, AffirmTrust does not verify an Applicant's right to use a trademark and does not resolve trademark disputes. AffirmTrust may reject any application or require revocation of any Certificate that is part of a trademark dispute.

3.2 Initial Identity Validation

AffirmTrust may use any legal means of communication or investigation to ascertain the identity of an Applicant. AffirmTrust may refuse to issue a certificate in its sole discretion.

3.2.1 Method to Prove Possession of Private Key

The Applicant must submit a CSR, generally in a PKCS#10 format, to establish that it holds the Private Key corresponding to the Public Key in the certificate request.

3.2.2 Authentication of Organization Identity

AffirmTrust requires the following verification depending on the Certificate type.

3.2.2.1 For Domain Validated (DV) Certificates

AffirmTrust validates the Applicant's ownership or control of the domain name(s) that will be listed in the Certificate. Domain name ownership or control is validated by:

(a) Relying on publicly available records from the Domain Name Registrar; or

(b) Communicating with one of the following email addresses: webmaster@domain.com, administrator@domain.com, admin@domain.com, hostmaster@domain.com, postmaster@domain.com, and any address listed in the technical, registrant, or administrative contact field of the domain's Domain Name Registrar record; or

(c) Requiring a practical demonstration of domain control (e.g., requiring the Applicant to make a specified change to a live page on the given domain).

(d) Any other validation method permitted under the CA/Browser Forum's Baseline Requirements.

AffirmTrust does not verify the organizational identity of Applicants for DV Certificates.

3.2.2.2 For Organization Validated (OV) Certificates

AffirmTrust requires OV Certificate applicants to include the organization name and address in the certificate application. AffirmTrust verifies the organizational identity of Applicants using reliable third party and government databases or through other direct means of communication with the entity or jurisdiction governing the organization's legal creation, existence, or recognition. If such efforts are insufficient to confirm the identity of the subject, AffirmTrust may require the Applicant to submit official company documentation, such as a business license, filed or certified articles of incorporation/organization, tax certificate, corporate charter, official letter, sales license, or other relevant documents. AffirmTrust verifies the authority of the person requesting the certificate on behalf of an organization in accordance with Section 3.2.5.

AffirmTrust also validates the Applicant's right to use the domain name(s) that will be listed in the Certificate by following the procedures of Sec. 3.2.2.1.

3.2.2.3 For Extended Validation (EV) Certificates

EV Certificates are validated in accordance with the EV Guidelines of the CA/Browser Forum. For additional information on validation steps, see Section 11 of the EV Guidelines found at https://cabforum.org/documents/.

3.2.3 Authentication of Individual Identity

AffirmTrust does not issue SSL server certificates to individuals.

3.2.4 Non-Verified Subscriber Information

Provided that the right to use a domain name is verified in accordance with Section 3.2.2.1, AffirmTrust may rely on the Subscriber's indication of the host or server name that forms the fully qualified domain name to be included in the SSL Certificate. Any other non-verified information included in a Certificate is designated as such in the Certificate.

3.2.5 Validation of Authority

3.2.5.1 For Organization Validated (OV) for Organizations

The authority of the individual requesting an OV Certificate on behalf of an organization verified under section 3.2.2.2 is validated as follows:

AffirmTrust will use a Reliable Method of Communication as defined in the CA/Browser Forum Baseline Requirements to verify the authenticity of the Applicant representative's certificate request. AffirmTrust may use the sources listed in Baseline Requirements Section 3.2.2.1 to verify the Reliable Method of Communication and may establish the authenticity of the certificate request directly with the Applicant's representative's or with an authoritative source within the Applicant's organization, such as the Applicant's main business offices, corporate offices, human resource offices, information technology offices, or other department that the CA deems appropriate.

3.2.5.2 For Extended Validation (EV) Certificates

The authority of the individual requesting an EV Certificate on behalf of an organization verified under section 3.2.2.3 is validated by verifying the authority of the Contract Signer and Certificate Approver in accordance with the EV Guidelines of the CA/Browser Forum. For additional information on validation steps, see Section 11 of the EV Guidelines, https://cabforum.org/documents/.

3.2.6 Criteria for Interoperation

No provision.

3.3 Identification and Authentication for Re-Key Requests

3.3.1 Identification and Authentication for Routine Re-Key

Subscribers may request automatic re-key of a Certificate prior to a Certificate's expiration. After receiving a request for re-key, AffirmTrust creates a new Certificate with the same Certificate contents except for a new Public Key and, optionally, an extended validity period. If the Certificate has an extended validity period, AffirmTrust may perform some revalidation of the Applicant but may also rely on information previously provided or obtained.

Subscribers re-establish their identity as follows:

OV Certificates:

Routine Re-Key Authentication:	Username and password
Re-Verification Required:	According to the Baseline Requirements

EV Certificates:

Routine Re-Key Authentication:	Username and password
Re-Verification Required:	According to the EV Guidelines

3.3.2 Identification and Authentication for Re-Key After Revocation

A subscriber requesting re-key after a Certificate is revoked for a reason other than during a renewal or update action undergoes the initial registration process.

3.4 Identification and Authentication for Revocation Request

Revocation requests are authenticated by Subscribers after logging in to their accounts and requesting revocation of particular certificates and choosing a reason for revocation.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application

Either the Applicant or an individual authorized to request certificates on behalf of the Applicant may submit certificate requests. For certificates that include a domain name, the Domain Name Registrar record maintained by the domain registrar presumptively indicates who has authority over the domain. If a certificate request is submitted by an agent of the domain owner, the agent must send AffirmTrust a document that authorizes Subscriber's use of the domain. Applicants are responsible for any data that the Applicant or an agent of the Applicant supplies to AffirmTrust.

EV Certificate requests must be submitted by an authorized Certificate Requester and approved by a Certificate Approver. The certificate request must be accompanied by a signed (in writing or electronically) Subscriber Agreement from a Contract Signer.

AffirmTrust does not issue certificates to any entity that is on a government denied list maintained by the United States or that is located in a country with which the laws of the United States prohibit doing business. For EV Certificates, AffirmTrust verifies that the Applicant, the

Applicant's Jurisdiction of Incorporation, Registration, and Place of Business are not included on such lists or subject to such prohibition.

4.1.2 Enrollment Process and Responsibilities

AffirmTrust requires each Applicant to submit a certificate request and application information prior to issuing a Certificate. AffirmTrust authenticates all communication from an Applicant and protects communication from modification.

Generally, Applicants request a Certificate by completing the request forms online. Applicants are solely responsible for submitting a complete and accurate certificate request for each certificate.

The enrollment process includes:

1. Agreeing to the applicable Subscriber Agreement (Terms of Service),
2. Paying any applicable fees,
3. Submitting a complete certificate application,
4. Generating a key pair, and
5. Delivering the public key of the key pair to AffirmTrust.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

After receiving an application, AffirmTrust verifies the application information and other information in accordance with Section 3.2. All EV Certificates are validated in accordance with the EV Guidelines. After verification is complete, AffirmTrust evaluates all the information and decides whether or not to issue the certificate.

At the present time, AffirmTrust does not review or process CAA records, but AffirmTrust does block issuance of certificates with certain names known to be top fraud targets, requiring additional authentication due diligence and manual approval and issuance. Any domain owner who wants to direct AffirmTrust not to issue certificates for its Fully Qualified Domain Names and/or Second Level Domain Names should send a message to abuse@affirmtrust.com.

In the future, AffirmTrust will begin reviewing and processing CAA records, and will amend this CPS with additional details at that time.

4.2.2 Approval or Rejection Of Certificate Applications

AffirmTrust rejects any certificate application that AffirmTrust cannot verify. AffirmTrust may also reject a certificate application if AffirmTrust believes that issuing the certificate could damage or diminish AffirmTrust's reputation or business including the AffirmTrust business.

EV Certificate issuance approval requires authentication by two separate AffirmTrust validation specialists. The second validation specialist cannot be the same individual who collected the authentication documentation and originally approved the EV Certificate. The second validation specialist reviews the collected information and documents for discrepancies or details that require further explanation. If the validation specialist has any concerns about the application, the second validation specialist may require additional explanations and documents. If satisfactory explanations and/or additional documents are not received within a reasonable time, AffirmTrust will reject the EV Certificate request and notify the Applicant accordingly.

If some or all of the documentation used to support the application is in a language other than English, an AffirmTrust employee or agent skilled in such language and having the appropriate training, experience, and judgment in confirming organizational identification and authorization performs the final cross-correlation and due diligence.

If the certificate application is not rejected and is successfully validated in accordance with this CPS, AffirmTrust will approve the certificate application and issue the Certificate. Additional Certificates containing the same validated Certificate information may be requested by the Subscriber via a confirmed communication and issued without further authentication during the period permitted before reauthentication of Certificate information is required. AffirmTrust is not liable for any rejected certificate and is not obligated to disclose the reasons for a rejection. Rejected Applicants may re-apply. Subscribers are required to check the data listed in the Certificate for accuracy prior to using the Certificate.

4.2.3 Time to Process Certificate Applications

Under normal circumstances, AffirmTrust confirms certificate application information and issues a digital certificate within a reasonable time frame. Issuance time frames are greatly dependent on when the Applicant provides the details and documentation necessary to complete validation. For non-EV SSL certificates, AffirmTrust will usually confirm submitted application data, complete the validation process, and issue or reject a certificate application within two working days after AffirmTrust receives all of the necessary details and documentation from the Applicant.

Occasionally, events outside of the control of AffirmTrust delay the issuance process. However, AffirmTrust makes reasonable effort to meet its issuance times and make Applicants aware of any factors that affect issuance times.

4.3 Certificate Issuance

4.3.1 CA Actions during Certificate Issuance

AffirmTrust verifies the source of the certificate request and the identity of the Applicant in a secure manner prior to issuing a certificate. Any database used to confirm Subscriber information is protected from unauthorized modification. After validation is complete, the Certificate is issued and sent to the Subscriber.

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

AffirmTrust may deliver Certificates in any secure manner within a reasonable time after issuance. Generally, AffirmTrust delivers Certificates via email to the email address designated by the Subscriber during the application process. The Subscriber is also provided a link to a user id/password-protected location on AffirmTrust's web server where the Subscriber may log in and download each Certificate or the zip file containing all Certificates in the trust chain.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

Subscribers are solely responsible for installing the issued Certificate on the Subscriber's computer or hardware security module. Certificates are considered accepted on the earlier of (a) the Subscriber's use of the Certificate or (b) 30 days after the Certificate's issuance.

4.4.2 Publication of the Certificate by the CA

AffirmTrust publishes all CA certificate in its repository. AffirmTrust publishes end-entity Certificates by delivering them to the Subscriber.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

AffirmTrust may publish Subscriber Certificates to one or more CT (Certificate Transparency) logs which may be viewed by the public.

4.5 Key pair and certificate usage

4.5.1 Subscriber private key and certificate usage

Subscribers are contractually obligated to protect their Private Keys from unauthorized use or disclosure, discontinue using a Private Key after expiration or revocation of the associated Certificate, and use Private Keys only as specified in the key usage extension.

4.5.2 Relying party public key and certificate usage

Relying Parties may only use software that is compliant with X.509 and other applicable standards. AffirmTrust does not warrant that any third party's software will support or enforce the controls and requirements found herein.

A Relying Party should use discretion when relying on a Certificate and should consider the totality of the circumstances and risk of loss prior to relying on a Certificate. If the circumstances indicate that additional assurances are required, the Relying Party must obtain such assurances before using the Certificate. Any warranties provided by AffirmTrust are only valid if a Relying Party's reliance was reasonable and if the Relying Party adhered to the Relying Party Agreement set forth in the AffirmTrust repository.

A Relying Party should rely on a digital signature or SSL/TLS handshake only if:

1. The digital signature or SSL/TLS session was created during the operational period of a valid Certificate and can be verified by referencing a valid Certificate,
2. The Certificate is not revoked and the Relying Party checked the revocation status of the Certificate prior to the Certificate's use by referring to the relevant CRLs or OCSP responses, and
3. The Certificate is being used for its intended purpose and in accordance with this CPS.

4.6 Certificate Renewal

4.6.1 Circumstance for Certificate Renewal

AffirmTrust may renew a Certificate if:

1. The associated public key has not reached the end of its validity period,
2. The Subscriber name and attributes are unchanged,
3. The associated private key remains uncompromised, and
4. Re-verification of the Subscriber's identity is not required under Section 3.3.1.

AffirmTrust makes reasonable efforts to notify Subscribers via email of the imminent expiration of a digital certificate and may begin providing notice of pending expiration 60 days prior to the expiration date (or such other period as may be chosen by the Subscriber). Certificate renewal may require payment of additional fees which are disclosed to Subscribers approaching their Certificate or enterprise account expiration date. Renewal after revocation is not supported.

4.6.2 Who May Request Renewal

Only an authorized representative of a Subscriber may request renewal of the Subscriber's Certificates. AffirmTrust may renew a Certificate without a corresponding request if the signing certificate is re-keyed.

4.6.3 Processing Certificate Renewal Requests

Renewal application requirements and procedures are generally the same as those used during the Certificate's original issuance. AffirmTrust validation personnel may reconfirm domain name ownership using current Domain Name Registrar information and may check state or other jurisdictional records to confirm geographic location, company control and good standing the jurisdiction of organization. If AffirmTrust cannot verify any information it rechecks, the Certificate is not renewed.

AffirmTrust will not reuse EV Certificate validation information if the age of the data exceeds the time specified in the EV Guidelines.

Some device platforms allow renewed use of the Private Key. If the Subscriber's other contact information and Private Key have not changed, the Subscriber may use the same CSR as was used for the previous Certificate.

4.6.4 Notification of New Certificate Issuance to Subscriber

AffirmTrust delivers renewed Certificates to Subscribers in a secure fashion, typically via email to the address provided by the Subscriber during the renewal process. AffirmTrust may deliver the Certificate by providing the Subscriber a link to a user id/password-protected location on AffirmTrust's web server where the subscriber may log in and download the Certificate.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

Renewed Certificates are considered accepted on the earlier of (i) the Subscriber's use of the Certificate or (ii) 30 days after the Certificate's renewal.

4.6.6 Publication of the Renewal Certificate by the CA

AffirmTrust publishes a renewed Certificate by delivering it to the Subscriber. Renewed CA certificates are published in AffirmTrust's repository.

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

AffirmTrust may publish Subscriber Certificates to one or more CT (Certificate Transparency) logs which may be viewed by the public.

4.7. Certificate Re-Key

4.7.1. Circumstance for Certificate Rekey

Re-keying a Certificate consists of creating a new Certificate with a new public key and serial number while keeping the subject information the same. The new Certificate may have a different validity period, key identifiers, CRL and OCSP distributions, and a different signing key. After re-keying a Certificate, AffirmTrust may revoke the old Certificate but may not further re-key, renew, or modify the old Certificate. Re-key after revocation is not supported.

4.7.2 Who May Request Certification of a New Public Key

AffirmTrust may initiate certificate re-key Certificates at the request of the Certificate subject or authorized representative.

4.7.3 Processing Certificate Re-Keying Requests

If the Subscriber's other contact information and Private Key have not changed, AffirmTrust can issue a replacement Certificate using the previously provided CSR. Otherwise, the Subscriber must submit a new CSR. AffirmTrust re-uses existing verification information unless re-verification is required under section 3.3.1 or AffirmTrust believes that the information has become inaccurate.

4.7.4 Notification of New Certificate Issuance to Subscriber

AffirmTrust notifies the Subscriber within a reasonable time after the Certificate issues.

4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate

Issued Certificates are considered accepted on the earlier of (a) the Subscriber’s use of the Certificate or (b) 30 days after the Certificate is rekeyed.

4.7.6 Publication of the Re-Keyed Certificate by the CA

AffirmTrust publishes rekeyed Certificates by delivering them to Subscribers.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

AffirmTrust may publish Subscriber Certificates to one or more CT (Certificate Transparency) logs which may be viewed by the public.

4.8 Certificate Modification

4.8.1 Circumstance for Certificate Modification

Modifying a Certificate means creating a new Certificate for the same subject with authenticated information that differs slightly from the old Certificate (e.g., changes to non-essential parts of names or attributes) provided that the modification otherwise complies with this CPS. The new Certificate may have the same or a different subject public key.

After modifying a Certificate, AffirmTrust can revoke the old Certificate but will not further re-key, renew, or modify the old Certificate.

4.8.2 Who May Request Certificate Modification

AffirmTrust modifies Certificates at the request of certain Certificate subjects or in its own discretion. AffirmTrust does not make certificate modification services available to all Subscribers.

4.8.3 Processing Certificate Modification Requests

After receiving a request for modification, AffirmTrust verifies any information that will change in the modified Certificate. AffirmTrust will only issue the modified Certificate after completing the verification process on all modified information. AffirmTrust will not issue a modified Certificate that has a validity period that exceeds the applicable time limits found in section 3.3.1 or 6.3.2.

4.8.4 Notification of New Certificate Issuance to Subscriber

AffirmTrust notifies the Subscriber within a reasonable time after the Certificate issues.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

Issued Certificates are considered accepted on the earlier of (a) the Subscriber's use of the Certificate or (b) 30 days after the Certificate is rekeyed.

4.8.6 Publication of the Modified Certificate by the CA

AffirmTrust publishes modified Certificates by delivering them to Subscribers.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

AffirmTrust may publish Subscriber Certificates to one or more CT (Certificate Transparency) logs which may be viewed by the public.

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for Revocation

Revocation of a Certificate permanently ends the operational period of the Certificate prior to the Certificate reaching the end of its stated validity period. Prior to revoking a Certificate, AffirmTrust verifies the identity and authority of the entity requesting revocation. AffirmTrust may revoke any Certificate in its sole discretion, including if AffirmTrust believes that:

1. The Subscriber requested revocation of its Certificate;
2. The Subscriber did not authorize the original certificate request and did not retroactively grant authorization;
3. Either the Private Key associated with the Certificate or the Private Key used to sign the Certificate was compromised;
4. The Subscriber or AffirmTrust breached a material obligation under the CPS or the relevant Subscriber Agreement;
5. Either the Subscriber's or AffirmTrust's obligations under the CPS are delayed or prevented by circumstances beyond the party's reasonable control, including computer or communication failure, and, as a result, another entity's information is materially threatened or compromised;
6. The Certificate was not issued in accordance with the CPS or applicable industry standards;
7. AffirmTrust received a lawful and binding order from a government or regulatory body to revoke the Certificate;

8. AffirmTrust ceased operations and did not arrange for another certificate authority to provide revocation support for the Certificates;
9. AffirmTrust's right to manage Certificates under applicable industry standards was terminated (unless arrangements have been made to continue revocation services and maintain the CRL/OCSP Repository);
10. A court or arbitrator revoked the Subscriber's right to use a name or mark listed in the Certificate, or the Subscriber failed to maintain a valid registration for such name or mark;
11. Any information appearing in the Certificate was or became inaccurate or misleading; or
12. The Subscriber was added as a denied party or prohibited person to a blacklist or is operating from a destination prohibited under the laws of the United States;

AffirmTrust will always revoke an AffirmTrust Certificate if it becomes aware that the binding between the subject and the subject's public key in the Certificate is no longer valid or if an associated Private Key is compromised.

4.9.2 Who Can Request Revocation

The Subscriber or another appropriately authorized party (such as an administrative contact, a Contract Signer, Certificate Approver, or Certificate Requester) may request revocation of a Certificate. AffirmTrust may require that the revocation request be made by either the organizational contact, billing contact or domain registrant.

AffirmTrust will revoke a Certificate if it receives sufficient evidence of compromise or loss of the private key and may revoke a Certificate of its own volition without reason, even if no other entity has requested revocation. Other entities may request revocation of a Certificate for problems related to fraud, misuse, or compromise by filing a "Certificate Problem Report" at abuse@affirmtrust.com, or such other email address as may be posted on AffirmTrust's website for this purpose. All certificate revocation requests must include the identity of the person or entity requesting revocation and the reason for revocation.

4.9.3 Procedure for Revocation Request

Entities submitting certificate revocation requests must list their identity and explain the reason for requesting revocation. AffirmTrust employs the following procedure after receiving a revocation request:

1. AffirmTrust personnel log the identity of person or entity making the request or problem report and the reason for requesting revocation. AffirmTrust may also include its own reasons for revocation in the log.
2. AffirmTrust requests confirmation of the revocation from a known administrator via out-of-band communication (e.g., telephone, fax, etc.).
3. If the request is authenticated as originating from the Subscriber, AffirmTrust will always revoke a Certificate.
4. For requests from third parties, AffirmTrust personnel begin investigating all Certificate Problem Reports within 24 hours after receipt and decide whether revocation is appropriate based on the following criteria:
    a. The nature of the alleged problem,
    b. The number of Certificate Problem Reports received about a particular Certificate or website,
    c. The identity of the complainants (for example, complaints from a law enforcement official that a web site is engaged in illegal activities have more

weight than a complaint from a consumer alleging they never received the goods they ordered), and
   d. Relevant legislation.
5. If revocation is appropriate, AffirmTrust personnel revoke the Certificate and cause the CRL to be updated.

Subscribers may revoke any of their Certificates 24 x 7 by use of their online subscriber account, with no approval or other action required by AffirmTrust.

4.9.4 Revocation Request Grace Period

AffirmTrust provides revocation grace periods to Subscribers on a case-by-case basis.

4.9.5 Time within Which CA Must Process the Revocation Request

AffirmTrust will revoke a CA certificate immediately once a Subscriber clicks the Revoke button on its online subscriber account, or within one hour after receiving instructions from the PKI Policy Authority. Other Certificates are revoked as quickly as practical after validating the revocation request in accordance with the process stated in Section 4.9.3.

4.9.6 Revocation Checking Requirement for Relying Parties

Prior to relying on information listed in a Certificate, a Relying Party must confirm the validity of each Certificate in the certificate path in accordance with IETF PKIX standards, including checks for Certificate validity, issuer-to-subject name chaining, policy and key use constraints, and revocation status through CRLs or OCSP responders identified in each certificate in the chain.

4.9.7 CRL Issuance Frequency

CRLs for end-user Certificates are issued at least once per day. CRLs for CA certificates are issued at least every 12 months. Under special circumstances, AffirmTrust may publish new CRLs prior to the expiration of the current CRL.

4.9.8 Maximum Latency for CRLs

CRLs are posted automatically to the online repository within a commercially reasonable time after generation, usually within minutes of generation. Irregular, interim, or emergency CRLs are posted no later than four hours after generation. Otherwise, AffirmTrust always posts regularly scheduled CRLs prior to the nextUpdate field in the previously issued CRL of the same scope.

4.9.9 On-Line Revocation/Status Checking Availability

AffirmTrust makes certificate status information available via OCSP. OCSP responses are provided within a commercially reasonable time after the request is received, subject to transmission latencies over the Internet.

4.9.10 On-Line Revocation Checking Requirements

A Relying Party must confirm the validity of a Certificate in accordance with section 4.9.6 prior to relying on the Certificate.

4.9.11 Other Forms of Revocation Advertisements Available

No provision.

4.9.12 Special Requirements re Key Compromise

If a Subscriber suspects or knows that the Private Key corresponding to the Public Key contained in the Subscriber's Certificate has been Compromised, the Subscriber shall immediately notify us, using the procedures set forth in Section 4.9.3, of such suspected or actual Compromise. The Subscriber shall immediately stop using such Certificate and shall remove such Certificate from any devices and/or software in which such Certificate has been installed. The Subscriber shall be responsible for investigating the circumstances of such Compromise or suspected Compromise and for notifying any Relying Parties that may have been affected by such Compromise or suspected Compromise.

4.9.13 Circumstances for Suspension

AffirmTrust does not support certificate suspension.

4.9.14 Who Can Request Suspension

No provision.

4.9.15 Procedure for Suspension Request

No provision.

4.9.16 Limits on Suspension Period

No provision.

4.10 Certificate Status Services

4.10.1 Operational Characteristics

Certificate status information is available via CRL and OCSP responder.

4.10.2 Service Availability

Certificate status services are available 24x7 without interruption.

4.10.3 Optional Features

No provision.

4.11 End of Subscription

A Subscriber's subscription service ends if its Certificate expires or is revoked or if the applicable Subscriber Agreement expires without renewal.

4.12 Key Escrow and Recovery

AffirmTrust does not escrow CA Private Keys or Subscriber private keys, or provide Subscriber

private key recovery services.

4.12.1 Key Escrow and Recovery Policy and Practices

No provision.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

No provision.

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1 Physical Controls

5.1.1 Site Location and Construction

The hardware and software for an AffirmTrust is located in a secure facility with physical security and access control procedures that meet or exceed industry standards. The CA equipment is located in a Security zone that is physically separated from AffirmTrust's other systems so that only authorized CA personnel can access it.

5.1.2 Physical Access

The room containing the AffirmTrust Certificate Authority software is designated a two (2) person zone, and controls are used to prevent a person from being in the room alone. Alarm systems are used to notify security personnel of any violation of the rules for access to an AffirmTrust Certificate Authority.

5.1.3 Power and Air Conditioning

The Security zone is equipped with:

- Filtered, conditioned, power connected to an appropriately sized UPS and generator;
- Heating, ventilation, and air conditioning appropriate for a commercial data processing facility; and
- Emergency lighting.

The environmental controls conform to local standards and are appropriately secured to prevent unauthorized access and/or tampering with the equipment. Temperature control alarms and alerts are activated upon detection of threatening temperature conditions.

5.1.4 Water Exposures

No liquid, gas, exhaust, etc. pipes traverse the controlled space other than those directly required for the area's HVAC system and for the pre-action fire suppression system. Water pipes for the pre-action fire suppression system are only filled on the activation of multiple fire alarms.

5.1.5 Fire Prevention and Protection

The AffirmTrust facility is fully wired for fire detection, alarm and suppression. Routine, frequent inspections of all systems are made to assure adequate operation.

5.1.6 Media Storage

All media is stored away from sources of heat and from obvious sources of water or other obvious hazards. Electromagnetic media (e.g. tapes) are stored away from obvious sources of strong magnetic fields. Archived material is stored in a room separate from the CA equipment until it is transferred to the archive storage facility.

5.1.7 Waste Disposal

Waste is removed or destroyed in accordance with industry best practice. Media used to store sensitive data is destroyed, such that the information is unrecoverable, prior to disposal.

5.1.8 Off-site Backup

As stipulated in Section 4.6.

5.2 Procedural Controls

AffirmTrust has a number of trusted roles for sensitive operations of the AffirmTrust software. To gain access to the Certificate Authority software used by AffirmTrust, operational personnel must undergo background investigations. AffirmTrust operations related to adding administrative personnel or changing Certification Authority policy settings require more than one (1) person to perform the operation.

5.3 Personnel Controls

Operational personnel for AffirmTrust will not be assigned other responsibilities that conflict with their operational responsibilities for AffirmTrust. The privileges assigned to operational personnel for AffirmTrust will be limited to the minimum required to carry out their assigned duties.

5.3.1 - 5.3.8 No separate provision.

5.4 Audit Logging Procedures

Significant security events in the AffirmTrust Certification Authorities are automatically time-stamped and recorded as audit logs in audit trail files. The audit trail files are processed (reviewed for policy violations or other significant events) on a regular basis. Authentication codes are used in conjunction with the audit trail files to protect against modification of audit logs. Audit trail files are archived periodically. All files including the latest audit trail file are moved to backup media and stored in a secure archive facility. The AffirmTrust Certification Authorities and all Registration Authorities operating under AffirmTrust record in detail every action taken to process an AffirmTrust Certificate Request and to issue an AffirmTrust Certificate, including all information generated or received in connection with an AffirmTrust Certificate Request, and every action taken to process the Request, including time, date, and personnel involved in the action.

The foregoing record requirements include, but are not limited to, an obligation to record the following events: (i) AffirmTrust key lifecycle management events, including: a. Key generation, backup, storage, recovery, archival, and destruction; and b. Cryptographic device lifecycle

management events. (ii) Certificate lifecycle management events, including: a. Certificate requests, renewal and re-key requests, and revocation; b. All verification activities required by this CPS; c. Date, time, phone number used, persons spoken to, and end results of verification telephone calls; d. Acceptance and rejection of Certificate Requests; e. Issuance of AffirmTrust Certificates; and f. Generation of Certificate Revocation Lists (CRLs) and OCSP messages. (iii) Security events, including: a. Successful and unsuccessful PKI system access attempts; b. PKI and security system actions performed; c. Security profile changes; d. System crashes, hardware failures, and other anomalies; e. Firewall and router activities; and f. Entries to and exits from the AffirmTrust facility. (iv) Log entries include the following elements: a. Date and time of entry; b. Identity of the person making the journal entry; and c. Description of entry. The time for the AffirmTrust Certification Authorities computer systems is synchronized with the service provided by the National Research Council Canada.

5.4.1 – 5.4.8 No separate provision.

5.5 Records Archival

The audit trail files, databases and revocation information for AffirmTrust Certification Authorities are archived. The archive of an AffirmTrust Certification Authorities' database and the archive of revocation information are retained for at least three (3) years. Archives of audit trail files are retained for at least seven (7) year(s) after any AffirmTrust Certificate based on that documentation ceases to be valid. The databases for AffirmTrust Certification Authorities are encrypted and protected by AffirmTrust software master keys. The archive media is protected through storage in a restricted-access facility to which only AffirmTrust-authorized personnel have access. Archive files are backed up as they are created. Originals are stored on-site and housed with an AffirmTrust system. Backup files are stored at a secure and separate geographic location.

5.5.1 – 5.5.7 No separate provision.

5.6 Key Changeover

AffirmTrust Certification Authorities' key pairs will be retired from service at the end of their respective lifetimes as defined in this CPS. New Certification Authority key pairs will be created as required to support the continuation of AffirmTrust Services. AffirmTrust will continue to publish CRLs signed with the original key pair until all Certificates issued using that original key pair have expired. The Certification Authority key changeover process will be performed such that it causes minimal disruption to Subscribers and Relying Parties.

5.7 Compromise and Disaster Recovery

AffirmTrust Certification Authorities have a disaster recovery plan to provide for timely recovery of services in the event of a system outage. The disaster recovery plan addresses the following:

(i) the conditions for activating the plans;
(ii) resumption procedures;
(iii) a maintenance schedule for the plan;
(iv) awareness and education requirements;
(v) the responsibilities of the individuals;
(vi) recovery point objective (RPO) of fifteen minutes
(vii) recovery time objective (RTO) of 24 hours for essential CA operations which include certificate issuance, certificate revocation, and issuance of certificate revocation status; and

(viii) testing of recovery plans.
In order to mitigate the event of a disaster, AffirmTrust has implemented the following:
(ix) secure on-site and off-site storage of backup HSMs containing copies of all CA Private Keys
(x) secure on-site and off-site storage of all requisite activation materials
(xi) regular synchronization of critical data to the disaster recovery site
(xii) regular incremental and daily backups of critical data within the primary site
(xiii) weekly backup of critical data to a secure off-site storage facility
(xiv) secure off-site storage of disaster recovery plan and disaster recovery procedures
(xv) environmental controls as described in §5.1
(xvi) high availability architecture for critical systems

AffirmTrust has implemented a secure disaster recovery facility that is greater than 250 km from the primary secure CA facilities.

AffirmTrust requires rigorous security controls to maintain the integrity of AffirmTrust Certification Authorities. The Compromise of the Private Key used by AffirmTrust is viewed by AffirmTrust as being very unlikely; however, AffirmTrust has policies and procedures that will be employed in the event of such a Compromise. At a minimum, all Subscribers shall be informed as soon as practicable of such a Compromise and information shall be posted in the AffirmTrust repository.

5.7.1 – 5.7.4 No separate provision

5.8 CA Termination

In the event that AffirmTrust ceases operation, all Certificates issued by AffirmTrust shall be revoked and the CRL life-time will be set to a period that meets any AffirmTrust obligations.

6. TECHNICAL SECURITY CONTROLS

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

The signing Key Pair for an AffirmTrust Certification Authority is created during the initial startup of the AffirmTrust Master Control application and is protected by the master key for such AffirmTrust Certification Authority.

When not generated by AffirmTrust, the Applicant or Subscriber is required to generate a new, secure, and cryptographically sound Key Pair to be used in association with the Subscriber's AffirmTrust Certificate or Applicant's AffirmTrust Certificate Application.

AffirmTrust Certification Authority Administrators

Keys Pairs for AffirmTrust Certification Authority administrators must be generated and protected on a cryptographic module that is compliant to at least FIPS 140-2 Level 2 certification standards. The cryptographic modules are prepared using the software provided by the module vendor. The cryptographic modules are personalized for the administrator by giving the card an identity and a password known by the administrator. The Key Pair is generated by creating the administrator as a user in the Certification Authority and performing an enrollment process which is authenticated with the administrator's module password.

6.1.2 Private Key Delivery to Subscriber

AffirmTrust Certificate Authorities do not generate the Key Pair on behalf of the Subscriber.

6.1.3 Public Key Delivery to Certificate Issuer

The Public Key to be included in an AffirmTrust Certificate is delivered to AffirmTrust Certification Authorities in a signed Certificate Signing Request (CSR) as part of the AffirmTrust certificate application process. The signature on the CSR will be verified by the AffirmTrust Certification Authority prior to issuing the AffirmTrust Certificate.

6.1.4 CA Public Key Delivery to Relying Parties

The Public-Key Certificate for AffirmTrust Certification Authorities are made available to Subscribers and Relying Parties through inclusion in third party software as distributed by the applicable software manufacturers. The Public Key Certificate for cross certified issuing Certification Authorities is provided to the Subscriber with the Subscriber Certificate.

Public Key Certificates for AffirmTrust Certification Authorities are also available for download from the Repository or Resources page of the AffirmTrust website.

6.1.5 Key Sizes

For AffirmTrust Certification Authorities, the minimum key size shall be no less than 2048 bit RSA or shall be elliptic curve cryptography (ECC) NIST P-384 or P-512.

6.1.6 Public Key Parameters Generation and Quality Checking

Certification Authority Key Pairs must be generated on a cryptographic module that meets or exceeds the requirements as defined in Section 6.1.1.

Root Certification Authority

Certificate issuance by the Root Certification Authority shall require an individual authorized by the CA (i.e. the CA system operator, system officer, or PKI administrator) to deliberately issue a direct command in order for the Root Certification Authority to perform a certificate signing operation.

Root Certification Authority Private Keys must not be used to sign Certificates except in the following cases:

(i) Self-signed Certificates to represent the Root CA itself;

(ii) Certificates for Subordinate CAs and Cross Certificates;

(iii) Certificates for infrastructure purposes (e.g. administrative role certificates, internal CA operational device certificates, and OCSP Response verification Certificates);

(iv) Certificates issued solely for the purpose of testing products with Certificates issued by a Root CA.

6.1.7 Key Usage Purposes (as per X.509 v3 Key Usage Field)

Certificates issued by an AffirmTrust Certification Authority contain the keyUsage and the extendkeyUsage Certificate extensions restricting the purpose for which an AffirmTrust Certificate can be used as listed in Appendix A. Subscribers and Relying Parties shall only use AffirmTrust Certificates in compliance with this AffirmTrust CPS and applicable laws.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

AffirmTrust Certification Authorities Private Keys must be stored and protected on cryptographic modules that meet or exceed the requirements as defined in Section 6.1.1. Private Keys on cryptographic modules are held in secure facilities under two-person control. RA Private Keys must be stored and protected on cryptographic modules that meet or exceed the requirements defined in Section 6.1.1.

6.2.2 Private Key (N Out of M) Multi-Person Control

A minimum of two person control shall be established on any AffirmTrust CA Private Key for all purposes including activation and backup, and may be implemented as a combination of technical and procedural controls. Persons involved in management and use of the AffirmTrust CA Private Keys shall be designated as authorized by the CA for this purpose. The names of the parties used for two-person control shall be maintained on a controlled list.

6.2.3 Private Key Escrow

AffirmTrust does not escrow the AffirmTrust Certification Authorities' Private Keys.

6.2.4 Private Key Backup

AffirmTrust CA Private Keys shall be backed up under the two-person control used to create the original version of the Private Keys. All copies of the AffirmTrust CA Private Key shall be securely protected.

Subscribers are responsible for protecting the Private Key associated with the Public Key in the Subscriber's Certificate.

6.2.5 Private Key Archival

Upon retirement of an AffirmTrust CA, the Private Keys will be archived securely using hardware cryptographic modules that meet the requirements Section 6.1.1. The Key Pairs shall not be used unless the CA has been removed from retirement or the keys are required temporarily to validate historical data. Private Keys required for temporary purposes shall be removed from archive for a short period of time.

The archived AffirmTrust CA Private Keys will be reviewed on an annual basis. After the minimum period of 5 years, the AffirmTrust CA Private Keys may be destroyed according to the requirements in Section 6.2.10. The AffirmTrust CA Private Keys must not be destroyed if they are still required for business or legal purposes.

6.2.6 Private Key Transfer Into or From a Cryptographic Module

AffirmTrust CA Private Keys shall be generated by and secured in a cryptographic module. In the event that a Private Key is to be transported from one cryptographic module to another, the Private Key must be migrated using the secure methodology supported by the cryptographic module.

6.2.7 Private Key Storage on Cryptographic Module

Private Keys are stored on a cryptographic module are secured in accordance with the requirements specified in FIPS 140.

6.2.8 Method of Activating Private Key

AffirmTrust CA Private Keys shall be activated under two-person control using the methodology provided with the cryptographic module.

Subscriber Private Keys shall be activated by the Subscriber to meet the requirements of the security software used for their applications. Subscribers shall protect their Private Keys corresponding to the requirements in Section 9.6.3.

6.2.9 Method of Deactivating Private Key

AffirmTrust CA Private Keys shall be deactivated when the CA is not required for active use. Deactivation of the Private Keys shall be done in accordance with the methodology provided with the cryptographic module.

AffirmTrust Certification Authority Administrators

The administrator's identity is deactivated in the AffirmTrust CA and the administrator's certificate is revoked.

6.2.10 Method of Destroying Private Key

AffirmTrust CA Private Key destruction will be two-person controlled and may be accomplished by executing a "zeroize" command or by destruction of the cryptographic module. Destruction of AffirmTrust CA Private Keys must be authorized by the AffirmTrust PKI Policy Authority.

If the AffirmTrust CA is removing a cryptographic module from service, then all Private Keys must be removed from the module. If the AffirmTrust CA cryptographic module is intended to provide tamper-evident characteristics is removed from service, then the device will be destroyed.

AffirmTrust Certification Authority Administrators

The administrator's private key is destroyed by reinitializing the cryptographic module.

6.2.11 Cryptographic Module Rating

See Section 6.2.1.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

AffirmTrust archives copies of Public Keys in accordance with Section 5.5.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

See Appendix A.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

AffirmTrust activates the cryptographic module containing its CA Private Keys according to the specifications of the hardware manufacturer. This method has been evaluated as meeting the requirements of FIPS 140-2 Level 3. The cryptographic hardware is held under two-person control as explained in Section 5.2.2 and elsewhere in this CPS. AffirmTrust will only transmit activation data via an appropriately protected channel and at a time and place that is distinct from the associated cryptographic module.

All AffirmTrust personnel and Subscribers are instructed to use strong passwords and to protect PINs and passwords. If AffirmTrust uses passwords as activation data for a signing key, AffirmTrust will change the activation data change upon rekey of the CA certificate.

6.4.2 Activation Data Protection

No provision.

6.4.3 Other Aspects of Activation Data

No provision.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

The workstations on which AffirmTrust operates are physically secured as described in Section 5.1. The operating systems on the workstations on which the AffirmTrust Certification Authorities operate enforce identification and authentication of users. Access to certificate authority software databases and audit trails is restricted as described in this CPS. All operational personnel that are authorized to have access to the AffirmTrust Certification Authorities are required to use hardware tokens in conjunction with a PIN to gain access to the physical room that contains the certification authority software being used for such AffirmTrust certification authorities.

6.5.2 Computer Security Rating

No provision.

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

AffirmTrust makes use of Commercial Off The Shelf (COTS) products for the hardware, software, and network components. Systems developed by the AffirmTrust Certification Authority are deployed in accordance with AffirmTrust software lifecycle development standards.

6.6.2 Security Management Controls

The configuration of the AffirmTrust system as well as any modifications and upgrades are documented and controlled. Methods of detecting unauthorized modifications to the CA equipment and configuration are in place to ensure the integrity of the security software, firmware, and hardware for correct operation. A formal configuration management methodology is used for installation and ongoing maintenance of the CA system. When first loaded, the CA software is verified as being that supplied from the vendor, with no modifications, and be the version intended for use.

6.6.3 Life Cycle Security Controls

No provision.

6.7 Network Security Controls

Remote access to AffirmTrust Certification Authority application via the Administration software interface is secured.

6.8 Time-Stamping

AffirmTrust provides a Time-Stamp Authority (TSA) service for use with specific AffirmTrust products as needed. The TSA authority supports RFC 3161 “Internet X.509 Public Key Infrastructure Time-Stamp Protocol” and Microsoft AuthenticodeTM time-stamp requests. Details of any acceptable use policy or limitations are included in the Subscription Agreement.

7. CERTIFICATE, CRL, AND OCSP PROFILES

Information for interpreting the following Certificate Profiles and CRL Profiles may be found in IETF's RFC 5280. AffirmTrust uses the ITU X.509, version 3 standard to construct digital certificates for use within the AffirmTrust PKI. AffirmTrust adds certain certificate extensions to the basic certificate structure for the purposes intended by X.509v3 as per Amendment 1 to ISO/IEC 9594-8, 1995.

7.1 Certificate Profile

7.1.1 Version Number(s)

All certificates are X.509 version 3 certificates.

7.1.2 Certificate Extensions

Certificate Extension	Criticality
Subject Key ID	Non-Critical
Authority Key ID	Non-Critical
Basic Constraints	Critical
Certificate Policies	Non-Critical

CRL Distribution Points	Non-Critical
Authority Information Access	Non-Critical
Key Usage	Critical
Extended Key Usage	Non-Critical
SubjectAlternativeNames	Non-Critical

7.1.3 Algorithm Object Identifiers

sha-1WithRSAEncryption	[iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5]
sha256WithRSAEncryption	[iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11]
sha384WithRSAEncryption	[iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 12]
ecdsa-with-sha384	[iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures (4) ecdsa-with-SHA2 (3) 3]

Also See Appendix A.

7.1.4 Name Forms

Each certificate includes a unique serial number that is never reused. Optional subfields in the subject of an EV Certificate must either contain information verified by AffirmTrust or be left empty. EV Certificates cannot contain metadata such as '.', '-', and ' ' characters or any other indication that the field is not applicable.

The Distinguished Name in a Certificate may contain the following information:

(1) Organization Name – Required in SSL Certificates
(2) Domain Name - Required in SSL Certificates
(3) Business Category – Required for EV Certificates
(4) Organizational Unit – Not supported unless special request
(5) Jurisdiction of Incorporation or Registration – Required in EV Certificates (as applicable)
(6) Registration Number - Required in EV Certificates
(7) Physical Address of Place of Business Number – Optional for street and postal code

The contents of the fields in EV Certificates must meet the requirements in Section 9 of the EV Guidelines.

7.1.5 Name Constraints

No provision.

7.1.6 Certificate Policy Object Identifier

An object identifier (OID) is a unique number that identifies an object or policy. The OIDs used by AffirmTrust are listed in Section 1.2.

7.1.7 Usage of Policy Constraints Extension

No provision.

7.1.8 Policy Qualifiers Syntax and Semantics

AffirmTrust may include brief statements in Certificates about the applicability of this CPS or limitations of liability and other terms associated with the use of a Certificate in the Policy Qualifier field of the Certificates policy extension.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

No provision.

7.2 CRL Profile

7.2.1 Version Number(s)

AffirmTrust issues version 2 CRLs that conform to RFC 3280. CRLs contain the following fields:

Field	Value
Issuer Signature Algorithm	sha-1WithRSAEncryption [1 2 840 113549 1 1 5] OR sha-256WithRSAEncryption [1 2 840 113549 1 1 11] OR ecdsa-with-sha284 [1 2 840 10045 4 3]
Issuer Distinguished Name	AffirmTrust
thisUpdate	CRL issue date in UTC format
nextUpdate	Date when the next CRL will issue in UTC format. The field is set to thisUpdate plus 24 hours
Revoked Certificates List	List of revoked Certificates, including the serial number and revocation date
Issuer's Signature	[Signature]

7.2.2 CRL and CRL Entry Extensions

CRLs have the following extensions:

Extension	Value
CRL Number	Never repeated monotonically increasing integer
Authority Key Identifier	Same as the Authority Key Identifier listed in the Certificate
Invalidity Date	Optional date in UTC format
Reason Code	Optionally included reason for the revocation

7.3 OCSP Profile

7.3.1 Version Number(s)

AffirmTrust's OCSP responders conform to version 1 of RFC 2560.

7.3.2 OCSP Extensions

No provision.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

The practices in this CPS are designed to meet or exceed the requirements of generally accepted industry standards, including the latest version of the AICPA/CICA (1) Trust Service Principles and Criteria for Certification Authorities, (2) WebTrust For Certification Authorities – Extended Validation Audit Criteria, and (3) WebTrust Principles, and Criteria for Certification Authorities – SSL Baseline with Network Security audit WebTrust Program for Certification Authorities.

8.1 Frequency or Circumstances of Assessment

AffirmTrust has an annual audit by an independent external auditor to assess AffirmTrust's compliance with the AICPA/CICA (1) Trust Service Principles and Criteria for Certification Authorities, (2) WebTrust For Certification Authorities – Extended Validation Audit Criteria, and (3) WebTrust Principles, and Criteria for Certification Authorities – SSL Baseline with Network Security audit WebTrust Program for Certification Authorities.

8.2 Identity/Qualifications of Assessor

Auditors must meet the requirements of Section 17.6 of the EV Guidelines and Baseline Requirements.

8.3 Assessor's Relationship to Assessed Entity

AffirmTrust uses an independent auditor that does not have a financial interest, business relationship, or course of dealing that could foreseeably create a significant bias for or against AffirmTrust.

8.4 Topics Covered by Assessment

The audit conforms to the WebTrust audit programs listed in Section 8.1, and covers AffirmTrust's business practices disclosure and the integrity of AffirmTrust's PKI operations.

8.5 Actions Taken as a Result Of Deficiency

If an audit reports any material noncompliance with applicable law, this CPS, or any other contractual obligations related to AffirmTrust’s services, then (1) the auditor will document the discrepancy, (2) the auditor will promptly notify AffirmTrust, and (3) AffirmTrust will develop a plan to cure the noncompliance. AffirmTrust will submit the plan to the PKI Policy Authority for approval and to any third party that AffirmTrust is legally obligated to satisfy. The PKI Policy Authority may require additional action if necessary to rectify any significant issues created by the non-compliance, including requiring revocation of affected Certificates.

8.6 Communication of Results

The results of each audit are reported to the PKI Policy Authority and to any third party entities which are entitled by law, regulation, or agreement to receive a copy of the audit results.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

9.1.1 Certificate Issuance or 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 Subscriber Agreement (Terms of Service) at the time the Certificate is issued or renewed, and may change from time to time without prior notice.

9.1.2 Certificate Access Fees

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

9.1.3 Revocation or Status Information Access Fees

AffirmTrust does not charge a fee as a condition of making the CRL or OCSP 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.

9.1.4 Fees for Other Services

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

9.1.5 Refund Policy

A Subscriber may apply a refund for the cost of an individual Certificate 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. As to AffirmTrust's refund policy for enterprise Subscribers, see the terms of the Subscriber Agreement.

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 4.9.3 of this CPS.

9.2 Financial Responsibility

9.2.1 Insurance Coverage

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

9.2.2 Other Assets

No provision.

9.2.3 Insurance or Warranty Coverage for End-Entities

AffirmTrust's warranty coverage for end-entities is specified in Subscriber Agreements and Relying Party Agreements.

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

The following information is considered confidential information and protected against disclosure using a reasonable degree of care:

1. Private Keys;
2. Activation data used to access Private Keys or to gain access to the CA system;
3. Business continuity, incident response, contingency, and disaster recovery plans;
4. Other security practices used to protect the confidentiality, integrity, or availability of information;
5. Information held by AffirmTrust as private information in accordance with Section 9.4;
6. Audit logs and archive records, including certificate application records and documentation submitted in support of certificate applications whether successful or rejected; and
7. Transaction records, financial audit records, and external or internal audit trail records and any audit reports (with the exception of an auditor's letter confirming the effectiveness of the controls set forth in this CPS)

9.3.2 Information Not Within the Scope of Confidential Information

All information published on the AffirmTrust website plus published certificate and revocation data is public information.

9.3.3 Responsibility to Protect Confidential Information

AffirmTrust's employees, agents, and contractors are responsible for protecting confidential information and are contractually obligated to do so. AffirmTrust systems are configured to protect confidential information.

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

AffirmTrust follows the Privacy Statement posted on its website when handling personal information. Personal information is only disclosed when required by law or when requested by the subject of personal information.

9.4.2 Information Treated as Private

AffirmTrust treats all personal information about an individual that is not publicly available in the contents of a Certificate or CRL as private information. AffirmTrust shall protect private information in its possession using a reasonable degree of care and appropriate safeguards.

9.4.3 Information Not Deemed Private

Certificates, CRLs, and the personal or corporate information appearing in them are not considered private information.

9.4.4 Responsibility to Protect Private Information

All personnel involved with the AffirmTrust PKI are expected to handle personnel information in strict confidence and meet the requirements of applicable law concerning the protection of personal data. All sensitive information is stored securely and protected against accidental disclosure.

9.4.5 Notice and Consent to Use Private Information

Personal data provided during the application, registration, and identity verification process that is not contained in Certificates is considered private information. AffirmTrust may only use private information as part of the account registration and certificate issuance process, with the subject's express written consent, or as required by applicable law or regulation. Notwithstanding the foregoing, personal information contained in Certificates may be published in online public repositories. All Subscribers consent to the global transfer of any personal data contained in Certificates.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

AffirmTrust may disclose private information, without notice, when required to do so by law or regulation.

9.4.7 Other Information Disclosure Circumstances

No provision.

9.5 Intellectual Property Rights

AffirmTrust, or AffirmTrust Group, own all intellectual property rights in AffirmTrust's services, including the AffirmTrust certificates, trademarks used in providing the services, and this CPS. "AffirmTrust" is a registered trademark and assumed business name which is used for the purpose of providing AffirmTrust products and services.

Certificates and revocation information are the exclusive property of AffirmTrust. AffirmTrust grants permission to reproduce and distribute certificates on a non-exclusive, royalty-free basis, provided that they are reproduced and distributed in full. AffirmTrust does not allow derivative works of its certificates or products without prior written permission. Private and Public Keys will remain the property of the Subscribers who rightfully hold them.

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

9.6.1.1 OV Server Certificate Limited Warranty

AffirmTrust provides the following limited warranty at the time of issuance of OV server Certificates: (i) it issued the Certificate substantially in compliance with this CPS; (ii) the information contained within the Certificate accurately reflects the information provided to

AffirmTrust by the Applicant in all material respects; and (iii) it has taken reasonable steps to verify that the information within the Certificate is accurate. The nature of the steps AffirmTrust takes to verify the information contained in a Certificate is set forth in Section 3 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.

9.6.1.2 EV Server Certificate Limited Warranty

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 or the Applicant Representative has acknowledged and accepted the Terms of Use (if applicable);

(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.

9.6.2 RA Representations and Warranties

No provision.

9.6.3 Subscriber Representations and Warranties

Subscribers are solely responsible for any misrepresentations they make to third parties and for all transactions that use Subscriber’s Private Key, regardless of whether such use was authorized.

Subscribers represent to AffirmTrust, Application Software Vendors, and Relying Parties that, for each Certificate, the Subscriber will:

1. Securely generate its Private Keys, and protect its Private Keys from compromise,
2. Provide accurate and complete information when communicating with AffirmTrust,
3. Confirm the accuracy of the certificate data prior to using the Certificate,
4. Promptly request revocation of the Certificate, and cease using it and its associated Private Key, if there is any actual or suspected misuse or compromise of the Subscriber’s Private Key associated with the Public Key included in the Certificate; and promptly request revocation of the Certificate, and cease using it, if any information in the Certificate is or becomes incorrect or inaccurate,
5. Ensure that individuals using certificates on behalf of an organization have received security training appropriate to the certificate,
6. Use the Certificate only for authorized and legal purposes, consistent with the certificate purpose, this CPS, any applicable CP, and the relevant Subscriber Agreement, including only installing SSL Certificates on servers accessible at the domain listed in the Certificate and not using code signing Certificates to sign malicious code or any code that is downloaded without a user’s consent,
7. Abide by the Subscriber Agreement and this CPS when requesting or using a

Certificate, and
8. Promptly cease using the Certificate and related Private Key after the Certificate's expiration.

9.6.4 Relying Party Representations and Warranties

Each Relying Party represents that, prior to relying on an AffirmTrust Certificate, it:

1. Made reasonable efforts to acquire sufficient knowledge on using digital certificates and PKI,
2. Studied the limitations on the usage of certificates and is aware of AffirmTrust's limitations on liability with respect to reliance on issued Certificates,
3. Has read, understands, and agrees to the Relying Party Agreement and this CPS,
4. Verified both the Certificate and any certificates in the certificate chain using the relevant CRL or OCSP,
5. Will not use a Certificate if the Certificate has expired or been revoked, and
6. Will take all reasonable steps to minimize the risk of relying on a digital signature created by an invalid, revoked, or expired Certificate, including only relying on a Certificate if appropriate after considering:

    a) Applicable law and the legal requirements for identification of a party, protection of the confidentiality or privacy of information, and enforceability of the transaction;
    b) The intended use of the Certificate as listed in the Certificate or this CPS,
    c) The data listed in the Certificate,
    d) The economic value of the transaction or communication,
    e) The potential loss or damage that would be caused by an erroneous identification or a loss of confidentiality or privacy of information in the application, transaction, or communication,
    f) The Relying Party's previous course of dealing with the Subscriber,
    g) The Relying Party's understanding of trade, including experience with computer-based methods of trade, and
    h) Any other indicia of reliability or unreliability pertaining to the Subscriber and/or the application, communication, or transaction.

Any reliance on a Certificate by a Relying Party that does not meet these requirements is at the party's own risk.

9.6.5 Representations and Warranties of Other Participants

No provision.

9.7 Disclaimers of Warranties

EXCEPT FOR THE LIMITED WARRANTY DESCRIBED IN SECTION 9.6.1 ABOVE, AFFIRMTRUST AND AFFIRMTRUST GROUP AFFILIATES 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 QUALITY, MERCHANTABILITY, NON-INFRINGEMENT, TITLE AND FITNESS FOR A PARTICULAR PURPOSE, 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 AND AFFIRMTRUST GROUP AFFILIATES FURTHER DISCLAIM 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 AND AFFIRMTRUST GROUP AFFILIATES DO 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 AND AFFIRMTRUST GROUP AFFILIATES HEREBY DISCLAIM 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 4.9.3 OF THIS CPS.

9.8 Limitations of Liability

9.8.1 AFFIRMTRUST, AFFIRMTRUST GROUP AFFILIATES, ANY RESELLERS, CO-MARKETERS, SUBCONTRACTORS, DISTRIBUTORS, AGENTS, SUPPLIERS, AND EMPLOYEES AND DIRECTORS OF ANY OF THE FOREGOING (COLLECTIVELY, “AFFIRMTRUST AND ITS ENTITIES”) SHALL NOT BE LIABLE IN CONTRACT, TORT (INCLUDING NEGLIGENCE), STRICT LIABILITY, FOR BREACH OF A STATUTORY DUTY OR IN ANY OTHER WAY (EVEN IF 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;
(IV) ANY OTHER INDIRECT, CONSEQUENTIAL, INCIDENTAL, MULTIPLE, SPECIAL, PUNITIVE, EXEMPLARY DAMAGES, OR
V) ANY LOSS OR DAMAGE THAT IS NOT DIRECTLY ATTRIBUTABLE TO THE USE OR RELIANCE ON A CERTIFICATE OR SERVICE PROVIDED UNDER THIS CPS INCLUDING, WITHOUT LIMITATION, ANY LOSS OR DAMAGE RESULTING FROM THE COMBINATION OR INTEGRATION OF THE CERTIFICATE OR SERVICE WITH ANY SOFTWARE OR HARDWARE NOT PROVIDED BY AFFIRMTRUST IF THE LOSS OR DAMAGE WOULD NOT HAVE OCCURRED AS A RESULT OF USE OF THE CERTIFICATE ALONE.

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 AGREEMENT, THE APPLICABLE CPS OR WITH REGARD TO THE USE OF OR RELIANCE ON THE CERTIFICATE.

9.8.2 IN NO EVENT SHALL THE TOTAL AGGREGATE LIABILITY OF AFFIRMTRUST AND ITS ENTITIES TO ANY APPLICANT, SUBSCRIBER, RELYING PARTY OR ANY OTHER PERSON, ENTITY, OR ORGANIZATION ARISING OUT OF OR RELATING TO THIS AGREEMENT, THE CPS AND ALL CERTIFICATES ISSUED (INCLUDING WITHOUT LIMITATION, THE INSTALLATION OF, USE OF OR RELIANCE UPON A CERTIFICATE) AND SERVICES PROVIDED UNDER THIS AGREEMENT UNDER ANY CAUSE OF ACTION, OR ANY CONTRACT, STRICT LIABILITY, TORT (INCLUDING NEGLIGENCE), OR OTHER LEGAL OR EQUITABLE THEORY OR IN ANY OTHER WAY, EXCEED THE FOLLOWING: THE AMOUNT PAID TO AFFIRMTRUST FOR THE SERVICES UNDER THIS AGREEMENT OVER THE 12 MONTHS IMMEDIATELY PRECEDING THE EVENTS GIVING RISE TO THE CLAIM, UP TO A MAXIMUM OF TEN THOUSAND U.S. DOLLARS (US$10,000.00) (EXCEPT THAT FOR ANY (i) EV CERTIFICATES ISSUED UNDER THIS AGREEMENT, AFFIRMTRUST AND ITS ENTITIES' AGGREGATE LIABLIITY IS LIMITED TO TWO THOUSAND U.S. DOLLARS (US$2,000.00) PER SUBSCRIBER OR RELYING PARTY PER EV CERTIFICATE, UP TO A MAXIMUM OF FIFTY THOUSAND U.S. DOLLARS (US$50,000.00)); AND (ii) DOMAIN VALIDATED (DV) CERTIFICATES ISSUED UNDER THIS AGREEMENT, AFFIRMTRUST AND ITS ENTITIES' AGGREGATE LIABILITY IS LIMITED TO THE AMOUNT PAID TO AFFIRMTRUST FOR THE DV CERTIFICATE GIVING RISE TO THE CLAIM OVER THE 12 MONTHS IMMEDIATELY PRECEDING THE EVENTS GIVING RISE TO THE CLAIM, UP TO A MAXIMUM OF ONE THOUSAND U.S. DOLLARS (US$1,000.00)).

9.8.3 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 and AffirmTrust Group Affiliates be liable for any damages to Applicants, Subscribers, Relying Parties or any other person, entity or organization arising out of or related to the use or misuse of, or reliance on any Certificate issued under this CPS that: (a) has expired or been revoked; (b) has been used for any purpose other than as set forth in the CPS; (c) has been tampered with; (d) 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 or AffirmTrust Group Affiliates (including without limitation the Subscriber or Relying Party); or (e) 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 and AffirmTrust Group Affiliates 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.

9.9 Indemnities

Unless otherwise set forth in this CPS and/or Subscriber Agreement, Applicant and Subscriber, as applicable, hereby agrees to indemnify and hold AffirmTrust and AffirmTrust Group Affiliates (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 negligently 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.

9.10 Term and Termination

9.10.1 Term

This CPS and any amendments are effective when published to AffirmTrust's online repository and remain in effect until replaced with a newer version.

9.10.2 Termination

This CPS and any amendments remain in effect until replaced by a newer version.

9.10.3 Effect of Termination and Survival

AffirmTrust will communicate the conditions and effect of this CPS's termination via the AffirmTrust repository. The communication will specify which provisions survive termination. At a minimum, responsibilities related to protecting confidential information will survive termination. Subscriber Agreements remain effective until the end of the Certificate's validity, even if this CPS terminates.

9.11 Individual Notices and Communications with Participants

AffirmTrust accepts notices related to this CPS that are addressed to the location specified in Section 2.2 of this CPS. Notices are deemed effective after the sender receives a valid acknowledgment of receipt from AffirmTrust. If an acknowledgement of receipt is not received within five days, the sender must resend the notice in paper form to the street address specified in Section 2.2 using either a courier service that confirms

delivery or via certified or registered mail with postage prepaid and return receipt requested. AffirmTrust may allow other forms of notice in its Subscriber Agreements.

9.12 Amendments

9.12.1 Procedure for Amendment

The PKI Policy Authority determines what amendments should be made to this CPS. Amendments are made by posting an updated version of the CPS to the online repository. Controls are in place to reasonably ensure that this CPS is not amended and published without the prior authorization of the PKI Policy Authority. This CPS is reviewed at least annually.

9.12.2 Notification Mechanism and Period

Notification of amendments to this CPS are made by posting an updated version of the CPS to the online repository. Amendments may be made at any time without any prior notice period.

9.12.3 Circumstances Under Which OID Must Be Changed

If the PKI Policy Authority determines an amendment necessitates a change in an OID, then the revised version of this CPS will also contain a revised OID. Otherwise, amendments do not require an OID change.

9.13 Dispute Resolution Provisions

Prior to commencing any litigation, AffirmTrust and all Subscribers and Relying Parties agree to seek an amicable settlement of any disputes or claims, provided that either party may commence litigation at any time to avoid prejudice to any rights under governing law.

9.14 Governing Law

The laws of the Province of Ontario, Canada, excluding its conflict of laws rules, shall govern the construction, validity, interpretation, enforceability and performance of the CPS, all Subscription Agreements and all Relying Party Agreements. The application of the United Nations Convention on Contracts for the International Sale of Goods to the CPS, any Subscription Agreements, and any Relying Party Agreements is expressly excluded. Any dispute arising out of or in respect to the CPS, any Subscription Agreement, any Relying Party Agreement, or in respect to any Certificates or any services provided in respect to any Certificates that is not resolved by alternative dispute resolution, shall be brought in the provincial or federal courts sitting in Ottawa, Ontario, and each person, entity, or organization hereby agrees that such courts shall have personal and exclusive jurisdiction over such disputes. In the event that any matter is brought in a provincial or federal court, Applicants, Subscribers, and Relying Parties waive any right that such Applicants, Subscribers, and Relying Parties may have to a jury trial.

9.15 Compliance with Applicable Law

Subscribers and Relying Parties acknowledge and agree to use Certificates in compliance with all applicable laws and regulations, including without limitation all applicable 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.

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

This CPS and the Relying Party Agreement represents the entire agreement between any Relying Party and AffirmTrust and supersedes any and all prior understandings and representations pertaining to their subject matters.

9.16.2 Assignment

AffirmTrust may assign its rights and obligations under this CPS at any time without notice or consent. Subscribers and Relying Parties may not assign their rights or obligations under this CPS without the prior written consent of AffirmTrust.

9.16.3 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.

9.16.4 Enforcement (Attorneys' Fees and Waiver Of Rights)

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.

9.16.5 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.

9.17 Other Provisions

9.17.1 Conflict of Provisions

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

9.17.2 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.

APPENDIX A TO AFFIRMTRUST CPS

1. AffirmTrust Root Certificate Information:

CA Root Name	Algorithm	CA Root Size	Signature Hash	CA Root Expires	SHA Hash Thumbprint
AffirmTrust Commercial	RSA	2048	SHA 256	12/31/2030	f9 b5 b6 32 45 5f 9c be ec 57 5f 80 dc e9 6e 2c c7 b2 78 b7
AffirmTrust Networking	RSA	2048	SHA 1	12/31/ 2030	29 36 21 02 8b 20 ed 02 f5 66 c5 32 d1 d6 ed 90 9f 45 00 2f
AffirmTrust Premium	RSA	4096	SHA 384	12/31/2040	d8 a6 33 2c e0 03 6f b1 85 f6 63 4f 7d 6a 06 65 26 32 28 27
AffirmTrust Premium ECC	ECC	384	SHA 384 ECDSA	12/31/2040	b8 23 6b 00 2f 1d 16 86 53 01 55 6c 11 a4 37 ca eb ff c3 bb

AffirmTrust will offer its certificate products from intermediate sub-CAs issued off of one or more of the above roots as indicated in the Product Offerings information described in Section 4 below.

2. Cross-Signed Intermediate sub-CAs

No provision.

3. Extended Validation (EV) OIDs:

Extended Validation (EV) Certificates will contain the following EV OIDs:

AffirmTrust Commercial Root: EV OID is 1.3.6.1.4.1.34697.2.1
AffirmTrust Networking Root: EV OID is 1.3.6.1.4.1.34697.2.2
AffirmTrust Premium Root: EV OID is 1.3.6.1.4.1.34697.2.3
AffirmTrust Premium ECC Root: EV OID is 1.3.6.1.4.1.34697.2.4

4. AffirmTrust Product Offerings:

AffirmTrust's product offerings and their specifications are as follows:

A. Server Certificate Offerings

(1) Product Name: "AffirmTrust DV Certificates".

Root certificate:	AffirmTrust Commercial
Issuing sub-CA root:	AffirmTrust Certificate Authority – DV1
Sub-CA Root key length:	2048

Valid until:	December 1, 2030
Serial No.:	2c:07:cf:f9:6c:e8:68:9a
SHA-1 Thumbprint:	48:c4:86:80:69:01:a1:49:47:0d:37:64:c4:b0:7c:a2:9c:88:a0:5c
Certificate Types:	Domain Validated (DV) server certificates
Maximum operational period for certificate:	Up to 39 months

(2) Product Name: “AffirmTrust OV Certificates”

Root certificate:	AffirmTrust Commercial
Issuing sub-CA root:	AffirmTrust Certificate Authority – OV1
Sub-CA Root key length:	2048
Valid until:	December 1, 2030
Serial No.:	18 7e 7f 3b f6 6f 23 cd
SHA-1 Thumbprint:	ef b2 01 f1 2d 3a ef 8a ea ab af 3f 13 a0 3a d2 b7 0a 8d 1a
Certificate Types:	Organization Validated (OV) server certificates
Maximum operational period for certificate:	Up to 39 months

(3) Product Name: “AffirmTrust EV Certificates”

Root certificate:	AffirmTrust Commercial
Issuing sub-CA root:	AffirmTrust Extended Validation CA – EV1
Sub-CA Root key length:	2048
Valid until:	December 1, 2030
Serial No.:	40 f0 bb aa 8a e0 c0 98
SHA-1 Thumbprint:	b9 9c 3a 4c 53 45 01 85 54 81 bf a1 ed ef 63 ae 11 7e af 06
Certificate Types:	Extended Validation (EV) server certificates
Maximum operational period for certificate:	Up to 27 months

B. Test Certificates

Test certificates may be issued from any existing intermediate Sub-CA root certificate, but such test certificates will be restricted in their use solely to test or demonstration environments.