AFFIRMTRUST™

# CERTIFICATION PRACTICE STATEMENT

Version 3.9

Effective Date: 30 September 2020

## REVISION HISTORY

| Issue | Date | Changes in this Revision |
|---|---|---|
| 3.6 | 31 May 2019 | Update to IP address validation methods and CPR procedure |
| 3.7 | July 25, 2019 | Update for Domain Name validation methods |
| 3.8 | September 30, 2019 | Update CAA |
| 3.9 | September 30, 2020 | Update email address for CPR, implementation of CAB Forum ballots (23, 24, 25, 28, 30, 31, 33 and 35), and removal of non-inclusive language |

## TABLE OF CONTENTS

# 1. INTRODUCTION

The AffirmTrust CAs issue Certificates, which include the following Certificate Types:

- DV Certificate(s)
- OV Certificate(s)
- EV Certificate(s)

## 1.1 Overview

This AffirmTrust Certification Practice Statement (the "CPS"), Version 3.3, effective date: 31 May 2018, 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 §1.6.1, 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 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.

## 1.3 PKI Participants

### 1.3.1 Certification Authorities

AffirmTrust is a certification authority (CA) that issues SSL 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

RAs under the AffirmTrust CA may accept Certificate Applications from Applicants and perform verification of the information contained in such Certificate Applications, according to the procedures established by the Policy Authority. A RA operating under a CA may send a request to such CA to issue a Certificate to the Applicant. Only RAs authorized by AffirmTrust are permitted to submit requests to a CA for the issuance of Certificates.

Third Party RAs may not be delegated to validate FQDNs nor IP Addresses per section 3.2.2.4 or section 3.2.2.5.

AffirmTrust CA may designate an Enterprise RA to verify Certificate requests from the Enterprise RA’s own organization. The requested FQDNs must be within the Enterprise RA’s domain namespace.

### 1.3.3 Subscribers

Subscribers may use AffirmTrust’s CA services to support transactions and communications. The subject of a Certificate is the party named in the Certificate. 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 revoked as indicated on the CRL or OCSP response.

### 1.3.5 Other Participants

No stipulation.

## 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.

Certificates issued under this CPS may not be used for “traffic management” or man-in-the-middle purposes.

## 1.5 Policy Administration

### 1.5.1 Organization Administering the document

The CPS is administered by the Policy Authority; it is based on the policies established by Entrust Datacard Limited.

### 1.5.2 Contact Person

The contact information for questions about Certificates is:

AffirmTrust Limited
1000 Innovation Drive, Suite 400
Ottawa, Ontario
Canada, K2K 3E7

Email: mailto:support@affirmtrust.com

Certificate Problem Reports, such as Certificate misuse, vulnerability reports or external reports of key compromise, must be emailed to abuse@affirmtrust.com.

### 1.5.3 Person Determining CPS Suitability for the Policy

The PKI Policy Authority determines the suitability and applicability of this CPS.

### 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 §9.10 and §9.12 below.

## 1.6 Definitions and Acronyms

### 1.6.1 Definitions

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 Datacard 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.

Application Software Supplier. A developer of Internet browser software or other software that displays or uses Certificates.

Authorization Domain Name. As defined in the Baseline Requirements.

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 Key Pair. As defined in the Baseline Requirements.

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 Problem Report. As defined in the Baseline Requirements.

Certificate Profile. As defined in the Baseline Requirements.

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

Certification Authority. A certification authority operated by or on behalf of AffirmTrust for the purpose of issuing, managing, revoking, renewing, and providing access to Certificates. The Certification Authority (i) creates and digitally signs Certificates that contain among other things a Subject's Public Key and other information that is intended to identify the Subject, (ii) makes Certificates available to facilitate communication with the Subject identified in the Certificate, and (iii) creates and digitally signs Certificate Revocation Lists containing information about Certificates that have been revoked and which should no longer be used or relied upon.

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

Domain Contact. As defined in the Baseline Requirements.

Domain Name Registrant. As defined in the Baseline Requirements.

Domain Name Registrar. As defined in the Baseline Requirements.

DNS CAA Email Contact. As defined in the Baseline Requirements.

DNS CAA Phone Contact. As defined in the Baseline Requirements.

DNS TXT Record Email Contact. As defined in the Baseline Requirements.

DNS TXT Record Phone Contact. As defined in the Baseline Requirements.

DV (Domain Validated) Certificate. An SSL 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.

Enterprise RA. As defined in the Baseline Requirements.

EV Certificate. An SSL Certificate that contains information specified in the EV Guidelines and that has been validated in accordance with those EV 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.

Fully-Qualified Domain Name. As defined in the Baseline Requirements.

Incorporating Agency. As defined in the EV SSL Guidelines.

Internal Name. As defined in the Baseline Requirements.

Key Compromise. As defined in the Baseline Requirements.

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. An SSL 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.

PKI Policy Authority. Those personnel who work for or on behalf of AffirmTrust and who are responsible for determining the policies and procedures that govern the operation of the CAs.

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.

Registration Agency. As defined in the EV SSL Guidelines.

Registration Authority. An entity that performs two functions: (1) the receipt of information from a Subject to be named in a Certificate, and (2) the performance of verification of information provided by the Subject following the procedures prescribed by the CAs. In the event that the information provided by a Subject satisfies the criteria defined by the CAs, an RA may send a request to a CA requesting that the CA generate, digitally sign, and issue a Certificate containing the information verified by the RA. An RA may be operated by AffirmTrust or by an independent third-party.

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 CA. The top level CA whose Root Certificate is distributed by Application Software Suppliers and that issues Subordinate CA Certificates.

Root Certificate. The self-signed Certificate issued by the Root CA to identify itself and to facilitate verification of Certificates issued to its Subordinate CAs.

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

SSL Certificate. A Certificate issued by a CA for use on secure servers.

Subject. A person, entity, or organization whose Public Key is contained in a Certificate.

Subordinate CA. A CA whose Certificate is signed by the Root CA, or another Subordinate CA.

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.

Wildcard Domain Name. A Domain Name consisting of a single asterisk character followed by a single full stop character (“*.”) followed by a Fully-Qualified Domain Name.

### 1.6.2 Acronyms

| | |
|---|---|
| ADN | Authorization Domain Name |
| CA | Certification Authority |
| CAA | Certification Authority Authorization |
| CPR | Certificate Problem Report |
| CPS | Certification Practice Statement |
| CRL | Certificate Revocation List |
| CSR | Certificate Signing Request |
| CT | Certificate Transparency |
| DBA | Doing Business As |
| DN | Distinguished Name |
| DNS | Domain Name System |
| DNSSEC | Domain Name System Security Extensions |
| DV | Domain Validated |
| ECC | Elliptic Curve Cryptography |
| EKU | Extended Key Usage |
| EV | Extended Validation |
| FIPS | (US Government) Federal Information Processing Standard |
| FQDN | Fully Qualified Domain Name |
| HTTP | Hyper Text Transfer Protocol |
| HTTPS | Hyper Text Transfer Protocol Secure |
| IANA | Internet Assigned Numbers Authority |
| ICANN | Internet Corporation for Assigned Names and Numbers |
| IETF | Internet Engineering Task Force |
| ISO | International Organization for Standardization |
| ITU-T | International Telecommunication Union - Telecommunication Standardization Sector |
| NIST | (US Government) National Institute of Standards and Technology |
| OCSP | Online Certificate Status Protocol |
| OID | Object Identifier |
| OV | Organization Validated |
| PA | Policy Authority |
| PIN | Personal Identification Number |
| PKI | Public-Key Infrastructure |
| RA | Registration Authority |
| RFC | Request for Comment |
| RSA | Rivest–Shamir–Adleman cryptosystem |
| SAN | Subject Alternative Name |
| SSL | Secure Sockets Layer |
| TLS | Transport Layer Security |
| URL | Universal Resource Locator |

# 2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

AffirmTrust maintains the Repository to store various information related to Certificates and the operation of the CAs and RAs. The CPS and various other related information is published in the Repository.

## 2.1 Repositories

AffirmTrust maintains the Repositories to allow access to Certificate-related and CRL Certificate revocation information. The information in the Repositories is accessible through a web interface, available on a 24x7 basis and is periodically updated as set forth in this CPS. The Repositories are the only approved source for CRL and other information about Certificates.

AffirmTrust will adhere to the latest version of the CPS published in the Repository.

The Repository can be accessed at https://www.affirmtrust.com/resources/.

Web Pages that can be used by application software suppliers to test their software with Subscriber Certificates that chain up to each publicly trusted Root Certificate are hosted at https://www.affirmtrust.com/resources/.

## 2.2 Publication of Certification Information

AffirmTrust publishes its CPS, CA Certificates, Subscriber Agreements (Terms of Service), Relying Party Agreements, and CRLs in online repositories.

## 2.3 Time or Frequency of Publication

AffirmTrust CPS will be re-issued and published at least once per year. The CPS will be updated with an incremented version number and a new date on an annual basis even if no other changes have been made to this document.

CRLs will be updated as per §4.9.7.

OCSP responses will be updated as per §4.9.10.

## 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

The PKI Policy Authority mandates the verification practices for verifying identification and authentication, and may, in its discretion, update such practices.

## 3.1 Naming

Before issuing an Certificate, the AffirmTrust CAs ensure that all Subject organization information in the Certificate conforms to the requirements of, and has been verified in accordance with the procedures prescribed in this CPS and matches the information confirmed and documented by the RA pursuant to its verification processes.

For EV Certificates, the CA and RA must follow the verification procedures in this CPS and the EV Guidelines and match the information confirmed and documented by the RA pursuant to its verification processes. Such verification procedures are intended to accomplish the following:

(i) Verify the Applicant's existence and identity, including;
   a. Verify the Applicant's legal existence and identity (as stipulated in the EV Guidelines),
   b. Verify the Applicant's physical existence (business presence at a physical address) , and
   c. Verify the Applicant's operational existence (business activity).

(ii) Verify the Applicant's authorization for the EV Certificate, including;
   a. Verify the name, title, and authority of the Contract Signer, Certificate Approver, and Certificate Requester;
   b. Verify that Contract Signer signed the Subscription Agreement; and
   c. Verify that a Certificate Approver has signed or otherwise approved the EV Certificate request.

### 3.1.1 Types of Names

The Subject names in a Certificate comply with the X.501 Distinguished Name (DN) form. The CAs shall use a single naming convention as set forth below.

1. DV Certificates
   (i) "Organizational Unit Name" (OU) states "Domain Validated"; and
   (ii) "Common Name" (CN) which is the hostname, the fully qualified hostname or path used in the DNS of the secure server on which the Applicant is intending to install the DV Certificate;

2. OV Certificates
   (iii) "Country Name" (C) which is the two-letter ISO 3166 code for the country in which the Applicant is located and plans to host the secure server on which the Applicant is intending to install the OV Certificate;
   (iv) "Organization Name" (O) which is the name of the organization in the case of a corporation, partnership, or other entity. In the case of a sole proprietorship, the organization name can be the name of the Applicant;
   (v) "Organizational Unit Name" (OU) which is an optional field. The OU field may be used to distinguish between different organizational groups within an organization (for example, to distinguish between human resources, marketing, and development);
   (vi) "Common Name" (CN) which is the hostname, the fully qualified hostname or path used in the DNS of the secure server on which the Applicant is intending to install the OV Certificate;
   (vii) "Locality" (L), which is the city or locality of the organization's place of business; and

(viii) "State" (ST) (if applicable), which is the state or province of the organization's place of business.

3. EV Certificates
   (ix) Same as OV Certificates, plus
   (x) "serialNumber" which is the registration number of Subscriber,
   (xi) "businessCategory" which is the applicable business category clause per the EV Guidelines,
   (xii) "jurisdictionOfIncorporationLocalityName" (if applicable) which is the jurisdiction of registration or incorporation locality of Subscriber,
   (xiii) "jurisdictionOfIncorporationStateOrProvinceName" (if applicable) which is the jurisdiction of registration or incorporation state or province of Subscriber, and
   (xiv) "jurisdictionOfIncorporationCountry" which is the jurisdiction of registration or incorporation country of Subscriber.

### 3.1.2 Need for Names to Be Meaningful

The Certificates issued pursuant to this CPS are meaningful only if the names that appear in the Certificates can be understood and used by Relying Parties. Names used in the Certificates must identify the person or object to which they are assigned in a meaningful way. AffurmTrust CAs shall not issue Certificates to the Subscribers that contain domain names, IP addresses, DN, URL, and/or e-mail addresses that the Subscribers do not legitimately own or control. Examples of fields and extensions where these names appear include subject DN and subject alternative names.

The value of the Common Name to be used in a Certificate shall be the Applicant's FQDN or path that is used in the DNS of the secure server on which the Applicant is intending to install the Certificate.

For EV Certificates, the FQDN for an EV Certificate cannot be an IP address or a Wildcard Domain Name.

### 3.1.3 Anonymity or Pseudonymity of Subscribers

No stipulation.

### 3.1.4 Rules for Interpreting Various Name Forms

No stipulation.

### 3.1.5 Uniqueness of Names

Names shall be defined unambiguously for each Subject in a Repository. The Distinguished Name attribute will usually be unique to the Subject to which it is issued. Each Certificate shall be issued a unique serial number within the name space of the Subordinate CA.

### 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

#### *3.2.2.1 Identity*

AffirmTrust requires the following verification depending on the Certificate type.

##### 3.2.2.1.1 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 in accordance with Sec. 3.2.2.4.

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

##### 3.2.2.1.2 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 §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. 3.2.2.4.

##### 3.2.2.1.3 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/.

Effective as of 1 October 2020, prior to the use of an Incorporating Agency or Registration Agency to fulfill these verification requirements, the agency information about the Incorporating Agency or Registration Agency will be disclosed at https://www.entrust.com/legal-compliance/approved-incorporating-agencies.

This agency information includes the following:

(i) Sufficient information to unambiguously identify the Incorporating Agency or Registration Agency (such as a name, jurisdiction, and website);
(ii) The accepted value or values for each of the subject:jurisdictionLocalityName (OID: 1.3.6.1.4.1.311.60.2.1.1), subject:jurisdictionStateOrProvinceName (OID: 1.3.6.1.4.1.311.60.2.1.2), and

subject:jurisdictionCountryName (OID: 1.3.6.1.4.1.311.60.2.1.3) fields, when a Certificate is issued using information from that Incorporating Agency or Registration Agency, indicating the jurisdiction(s) that the agency is appropriate for; and,

(iii) A revision history that includes a unique version number and date of publication for any additions, modifications, and/or removals from this list.

#### *3.2.2.2 DBA/Tradename*

If the subject identity information is to include a DBA or tradename, the Registration Authority must verify the Applicant's right to use the DBA/tradename using at least one of the following:

1. Documentation provided by, or communication with, a government agency in the jurisdiction of the Applicant's legal creation, existence, or recognition;
2. A Reliable Data Source;
3. Communication with a government agency responsible for the management of such DBAs or tradenames;
4. An Attestation Letter accompanied by documentary support; or
5. A utility bill, bank statement, credit card statement, government-issued tax document, or other form of identification that the CA determines to be reliable.

#### *3.2.2.3 Verification of Country*

Verification of country will be done in accordance with the methods of Sec. 3.2.2.1.

#### *3.2.2.4 Validation of Domain Authorization Control*

AffirmTrust shall confirm that, as of the date the Certificate was issued, either the CA or the Registration Authority validated each Fully-Qualified Domain Name (FQDN) listed in the Certificate using at least one of the methods listed below.

Completed validations of Applicant authority may be used for the issuance of multiple SSL Certificates over time. For purposes of domain validation, the term Applicant includes the Applicant's Parent Company, Subsidiary Company, or Affiliate.

AffirmTrust shall maintain a record of which domain validation method was used to validate every domain.

##### 3.2.2.4.1 Validating the Applicant as a Domain Contact

This method of domain validation is not used.

##### 3.2.2.4.2 Email, Fax, SMS, or Postal Mail to Domain Contact

Confirm the Applicant's control over the FQDN by sending a Random Value via email, fax, SMS, or postal mail and then receiving a confirming response utilizing the Random Value. The Random Value must be sent to an email address, fax/SMS number, or postal mail address identified as a Domain Contact.

Each email, fax, SMS, or postal mail may confirm control of multiple ADNs.

The CA or RA may send the email, fax, SMS, or postal mail identified under this section to more than one recipient provided that every recipient is identified by the Domain Name Registrar as representing the Domain Name Registrant for every FQDN being verified using the email, fax, SMS, or postal mail.

The Random Value shall be unique in each email, fax, SMS, or postal mail.

The CA or RA may resend the email, fax, SMS, or postal mail in its entirety, including re-use of the Random Value, provided that the communication's entire contents and recipient(s) remain unchanged.

The Random Value will remain valid for use in a confirming response for no more than 30 days from its creation.

#### 3.2.2.4.3 Phone Contact with Domain Contact

Confirm the Applicant's control over the FQDN by calling the Domain Name Registrant's phone number and obtaining a response confirming the Applicant's request for validation of the FQDN. The CA or RA shall place the call to a phone number identified by the Domain Name Registrar as the Domain Contact.

Each phone call shall be made to a single number and may confirm control of multiple FQDNs, provided that the phone number is identified by the Domain Registrar as a valid contact method for every Base Domain Name being verified using the phone call.
This method will not be re-used after May 31, 2019.

#### 3.2.2.4.4 Constructed Email to Domain Contact

Confirm the Applicant's control over the FQDN by (i) sending an email to one or more addresses created by using 'admin', 'administrator', 'webmaster', 'hostmaster', or 'postmaster' as the local part, followed by the at-sign ("@"), followed by an ADN, (ii) including a Random Value in the email, and (iii) receiving a confirming response utilizing the Random Value.

Each email may confirm control of multiple FQDNs, provided the ADN used in the email is an ADN for each FQDN being confirmed.

The Random Value shall be unique in each email.

The email may be re-sent in its entirety, including the re-use of the Random Value, provided that its entire contents and recipient shall remain unchanged.

The Random Value shall remain valid for use in a confirming response for no more than 30 days from its creation.

#### 3.2.2.4.5 Domain Authorization Document

This method of domain validation is not used.

#### 3.2.2.4.6 Agreed-Upon Change to Website

This method of domain validation is not used.

#### 3.2.2.4.7 DNS Change

Confirm the Applicant's control over the FQDN by confirming the presence of a Random Value in a DNS CNAME, TXT or CAA record for an ADN or an ADN that is prefixed with a label that begins with an underscore character.

If a Random Value is used, the CA or RA shall provide a Random Value unique to the Certificate request and shall not use the Random Value after (i) 30 days or (ii) if the Applicant submitted the Certificate request, the timeframe permitted for reuse of validated information relevant to the Certificate.

#### 3.2.2.4.8 IP Address

This method of domain validation is not used.

#### 3.2.2.4.9 Test Certificate

This method of domain validation is not used.

#### 3.2.2.4.10 TLS Using a Random Number

This method of domain validation is not used.

#### 3.2.2.4.11 Any Other Method

This method of domain validation is not used.

#### 3.2.2.4.12 Validating Applicant as a Domain Contact

This method of domain validation is not used.

#### 3.2.2.4.13 Email to DNS Contact

Confirm the Applicant's control over the FQDN by sending a Random Value via email and then receiving a confirming response utilizing the Random Value. The Random Value will be sent to a DNS CAA Email Contact. The relevant CAA Resource Record Set will be found using the search algorithm defined in RFC 8659 Section 3.

Each email may confirm control of multiple FQDNs, provided that each email address is a DNS CAA Email Contact for each ADN Name being validated. The same email may sent to multiple recipients as long as all recipients are the DNS CAA Email Contacts for each ADN being validated.

The Random Value shall be unique in each email. The email may be re-sent in its entirety, including the reuse of the Random Value, provided that its entire contents and recipient(s) remain unchanged. The Random Value shall remain valid for use in a confirming response for no more than 30 days from its creation.

#### 3.2.2.4.14 Email to DNS TXT Contact

Confirm the Applicant's control over the FQDN by sending a Random Value via email and then receiving a confirming response utilizing the Random Value. The Random Value will be sent to a DNS TXT Record Email Contact for the ADN selected to validate the FQDN.

Each email may confirm control of multiple FQDNs, provided that each email address is DNS TXT Record Email Contact for each ADN being validated. The same email may be sent to multiple recipients as long as all recipients are the DNS TXT Record Email Contacts for each ADN being validated.

The Random Value shall be unique in each email. The email may be re-sent in its entirety, including the reuse of the Random Value, provided that its entire contents and recipient(s) remain unchanged. The Random Value shall remain valid for use in a confirming response for no more than 30 days from its creation.

#### 3.2.2.4.15 Phone with Domain Contact

Confirm the Applicant’s control over the FQDN by calling the Domain Contact’s phone number and obtain a confirming response to validate the ADN. Each phone call may confirm control of

multiple ADNs provided that the same Domain Contact phone number is listed for each ADN being verified and they provide a confirming response for each ADN.

In the event that someone other than a Domain Contact is reached, the CA may request to be transferred to the Domain Contact.

In the event of reaching voicemail, the CA may leave the Random Value and the ADN(s) being validated. The Random Value must be returned to the CA to approve the request.

The Random Value shall remain valid for use in a confirming response for no more than 30 days from its creation.

#### 3.2.2.4.16 Phone Contact with DNS TXT Record Phone Contact

Confirm the Applicant's control over the FQDN by calling the DNS TXT Record Phone Contact's phone number and obtain a confirming response to validate the ADN. Each phone call may confirm control of multiple ADNs provided that the same DNS TXT Record Phone Contact phone number is listed for each ADN being verified and they provide a confirming response for each ADN.

The CA may not knowingly be transferred or request to be transferred as this phone number has been specifically listed for the purposes of domain validation.

In the event of reaching voicemail, the CA may leave the Random Value and the ADN(s) being validated. The Random Value must be returned to the CA to approve the request.

The Random Value shall remain valid for use in a confirming response for no more than 30 days from its creation.

#### 3.2.2.4.17 Phone Contact with DNS CAA Phone Contact

Confirm the Applicant's control over the FQDN by calling the DNS CAA Phone Contact's phone number and obtain a confirming response to validate the ADN. Each phone call may confirm control of multiple ADNs provided that the same DNS CAA Phone Contact phone number is listed for each ADN being verified and they provide a confirming response for each ADN. The relevant CAA Resource Record Set must be found using the search algorithm defined in RFC 8659 Section 3.

The CA may not knowingly be transferred or request to be transferred as this phone number has been specifically listed for the purposes of domain validation.

In the event of reaching voicemail, the CA may leave the Random Value and the ADN(s) being validated. The Random Value must be returned to the CA to approve the request.

The Random Value shall remain valid for use in a confirming response for no more than 30 days from its creation.

#### 3.2.2.4.18 Phone Contact with DNS CAA Phone Contact

Confirm the Applicant's control over the FQDN by verifying that the Request Token or Random Value is contained in the contents of a file.

(i) The entire Request Token or Random Value must not appear in the request used to retrieve the file, and

(ii) the CA MUST receive a successful HTTP response from the request (meaning a 2xx HTTP status code must be received).

The file containing the Request Token or Random Number:

(iii) Must be located on the Authorization Domain Name, and
(iv) Must be located under the "/.well-known/pki-validation" directory, and
(v) Must be retrieved via either the "http" or "https" scheme, and
(vi) Must be accessed over an Authorized Port.

If the CA follows redirects the following apply:
(vii) Redirects must be initiated at the HTTP protocol layer (e.g. using a 3xx status code).
(viii) Redirects must be the result of an HTTP status code result within the 3xx Redirection class of status codes, as defined in RFC 7231, Section 6.4.
(ix) Redirects must be to resource URLs with either via the "http" or "https" scheme.
(x) Redirects must be to resource URLs accessed via Authorized Ports.

If a Random Value is used, then:
(xi) The CA must provide a Random Value unique to the certificate request.
(xii) The Random Value must remain valid for use in a confirming response for no more than 30 days from its creation. The CPS MAY specify a shorter validity period for Random Values, in which case the CA must follow its CPS.

Note: Once the FQDN has been validated using this method, the CA may also issue Certificates for other FQDNs that end with all the labels of the validated FQDN. This method is suitable for validating Wildcard Domain Names.

#### 3.2.2.4.19 Agreed-Upon Change to Website - ACME

This method of domain validation is not used.

#### 3.2.2.4.20 LS Using ALPN

This method of domain validation is not used.

### *3.2.2.5 Authentication of an IP Address*

AffirmTrust CAs do not issue Certificates with IP addresses.

### *3.2.2.6 Wildcard Validation*

AffirmTrust follows a documented procedure that determines if a wildcard character in a domain name occurs in the first label position to the left of a “registry-controlled” label or “public suffix” (e.g. “.com“,”.co.uk”, see RFC 6454 Section 8.2 for further explanation). If a wildcard falls within the label immediately to the left of a registry-controlled or public suffix, AffirmTrust refuses issuance unless the Applicant proves its rightful control of the entire domain namespace.

### *3.2.2.7 Data Source Accuracy*

Prior to using any data source as a Reliable Data Source, the Registration Authority shall evaluate the source for its reliability, accuracy, and resistance to alteration or falsification.

### *3.2.2.8 CAA Records*

Entrust Datacard policy on CAA records is stated in §4.2.4.

### 3.2.3 Authentication of Individual Identity

AffirmTrust does not issue SSL Certificates to individuals.

### 3.2.4 Non-Verified Subscriber Information

No stipulation.

### 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 §3.2.2.1 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 §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

AffirmTrust CAs shall disclose all cross-certificates that identify AffirmTrust as the subject per §4.4.3, provided that AffirmTrust arranged for or accepted the establishment of the trust relationship (i.e. the cross-certificate at issue).

## 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

As stipulated in §3.3.1.

## 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 entities on a government denied list maintained by Canada or that is located in a country with which the laws of Canada prohibit doing business.

### 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.

By executing the Subscriber Agreement, Subscribers warrant that all of the information contained in the Certificate request is correct.

## 4.2 Certificate Application Processing

### 4.2.1 Performing Identification and Authentication Functions

For non-EV Certificates, AffirmTrust may use the documents and data provided to verify Certificate information, or may reuse previous validations themselves provided the data or documentation was obtained from a source specified in this CPS or completed the validation itself no more than 825 days prior to issuing the Certificate.

For EV Certificates, AffirmTrust may use the documents and data provided to verify Certificate information, or may reuse previous validations themselves provided the data or documentation was obtained from a source specified in this CPS or completed the validation itself no more than 13 months prior to issuing the Certificate.

Information from domain validations completed using methods specified in §3.2.2.4.1 will not be re-used on or after August 1, 2018.

AffirmTrust maintains procedures to identify high risk Certificate requests that require additional verification activity prior to Certificate issuance. High risk procedures include processes to verify high risk domain names and/or evaluate deceptive domain names.

### 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.

AffirmTrust CA will not issue Certificates containing Internal Names.

### 4.2.3 Time to Process Certificate Applications

No stipulation.

### 4.2.4 Certification Authority Authorization (CAA) Records

Prior to issuing Certificates, AffirmTrust checks for Certification Authority Authorization (CAA) records for each dNSName in the subjectAltName extension of the Certificate to be issued, according to the procedure in RFC 8659, following the processing instructions set down in RFC 8659 for any records found. If the Certificate is issued, it will be issued within the TTL of the CAA record, or 8 hours, whichever is greater.

When processing CAA records, AffirmTrust processes the issue, issuewild, and iodef property tags as specified in RFC 6844. AffirmTrust may not act on the contents of the iodef property tag.

AffirmTrust respects the critical flag and will not issue a Certificate if it encounters an unrecognized property with this flag set.

AffirmTrust may not check CAA records for the following exceptions:

(i) For Certificates for which a Certificate Transparency pre-certificate was created and logged in at least two public logs, and for which CAA was checked.

(ii) For Certificates issued by a technically constrained Subordinate CA Certificate as set out in Baseline Requirements section 7.1.5, where the lack of CAA checking is an explicit contractual provision in the contract with the Applicant.

(iii) If the CA or an Affiliate of the CA is the DNS Operator (as defined in RFC 7719) of the domain's DNS.

AffirmTrust treats a record lookup failure as permission to issue if:

(iv) the failure is outside the CA's infrastructure;

(v) the lookup has been retried at least once; and

(vi) the domain's zone does not have a DNSSEC validation chain to the ICANN root.

AffirmTrust documents potential issuances that were prevented by a CAA record in sufficient detail to provide feedback to the CAB Forum on the circumstances, and will dispatch reports of such issuance requests to the contact(s) stipulated in the CAA iodef record(s), if present. AffirmTrust support mailto: and https: URL schemes in the iodef record.

AffirmTrust's CAA identifying domain is "**affirmtrust.com**".

## 4.3 Certificate Issuance

### 4.3.1 CA Actions during Certificate Issuance

Certificate issuance by the Root CA 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 CA to perform a Certificate signing operation. 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 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 Certificates 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

Subordinate CA Certificates shall be disclosed in the CA Common Database (i.e., https://ccadb.force.com) within one week of Certificate issuance.

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 §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

AffirmTrust will process Certificate renewal requests with validated verification data. Previous verification data may be used as specified in §4.2.1.

Certificates may be renewed using the previously accepted Public Key, if the Public Key meets the key size requirements of §6.1.5.

### 4.6.4 Notification of New Certificate Issuance to Subscriber

AffirmTrust delivers renewed Certificates to Subscribers 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

As stipulated in §4.4.1.

### 4.6.6 Publication of the Renewal Certificate by the CA

As stipulated in sections 4.4.2.

### 4.6.7 Notification of Certificate Issuance by the CA to Other Entities

As stipulated in §4.4.3.

## 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.

### 4.7.2 Who May Request Certification of a New Public Key

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

### 4.7.3 Processing Certificate Re-Keying Requests

AffirmTrust re-uses existing verification information unless re-verification is required under §3.3.1 or AffirmTrust believes that the information has become inaccurate.

### 4.7.4 Notification of New Certificate Issuance to Subscriber

As stipulated in §4.6.4.

### 4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate

As stipulated in §4.4.1.

### 4.7.6 Publication of the Re-Keyed Certificate by the CA

As stipulated in §4.4.2.

### 4.7.7 Notification of Certificate Issuance by the CA to Other Entities

As stipulated in §4.4.3.

## 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 §3.3.1 or 6.3.2.

### 4.8.4 Notification of New Certificate Issuance to Subscriber

As stipulated in §4.6.4.

### 4.8.5 Conduct Constituting Acceptance of Modified Certificate

As stipulated in §4.4.1.

### 4.8.6 Publication of the Modified Certificate by the CA

As stipulated in §4.4.2.

### 4.8.7 Notification of Certificate Issuance by the CA to Other Entities

As stipulated in §4.4.3.

## 4.9 Certificate Revocation and Suspension

### 4.9.1 Circumstances for Revocation

#### *4.9.1.1 Reasons for Revoking a Subscriber Certificate*

AffirmTrust shall be entitled to revoke and may revoke, and an RA operating under an AffirmTrust CA shall be entitled to request revocation of and shall request revocation of, a Subscriber's Certificate if AffirmTrust or the RA has knowledge of or a reasonable basis for believing that of any of the events listed in this section have occurred:

AffirmTrust will revoke a Certificate within 24 hours if one or more of the following occurs:

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. AffirmTrust obtains evidence that the Subscriber's Private Key corresponding to the Public Key of the Certificate suffered a Key Compromise;
4. The CA is made aware of a demonstrated or proven method that can easily compute the Subscriber's Private Key based on the Public Key in the Certificate (such as a Debian weak key, see https://wiki.debian.org/SSLkeys); or
5. AffirmTrust obtains evidence that the validation of the domain authorization or control for any FQDN in the Certificate should not be relied upon.

AffirmTrust should revoke a Certificate within 24 hours and must revoke a Certificate within 5 days if one or more of the following occurs:

6. The Certificate no longer complies with the requirements of Sections 6.1.5 and 6.1.6;
7. AffirmTrust obtains evidence that the Certificate was misused;
8. AffirmTrust is made aware that the Subscriber has violated one or more of its material obligations under the Subscriber Agreement;
9. AffirmTrust is made aware of any circumstance indicating that use of a FQDN in the Certificate is no longer legally permitted (e.g. a court or arbitrator has revoked a Domain Name Registrant's right to use the Domain Name, a relevant licensing or services agreement between the Domain Name Registrant and the Applicant has terminated, or the Domain Name Registrant has failed to renew the Domain Name;
10. AffirmTrust is made aware that a Certificate with a Wildcard Domain Name has been used to authenticate a fraudulently misleading subordinate FQDN;
11. AffirmTrust is made aware of a material change in the information contained in the Certificate;
12. AffirmTrust is made aware that the Certificate was not issued in accordance with this CPS;
13. AffirmTrust determines that any of the information appearing in the Certificate is inaccurate;
14. AffirmTrust's right to issue Certificates under this CPS expires or is revoked or terminated, unless the AffirmTrust has made arrangements to continue maintaining the CRL/OCSP Repository;
15. Revocation is required by this CPS;
16. AffirmTrust is made aware of a demonstrated or proven method that exposes the

Subscriber's Private Key to compromise or if there is a clear evidence that the specific method used to generate the Private Key was flawed;
17. The technical content or format of the Certificate presents an unacceptable risk to Application Software Suppliers or Relying Parties; or
18. Any other reason that may be reasonably expected to affect the integrity, security, or trustworthiness of a Certificate or AffirmTrust.

#### *4.9.1.2 Reasons for Revoking a Subordinate CA Certificate*

AffirmTrust shall revoke a Subordinate CA Certificate within seven (7) days if one or more of the following occurs:

1. The Subordinate CA requests revocation in writing;
2. The Subordinate CA notifies the Issuing CA that the original Certificate request was not authorized and does not retroactively grant authorization;
3. The Issuing CA obtains evidence that the Subordinate CA's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise or no longer complies with the requirements of Sections 6.1.5 and 6.1.6,
4. The Issuing CA obtains evidence that the Certificate was misused;
5. The Issuing CA is made aware that the Certificate was not issued in accordance with or that Subordinate CA has not complied with the Baseline Requirements or this CPS;
6. The Issuing CA determines that any of the information appearing in the Certificate is inaccurate or misleading;
7. The Issuing CA or Subordinate CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Certificate;
8. The Issuing CA's or Subordinate CA's right to issue Certificates under the Baseline Requirements expires or is revoked or terminated, unless the Issuing CA has made arrangements to continue maintaining the CRL/OCSP Repository; or
9. Revocation is required by the Issuing CA's CPS.

### 4.9.2 Who Can Request Revocation

AffirmTrust, RAs and Subscribers may initiate revocation. Additionally Relying Parties, Application Software Suppliers, and other third parties may submit Certificate problem reports informing AffirmTrust CA of reasonable cause to revoke the Certificate.

The Subscriber or another appropriately authorized party (such as an administrative contact, a Contract Signer, Certificate Approver, or Certificate Requester) may request revocation of their Certificate at any time for any reason. If a Subscriber requests revocation of their Certificate, the Subscriber must be able to validate themselves as set forth in §3.4 to the RA that processed the Subscriber's Certificate Application. AffirmTrust shall not be required to revoke and the RAs operating under AffirmTrust CA shall not be required to request revocation of a Certificate until a Subscriber can properly validate themselves as set forth in §4.9.3. AffirmTrust shall be entitled to revoke and shall revoke, and an RA operating under an AffirmTrust shall be entitled to request revocation of and shall request revocation of, a Subscriber's Certificate at any time for any of the reasons set forth in §4.9.1.

Subscribers, Relying Parties, Application Software Suppliers, Anti-Malware Organizations and other third parties may submit Certificate problem reports informing AffirmTrust of a reasonable cause to revoke the Certificate.

### 4.9.3 Procedure for Revocation Request

A Subscriber shall request revocation of their Certificate if the Subscriber has a suspicion or knowledge of or a reasonable basis for believing that of any of the following events have

occurred:

1. Compromise of the Subscriber's Private Key;
2. Knowledge that the original Certificate request was not authorized and such authorization will not be retroactively granted;
3. Change in the information contained in the Subscriber's Certificate;
4. Change in circumstances that cause the information contained in Subscriber's Certificate to become inaccurate, incomplete, or misleading.

A Subscriber request for revocation of their Certificate may be verified by (i) Subscriber authentication credentials, or (ii) authorization of the Subscriber through a reliable method of communication. .

If a Subscriber's Certificate is revoked for any reason, the Subscriber shall be notified by sending an email to the technical and security contacts listed in the Certificate Application. Revocation of a Certificate shall not affect any of the Subscriber's contractual obligations under this CPS, the Subscriber's Subscription Agreement, or any Relying Party Agreements.

Subscribers, Relying Parties, ASVs, Anti-Malware Organizations and other third parties may submit a Certificate Problem Report by notification through the contact information specified in §1.5.2. If a CPR is received, the CA shall:

5. Log the CPR as high severity into a ticketing system for tracking purposes;
6. Review the CPR and engage the necessary parties to verify the CPR, draft a CPR investigation report and provide the CPR investigation report to the Subscriber and the party that provided the CPR within 24 hours from receipt of the CPR;
7. Determine if there was Certificate mis-issuance. In the case of Certificate miss-issuance, the incident must be 1) escalated to the PKI Policy Authority team and to service management and 2) a Certificate mis-issuance report must be publicly posted within one business day;
8. If Certificate revocation is required, perform revocation in accordance with the requirements of §4.9.1.1;
9. Update the Certificate mis-issuance report within 5 days from receipt of CPR; and
10. Complete the CPR investigation report when the incident is closed and provide a copy to the Subscriber and the party that provided the CPR.

### 4.9.4 Revocation Request Grace Period

In the case of Private Key Compromise, or suspected Private Key Compromise, a Subscriber shall request revocation of the corresponding Certificate immediately upon detection of the Compromise or suspected Compromise. Revocation requests for other required reasons shall be made as soon as reasonably practicable.

### 4.9.5 Time within Which CA Must Process the Revocation Request

Within 24 hours after receiving a Certificate problem report AffirmTrust will investigate the facts and circumstances related to the Certificate problem report and provide a preliminary report to both the Subscriber and the entity who filed the Certificate problem report.

After reviewing the facts and circumstances, AffirmTrust will work with the Subscriber and any entity reporting the Certificate problem report or other revocation-related notice to establish whether or not the Certificate will be revoked, and if so, a date which AffirmTrust will revoke the Certificate. The period from receipt of the Certificate problem report or revocation-related notice

to published revocation will not exceed the timeframe set forth in §4.9.1.1. The date selected by the CA will consider the following criteria:

(i) The nature of the alleged problem (scope, context, severity, magnitude, risk of harm);
(ii) The consequences of revocation (direct and collateral impacts to Subscribers and Relying Parties);
(iii) The number of Certificate problem reports received about a particular AffirmTrust Certificate or Subscriber;
(iv) The entity making the complaint (for example, a complaint from a law enforcement official that a Web site is engaged in illegal activities should carry more weight than a complaint from a consumer alleging that she didn't receive the goods she ordered); and
(v) Relevant legislation.

### 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

AffirmTrust CAs shall issue CRLs as follows:

1. CRLs for AffirmTrust Certificates issued to Subordinate CAs shall be issued at least once every twelve months or with 24 hours after revoking a Subordinate CA Certificate. The next CRL update shall not be more than twelve months from the last update.
2. CRLs for AffirmTrust SSL Certificates shall be issued at least once every 24 hours. The next CRL update is 7 days from the last update.

### 4.9.8 Maximum Latency for CRLs

No stipulation.

### 4.9.9 On-Line Revocation/Status Checking Availability

On-line revocation/status checking of Certificates is available on a continuous basis by CRL or On-line Certificate Status Protocol (OCSP).

OCSP responses are signed by an OCSP responder whose Certificate is signed by the CA that issued the Certificate whose revocation status is being checked. The OCSP signing Certificate contains an extension of type id-pkix-ocsp-nocheck, as defined by RFC6960.

### 4.9.10 On-Line Revocation Checking Requirements

AffirmTrust CAs support an OCSP capability using the GET and POST methods for Certificates issued in accordance with this CPS.

AffirmTrust shall sign and make available OCSP as follows:

(i) OCSP responses for Certificates issued to Subordinate CAs shall be issued at least once every twelve months or within 24 hours after revoking a Subordinate CA.

(ii) OCSP responses for Certificates issued to end entities shall be issued at least once every 24 hours. OCSP responses will have a maximum expiration time of seven days.

If the OCSP responder receives a request for status of an AffirmTrust Certificate serial number that is “unsused”, then the responder will not respond with a "good" status.

The on-line locations of the CRL and the OCSP response are included in the Certificate to support software applications that perform automatic Certificate status checking.

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

### 4.9.11 Other Forms of Revocation Advertisements Available

No stipulation.

### 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 §3.4, 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

The Repository will not include entries that indicate that a Certificate has been suspended.

### 4.9.14 Who Can Request Suspension

Not applicable.

### 4.9.15 Procedure for Suspension Request

Not applicable.

### 4.9.16 Limits on Suspension Period

Not applicable.

## 4.10 Certificate Status Services

### 4.10.1 Operational Characteristics

Revocation entries on a CRL or OCSP response are not removed until after the expiry date of the revoked AffirmTrust Certificate.

### 4.10.2 Service Availability

AffirmTrust CAs shall operate and maintain its CRL and OCSP capability with resources sufficient to provide a response time of ten seconds or less under normal operating conditions.

AffirmTrust CAs shall maintain an online 24x7 Repository that application software can use to automatically check the current status of all unexpired Certificates issued by the CA.

AffirmTrust CAs shall maintain a continuous 24x7 ability to respond internally to a high-priority Certificate problem report, and where appropriate, forward such a complaint to law enforcement authorities, and/or revoke a Certificate that is the subject of such a complaint.

### 4.10.3 Optional Features

No stipulation.

## 4.11 End of Subscription

No stipulation.

## 4.12 Key Escrow and Recovery

### 4.12.1 Key Escrow and Recovery Policy and Practices

No stipulation.

### 4.12.2 Session Key Encapsulation and Recovery Policy and Practices

No stipulation.

# 5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

The CA/Browser Forum's Network and Certificate System Security Requirements are incorporated by reference as if fully set forth herein.

## 5.1 Physical Controls

### 5.1.1 Site Location and Construction

The computing facilities that host the AffirmTrust CA services are located in Ottawa, Canada. The CA equipment is located in a security zone that is physically separated from AffirmTrust's other systems to restrict access to personnel in Trusted Roles. The security zone is constructed with privacy and secured with slab-to-slab wire mesh. The security zone is protected by electronic control access systems, alarmed doors and is monitored via a 24x7 recorded security camera and motion detector system.

### 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 §5.5.

## 5.2 Procedural Controls

### 5.2.1 Trust Roles

AffirmTrust has a number of trusted roles for sensitive operations of the CA software.

### 5.2.2 Number of Persons Required per Task

AffirmTrust CA operations related to changing CA policy settings require more than one person with a trusted role to perform the operation.

AffirmTrust CA Private Keys are backed up, stored, and recovered only by personnel in trusted roles using dual control in a physically secured environment.

### 5.2.3 Identification and Authentication for Each Role

Personnel in trusted roles must undergo background investigations and must be trained for their specific role.

### 5.2.4 Roles Requiring Separation of Duties

No stipulation.

## 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 Qualifications, Experience and Clearance Requirements

Prior to the engagement of any person in the certificate management process, the AffirmTrust CA shall verify the identity and trustworthiness of such person.

### 5.3.2 Background Check Procedures

No stipulation.

### 5.3.3 Training Requirements

AffirmTrust CAs must provide a trusted role of Validation Specialist to perform information verification duties with skills-training that covers basic PKI knowledge, authentication and vetting policies and procedures (including this CPS), common threats to the information verification process (including phishing and other social engineering tactics), and the Baseline Requirements.

Validation Specialists receive skills-training prior to commencing their job role and are required them to pass an examination on the applicable information verification requirements.

AffirmTrust CAs maintain records of such training and ensures that personnel entrusted with Validation Specialist duties maintain an appropriate skill level.

### 5.3.4 Retraining Frequency and Requirements

AffirmTrust CAs provide refresher training and informational updates sufficient to ensure that all personnel in trusted roles retain the requisite degree of expertise.

### 5.3.5 Job Rotation Frequency and Sequence

No stipulation.

### 5.3.6 Sanctions for Unauthorized Actions

No stipulation.

### 5.3.7 Independent Contractor Requirements

Third Party Registration Authority's personnel involved in the issuance of an AffirmTrust Certificate shall meet the training and skills requirements of §5.3.3 and the document retention and event logging requirements of §5.4.1.

### 5.3.8 Documentation Supplied to Personnel

No stipulation.

## 5.4 Audit Logging Procedures

Significant security events in the AffirmTrust CAs 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. 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 time for the AffirmTrust CAs computer systems is synchronized with the service provided by the National Research Council Canada.

### 5.4.1 Types of Events Recorded

The AffirmTrust CAs 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) CA Certificate and key lifecycle events, including:
   a. Key generation, backup, storage, recovery, archival, and destruction;
   b. Certificate requests, renewal, and re-key requests, and revocation;
   c. Approval and rejection of Certificate requests;
   d. Cryptographic device lifecycle management events.
   e. Generation of CRLs and OCSP entries; and

f. Introduction of new Certificate Profiles and retirement of existing Certificate Profiles.

(ii) Subscriber Certificate lifecycle management events, including:
a. Certificate requests, renewal and re-key requests, and revocation;
b. All verification activities required by this CPS;
c. Approval and rejection of Certificate Requests;
d. Issuance of Certificates; and
e. Generation of CRLs and OCSP entries.

(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.

Log entries include the following elements:
1. Date and time of record;
2. Identity of the person making the journal record; and
3. Description of record.

### 5.4.2 Frequency of Processing Log

No stipulation.

### 5.4.3 Retention Period for Audit Log

AffirmTrust CA will retain, for at least two years:

(i) CA Certificate and key lifecycle management event records, as set forth in §5.4.1(i), after either: the destruction of the CA key, or the revocation or expiration of the CA Certificate, whichever occurs later;

(ii) Subscriber Certificate lifecycle management event records, as set forth in Section 5.4.1(ii), after the revocation or expiration of the Subscriber Certificate; and

(iii) Any security event records, as set forth in 5.4.1(iii), after the event occurred.

### 5.4.4 Protection of Audit Log

No stipulation.

### 5.4.5 Audit Log Backup Procedures

No stipulation.

### 5.4.6 Audit Collection System

No stipulation.

### 5.4.7 Notification to Event Causing Subject

No stipulation.

### 5.4.8 Vulnerability Assessments

AffirmTrust CAs annually perform a risk assessment that:

(i) Identifies foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of any certificate data or

certificate management processes;

(ii) Assesses the likelihood and potential damage of these threats, taking into consideration the sensitivity of the certificate data and certificate management processes; and

(iii) Assesses the sufficiency of the policies, procedures, information systems, technology, and other arrangements that the AffirmTrust CA has in place to counter such threats.

Based on the risk assessment, a security plan is developed, implemented, and maintained consisting of security procedures, measures, and products designed to achieve the objectives set forth above and to manage and control the risks identified during the risk assessment. The security plan includes administrative, organizational, technical, and physical safeguards appropriate to the sensitivity of the certificate data and certificate management processes. The security plan also takes into account then-available technology and the cost of implementing the specific measures, and implements a reasonable level of security appropriate to the harm that might result from a breach of security and the nature of the data to be protected.

## 5.5 Records Archival

### 5.5.1 Types of Records Archived

The audit trail files, databases and revocation information for AffirmTrust CAs are archived.

### 5.5.2 Retention Period for Archive

AffirmTrust CA will retain all documentation relating to certificate requests and the verification thereof, and all Certificates and revocation thereof, for at least seven years after any Certificate based on that documentation ceases to be valid.

### 5.5.3 Protection of Archive

The databases for AffirmTrust CAs are protected by encryption. 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.

### 5.5.4 Archive Backup Procedures

No stipulation.

### 5.5.5 Requirements for Time stamping of Records

No stipulation.

### 5.5.6 Archive Collection System

No stipulation.

### 5.5.7 Procedures to Obtain and Archive Information

No stipulation.

### 5.5.8 Vulnerability Assessments

No stipulation.

## 5.6 Key Changeover

AffirmTrust CAs' key pairs will be retired from service at the end of their respective lifetimes as defined in this CPS. New CA 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 CA key changeover process will be performed such that it causes minimal disruption to Subscribers and Relying Parties.

## 5.7 Compromise and Disaster Recovery

### 5.7.1 Incident and Compromise Handling procedures

AffirmTrust CAs 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 section5.1
(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 CAs. 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 and Application Software Suppliers shall be informed as soon as practicable of such a Compromise and information shall be posted in the AffirmTrust Repository.

### 5.7.2 Computing Resources, Software and/or Data are Corrupted

No stipulation.

### 5.7.3 Entity Private Key Compromise Procedures

No stipulation.

### 5.7.4 Business Continuity Capabilities after a Disaster

No stipulation.

## 5.8 CA Termination

In the event of CA termination, AffirmTrust will:

(i) Provide notice and information about the CA termination by sending notice to Subscribers with unrevoked unexpired certificates and Application Software Suppliers and by posting such information in the Repository; and
(ii) Transfer all responsibilities to a qualified successor entity.

If a qualified successor entity does not exist, AffirmTrust will:

(iii) Transfer those functions capable of being transferred to a reliable third party and arrange to preserve all relevant records with a reliable third party or a government, regulatory, or legal body with appropriate authority;
(iv) Revoke all Certificates that are still unrevoked or unexpired on a date as specified in the notice and publish final CRLs;
(v) Destroy all CA Private Keys; and
(vi) Make other necessary arrangements that are in accordance with this CPS.

# 6. TECHNICAL SECURITY CONTROLS

## 6.1 Key Pair Generation and Installation

### 6.1.1 Key Pair Generation

#### *6.1.1.1 CA Key Generation*

AffirmTrust will perform the following when generating a CA Key Pair:

(i) Prepare and follow a Key Pair generation script;
(ii) Have a qualified auditor witness the CA Key Pair generation process;
(iii) Have a qualified auditor issue a report opining that the AffirmTrust CA followed its CA Key Pair generation ceremony during its key generation process and the controls to ensure the integrity and confidentiality of the CA Key Pair;
(iv) Generate the CA Key Pair in a physically secured environment;
(v) Generate the CA Key Pair using personnel in trusted roles under the principles of multiple person control and split knowledge;
(vi) Generate the CA Key Pair within cryptographic modules meeting the applicable requirements of §6.2.11;
(vii) Log its CA Key Pair generation activities; and
(viii) Maintain effective controls to provide reasonable assurance that the Private Key was generated and protected in conformance with the procedures described in this CPS and (if applicable) its CA Key Pair generation script.

Keys Pairs for AffirmTrust CA administrators must be generated and protected on a cryptographic module that meets or exceeds the requirements defined in §6.2.11. 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 CA and performing an enrollment process which is authenticated with the administrator's module password.

#### *6.1.1.2 RA Key Pair Generation*

No stipulation.

#### *6.1.1.3 Subscriber Key Pair Generation*

The Applicant or Subscriber is required to generate or initiate 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 will reject a Certificate request if one or more of the following conditions are met:

(i) The Key Pair does not meet the requirements set forth in §6.1.5 and/or §6.1.6;
(ii) There is clear evidence that the specific method used to generate the Private Key was flawed;
(iii) The CA is aware of a demonstrated or proven method that exposes the Private Key to compromise;
(iv) The CA has previously been made aware that the Private Key has suffered a Key Compromise, such as through the provisions of Section 4.9.1.1;
(v) The CA is aware of a demonstrated or proven method to easily compute the Private Key based on the Public Key (such as a Debian weak key, see https://wiki.debian.org/SSLkeys).

AffirmTrust CA will not generate a Key Pair on behalf of a Subscriber, and will not accept a Certificate request using a Key Pair previously generated by the CA.

### 6.1.2 Private Key Delivery to Subscriber

AffirmTrust Certificate Authorities do not generate, archive or deliver 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 CAs 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 CA prior to issuing the AffirmTrust Certificate.

### 6.1.4 CA Public Key Delivery to Relying Parties

The Public-Key Certificate for AffirmTrust CAs 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 CAs is provided to the Subscriber with the Subscriber Certificate.

Public Key Certificates for AffirmTrust CAs are also available for download from the Repository.

### 6.1.5 Key Sizes

For RSA Key Pairs the CA shall ensure that the modulus size, when encoded, is at least 2048 bits, and that the modulus size, in bits, is evenly divisible by 8.

CA Key Size
For CAs using RSA keys, the size shall be 2048, 3072 or 4096-bits. For CAs using ECC keys, the size shall be NIST P-384.

Subscriber Certificate Key Size
The RSA key size shall be 2048, 3072 or 4096-bits. The ECC key size shall be NIST P-256 or P-384.

### 6.1.6 Public Key Parameters Generation and Quality Checking

For RSA public keys, AffirmTrust shall confirm that the value of the public exponent is an odd number equal to 3 or more. Additionally, the public exponent will be in the range between $2^{16}+1$ and $2^{256}-1$. The modulus will also have the following characteristics: an odd number, not the power of a prime, and have no factors smaller than 752.

For ECC public keys, AffirmTrust shall confirm the validity of all keys using either the ECC Full Public Key Validation Routine or the ECC Partial Public Key Validation Routine.

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

Root CA 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.

## 6.2 Private Key Protection and Cryptographic Module Engineering Controls

AffirmTrust CA has implemented physical and logical safeguards to prevent unauthorized Certificate issuance. Protection of the CA Private Key outside the validated system consist of physical security, encryption, or a combination of both, implemented in a manner that prevents disclosure of the CA Private Key. AffirmTrust CA encrypts its Private Key with an algorithm and key-length that are capable of withstanding cryptanalytic attacks for the residual life of the encrypted key.

### 6.2.1 Cryptographic Module Standards and Controls

AffirmTrust CAs Private Keys must be stored and protected on cryptographic modules that meet or exceed the requirements as defined in §6.1.11. 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 §6.1.11.

### 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 CAs' 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 §6.1.11. 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 §6.2.10. The AffirmTrust CA Private Keys must not be destroyed if they are still required for business or legal purposes.

Third parties will not archive AffirmTrust CA Private Keys.

### 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.

If the Private Key of an AffirmTrust Subordinate CA is communicated to an unauthorized third party, then the Subordinate CA shall revoke all Certificates corresponding to Private Key.

### 6.2.7 Private Key Storage on Cryptographic Module

AffirmTrust CA Private Keys are stored on a cryptographic module as defined in §6.2.11.

### 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 §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.

For AffirmTrust CA 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.

For AffirmTrust CA Administrators, the administrator's private key is destroyed by reinitializing the cryptographic module.

### 6.2.11 Cryptographic Module Rating

AffirmTrust CA Key Pairs must be generated and protected on a cryptographic module that is compliant to at least FIPS 140-2 Level 3 certification standards.

For AffirmTrust CA Administrators, Key Pairs for CA administrators must be generated and

protected on a cryptographic module that is compliant to at least FIPS 140-2 Level 2 certification standards.

## 6.3 Other Aspects of Key Pair Management

### 6.3.1 Public Key Archival

No stipulation.

### 6.3.2 Certificate Operational Periods and Key Pair Usage Periods

AffirmTrust CA 2048-bit RSA Key Pairs may have a validity period expiring no later than 31 December 2030.

DV and OV Certificates issued before 1 March 2018 may have a validity period of up to, but no more than, 39 months. DV and OV Certificates issued on or after 1 March 2018 may have a validity period of up to, but no more than, 825-days. DV and OV Certificates issued on or after 1 September 2020 may have a validity period of up to, but no more than, 398-days.

EV Certificates may have a validity period of up to, but no more than, 825-days. EV Certificates issued on or after 1 September 2020 may have a validity period of up to, but no more than, 398-days.

## 6.4 Activation Data

### 6.4.1 Activation Data Generation and Installation

No stipulation.

### 6.4.2 Activation Data Protection

No stipulation.

### 6.4.3 Other Aspects of Activation Data

No stipulation.

## 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 §5.1. The operating systems on the workstations on which the AffirmTrust CAs 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 CAs are required to use hardware tokens in conjunction with a PIN to gain access to the physical room that contains the CA software being used for such AffirmTrust CAs.

AffirmTrust enforces multi-factor authentication for all Registration Authority accounts capable of causing Certificate issuance.

For Subscriber accounts, AffirmTrust has implemented technical controls operated to restrict Certificate issuance to a limited set of pre-approved domains.

### 6.5.2 Computer Security Rating

No stipulation.

## 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 CA 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 stipulation.

## 6.7 Network Security Controls

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

## 6.8 Time-Stamping

No stipulation.

# 7. CERTIFICATE, CRL, AND OCSP PROFILES

The profile for the Certificates and Certificate Revocation List (CRL) issued by a CA conform to the specifications contained in the IETF RFC 5280 Internet X.509 PKI Certificate and Certificate Revocation List (CRL) Profile.

## 7.1 Certificate Profile

AffirmTrust issues Certificates in accordance with the X.509 version 3. Certificate profiles for Root CA Certificate, Subordinate CA Certificates, and Subscriber Certificates are described in Appendix B and the sections below.

AffirmTrust Certificates have a serial number greater than zero (0) that contains at least 64 unpredictable bits.

### 7.1.1 Version Number(s)

All Certificates are X.509 version 3 certificates.

### 7.1.2 Certificate Extensions

#### *7.1.2.1 Root CA Certificate*

Certificate extensions are as set as stipulated in IETF RFC 5280 and in accordance with Appendix B.

#### *7.1.2.2 Subordinate CA Certificate*

Certificate extensions are as set as stipulated in IETF RFC 5280 and in accordance with Appendix B.

Effective January 1, 2019, the extension requirements for extended key usage are:

(i) Must contain an EKU extension,
(ii) Must not include the anyExtendedKeyUsage EKU, and
(iii) Must not include both id-kep-serverAuth and id-kp-emailProtection EKUs in the same certificate.

#### *7.1.2.3 Subscriber Certificate*

Certificate extensions are as set as stipulated in IETF RFC 5280 and in accordance with Appendix B.

### 7.1.3 Algorithm Object Identifiers

#### *7.1.3.1 SubjectPublicKeyInfo*

For RSA, the CA will indicate an RSA key using the rsaEncryption (OID: 1.2.840.113549.1.1.1) algorithm identifier. The parameters must be present and must be explicit NULL.
For ECDSA, the CA must indicate an ECDSA key using the id-ecPublicKey (OID: 1.2.840.10045.2.1) algorithm identifier. The parameters must use the namedCurve encoding:

(i) For P-256 keys, the namedCurve must be secp256r1 (OID: 1.2.840.10045.3.1.7), or
(ii) For P-384 keys, the namedCurve must be secp384r1 (OID: 1.3.132.0.34).

#### *7.1.3.2 SubjectPublicKeyInfo*

All objects signed by a CA Private Key must conform to these requirements on the use of the AlgorithmIdentifier or AlgorithmIdentifier-derived type in the context of signatures.

For RSA, the CA must use one of the following signature algorithms and encodings.

(i) RSASSA-PKCS1-v1_5 with SHA-256
(ii) RSASSA-PKCS1-v1_5 with SHA-384
(iii) RSASSA-PKCS1-v1_5 with SHA-512

For ECDSA, the CA must use the appropriate signature algorithm and encoding based upon the signing key used.

(iv) If the signing key is P-256, the signature MUST use ECDSA with SHA-256.
(v) If the signing key is P-384, the signature MUST use ECDSA with SHA-384.
(vi) If the signing key is P-521, the signature MUST use ECDSA with SHA-512.

### 7.1.4 Name Forms

#### *7.1.4.1 Name Encoding*

For every valid Certification Path (as defined by RFC 5280, Section 6) for all Certificate and Subordinate CA Certificate, the following must be met:

(i) For each Certificate in the Certification Path, the encoded content of the issuer distinguished name field of a Certificate shall be byte-for-byte identical with the encoded form of the Subject distinguished name field of the issuing CA certificate.
(ii) For each CA Certificate in the Certification Path, the encoded content of the Subject distinguished name field of a Certificate shall be byte-for-byte identical among all Certificates whose Subject distinguished names can be compared as equal according to RFC 5280, Section 7.1, and including expired and revoked Certificates

#### *7.1.4.2 Subject Information – Subscriber Certificates*

Subject information must meet the requirements stated in Appendix B.
Name forms for Subscriber Certificates are as stipulated in §3.1.1. All other optional attributes must contain information that has been verified by the CA or RA. Optional attributes will not contain only metadata such as '.', '-', and ' ' (i.e. space) characters, and/or any other indication that the value is absent, incomplete, or not applicable.

Entries in the dNSName are in the "preferred name syntax" as specified in IETF RFC 5280 and thus do not contain underscore characters.

AffirmTrust will not issue a Certificate with a domain name containing a Reserved IP Address or Internal Name.

#### *7.1.4.3 Subject Information – Root Certificate and Subordinate CA Certificates*

Subject information must meet the requirements stated in Appendix B.

### 7.1.5 Name Constraints

AffirmTrust does not support the issuance of technically constrained Subordinate CA Certificates.

### 7.1.6 Certificate Policy Object Identifier

#### *7.1.6.1 Reserved Certificate Policy Identifiers*

Subscriber Certificates must include one of the following reserved Certificate Policy Identifiers, if the CA is asserting the Certificate meets the associated certificate policy:

| | |
|---|---|
| Domain Validated Certificate | 2.23.140.1.2.1 |
| Organization Validated Certificate | 2.23.140.1.2.2 |
| Extended Validation Certificate | 2.23.140.1.1 |

#### *7.1.6.2 Root CA Certificates*

AffirmTrust Root CA Certificates do not contain the certificate policy object identifiers.

#### *7.1.6.3 Subordinate CA Certificates*

AffirmTrust Subordinate CA Certificates must include either the “any policy” certificate policy object identifier or one or more explicit certificate policy object identifiers that indicates compliance with a specific certificate policy. Certificate policy object identifiers are listed in section 7.1.6.1 and section 7.1.6.4.

#### *7.1.6.4 Subscriber Certificates*

Certificates include one of the following certificate policy identifiers:

| | |
|---|---|
| EV Certificates: | 1.3.6.1.4.1.34697.2.1,<br>1.3.6.1.4.1.34697.2.2,<br>1.3.6.1.4.1.34697.2.3, or<br>1.3.6.1.4.1.34697.2.4 |
| OV Certificates: | 1.3.6.1.4.1.34697.2.5 |
| DV Certificates: | 1.3.6.1.4.1.34697.2.6 |

### 7.1.7 Usage of Policy Constraints Extension

No stipulation.

### 7.1.8 Policy Qualifiers Syntax and Semantics

AffirmTrust CAs include policy qualifiers in all Subscriber Certificates as stipulated in Appendix B.

### 7.1.9 Processing Semantics for the Critical Certificate Policies Extension

No stipulation.

## 7.2 CRL Profile

The following fields of the X.509 version 2 CRL format are used by the CAs:

- version: set to v2
- signature: identifier of the algorithm used to sign the CRL
- issuer: the full Distinguished Name of the CA issuing the CRL
- this update: time of CRL issuance
- next update: time of next expected CRL update
- revoked Certificates: list of revoked Certificate information

### 7.2.1 Version Number(s)

reasonCode (OID 2.5.29.21)

The CRLReason code extension is used for all revoked Certificates. The CRLReason indicated must not be unspecified (0) or certificateHold (6). This extension must not be marked critical. The most appropriate reason must be selected by the Subscriber or the CA from one the following:

(i) keyCompromise (1), if the key to the certificate has been or is suspected to be compromised
(ii) cACompromise (2), if the CA has been or is suspected to be compromised
(iii) affiliationChanged (3), if verified information in the Certificate has changed and as such the Relying Parties should no longer trust the Certificate
(iv) superseded (4), if the Certificate has been reissued, rekeys or renewed by another Certificate
(v) cessationOfOperation (5), if the application or device is no longer in service

### 7.2.2 CRL and CRL Entry Extensions

No stipulation.

## 7.3 OCSP Profile

The profile for the Online Certificate Status Protocol (OCSP) messages issued by a CA conform to the specifications contained in the IETF RFC 6960 Internet X.509 PKI Online Certificate Status Protocol (OCSP) Profile.

Effective 2020-09-30, if an OCSP response is for a Root CA or Subordinate CA Certificate, including Cross Certificates, and that certificate has been revoked, then the revocationReason field within the RevokedInfo of the CertStatus shall be present.

Effective 2020-09-30, the CRLReason indicated shall contain a value permitted for CRLs, as specified in §7.2.2.

### 7.3.1 Version Number(s)

No stipulation.

### 7.3.2 OCSP Extensions

The singleExtensions of an OCSP response shall not contain the reasonCode (OID 2.5.29.21) CRL entry extension.

# 8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

## 8.1 Frequency or Circumstances of Assessment

AffirmTrust CAs and RAs shall be audited for compliance with the practices and procedures set forth in the CPS. The period during which the CA issues Certificates will be divided into an unbroken sequence of audit periods. An audit period will not exceed one year in duration.

## 8.2 Identity/Qualifications of Assessor

The compliance audit of AffirmTrust CAs shall be performed by an auditor which possesses the following qualifications and skills:

i. Independence from the subject of the audit;
ii. Ability to conduct an audit that addresses the criteria of the audit schemes specified in Sec. 8.4;
iii. Employs individuals who have proficiency in examining PKI technology, information security tools and techniques, information technology and security auditing, and the third-party attestation function;
iv. Licensed by WebTrust;
v. Bound by law, government regulation, or professional code of ethics; and
vi. Maintains professional liability/errors and omissions insurance policy limits of at least one million US dollars coverage.

## 8.3 Assessor's Relationship to Assessed Entity

The certified public accounting firm selected to perform the compliance audit for the CAs and RAs shall be independent from the entity being audited.

## 8.4 Topics Covered by Assessment

The compliance audit shall test compliance of the AffirmTrust CAs and RAs against the policies and procedures set forth, as applicable in:

i. This CPS;
ii. WebTrust Program for Certification Authorities;
iii. WebTrust Program for Baseline Requirements; and
iv. WebTrust Program for EV Guidelines.

## 8.5 Actions Taken as a Result Of Deficiency

Upon receipt of a compliance audit that identifies any deficiencies, AffirmTrust shall use commercially reasonable efforts to correct any such deficiencies in an expeditious manner.

## 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.

The results of the most recent compliance audit will be posted within three months from the end of the audit period to the Repository. In the event of a delay greater than three months, the CA will provide an explanatory letter signed by the qualified auditor. The audit results will also be posted to the CA Common Database (i.e., https://ccadb.force.com).

The audit report shall contain at least the following information:

(i) name of the organization being audited;

(ii) name and address of the organization performing the audit;
(iii) the SHA-256 fingerprint of all Roots and Subordinate CA Certificates, including Cross Certificates, that were in-scope of the audit, where the fingerprint uses uppercase letters and does not contain colons, spaces or line feeds;
(iv) audit criteria, with version number(s), that were used to audit each of the certificates (and associated keys);
(v) a list of the CA policy documents, with version numbers, referenced during the audit;
(vi) whether the audit assessed a period of time or a point in time;
(vii) the start date and end date of the Audit Period, for those that cover a period of time;
(viii) the point in time date, for those that are for a point in time;
(ix) the date the report was issued, which will necessarily be after the end date or point in time date;
(x) (for audits conducted in accordance with any of the ETSI standards) a statement to indicate if the audit was a full audit or a surveillance audit, and which portions of the criteria were applied and evaluated, e.g. DVCP, OVCP, NCP, NCP+, LCP, EVCP, EVCP+, QCP-w, Part 1 (General Requirements), and/or Part 2 (Requirements for Trust Service Providers); and
(xi) (for audits conducted in accordance with any of the ETSI standards) a statement to indicate that the auditor referenced the applicable CA/Browser Forum criteria, such as this document, and the version used.

The authoritative version of the audit report must be English language, available as a PDF and text searchable for all required information.

## 8.7 Self-Audits

AffirmTrust CAs which issue monitor adherences to this CPS and the Baseline Requirements and strictly control its service quality by performing self-audits on at least a quarterly basis against a randomly selected sample of the greater of one Certificate or at least three percent of the Certificates issued by it during the period commencing immediately after the previous self-audit sample was taken.

# 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 §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 stipulation.

### 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 §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 stipulation.

## 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 §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 stipulation.

### 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 stipulation.

## 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 §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 §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 §4 below.

## 2. Cross-Signed Intermediate sub-CAs

No stipulation.

## 3. 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 |

(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 |

(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 |

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.

# APPENDIX B

## AFFIRMTRUST CERTIFICATE PROFILES

### Root CA Certificate

| Field | Critical Extension | Content |
|---|---|---|
| Issuer | | Must match subject |
| Subject | | Must contain countryName, organizationName and commonName |
| Extension: subjectKeyIdentifier | Not critical | 160-bit SHA-1 hash of subjectPublicKey per RFC 5280 |
| Extension: basicConstraints | Critical | cA is TRUE; pathLenConstraint is not present |
| Extension: keyUsage | Critical | keyCertsign and cRLSign bits are set |

### Subordinate CA Certificate

| Field | Critical Extension | Content |
|---|---|---|
| Validity: notAfter | | Not later than the notAfter of the signing certificate |
| Subject | | Must contain countryName, organizationName and commonName |
| Extension: subjectKeyIdentifier | Not critical | 160-bit SHA-1 hash of subjectPublicKey per RFC 5280 |
| Extension: authorityKeyIdentifier | Not critical | Matches subjectKeyIdentifier of signing certificate |
| Extension: certificatePolicies | Not critical | Must contain at least one set of policyInformation containing at least a policyIdentifier |
| Extension: basicConstraints | Critical | cA is TRUE |
| Extension: keyUsage | Critical | keyCertsign and cRLSign bits are set |
| Extension: extKeyUsage | Not critical | Must be present |
| Extension: authorityInfoAccess | Not critical | Must contain one AccessDescription with an accessMethod of ocsp and a Location of type uniformResourceIdentifier |
| Extension: cRLDistributionPoints | Not critical | Must have at least one DistributionPoint containing a fullName of type uniformResourceIdentifier |

**DV Certificate**

| Field | Critical Extension | Content |
|---|---|---|
| Subject | | Must contain commonName |
| Extension: subjectKeyIdentifier | Not critical | 160-bit SHA-1 hash of subjectPublicKey per RFC 5280 |
| Extension: authorityKeyIdentifier | Not critical | Matches subjectKeyIdentifier of signing certificate |
| Extension: certificatePolicies | Not critical | Must contain at least one set of policyInformation containing at least a policyIdentifier |
| Extension: basicConstraints | Not critical | Empty or not present |
| Extension: subjectAltName | Not critical | Must contain at least one name and all names must either be of type dNSName or iPAddress |
| Extension: keyUsage | Not critical | digitalSignature and keyExchange bits are set |
| Extension: extKeyUsage | Not critical | Must include serverAuth and/or clientAuth |
| Extension: authorityInfoAccess | Not critical | Must contain one AccessDescription with an accessMethod of caIssuers and a Location of type uniformResourceIdentifier and one AccessDescription with an accessMethod of ocsp and a Location of type uniformResourceIdentifier |
| Extension: cRLDistributionPoints | Not critical | Must have at least one DistributionPoint containing a fullName of type uniformResourceIdentifier |

**OV Certificate**

| Field | Critical Extension | Content |
|---|---|---|
| Subject | | Must contain countryName, localityName organizationName and commonName |
| Extension: subjectKeyIdentifier | Not critical | 160-bit SHA-1 hash of subjectPublicKey per RFC 5280 |
| Extension: authorityKeyIdentifier | Not critical | Matches subjectKeyIdentifier of signing certificate |
| Extension: certificatePolicies | Not critical | Must contain at least one set of policyInformation containing at least a policyIdentifier |
| Extension: basicConstraints | Not critical | Empty or not present |
| Extension: subjectAltName | Not critical | Must contain at least one name and all names must either be of type dNSName or iPAddress |
| Extension: keyUsage | Not critical | digitalSignature and keyExchange bits are set |
| Extension: extKeyUsage | Not critical | Must include serverAuth and/or clientAuth |
| Extension: authorityInfoAccess | Not critical | Must contain one AccessDescription with an accessMethod of caIssuers and a Location of type uniformResourceIdentifier and one AccessDescription with an accessMethod of ocsp and a Location of type uniformResourceIdentifier |
| Extension: cRLDistributionPoints | Not critical | Must have at least one DistributionPoint containing a fullName of type uniformResourceIdentifier |

### EV Certificate

| Field | Critical Extension | Content |
|---|---|---|
| Subject | | Must contain countryName, localityName jurisdiction country, organizationName business category, serial number of subscriber and commonName |
| Extension: subjectKeyIdentifier | Not critical | 160-bit SHA-1 hash of subjectPublicKey per RFC 5280 |
| Extension: authorityKeyIdentifier | Not critical | Matches subjectKeyIdentifier of signing certificate |
| Extension: certificatePolicies | Not critical | Must contain at least one set of policyInformation containing at least a policyIdentifier |
| Extension: basicConstraints | Not critical | Empty or not present |
| Extension: subjectAltName | Not critical | Must contain at least one name and all names must either be of type dNSName |
| Extension: keyUsage | Not critical | digitalSignature and keyExchange bits are set |
| Extension: extKeyUsage | Not critical | Must include serverAuth and/or clientAuth |
| Extension: authorityInfoAccess | Not critical | Must contain one AccessDescription with an accessMethod of caIssuers and a Location of type uniformResourceIdentifier and one AccessDescription with an accessMethod of ocsp and a Location of type uniformResourceIdentifier |
| Extension: cRLDistributionPoints | Not critical | Must have at least one DistributionPoint containing a fullName of type uniformResourceIdentifier |