Certification Practice Statement

Internet Security Research Group (ISRG)

Version 1.1

Updated September 9, 2015
Approved by ISRG Policy Management Authority

Web Site: https://letsencrypt.org

Copyright Notice

Table of Contents

Change History

Date	Changes / Authors	Version
05 May 2015	Original Authors: Warren Brunson, Shelley Johnson	1.0
09 September 2015	Added/corrected a number of policy URIs, removed LDAP as mechanism for publishing certificate information, removed administrative contact requirement for DV-SSL subscribers, removed mention of web-based revocation option, removed description of customer service center, substantial changes to all of Section 9 regarding legal matters, other minor fixes/improvements. Authors: Josh Aas	1.1

Preface

This Certification Practice Statement (CPS) is prepared for use with the ISRG Certificate Policy, Version 1.1.

What's New in This Revision

Added/corrected a number of policy URIs, removed LDAP as mechanism for publishing certificate information, removed administrative contact requirement for DV-SSL subscribers, removed mention of web-based revocation option, removed description of customer service center, clarified insurance or warranty coverage for end-entities, clarified dispute resolution, clarified confidentiality of business information, clarified limitations of liability, clarified terms surviving termination, other minor fixes/improvements.

1 Introduction

1.1 Overview

As the Certification Practice Statement (CPS) of the Internet Security Research Group (ISRG), this document states the practices that ISRG and its PKI participants employ in providing certification services. Such services include, but are not limited to, issuing, managing, validating, revoking, and renewing Certificates in accordance with the requirements of the ISRG Certificate Policy (CP).

The CP is the governing document with respect to the ISRG PKI and its Certificate offerings, and as such it establishes the legal, technical, and business requirements surrounding the Certificate life cycle – the Certificate-related activities mentioned above, and associated trust services. The CP requirements apply to all ISRG PKI participants.

This CPS, therefore, describes how the CP requirements are met by the ISRG PKI – specifically, how the Certificate life cycle events are managed, and how the core PKI infrastructure is kept secure.

This CPS conforms to the Internet Engineering Task Force (IETF) RFC 3647 for CP and CPS document organization. In addition, the practices described in this CPS comply with the CA/Browser Forum (CAB Forum) Baseline Requirements, version 1.1.9, in effect at the time of publication of this document, as published at https://cabforum.org. This CPS and the CP it conforms to are published and are publicly available online at https://letsencrypt.org/repository/.

1.2 Identification

1.2.1 Alphanumeric Identifier

The alphanumeric identifier (i.e., the title) for this CPS is the "ISRG Certificate Practices Statement, 9 9 2015" or “isrg-cps-v2015 9 9”.

1.2.2 Object Identifier

The following certificate types and OIDs will be recognized for use within the PKI established by the Policy for this CPS. The certificate types listed below vary depending upon the identity of the Subscriber (electronic device or individual). Certificates issued under the CP and this CPS will contain the OID listed below in the Certificate Policies field of the Certificate:

- DV-SSL Certificate (ISRG OWNED POLICY OID) and (2.23.140.1.2.1) – issued to machines of Subscribers that demonstrate control of a domain in accordance with Section 3.2.4.
- Administrative Certificates – used solely for the management and operation of the PKI, including:
  - Administrators
  - Others as needed
- Other Types – as allowed by the CP and this CPS and upon approval of the PMA.

The Certificate profiles for these Certificates may be found in Section 7.

1.3 PKI Participants

1.3.1 Certification Authority (CA)

The CA is responsible for the creation, maintenance, and enforcement of this CP.

The CA is responsible for all aspects of the creation, issuance, validation, revocation, and management of Certificates including: (i) the application and enrollment process; (ii) the identification and authentication process; (iii) the actual Certificate manufacturing process; (iv) publication of the Certificate; (v) revocation of the Certificate; (vi) renewal of the Certificate; and (vii) ensuring that all aspects of the CA services and CA operations and infrastructure related to Certificates issued under this Policy are performed in accordance with the requirements, representations, and warranties of this Policy.

The CA operates a Policy Management Authority (PMA) that reviews and approves this Policy, any applicable CPS, and revisions to this Policy and each such CPS.

The CA may delegate some or all of these duties to other organizations.

CAs (CAs who have cross-certified or are otherwise authorized to issue Certificates by the PMA) may enter into arrangements to provide notification of certificate issuance and revocation to each other and to share other information relevant to the operation of the PKI established by this Policy. The CA must make an OCSP Responder available to end entities in accordance with Section 4.10. The CA must notify a Subscriber when a Certificate bearing that Subscriber's DN is issued or revoked.

The CA will revoke the Certificate for any of the reasons specified in the CA/B Forum Baseline Requirements.

The CA issues Certificates to Applicants, who may be individuals or organizations.

The CA will issue DV-SSL Certificates to machines of Applicants who demonstrate control a Fully Qualified Domain Name (FQDN). A DV-SSL Certificate issued to a Subscriber must contain one or more policy identifier(s), defined by the CA, in the Certificate's certificatePolicies extension that indicates adherence to and compliance with the CAB/F Baseline Requirements. The issuing CA shall document in its Certification Practice Statement that the DV-SSL Certificates it issues containing the specified policy identifier(s) are managed in accordance with these CAB/F Baseline Requirements. The CA shall not include a Domain Name in a Subject attribute except as specified in Sections 9.2.1 and 9.2.2 of the CAB/F Baseline Requirements.

The CA will issue Administrative Certificates to itself including self-signed subordinate CA Certificates, and other device Certificates such as OCSP responder Certificates.

In addition, the CA will issue Administrative Certificates to individuals who are employed by or otherwise affiliated with the CA for the purpose of administering the CA infrastructure.

The CA will require, as part of the Subscriber Agreement or Terms of Use Agreement, that the Applicant make the commitments and warranties set forth among Section 1.3.4 and Section 9.6.3 of this Policy, for the benefit of the CA and the Certificate Beneficiaries.

The CA will enter a Relying Party Agreement with each Relying Party. The CA will ensure that all Relying Party Agreements incorporate by reference the provisions of this Policy regarding the CA's and the Relying Party's rights and obligations.

The CA will ensure that is agreements with other PKI Participants incorporate by reference the provisions of this Policy, or provide the respective contracting parties the protections established by this policy.

1.3.2 Policy Management Authority (PMA)

The PMA for the CP and this CPS is determined by the management of ISRG. This PMA will administer the policy decisions regarding the CP and the CPS in the manner provided in the document entitled "Policy Management Authority" and adopted by the management of ISRG on July 14, 2015.

The PMA shall develop, implement, enforce, and annually update a Certificate Policy and/or Certification Practice Statement that describe in detail how the CA implements the CA/B Forum Baseline Requirements, currently version 1.3.0, and maintains compliance with IdenTrust TrustID Certificate Policy.

1.3.3 *Registration Authorities (RAs)*

The CA shall be ultimately responsible for all Certificates it issues. However, under the Policy, the CA may subcontract registration and Identification and Authentication (I&A) functions to an organization that agrees to fulfill the functions of an RA in accordance with the terms of the Policy, and that will accept DV-SSL Certificate applications and collect and verify Applicant identity information to be entered into a Certificate. RA functions may also be carried out by a combination of human and/or intelligent computational automated processes. An RA operating under this Policy is responsible only for those duties assigned to it by the CA pursuant to an agreement with the CA or as specified in this Policy.

ISRG serves as its own RA.

1.3.4 *Applicants/Subscribers*

In addition to other responsibilities of Applicant/Subscriber set forth in the Policy, Applicant/Subscriber has the responsibilities set forth below.

1. Provide complete and accurate responses to all requests for information made by the CA (or an RA) during Applicant registration, Certificate application, and I&A processes; and upon issuance of a Certificate naming the Applicant as the Subscriber, review the Certificate to ensure that all Subscriber information included in it is accurate, and to Accept or reject the Certificate in accordance with Section 4.4.

2. If the CA and Subscriber are not Affiliated, the Subscriber and the CA are parties to a legally valid and enforceable Certificate Agreement that satisfies these Requirements, or, if the CA and Subscriber are Affiliated, the Applicant Representative acknowledged and accepted the Terms of Use.

3. Generate a Key Pair using a Trustworthy System, and take reasonable precautions to prevent any compromise, modification, loss, disclosure, or unauthorized use of the Private Key.

4. Use the Certificate and the corresponding Private Key exclusively for purposes authorized by the Policy and only in a manner consistent with the Policy, including but not limited, in the case of Code Signing certificates, to not using the Private Key to digitally sign hostile code, including spyware or other malicious software (malware) downloaded without user consent.

5. Instruct the CA (or an RA) to revoke the Certificate promptly upon any actual or suspected loss, disclosure, or other compromise of the Private Key.

A Subscriber who is found to have acted in a manner counter to these obligations will have his, her, or its Certificate revoked, and will forfeit all claims he, she, or it may have against PKI Service Providers.

Except to the extent otherwise specified in the Policy, a Subscriber's obligations will be governed by the Terms of Use or the Certificate Agreement between the Subscriber and the CA.

The Subscriber Agreement or Terms of Use Agreement must contain provisions imposing on the Applicant itself (or made by the Applicant on behalf of its principal or agent under a subcontractor or hosting service relationship) the obligations and warranties set forth below.

1. Accuracy of Information. An obligation and warranty to provide accurate and complete information at all times to the CA, both in the certificate request and as otherwise requested by the CA in connection with the issuance of the Certificate(s) to be supplied by the CA.
2. Protection of Private Key. An obligation and warranty by the Applicant to take all reasonable measures to maintain sole control of, keep confidential, and properly protect at all times the Private

Key that corresponds to the Public Key to be included in the requested Certificate(s) (and any associated activation data or device, e.g. password or token).

3. Acceptance of Certificate. An obligation and warranty that the Subscriber will review and verify the Certificate contents for accuracy.
4. Use of Certificate. An obligation and warranty to install the Certificate only on servers that are accessible at the subjectAltName(s) listed in the Certificate, and to use the Certificate solely in compliance with all applicable laws and solely in accordance with the Subscriber or Terms of Use Agreement.
5. Reporting and Revocation. An obligation and warranty to promptly cease using a Certificate and its associated Private Key, and promptly request the CA to revoke the Certificate, in the event that: (a) any information in the Certificate is, or becomes, incorrect or inaccurate, or (b) there is any actual or suspected misuse or compromise of the Subscriber's Private Key associated with the Public Key included in the Certificate.
6. Termination of Use of Certificate. An obligation and warranty to promptly cease all use of the Private Key corresponding to the Public Key included in the Certificate upon revocation of that Certificate for reasons of Key Compromise.
7. Responsiveness. An obligation to respond to the CA's instructions concerning Key Compromise or Certificate misuse within a specified time period.
8. Acknowledgment and Acceptance. An acknowledgment and acceptance that the CA is entitled to revoke the certificate immediately if the Applicant were to violate the terms of the Subscriber or Terms of Use Agreement or if the CA discovers that the Certificate is being used to enable criminal activities such as phishing attacks, fraud, or the distribution of malware.

1.3.5 *Relying Parties*

Relying Parties are entities (individuals or organizations) that act in reliance upon a Certificate issued by the CA. In order to receive benefit from the Policy, Relying Parties must comply with applicable terms and conditions of the Policy and associated Certification Practices Statement including, but not limited to, checking the validity of the Certificate through an appropriate OCSP or other reliable response mechanism.

Prior to relying on or using a Certificate issued under the Policy, a Relying Party is obligated to:

1. Ensure that the Certificate and intended use are appropriate under the provisions of the Policy;
2. Use the Certificate only in accordance with the certification path validation procedure specified in X.509 and PKIX; and
3. Check the status of the Certificate by the OSCP Responder, as applicable, in accordance with the requirements stated in Section 4.10.
4. For digital signatures created during the Operational Period of a Certificate, a Relying Party has a right to rely on the Certificate only under circumstances constituting Reasonable Reliance as defined in Section 1.6 of the Policy.
5. If a Relying Party relies on a Certificate that was expired or that the Relying Party knew or should have known was revoked at the time of reliance (e.g., a decision to rely on a revoked Certificate based on the reasons for revocation, information from other sources, or specific business considerations pertaining to the Relying Party), the Relying Party does so at its own risk and, in so relying, waives any warranties that any PKI Service Provider may have provided.

In no event shall a Relying Party Agreement waive or otherwise lessen the obligations of a Relying Party set forth in the Policy. Except to the extent otherwise specified in the Policy, a Relying Party's obligations will be governed by the Relying Party Agreement between the Relying Party and the CA.

1.3.6 *Other Participants*

1.3.6.1 *Certificate Manufacturing Authority (CMA)*

A CMA is responsible for the functions of manufacturing, issuing, revoking, and renewing Certificates. CMAs, if used, are obligated to adhere to the practices in this CPS and to the policies set forth in the CP.

The CA is ultimately responsible for the manufacture of all ISRG Certificates. However, it may subcontract manufacturing functions to third-party CMAs who agree to be bound by this CPS and the CP.

1.3.6.2 Repository

The CA will perform the role and functions that require the use of a Repository. The CA may subcontract performance of the Repository functions to a third party organization, which will be bound by the Policy, but the CA remains responsible for the performance of those services in accordance with the Policy.

A Repository is responsible for maintaining a secure system for storing and retrieving Certificates, a current copy, or a link to a current copy, of the Policy, and other information relevant to Certificates, and for providing information regarding the status of Certificates as valid or invalid that can be determined by a Relying Party.

The CA maintains a 24 x 7 publicly-accessible Repository with current information regarding the status (valid or revoked) of all unexpired Certificates.

1.4 Certificate Usage

1.4.1 Allowed Certificate Uses

DV-SSL certificates issued in compliance with the Policy can be used only to establish secure online communication hosts (as identified by the FQDN provided in the certificate) and clients using SSL/TLS protocols.
Applications for which Administrative Certificates are suitable include, but are not limited to, applications that:

- Generation of other Certificates such as DV-SSL, Intermediate CA and device; and
- Administration of software and hardware components within the CA.

1.4.2 Prohibited Certificate Uses

DV-SSL Certificates may not be used for:

1. Any purpose not explicitly defined in Section 1.4.1 of this Policy
2. 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
    e. Any other system whose failure could lead to injury, death, or environmental damage
3. Transactions in which applicable law prohibits the use of digital signatures for such transactions
4. Transactions that are otherwise prohibited by law
5. Software or hardware architectures that provide facilities for interference with encrypted communications, including but not limited to:
    a. Active eavesdropping (e.g., Man-in-the-middle [MitM] attacks)
    b. Traffic management of domain names or internet protocol (IP) addresses that the organization does not own or control

(Note: these restrictions shall apply regardless of whether a relying party communicating through the software or hardware architecture has knowledge of its providing facilities for interference with encrypted communications.)

Administrative Certificates may not be used for any purpose other than administering the operation of the CA, RA, CMA, CSA, and Repository infrastructures and related activities.

1.4.3 Cross-Certification

The PMA approves cross-certification between the CA and other Certification Authorities, and must inform Subscribers of the uses allowed within the cross-certified PKI. Any cross-certification to external organizations will only be done after approval by the PMA or its designee.

The CA will disclose all Cross Certificates that identify the CA as the Subject, provided that the CA arranged for or accepted the establishment of the trust relationship (i.e. the Cross Certificate at issue). If the CA is cross-certifying with another external party, it will not be authorized or allowed to issue that entity a Subordinate Certificate unless it is compliant with the CA/B Forum Baseline Requirements and conforms to the CP of the cross-certifying entity and the requirements therein.

1.5 Policy Administration

1.5.1 Organization Administering this CPS

This CPS is owned and administered by ISRG, and is administered by the ISRG PMA.

1.5.2 Contact Person

Questions regarding this CPS or the procedures described within it should be directed to:

Policy Management Authority
Internet Security Research Group
331 E Evelyn Ave
Mountain View, CA 94041

1.5.3 Person Determining CPS Suitability for the Certificate Policy

The PMA will determine the suitability of this CPS to the Certificate Policy.

1.5.4 CPS Approval Procedure

The PMA will examine this proposed CPS for compliance with the CP, and may, at its discretion, consult with subject matter experts in relation to the suitability of CPS provisions. The PMA will approve or reject this CPS using procedures outlined in its charter.

1.6 Definitions and Acronyms

1.6.1 Definitions

Accept or Acceptance: An act that triggers rights and obligations of an Applicant with respect to the Certificate being applied for under the applicable Certificate Agreement or Relying Party Agreement. Indications of Acceptance may include (i) using the Certificate (after issuance); (ii) failing to notify the CA of any problems with the Certificate within a reasonable time after receiving it, or (iii) other manifestations of assent. "Accepted" shall have a corollary meaning.

Affiliate: A corporation, partnership, joint venture or other entity controlling, controlled by, or under common control with another entity, or an agency, department, political subdivision, or any entity operating under the direct control of a Government Entity. "Affiliated" shall have a corollary meaning.

Applicant: The natural person or Legal Entity that applies for (or seeks renewal of) a Certificate. Once the Certificate issues and is Accepted by the Applicant, the Applicant is referred to as the Subscriber. For Certificates issued to devices, the Applicant is the entity that controls or operates the device named in the Certificate, even if the device is sending the actual certificate request.

Applicant Representative: A natural person or human sponsor who is either the Applicant, employed by the Applicant, or an authorized agent who has express authority to represent the Applicant who (i) who signs and submits, or approves a certificate request on behalf of the Applicant, and/or (ii) who signs and submits a Certificate Agreement on behalf of the Applicant, and/or (iii) acknowledges and agrees to the Terms of Use applicable to the Certificate on behalf of the Applicant when the Applicant is an Affiliate of the CA.

Application Software Supplier: A supplier of internet browser software or other relying-party application software that displays or uses Certificates and incorporates Root Certificates.

CA Certificate: A Certificate at the beginning of a certification chain within the CA's PKI hierarchy of the CA. The CA Certificate contains the Public Key that corresponds to the CA Private Signing Key that the CA uses to create or manage Certificates. CA Certificates and their corresponding Public Keys may be embedded in software or obtained or downloaded by the affirmative act of a Relying Party in order to establish a certification chain. Based upon the Certificate's use, a CA Certificate may be a Root CA Certificate or a Subordinate CA Certificate.

CA Private Signing Key: The Private Key that corresponds to the CA's Public Key listed in its CA Certificate and used to sign other Certificates such as subordinate CA certificates. The CA Private Signing Key is not used to sign Subscriber Certificates.

CA Private Root Key: The Private Key used to sign CA Certificates.

Certificate: An electronic document that uses a digital signature to bind a Public Key to an identity. Within this CPS, specifically a Certificate issued under the Root Certificate.

Certificate Agreement: The contract between a Subscriber and the CA and/or RA that details the procedures, rights, responsibilities, and obligations of each party with respect to a Certificate issued to the Subscriber.

Certificate Data: Certificate requests and data related thereto (whether obtained from the Applicant or otherwise) in the CA's possession or control or to which the CA has access.

Certificate Management Process: Processes, practices, and procedures associated with the use of keys, software, and hardware, by which the CA verifies Certificate Data, issues Certificates, maintains a Repository, and revokes Certificates.

Certificate Manufacturing Authority (CMA): An organization that manufactures or creates Certificates.

Certificate Policy: A named set of rules that indicates the applicability of Certificates to particular communities and classes of applications and specifies the Identification and Authentication processes performed prior to Certificate issuance, the Certificate Profile and other allowed uses of Certificates; see also Policy.

Certificate Problem Report: Complaint of suspected Key Compromise, Certificate misuse, or other types of fraud, compromise, misuse, or inappropriate conduct related to Certificates.

Certificate Profile: The protocol used in Section 7 of this CPS to establish the allowed format and contents of data fields within DV-SSL and Administrative Certificates issued under the CP and this CPS, which identify the CA, the Subscriber, the Validity Period of the Certificate, and other information that identifies the Subscriber.

Certificate Revocation List (CRL): A regularly updated time-stamped list of revoked Certificates that is created and digitally signed by the CA that issued the Certificates.

Certificate Status Authority (CSA): An organization that uses data in a Repository to provide certificate revocation status and/or complete certificate path validation (including revocation checking) to the Relying Parties through Online Certificate Status Protocol or Certificate Revocations List capabilities.

Certification Authority: An organization that is responsible for the creation, issuance, revocation, and management of Certificates. The term applies equally to both Root CAs and Subordinate CAs. Also known as a Certificate Authority.

Certification Practice Statement: One of several documents forming the governance framework in which Certificates are created, issued, managed, and used.

Country: Either a member of the United Nations OR a geographic region recognized as a sovereign nation by at least two UN member nations.

Cross Certificate: A certificate that is used to establish a trust relationship between two Root CAs.

Cryptomodule: Secure software, device or utility that: (i) generates Key Pairs, (ii) stores cryptographic information, and/or (iii) performs cryptographic functions.

Delegated Third Party: A natural person or Legal Entity that is not the CA but is authorized by the CA to assist in the Certificate Management Process by performing or fulfilling one or more of the CA requirements found herein.

Distinguished Name (DN): The unique identifier for a Subscriber so that he, she or it can be located in a directory (e.g., the DN might contain the following attributes: (i) common name (cn); (ii) e-mail address (mail); (iii) organization name (o); (iv) organizational unit (ou); (v) locality (l); (vi) state (st); and (vii) country (c)).

Domain Authorization Document: Documentation provided by, or a CA's documentation of a communication with, a Domain Name Registrar, the Domain Name Registrant, or the person or entity listed in WHOIS as the Domain Name Registrant (including any private, anonymous, or proxy registration service) attesting to the authority of an Applicant to request a Certificate for a specific Domain Namespace.

Domain Name: The label assigned to a node in the Domain Name System.

Domain Namespace: The set of all possible Domain Names that are subordinate to a single node in the Domain Name System.

Domain Name Registrant: Sometimes referred to as the "owner" of a Domain Name, but more properly the person(s) or entity(ies) registered with a Domain Name Registrar as having the right to control how a Domain Name is used, such as the natural person or Legal Entity that is listed as the "Registrant" by WHOIS or the Domain Name Registrar.

Domain Name Registrar: A person or entity that registers Domain Names under the auspices of or by agreement with: (i) the Internet Corporation for Assigned Names and Numbers (ICANN), (ii) a national Domain Name authority/registry, or (iii) a Network Information Center (including their affiliates, contractors, delegates, successors, or assigns).

Domain Validation: The process of validating a Domain through demonstrated control by the Applicant or Subscriber. The validation is achieved through a response to a request from a client, e-mail, or records indicating ownership of the Domain (i.e., WHOis) by the Applicant or Subscriber. Once this completed through either manual or automated processes, the Domain is validated.

Expiry Date/Expiration Date: The "Not After" date in a Certificate that defines the end of a Certificate's validity period. `

Fully-Qualified Domain Name: A Domain Name that includes the labels of all superior nodes in the Internet Domain Name System.

High-Risk Certificate Request: A Request that the CA flags for additional scrutiny by reference to internal criteria and databases maintained by the CA, which may include names at higher risk for phishing or other fraudulent usage, names contained in previously rejected certificate requests or revoked Certificates, names listed on the Miller Smiles phishing list or the Google Safe Browsing list, or names that the CA identifies using its own risk-mitigation criteria.

High-Security Zone: An area to which access is controlled through an entry point and limited to authorized, appropriately screened personnel and properly escorted visitors, accessible only from Security Zones, separated from Security Zones and Operations Zones by a perimeter. High-Security Zones are monitored 24 hours a day and 7 days a week by security staff, other personnel and electronic means.

Identification and Authentication: The process of validating the identity of an Applicant and confirming the Applicant's control over a domain (for DV-SSL Certificates), or confirming the Applicant's position within an organization (for Administrative Certificates).

Internal Name: A string of characters (not an IP address) in a Common Name or Subject Alternative Name field of a Certificate that cannot be verified as globally unique within the public DNS at the time of certificate issuance because it does not end with a Top Level Domain registered in IANA's Root Zone Database.

ISRG Certificate: A Certificate issued pursuant to the Certificate Policy and this CPS.

Issue Certificates/Issuance: The act performed by a CA in creating a Certificate, listing itself as "Issuer" of that Certificate, and notifying the Applicant of the contents of the Certificate and that the Certificate is ready and available for Acceptance.

Issuer: The CA that creates a Certificate and makes it available for Acceptance by the Applicant.

Key Compromise: A Private Key is said to be compromised if its value has been disclosed to an unauthorized person, an unauthorized person has had access to it, or there exists a practical technique by which an unauthorized person may discover its value. A Private Key is also considered compromised if methods have been developed that can easily calculate it based on the Public Key (such as a Debian weak key, see http://wiki.debian.org/SSLkeys) or if there is clear evidence that the specific method used to generate the Private Key was flawed.

Key Generation: The process of creating a Key Pair.

Key Pair: The Private Key and its associated Public Key.

Legal Entity: An association, corporation, partnership, proprietorship, trust, government entity or other entity with legal standing in a country's legal system.

Man-in-the-Middle Attack (MitM): An attack on an authentication protocol in which the attacker positions himself or herself in between the claimant and verifier so that he or she can intercept and alter data traveling between them.

Object Identifier (OID): A unique alphanumeric or numeric identifier registered under the International Organization for Standardization's applicable standard for a specific object or object class.

OCSP Responder: An online server operated under the authority of the CA and connected to its Repository for processing Certificate status requests. See also, Online Certificate Status Protocol.

Online Certificate Status Protocol: An online Certificate-checking protocol that enables relying-party application software to determine the status of an identified Certificate. See also OCSP Responder.

Operational Period: A Certificate's actual term of validity, beginning with the start of the Validity Period and ending on the earlier of (i) the end of the Validity Period disclosed in the Certificate, or (ii) the revocation of the Certificate.

Operations Zone: An area where access is limited to personnel who work there and to properly escorted visitors. Operations Zones should be monitored at least periodically and should preferably be accessible only from a Reception Zone.

PKI Service Providers: The PMA, CAs, RAs, CMAs, and Repositories participating in the PKI defined by the CP and this CPS.

Policy: The ISRG Certificate Policy that this CPS supports; also known herein as the "CP."

Policy Management Authority (PMA): A group within a CA that is responsible for setting, implementing, and administering policy decisions regarding the CA, including but not limited to those related to its Certificate Policy and Certification Practices Statement.

Private Key: The key of a Key Pair that is kept secret by the holder of the Key Pair, and that is used to create digital signatures and/or to decrypt electronic records or files that were encrypted with the corresponding Public Key.

Public Key: The key of a Key Pair publicly disclosed by the holder of the corresponding Private Key and used by the recipient to validate digital signatures created with the corresponding Private Key and/or to encrypt messages or files to be decrypted with the corresponding Private Key.

Public Key Infrastructure (PKI): A set of hardware, software, people, organizations, procedures, rules, policies, and obligations used to facilitate the trustworthy creation, issuance, management, and use of Certificates and keys based on Public Key cryptography.

Publicly-Trusted Certificate: A Certificate that is trusted by virtue of the fact that its corresponding Root Certificate is distributed as a trust anchor in widely-available application software.

Qualified Auditor: A natural person or Legal Entity that meets the requirements of Section 17.6 (Auditor Qualifications) in the CA/B Forum Baseline Requirements.

Reasonable Reliance: For purposes of the CP and this CPS, a Relying Party's decision to rely on an DV-SSL Certificate will be considered Reasonable Reliance if he, she or it:

- Verified that the digital signature in question (if any) was created by the Private Key corresponding to the Public Key in the Certificate during the time that the Certificate was valid, and that the communication signed with the digital signature had not been altered;
- Verified that the Certificate in question was valid at the time of the Relying Party's reliance, by conducting a status check of the Certificate's then-current validity as required by the CA; and
- Used the Certificate for purposes appropriate under the CP and this CPS and under circumstances where reliance would be reasonable and in good faith in light of all the circumstances that were known or should have been known to the Relying Party prior to reliance. A Relying Party bears all risk of relying on a Certificate while knowing or having reason to know of any facts that would cause a person of ordinary business prudence to refrain from relying on the Certificate.

Reception Zone: A zone that is accessible by the public and from which access may be gained to higher security zones with appropriate security controls.

Registered Domain Name: A Domain Name that has been registered with a Domain Name Registrar.

Registration Authority (RA): Any Legal Entity that is responsible for identification and authentication of subjects of Certificates, but is not a CA, and hence does not sign or issue Certificates. An RA may assist in the certificate application process or revocation process or both. When "RA" is used as an adjective to

describe a role or function, it does not necessarily imply a separate body, but can be part of the CA. In this CPS, ISRG acts as its own RA and is responsible for all RA-designated activities.

Reliable Data Source: An identification document or source of data used to verify Subject Identity Information that is generally recognized among commercial enterprises and governments as reliable, and which was created by a third party for a purpose other than the Applicant obtaining a Certificate.

Reliable Method of Communication: A method of communication, such as a postal/courier delivery address, telephone number, or email address, that was verified using a source other than the Applicant Representative.

Relying Party: Any natural person or Legal Entity that relies on a Valid Certificate. An Application Software Supplier is not considered a Relying Party when software distributed by such Supplier merely displays information relating to a Certificate.

Relying Party Agreement: An agreement between CA and a Relying Party setting forth the terms and conditions governing reliance or other permitted use by the Relying Party on an ISRG Certificate, which such agreement details the procedures, rights, responsibilities, and obligations of each of CA and Relying Party.

Repository: An online database containing publicly-disclosed PKI governance documents (such as Certificate Policies and Certification Practice Statements) and Certificate status information, either in the form of a CRL or an OCSP response.

Reserved IP Address: An IPv4 or IPv6 address that the IANA has marked as reserved, as shown in the following references:
http://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xml
http://www.iana.org/assignments/ipv6-address-space/ipv6-address-space.xml

Restricted Zones: Any one of (i) an Operations Zone; (ii) a Security Zone; and (iii) a High Security Zone.

Revocation: The act of making a Certificate permanently ineffective from a specified time forward. Revocation is effected by notation or inclusion in a set of revoked Certificates or other directory or database of revoked Certificates (e.g., inclusion in a CRL).

Root Certification Authority: The top level Certification Authority 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.

Security Zone: An area to which access is limited to authorized personnel and to authorized and properly escorted visitors. Security Zones should preferably be accessible from an Operations Zone, and through a specific entry point. A Security Zone need not be separated from an Operations Zone by a secure perimeter. A Security Zone should be monitored 24 hours a day and 7 days a week by security staff, other personnel or electronic means.

Split-Knowledge Technique: A security procedure where no single individual possesses the equipment, knowledge or expertise to view, alter or otherwise have access to sensitive or confidential information in a particular PKI.

Subject: The natural person, device, system, unit, or Legal Entity identified in a Certificate as the Subject. The Subject is either the Subscriber or a device under the control and operation of the Subscriber.

Subject Identity Information: Information that identifies the Certificate Subject. Subject Identity Information does not include a domain name listed in the subjectAltName extension or the Subject commonName field.

Subordinate CA Certificate: A Certificate that is signed by a Root CA and subsequently listed in the Certificate chain. Subordinate CA Certificates and their corresponding Public Key may be embedded in software or obtained or downloaded by the affirmative act of a Relying Party in order to establish a certification chain within the PKI hierarchy.

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

Subscriber: A natural person or Legal Entity to whom a Certificate is issued and who is legally bound by a Certificate Agreement or Terms of Use Agreement. An Applicant becomes a Subscriber when the Certificate is issued and accepted.

Technically Constrained Subordinate CA Certificate: A Subordinate CA certificate that uses a combination of Extended Key Usage settings and Name Constraint settings contained within the Certificate to limit the scope within which the Subordinate CA Certificate may issue Subscriber or additional Subordinate CA Certificates.

Terms of Use: Provisions regarding the safekeeping and acceptable uses of a Certificate issued in accordance with these Requirements.

Trusted Role: A role involving functions that may introduce security problems if not carried out properly, whether accidentally or maliciously. The functions of Trusted Roles form the basis of trust for the entire PKI. Such roles may include system administrators, CA administrators and CA operations personnel, help desk personnel, security personnel, and security auditors. Specific Trusted Roles for the PKI are described in this CPS.

Trustworthy System: Computer hardware, software, and procedures that are: reasonably secure from intrusion and misuse; (ii) provide a reasonable level of availability, reliability, and correct operation; (iii) are reasonably suited to performing their intended functions; and (iv) enforce the applicable security policy.

Unregistered Domain Name: A Domain Name that is not a Registered Domain Name.

Valid Certificate: A Certificate that passes the validation procedure specified in RFC 5280.

Validity Period: The period of time measured from the date when the Certificate is issued until the Expiry Date.

Wildcard Certificate: A Certificate containing an asterisk (*) in the left-most position of any of the Subject Fully-Qualified Domain Names contained in the Certificate.

1.6.2 *Acronyms*

ACME	Automated Certificate Management Environment
CA	Certification Authority
CMA	Certificate Manufacturing Authority
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSA	Certificate Status Authority
DN	Distinguished Name
DSA	Digital Signature Algorithm
DV	Domain Validated
I&A	Identification and Authentication
ISO	International Standards Organization
OID	Object Identifier
PKI	Public Key Infrastructure
PMA	Policy Management Authority

RA	Registration Authority
SSL	Secure Sockets Layer
X.500	The ITU-T (International Telecommunication Union-T) standard that establishes a distributed, hierarchical directory protocol organized by country, region, organization, etc.
X.501	The ITU-T (International Telecommunication Union-T) standard for use of Distinguished Names in an X.500 directory.
X.509	The ITU-T (International Telecommunication Union-T) standard for Certificates. X.509, version 3, refers to Certificates containing or capable of containing extensions.

2 Publication and Repository Responsibilities

2.1 Repository Obligations

The CA operates and maintains a Repository in order to support its PKI operations and to provide information concerning the status of all Certificates issued. The Repository consists of documents and signed objects made available on https://letsencrypt.org/repository/.

The Repository contains records of all certificates, including those that have expired or have been revoked. The CP and this CPS does not support certificate suspension for DV-SSL Certificates.

2.2 Publication of Certification Information

2.2.1 Publication of Certificates and Certificate Status

The Certificates contain pointers to locations where Certificate-related information is published.

Root CRLs are made available at a URI specified in each certificate issued by a Root.

Relying Parties may access the Repository 24x7x365 using the OCSP method, by which browsers or other applications can query the system in real time to get a validation response. Responses will include but may not be limited to "Valid," "Revoked," "Expired," or "Unknown." A response of "Unknown" indicates that the query was incorrectly submitted to the CA Repository and the Certificate is not part of the ISRG PKI.

ISRG maintains a minimum of 99% availability overall per year, and scheduled down-time does not exceed 0.5% annually, excluding network outages.

2.2.2 Publication of CA Information

The following information is published and available publicly in the Repository:

- A copy of the CP;
- A copy of this CPS;
- Other information related to the PKI

The internet address for accessing this information is https://letsencrypt.org/repository/

2.2.3 Interoperability

Only one interconnection between the CA system is authorized: between the CA internal networks and the internet. The CA does not interoperate with any other computing system.

2.3 Frequency of Publication

All the information required by the CP to be published in the Repository, including Certificate information, is published immediately after such information is available. Certificates are published immediately after Acceptance by their respective Applicants (who are thereafter known as Subscribers). Information relating to the status of a Certificate is published in accordance with the CP.

When changes to the CP are approved and implemented by the PMA, all needed changes in practices are incorporated into this CPS and published upon approval by the PMA.

2.4 Access Controls on Repositories

The CA imposes no access controls on:

- The Certificate Policy;
- The CA Certificate; or
- Current versions of the CA's CPS. The CA may impose access controls on Certificates and Certificate status information, in accordance with provisions of the CP and this CPS.

The Repository contains publicly accessible information, and the CA and CSA does not restrict read-only access to its contents. However, the CA has implemented logical and physical security measures to prevent unauthorized persons from adding to, deleting, or modifying Repository information, including Certificate-related information. Such controls ensure authentication of Applicants and Subscribers with respect to their own personal registration information, Certificate(s) if any, and the status of such Certificate(s). Application and registration information are managed separately from the publicly available Certificate status Repository.

3 Identification and Authentication

3.1 Naming

3.1.1 Types of Names

The subject name used for Certificates is the Subscriber's authenticated common name. In the case of a DV-SSL Certificate, this is the name of the authenticated Domain Name. In the case of an Administrative Certificate, this is the legal name of the Subscriber. Each Subscriber is required to have a clearly distinguishable and unique X.501 Distinguished Name (DN) in the Certificate subject name field in accordance with PKIX Part 1. The DN is in the form of an X.501 printable string that is not blank. If the CA determines that the combination of domain name and common name is identical to that of another ISRG-issued Certificate, then the CA will ask the Applicant to select another common name.

Certificates contain non-null Distinguished Names (DNs). The names on Certificate may be present in multiple fields including the Issuer DN, Subject DN and Subject Alternative Name.

A Certificate's Issuer DN is the same Subject DN of the Certificate that issued it. This rule applies to all Certificates except the Root CA Certificate whose Issuer DN and Subject DN are identical.

Root CA Certificate
The Issuer DN and Subject DN consist of the Common Name, Organization and Country.

Subordinate CA Certificate
The Issuer DN is the Subject DN from the Root CA Certificate.
The Subject DN consists of Common Name, Organization and Country.

DV-SSL Certificate
The Issuer DN is the Subject DN from the DV-SSL Subordinate CA Certificate.
The Subject DN consists of Common Name.
The Subject Alternative Name contains at least one DNSName entry for each Fully Qualified Domain Name.

Administrative Certificate
The Issuer DN is the Subject DN from the Root CA or Subordinate CA Certificate that issued it.
The Subject DN consists of Common Name, Organization, Organization Unit and Country.
The Subject Alternative Name contains an rfc822Name entry for the Subscriber's email.

OCSP Responder Certificate
The Issuer DN is the Subject DN from the Root CA or Subordinate CA Certificate that issued it.
The Subject DN consists of Common Name, Organizational and Country.
The Subject Alternative Name contains a DNSName with the DNS name of the OCSP Responder

Specific content for each name is specified in Section 7.1.4 of this CPS.

3.1.2 Need for Names To Be Meaningful

The contents of each Certificate Subject and Name field have an association with the authenticated Domain Name submitted by the Subscriber. A Certificate issued for an electronic device includes the authenticated name of the electronic device and/or name of the responsible individual or organization. An Administrative Certificate issued to an individual contains the authenticated common name – a combination of first name, surname, and optionally initials.

The identifiers in a Certificate for Subscriber and Issuer have the meaning specified in Section **Error! Reference source not found.**. By interpreting a Certificate in light of the relevant Certificate profile, a Relying Party can infer the following, among other things, that:

A subjectAltName:dNSName field identifies the component by its fully qualified domain name(s). The content of the dNSName field is readily understandable by humans.

A subject:commonName field lists the human Subscriber of the Certificate. The content of the commonName field is readily understandable by humans. In the case of a human, it is the human's legal name, i.e. the name by which they are commonly known in business contexts.

A subjectAltName:rfc822name lists the Subscriber's e-mail address, at which the Subscriber can receive messages via SMTP.

3.1.3 *Anonymity or Pseudonymity of Subscribers*

No anonymous or pseudonymous Certificates are issued under this CPS.

3.1.4 *Rules for Interpreting Various Name Forms*

Rules for interpreting name forms are listed in the Certificate profiles of Sections 7 and 10. Further information about domain names is found in RFC 1034 and RFC 1035.

3.1.5 *Uniqueness of Names*

The Subject name listed in a Certificate is unambiguous and is unique for a Subscriber for all Certificates issued by the CA and conforms to X.500 standards for name uniqueness. Uniqueness of names for DV-SSL Certificates is based on the use of its Fully Qualified Domain Name. The uniqueness of a domain name is guaranteed by Internet Corporation for Assigned Names and Numbers (ICANN).

Uniqueness of Subscriber's name is based on the combination of the Subject: commonName and SubjectAltName: rfc822Name. Since the email in the rfc822Name is unique, the combination is guaranteed uniqueness.

3.1.6 *Recognition, Authentication, and Role of Trademarks*

3.1.6.1 *Name Claim Dispute Resolution Procedure*

The CA reserves the right to make all decisions regarding Subscriber names in Certificates. A party requesting a Certificate will be required to demonstrate its right to use a particular name. The CA will investigate and correct if necessary any name collisions brought to its attention. If appropriate, the CA will coordinate with and defer to the appropriate naming authority.

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

Applicants are required to prove possession of the Private Key corresponding to the Public Key in a Certificate request, which can be done by signing the request with the Private Key through either an application (for an Administrative Certificate) or a pre-established exchange between the machine and the ACME client (for a DV-SSL Certificate). The CA establishes that the Applicant is in possession of the Private Key corresponding to the Public Key submitted with the application in accordance with an appropriate secure protocol, such as that described in the IETF PKIX Certificate Management Protocol.

In the case where the Private Key for an Administrative Certificate is generated directly on a token, or in a key generator that benignly transfers the key to a token, then the Applicant is deemed to be in possession of the Private Key at the time of generation or transfer. If the Applicant is not in possession of the token when the key is generated, then the token will be delivered immediately to the Applicant via a trustworthy and accountable method (see Section 6.2).

3.2.2 Authentication of Domains and Administrative Certificates

The issuance of DV-SSL and Administrative Certificates will be based on I&A performed by the CA or RA. Process documentation for DV-SSL Certificates include: Record of the Certificate request in the ACME client and Proof of control over the authenticated Domain Name. Process documentation for CA Administrative Certificates includes documentation that is submitted to the CA for verification of affiliation.

3.2.2.1 Acceptable Forms of Identification Documents for Applicants

For DV-SSL Certificates and for Administrative Certificates issued for devices, the CA provides a secure means of validating the Applicant's ownership of, or control over, the device and domain name for which a Certificate is requested. The means of validating such ownership are consistent with the relevant CA/B Forum Baseline Requirements. For domain ownership, the validation consists of an electronic evaluation of the Applicant's submitted information and completion of active challenges provided to the ACME client, directed by the CA. Therefore the request submitted must contain the relevant information for this check including;

- Fully Qualified Domain Name;
- Domain URL.

For Administrative Certificates issued to individuals, the CA provides a secure means of validating the identity of the Applicant; such means include satisfactory proof of identity and of organizational affiliation with the CA. To validate this information, the Human Resources department of the CA will validate the individual's affiliation with the company by confirming the following:

- Name of Applicant;
- Title; and
- Documentation that provides confirmation of employment (tax forms, etc.).

Once this information is confirmed, the Human Resource department will document the approval through an e-mail or paperwork that is scanned to file and distributed to the group,

3.2.2.2 Performance of Electronic Identification

For DV-SSL Certificates, the CA provides a secure means of validating the Applicant's control over, the device and domain name for which a Certificate is requested. The means of validating such ownership is consistent with the relevant CA/B Forum Baseline Requirements.

When an Applicant applies for a DV-SSL Certificate, identification will be performed on the basis of demonstrating control of the Domain Name requested. There are several different challenges that the ACME client may be asked to respond to during the process, e.g. the server might challenge the device or Applicant to provision a record in the DNS under that Domain Name requested to be part of the Certificate or to provision a file on a web server referenced by an A record under that Domain Name. When the Applicant prompts the machine to submit this information, a response from the server will indicate whether what the Applicant provided was successfully verified as proof of control over the authenticated Domain Name or not. By providing the correct information to the response that is requested, the Applicant has demonstrated control over the authenticated Domain Name and can proceed to Issuance, retrieval, and installation of that DV-SSL Certificate.

Administrative CA Certificates require verification by a separate individual affiliated with the CA in a position to verify affiliation of the Applicant (i.e., H.R. or another entity with access to corporate records). When it is determined that an individual will require a CA Administrative Certificate, that individual will fill out an application form and submit that physically or electronically VIA e-mail or attached form to an e-mail and will be approved electronically by the CA affiliate that determines the individual is affiliated and in a position that requires the Administrative Certificate.

The requirements for renewal and rekey of DV-SSL Certificates and Administrative Certificates shall be the same as those above.

3.2.2.3 gTLD Domain Validation

Certificates containing a new gTLD under consideration by ICANN will not be issued. The CA Server will periodically be updated with the latest version of the Public Suffix List and will consult the ICANN domains section for every requested DNS identifier. CA server will not validate or issue for DNS identifiers that do not have a Public Suffix in the ICANN domains section. The Public Suffix List is updated when new gTLDs are added, and never includes new gTLDs before they are resolvable.

3.2.3 Non-Verified Subscriber Information

Non-verified Applicant information will not be included in the Certificate.

3.2.4 Validation of Authority

For DV-SSL Certificates, demonstration of control over the device and domain is conducted electronically through the ACME client and shall consist of validation of the information presented as described above.

For Administrative Certificates issued to individuals, the information submitted by the Applicant shall consist of at least the following items:

- Full name; and
- Validation from the Human Resources department of the CA that confirms affiliation to the CA.

3.2.4.1 Verification of the Certificate Request

A DV-SSL Certificate request identifying an electronic device as the subject of a Certificate can only be made by the machine that has previously been verified by the ACME client as being used by the Applicant requesting the DV-SSL Certificate. To verify the authenticity of a DV-SSL Certificate request for a FQDN, the Applicant responds to requests from the ACME client from servers to verify requested changed to their domain as described in Section 3.2.2.2.

Administrative Certificate requests are verified by the elected affiliates of the CA that determine the Applicant's affiliation and role with the CA. The affiliate will check the records of the company to confirm the trusted role duties of the Applicant and to confirm their affiliation and verify the validity of the Administrative Certificate. This confirmation of the validity will be recorded digitally by the affiliate through an e-mail or saved form confirming the verification by the affiliate.

3.2.4.2 Verification against the Denied List

In accordance with the CA/B Forum Baseline Requirements, the CA maintains an internal database of all previously revoked DV-SSL Certificates and previously rejected certificate requests due to suspected phishing or other fraudulent usage or concerns. The CA uses this information to identify subsequent suspicious certificate requests.

If a new request for a previously denied DV-SSL Certificate is made, the application is rejected immediately by the CA, which notifies the ACME client of the rejection.

3.2.4.3 Verification against High Risk Certificate Requests

The CA develops, maintains, and implements documented procedures that identify and require additional verification activity for High Risk Certificate Requests prior to the Certificate's approval, as reasonably necessary to ensure that such requests are properly verified by doing the following:

To prevent potential phishing, fraudulent use and to take further precautions against potential compromise, The CA maintains a list of prior high risk requests and checks a third-party authority list specifying current high risk Domain Names. This list is used by servers to identify potential risks. Should an application with any potential risk posed to the CA or a Domain Name listed on the third-party authority list, it will be flagged and brought to the attention of management to complete further internal verification. To prevent high-risk Issuance of a DV-SSL Certificate this internal verification will require one or more the following pieces of evidence:

- Request further documentation confirming control of the domain from the Applicant;
- Careful examination of the FQDN to confirm whether the intent of the Domain Registrant or Applicant is to imitate or mislead customers of an FQDN on the high risk third party authority list in order to commit fraudulent or phishing activities (e.g. www.g00gle.com, www.1dentrust.com, etc.) and specific filters that are established at the system level to deny initial applications (e.g., non-US ASCII characters);
- Manual review of all information provided in the online application form; and/or
- Other verifiable proof as deemed necessary by the CA management.

3.2.4.4 Data Source Accuracy

Prior to using any data source as a Reliable Data Source, the CA evaluates the source for its reliability, accuracy, and resistance to alteration or falsification. The CA considers the following during its evaluation:

1. The age of the information provided;
2. The frequency of updates to the information source;
3. The data provider and purpose of the data collection;
4. The public accessibility of the data availability; and
5. The relative difficulty in falsifying or altering the data.

Applicant information is verified by cross-checking it with trusted information in a database of user-supplied information, from a third party vendor of such business information, or from the Organization's financial institution references. The CA will evaluate the data source's accuracy and reliability. The CA will not use a data source to verify Applicant information if the data source is deemed not reasonably accurate or reliable as per requirements listed above.

Databases maintained by the CA, its owner, or its affiliated companies do not qualify as a Reliable Data Source if the primary purpose of the database is to collect information for the purpose of fulfilling the validation requirements under the CA/B Forum Baseline Requirements.

3.2.5 Criteria for Interoperation

The CP specifies that this CPS can opt for cross-certification with other PKIs. Criteria for cross-certification includes review and approval of the Policy and its associated CPS by the PMA of the PKI for which cross-certification is desired, and review and of the cross-certifying PKI's CP and CPS by the CA's PMA. This CP and CPS must comply with the requirements of the CP and CPS of the desired CA that this CA wishes to cross-certify with prior to consideration. Upon approval by both PMAs, cross-certification may be accomplished.

3.2.6 *Authentication of Device Identity*

A DV-SSL Certificate request identifying an electronic device as the subject of a Certificate may only be made by a human sponsor working through the ACME client that demonstrates control of the device and affiliation with the domain, as described in Section 3.2.2.1 above. The DV-SSL will be issued by the CA once the application can be fully verified by the I&A process specified by this CPS. By following these procedures of I&A, the CA seeks to reduce the likelihood that the information contained in the Certificate Profile is misleading.

3.3 Identification and Authentication (I&A) for Renewal

As long as a Subscriber's Certificate has not been revoked, the Subscriber, within three months prior to the end of the Certificate's Validity Period, can request issuance of a new DV-SSL Certificate with the same Key Pair. Such a request must be made to the CA, and is made electronically via a digitally established relationship between the CA server and ACME client on the machine and based on the Key Pair in the original Certificate.

3.3.1 *Identification and Authentication for Rekey Requests*

Rekey is not available as per the ISRG CP.

3.3.2 *Certificate Renewal*

As long as an Subscriber's Certificate has not expired, been revoked, or suspended (for Administrative Certificates only), the Subscriber or the machine with the DV-SSL Certificate can request Issuance of a new Certificate with the same Key Pair within three months prior to the end of the Certificate's Validity Period and the CA will rely on the information on file that was initially verified. If any information has changed in the Certificate (e.g. last name, any additional FQDNs listed under the SAN extension, etc.) the identity must be re-established through the initial identity-proofing process specified for the required Certificate in Section 3.2.

3.3.3 *Certificate Update*

For all update requests, identity must be re-established through the initial identity-proofing process specified in Section 3.2 for the corresponding Certificate type.

3.3.4 *I&A for Renewal After Revocation*

Revoked or expired DV-SSL Certificates and Administrative Certificates cannot be renewed or updated. Applicants without a valid DV-SSL or Administrative Certificate will be re-authenticated by the CA through a new application according to the corresponding Certificate based on the I&A processes listed in Section 3.2., the same as with an initial Applicant registration, and will be issued a new Certificate.

3.4 I&A for Revocation and Suspension Requests

Revocation requests authenticated on the basis of the Certificate's associated Key Pair through the ACME client for DV-SSL Certificates or by digital authentication of the Administrative Certificate are always accepted as valid. Other Revocation or suspension request authentication mechanisms may be used as well, including a request in writing through an e-mail posted on the ISRG website.. These authentication mechanisms balance the need to prevent unauthorized Revocation or suspension requests against the need to quickly revoke or suspend Certificates. These mechanisms are explained is Section 4.9.

Suspension of a DV-SSL Certificate is not permitted as per the requirements listed in the CA/B Forum Baseline Requirements Section 13.2.7. Therefore requests for suspension of a DV-SSL Certificate will not be accepted and the requestor will receive instruction to revoke the DV-SSL Certificate.

CPS

4 Certificate Life Cycle Operational Requirements

4.1 Certificate Application

This CPS used the following procedures for satisfying the security requirements of this PKI. The following steps are required when applying for a Certificate:

1. Establish identity of subject (per Section 3.2 for DV-SSL Certificates and Administrative Certificates);
2. Obtain a Key Pair for each Certificate required;
3. Prove to the CA that the Public Key forms a functioning Key Pair with the Private Key held by the Applicant; and

Prior to the issuance of a Certificate, the CA obtains the following documentation from the Applicant:

1. A certificate request, which may be electronic; and
2. An executed Subscriber or Terms of Use Agreement that is electronic.

The CA will obtain any additional documentation that it determines necessary to meet the requirements of the CP and this CPS.

Prior to the issuance of a Certificate, the CA obtains from the Applicant a certificate request in a form prescribed by the CA and that complies with the CP, this CPS, and the CA/B Forum Baseline Requirements. One certificate request can suffice for multiple Certificates to be issued to the same Applicant, subject to the aging and updating requirement in the CA/B Forum Baseline Requirements, provided that each Certificate is supported by a valid, current certificate request signed by the appropriate Applicant Representative on behalf of the Applicant. The certificate request is made, submitted and/or signed electronically.

The certificate request is required to contain a request from, or on behalf of, the Applicant for the issuance of a Certificate, and a certification by, or on behalf of, the Applicant that all of the information contained therein is correct.

4.1.1 Application Initiation

A Certificate application may be submitted by:

DV SSL Certificates
The application process is initiated by an individual Applicant who:

- Can demonstrate control over the device; and
- Can demonstrate control over the domain.

Administrative Certificates
The application process is initiated by an Applicant who:

- Is an employee of the CA who has been appointed as a CA Administrator; and
- Is verified as an affiliate of the CA by a separate affiliated individual (e.g. H.R. employee or other appointed individual in the CA organization).

4.1.1.1 Information Collection

During the application phase of registration, Applicant information is collected in one of the following ways based on the type of Certificate requested:

DV-SSL Certificates:

- Individual Applicants who provide registration information via the ACME client process over a server-authenticated SSL/TLS secured session hosted by the CA.

Administrative Certificates

- An employee of the CA who has been appointed as a CA Administrator or another relevant trusted role requiring an Administrative Certificate by one of the CA's management authorities.

All Applicants must provide the following information:

DV-SSL Certificates:

- Domain Name(s); and
- RSA PKCS#10 Certificate signing request (CSR).

Administrative Certificates

- Applicant's name;
- Applicant's email address;
- Applicant's job title;
- Applicant's phone Number; and
- An Account Password (see below additional details).

For Administrative Certificates, an Account Password selected by the Applicant and consisting of at least 8 characters, which will be utilized for user authentication along with Activation Data provided in an out-of-band method (for use during Certificate retrieval). As part of the online application process only, the Applicant is required to create three questions and secret answers, which together serve as a mechanism to reset the Account Password in case the Applicant forgets it before he or she is able to download the Certificate. This process is activated by the Subscriber providing his or her Activation Code, which was received initially in an e-mail when the account was first opened and by clicking on an Account Password reset uniform resource locator (URL). A one-time-code and specified URL is sent to the email address on file for the Applicant. After receiving the email, the Applicant must enter both the Activation Code and the one-time-code at the specified URL in order to gain access to the three questions that were selected during registration. The three questions were selected by the Applicant from a list of ten questions that were randomly selected from a pool of password-reset questions. If the answers are correct, the Subscriber is allowed to change the Account Password, which is immediately hashed and stored in the CA system for further use.

4.1.2 Enrollment Process and Responsibilities

The CA has designed enrollment processes that facilitate the submission of registration information from the Applicant to the CA. Options include but are not limited to: Direct submission over the ACME client to the server for DV-SSL Certificates; and for Administrative Certificates include secure submission directly to the CA via encrypted electronic delivery, or physical delivery of forms to the CA.

4.1.2.1 Applicant Education and Disclosure

At the time of application for a DV-SSL Certificate or Administrative Certificate, Applicants are advised of the advantages and potential risks associated with using their respective Certificates and Subscribers are provided with information regarding the use of Private Keys and Digital Signatures (with regard to an Administrative Certificate). The CA uses two main mechanisms to educate and disclose the information: The CA's main website, which enable access to the CP and this CPS; and the Certificate Agreement that is provided prior and during the enrollment process.

4.1.2.2 CA Secure Registration Messaging Protocol

An RA may enter into an agreement with the CA to host its own registration process and interface with the CA or CMA's Certificate manufacturing architecture via the CA's secure registration messaging protocol for the creation, delivery and management of Certificates. The RA will be contractually bound to adhere to

the applicable provisions of the CP and this CPS and to provide registration services in strict accordance with the practices set forth in Sections 3 and 4.

4.2 Certificate Application Processing

An Applicant for a DV-SSL Certificate or Administrative Certificate completes a Certificate application and provides requested information in a form prescribed by this CPS and corresponding CP.

Information in the Certificate application is verified as accurate before Certificates are issued as specified in Section 3.2.

4.2.1 Performing Identification and Authentication (I&A) Functions

For DV-SSL Certificates and for Administrative Certificates issued for devices, the CA validates the Applicant's and machine's control over the device and domain name for which a Certificate is requested, using processes that are consistent with the relevant CA/B Forum Baseline Requirements. For domain ownership, the validation consists of comparison of the Applicant's submitted information through the ACME client with the information the CA server is able to verify.

The I&A information for an Applicant or current Subscriber is collected electronically (or manually when requested) and processed electronically through server responses or examined by the RAs operating for the CA identified in Section 1.3.3. Such information is verified according to the I&A processes described in Section 3.2 and 3.3.

The CA checks for relevant CAA records prior to issuing certificates. The CA acts in accordance with CAA records if present.

4.2.2 Approval or Rejection of Certificate Applications

The CA approves an Applicant's Certificate application or request from the ACME client for a DV-SSL Certificate if the I&A processes described in Section 3.2 and 3.3 are completed successfully.

Certificate applications will be approved or rejected within 30 days of application receipt by the CA, or such other period that is compliant with the CA/B Forum Baseline Requirements.

The CA terminates an Applicant registration process if:

- The Applicant's identity (for Administrative Certificate) or demonstrated control of the domain as per the challenge presented to the ACME client, by the CA server (for DV-SSL Certificates) cannot be established in accordance with identity proofing requirements;
- Not all forms necessary to establish I&A for Administrative Certificates are submitted on a timely basis;
- For DV-SSL Certificates, the Applicant is unable to establish or provide verifiable evidence to that they are authorized to request the Certificate for the FQDN from the Domain Administrator in a form prescribed by the CA/B Forum; and/or
- The CA is unable to verify or process the Applicant's payment information (where payment information is required).

Upon application rejection, the CA provides information to the Certificate Applicant:

- Indicating a failure of identity proofing process; and
- Informing the Applicant of the process necessary to resume processing of the application.

Upon application rejection, the CA records applicable transaction data including the following:

- Applicant's name as it appears in the Applicant's request for a Certificate;
- Method of application (e.g., online, in-person) for each data element accepted for proofing, including electronic forms;
- Name of document presented for identity proofing including the name of its issuing authority, the date of issuance, and the date of expiration (not required for DV-SSL Certificates);
- All fields verified;
- Source of verification (i.e., which databases used for cross-checks);
- Method of verification (e.g., online, in-person);
- Date/time of verification;
- Names of entities providing identification services, including contractors, subcontractors, if any;
- Fields that failed verification;
- Status of current registration process (suspended or ended);
- All identity proofing data;
- All associated error messages and codes; and
- Date/time of process completion;

For DV-SSL Certificate requests in addition to the majority of the list above (noted when not applicable), the rejection transaction record will include:

- The FQDN(s) requested;
- Whether or not the IP address was valid;
- Whether or not the ccTLD was accurate, if Country is included in the Subject; and
- Whether or not the Domain Name was on the denied or high risk request lists.

4.2.3 *Time To Process Certificate Applications*

No stipulation.

4.3 Certificate Issuance

After all application and approval processes identified in the CP and this CPS are completed, the CA will:

- Issue the requested DV-SSL Certificate;
- Notify the Applicant of the DV-SSL Certificate's issuance; and
- Make the DV-SSL Certificate available to the Applicant for Acceptance.

The procedures for notifying the Applicant of the DV-SSL Certificate's issuance, and the procedure used to deliver or make the Certificate available to the Applicant is secure and confidential, and complies with the applicable portions of the CA/B Forum Baseline Requirements.

4.3.1 *CA Actions during Certificate Issuance*

Issuance of a Certificate occurs once an application for that Certificate has been approved by an RA for Administrative Certificates or an authorization from the CA server for a DV-SSL Certificate.

For an Administrative Certificate, the CA electronically delivers the unique Activation Code, along with instructions, through an out-of-band process to the Applicant, and the Applicant initiates a web-based retrieval process. Once the Certificate is retrieved successfully, the Applicant becomes a Subscriber. The terms are combined below as the Issuance process is described in more detail.

For each Certificate Issuance to an Applicant/Subscriber for an Administrative Certificate, the following occurs during the same server-authenticated SSL/TLS session:

1. The Applicant/Subscriber initiates the Certificate retrieval by accessing via a browser a URL (Retrieval URL) provided within their retrieval kit. In the resulting web session, the CA or RA system authenticates itself to the Subscriber and encrypts all communication utilizing a server-authenticated

SSL/TLS encrypted channel verifiable by a Certificate issued by a distinct Certificate Authority natively trusted in browsers through its Cross-Certified Entity relationship.

2. The Applicant/Subscriber authenticates himself or herself to the web server used in the retrieval process by supplying the Activation Code delivered within the retrieval kit together with the Account Password selected by the Applicant/ Subscriber during application process described in Section 4.1. This two-factor authentication is required for all Certificate retrievals by an Applicant/Subscriber from the CA.

3. Upon authentication of the Applicant/Subscriber to the Retrieval URI and verification of 'approved' status of the Applicant/Subscriber's Certificate application, the system initiates Key generation for Signing Keys (invoked locally on the Applicant/Subscriber's machine using an ActiveX control and MS CAPI, Browser Add-on, or equivalent). The resulting public Signing Key is encapsulated in a Certificate request in the form prescribed by RSA PKCS#10.

4. The PKCS#10 Certificate request for the Signing Certificate is submitted to the CA for Certificate generation. The information in the Subscriber database previously verified during the identity proofing process, as approved for Certificate Issuance, overrides the Subject DN information submitted in the PKCS#10. However, the binding between the Public Key within the PKCS#10 Certificate request and the Private Key is maintained—the signature on the PKCS#10 Certificate request is verified by the CA to ensure that it was signed with the corresponding Private Key prior to building the Certificate.

5. Encryption Key Pair and Encryption Certificate generation occur using the same verified information contained in the Subscriber database. The Encryption Key and Certificate are generated by the CA system and they are downloaded to the Cryptomodule using an RSA PKCS#12 format protected by a strong password. This process happens in the background and it is transparent to the Applicant/Subscriber using the same ActiveX control and MS CAPI, Browser Add-on, or equivalent mentioned in step 3 above.

6. The CA delivers the Applicant/Subscriber's Certificates to the Certificate store (in either a browser or a hardware Cryptomodule for Administrative Certificates) using a format adhering to RSA PKCS #7 for the Signing Certificate and PKCS #12 for the Encryption Key Pair and Certificate.

7. In addition, the CA delivers the Root CA Certificate and the Certificate in RSA PKCS #7 format with instructions to download them into the Subscriber's Certificate store. On supported platforms, the installation of both the Root and Certificates are automated via a web interface.

8. Installation of the Subscriber's Signing Certificate and Root CA Certificate is confirmed by initiating a client-authenticated SSL/TLS session between the CA's Retrieval URL, and the Subscriber's client platform. The now Subscriber is instructed to select his or her Signing Certificate for authentication. The process of mutual authentication ensures that the Certificate has been installed successfully and that cryptographic integrity exists between the Subscriber's Signing, the Intermediate and the Root CA Certificates.

9. Upon successful installation of the Subscriber's Certificates, both Signing and Encryption Certificates will be published in the CA's Repository.

For each Certificate Issuance to an Applicant/Subscriber of a DV-SSL Certificate, the following occurs during a server-authenticated SSL/TLS session while operating within the ACME client:

1. The Applicant/Subscriber initiates the Certificate retrieval by triggering request and retrieval process through the ACME client which has previously established an exchange of authorization tokens. . In the resulting web session, the CA server authenticates itself to the Subscriber, and vice versa, with the authorization tokens. The communication is encrypted utilizing a server-authenticated SSL/TLS encrypted channel verifiable by a Certificate issued by a trusted authority..

2. The Applicant/Subscriber authenticates himself or herself to the CA server through the ACME client used in the retrieval process. The ACME client communicates with the CA to receive a series of challenges to determine authenticity of the DV-SSL Certificate request for the specified domains as described in section 4.1. Upon successfully completing the challenges, the DV-SSL Certificate is authorized by the CA server, retrieved, and installed by the Subscriber's system. For additional exchanges, the CA server utilizes an authorization token which will be used to identify the ACME client to the CA server. This two-factor authentication is required for all Certificate retrievals by an Applicant/Subscriber from the CA.

(Note that the Applicant generates the Key Pair for the Device and submits the PKCS#10 Certificate request). The automated process will also verify the Public Key of a Device that is requested has less than 2048 bit encryption and if it uses a known weak Private Key. If either or both are automatically detected in the secure session, the Applicant will be required to correct the determined issue before the DV-SSL Certificate can be issued.

The Certificate Issuance process described in this Section will ensure that this CPS is in compliance with the CP.

- The CA has verified the source of the Certificate request;
- The CA has confirmed the authenticity and authority of the source of information contained within the Subscriber's Certificates;
- The CA has built and signed the Subscriber's Certificates in a secure manner.
- The CA has delivered the Subscriber's Certificates, the necessary subordinate and Root CA Certificates to the Subscriber; and
- The CA has published the Subscriber's Certificates to the CA's Repository.

Upon Issuance of a DV-SSL Certificate or Administrative Certificate, the CA warrants to all Program Participants that:

- Upon receiving a request for a Certificate, the CA has managed the Certificate in accordance with the requirements of the CP;
- The CA has complied with all requirements in the CP when identifying the Subscriber and issuing the Certificate;
- There are no misrepresentations of fact in the Certificate known to the CA and the CA has verified the information in the Certificate in accordance with Section 3.2;
- Information provided by the Subscriber for inclusion in the Certificate has been accurately transcribed to the Certificate; and
- The Certificate meets the material requirements of the CP.

For DV-SSL Certificates, the Issuance of a Certificate also verifies:

- The Subscriber has the right to use the Domain Name(s) at the time of application and I&A;
- The Subscriber was authorized to obtain that Certificate from the Domain Name Administrator at the time of application and I&A;
- The information included on the Certificate is accurate at the time of application and I&A;
- The information included on the Certificate is not misleading ;
- The Subscriber has signed and is bound by the Certificate Agreement;
- The CA will maintain a publicly accessible Repository for verification of the status of the DV-SSL Certificate; and
- The CA will revoke the DV-SSL Certificate for any of the reasons listed in Section 4.9.

These warranties are articulated in the Certificate Agreement provided to the Applicant/Subscriber during the registration process.

Alternative methods for Issuance of Certificates are not implemented at this time.

Prior to the issuance of a Certificate, The CA obtains, for the express benefit of the CA and the Certificate Beneficiaries, either:

1. The Applicant's agreement to the Subscriber Agreement with the CA, or
2. The Applicant's agreement to the Terms of Use agreement.

The CA implements a process to ensure that each Subscriber or Terms of Use Agreement is legally enforceable against the Applicant. In either case, the Agreement must apply to the Certificate to be issued pursuant to the certificate request. The CA may use an electronic or "click-through" Agreement provided that the CA has determined that such agreements are legally enforceable. A separate Agreement is used for each certificate request, or a single Agreement may be used to cover multiple future certificate requests and the resulting Certificates, so long as each Certificate that The CA issues to the Applicant is clearly covered by that Subscriber or Terms of Use Agreement.

4.3.2 *Notification to Applicant of Certificate Issuance*

Upon successful completion of the Applicant I&A process explained in Section 3.2.2, and prior to Certificate Issuance explained in Section 4.3.1, the CA notifies the Applicant about the approval of the Certificate.

For Administrative Certificates, notifications are sent to the Applicant's e-mail address containing enough information to guide the Applicant through the Issuance process. Information may include a Uniform Resource Locator (URL), an Activation Code (i.e., a mutually shared secret) and basic instructions. Alternatively, the Activation Code may be delivered to a verified phone or cellular phone number that is associated with the Applicant while the retrieval URL is delivered in-band via email.

For DV-SSL Certificates, notification is exchanged between the ACME client installed on the Applicant's machine and the CA server. Notification of Certificate Issuance to others are effectuated by publication of the DV-SSL Certificate in a recognized Repository.

4.4 Certificate Acceptance

At the time of application for a Certificate, the CA or RA requires the Applicant to sign the Certificate Agreement. The Certificate Agreement calls for the Applicant to perform his or her responsibilities under Section 9.5.14 of the CP and this CPS in applying for, receiving, and using the Certificate. The Applicant is also required to request Revocation when appropriate. At this point, the Applicant is a Subscriber, and is so designated in the following sections.

4.4.1 *Conduct Constituting Certificate Acceptance*

The following conduct constitutes certificate acceptance:

- Downloading a Certificate or installing a Certificate from a message attaching it; or
- Failure of the Subscriber to object to the Certificate or its content.

By Accepting a DV-SSL Certificate or Administrative Certificate, the Applicant/Subscriber warrants that all of the information provided by it and included in the Certificate, and all representations made by the Applicant as part of the application and I&A process, are true and not misleading.

4.4.2 *Publication of the Certificate by the Authorized CA*

Pursuant to Section 2.2.1, Certificates are published in the Repository upon Issuance by the CA and CSA. The Repository is publicly available.

4.4.3 *Notification of Certificate Issuance by the Authorized CA to Other Entities*

No stipulation.

4.5 Key Pair and Certificate Usage

DV-SSL Certificates and Administrative Certificates may not be used for purposes counter to the principles and applications outlined in the CP and this CPS.

4.5.1 Subscriber Private Key and Certificate Usage

Through a combination of online processes, including registration and retrieval; and printed or online forms, including the Certificate Agreement, each Applicant for a DV-SSL Certificate and Administrative Certificate:

- Provides complete and accurate responses to all requests for information made by the CA (or RA) during the Applicant/Subscriber registration, Certificate application, and I&A processes;
- Generates a Key Pair using a reasonably trustworthy system, and take reasonable precautions to prevent any compromise, modification, loss, disclosure, or unauthorized use of the Private Key;
- Upon Issuance of a Certificate naming the Applicant/Subscriber as the holder of the Certificate, reviews the Certificate to ensure that all information included in it is accurate, and to accept or reject the Certificate per conduct listed in Section 5.4.1;
- Promises to protect a Private Keys at all times, in accordance with the applicable Certificate Agreement, this CPS, the CP and any other obligations that the Subscriber may otherwise have;
- Uses the Certificate and the corresponding Private Key exclusively for purposes authorized by the CP and only in a manner consistent with the CP;
- Instructs the CA (or an RA) to revoke or request a Revocation of the Certificate promptly upon any actual or suspected loss, disclosure, or other compromise of the Private Key, or, in the case of an Administrative Certificate, whenever the employee is no longer affiliated with the CA; and
- Responds as required to notices issued by the CA.

Subscribers who receive Certificates from the CA assert that they will comply with these requirements as well as those in the CP by either signing the Certificate Agreement online or in paper copy; or, by undergoing a full registration process prior to receiving the Certificate. Additional information concerning the rights and obligations of Subscribers may be found in Sections 9.5 of this CPS.

Key usage is discussed below in Section 6.1.4.

Subscribers are instructed to protect their private keys from unauthorized use and discontinues use of the Private Key following expiration or revocation of the Certificate. Parties other than the Subscriber will not archive the Subscriber Private Key as set forth in Section 4.12.

4.5.2 Relying Party Public Key and Certificate Usage

Relying Parties must evaluate the environment and the associated threats and vulnerabilities and determine the level of risk they are willing to accept based on the sensitivity or significance of the information. This evaluation is done by each Relying Party for each application and is not controlled by the CP or this CPS. Relying Parties who rely on stale CRLs do so at their own risk. See Section 4.9.

Parties who rely upon the Certificates issued under the CP or this CPS should preserve original signed data, the applications necessary to read and process that data, and the cryptographic applications needed to verify the Digital Signatures on that data for as long as it may be necessary to verify the signature on that data.

Assuming that the use of the Certificate is appropriate, Relying Parties use software that is compliant with X.509 and applicable IET PKIX standards. Such operations include identifying a Certificate Chain and verifying the digital signatures on all Certificates in the Certificate Chain. The CA and CSA specify the

mechanism(s) used to determine the validity of a Certificate (e.g., CRL or OCSP), and acquire, process, and use this information in accordance with their obligations as Relying Parties.

4.6 Certificate Renewal

This process will consist of issuing a new Certificate with a new validity period and serial number while retaining all other information in the original Certificate, including the Public Key.. A Certificate may be renewed if the Key Pair has not reached the end of its validity, the Private Key has not been compromised, the Certificate information and attributes are correct. The old Certificate need not be revoked, but will not be further renewed.

After Certificate renewal, the old Certificate is not revoked but the CA may or may not revoke it.

4.6.1 Circumstance for Certificate Renewal

A Certificate may be renewed if the Key Pair has not reached the end of its validity, the Private Key has not been compromised, and the Certificate information and attributes are correct. Thus, the CA may choose to implement a three-year re-key period with an initial issue and two annual renewals before Renewal is required. The old Certificate need not be revoked, but must not be further renewed or updated.

4.6.2 Who May Request Renewal

Only the Subscriber can request a new Certificate with the same Key Pair. For DV-SSL Certificates, this is done electronically or by other means in which the Subscriber's identity, ownership or control over the domain, and ownership or control over the device can be verified. For Administrative Certificates, this is done electronically or by other means in which the Subscriber's identity and affiliation with the CA is verified.

CSAs are operated within the CA facilities and are managed by the CA Administrator who requests that the OCSP Responder Certificate is renewed.

4.6.3 Processing Certificate Renewal Requests

Prior to the expiration date, the CS's or the RA's system will notify via email when 20% of the certificate's lifetime remains if a contact email address was provided.

In the Certificate management online interface or the ACME client the Subscriber:

- Checks to ensure that no information in the Certificate has changed;
- Reviews and accepts the terms of the Certificate Agreement

For DV-SSL Certificates, the Subscriber will follow the same steps to check the content for the DV-SSL Certificate is still accurate and valid. If the Subscriber indicates that any of the contents of the DV-SSL Certificate have changed during the Renewal (e.g. the FQDN(s) or other information included in the Certificate Profile), the CA will request verification information in accordance with the verification processes set forth in Section 3.2 before the Renewal process can be completed.

The CA will authenticate the Subscriber by using the identity proofing processes required for the corresponding Certificate in accordance with Section 3.2. Once the Subscriber is authenticated, the CA will then follow the Certificate Issuance process described in Section 4.3.

For CSAs, prior to expiration of each OCSP Responder Certificate, the OCSP Responder signing Key is re-signed during a Certificate renewal ceremony performed in the Secure Room under 2-person control where the ceremony is scripted, witnessed and video-recorded.

4.6.4 Notification of New Certificate Issuance to Subscribers

For notification sent to Subscribers, see Section 4.3.2.

The CA Administrator is present and needs no notice of OCSP Responder Certificate Issuance.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

For conduct accepted by Subscribers, see Section 4.4.1.

The CA Administrator accepts the OCSP Responder Certificate by allowing it to be published in the Repository and installing the newly issued Certificate to the OCSP Responder to be sent out with the responses.

4.6.6 Publication of the Renewal Certificate by the Authorized CA

For publication of the renewed Certificates for Subscribers, see Section 4.4.2.

The OCSP Responder Certificate is published in the Repository.

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

For relevance to Subscribers, see Section 4.4.3.

For the OCSP Responder Certificate, o other entities are notified of Certificate Issuance by the CA.

4.7 Certificate Re-key

Re-keying a Certificate consists of creating a new Certificate with a different Public Key (and serial number) while retaining the remaining content of the old Certificate that describes the subject and assigning a new validity period to such Certificate. The new Certificate may be assigned different Key identifiers, specify a different CRL distribution point, and/or be signed with a different Key.

Re-key is not performed under this program.

4.7.1 Circumstances for Certificate Rekey

Re-key is not performed under this program.

4.7.2 Who May Request Certificate of a New Public Key

Re-key is not performed under this program.

4.7.3 Processing Certificate Rekey Requests

Re-key is not performed under this program.

4.7.4 Notification of New Certificate Issuance to Subscriber

Re-key is not performed under this program.

4.7.5 Conduct Constituting Acceptance of a Rekeyed Certificate

Re-key is not performed under this program.

4.7.6 Publication of the Rekeyed Certificate by the Authorized CA

Re-key is not performed under this program.

4.7.7 *Notification of Certificate Issuance by the Authorized CA to Other Entities*

Re-key is not performed under this program

4.8 Modification

Certificate modification consists of creating new Certificates with subject information that may differ from the old Certificate.

Replacement, is a form of modification available for all Certificate types with the exception of DV-SSL Certificates. For this type of modification all original information is kept and the new Certificate has a new associated Key but retains the same expiration date.

When other information in the Certificate's subject field changes (e.g., last name, CA affiliation), Certificate modification is not used. Instead, a new application for a Certificate is required.

Root CA Certificate and Subordinate CA Certificate modification consists of creating a new Certificate where information can be changed including different fields such as subject, Certificate policies, CRL distribution point and authority information access. The associated Public Key and original expiration date are maintained.

4.8.1 *Circumstances for Certificate Modification*

The CA allows the modification of only valid Certificates (i.e., Certificate is neither revoked nor expired). The new Certificate, with a new Key Pair, is issued with the same expiration date as the original Certificate.

In the case of Certificate replacement the CA allows the replacement of Certificates when the Subscriber's Private Key has not been compromised and there are no changes to the Certificate. Note that in the case where a non-escrowed Private Key is lost or damaged, the Certificate cannot be replaced or recovered and the identity of the Subscriber must be established through the initial registration process described in Section 3.2.

A Root and Subordinate CAs Certificates may be modified if approved in writing by the PMA.

4.8.2 *Who May Request Certificate Modification*

Subscribers of Administrative Certificates with valid Certificates are entitled to request email modification and replacements. See Section 3.2.3 (Identification and Authentication) and Section 4.1.1 (Who can submit a Certificate application) for specific details.

The CA may request a modification of its own Root and Subordinate CA Certificates.

4.8.3 *Processing Certificate Modification Requests*

Upon receiving an authenticated request to replace a damaged or lost Certificate from a Subscriber for an Administrative Certificate, the CA replaces the Certificate and records the following Certificate replacement transaction data:

(a) Certificate serial number;
(b) Certificate common name;
(c) Subject Alternative name;
(d) Certificate policy OID;
(e) Date/time of completion of replacement process; and
(f) All associated replacement data.

Modification of a Root Certificate or Subordinate CA Certificate requires that a request is provided in written to the PMA, to address interoperability concerns. Proposals to modify CA Certificates are processed as follows:

A survey of the applications deployed in the PKI and an analysis of whether the proposed modification creates interoperability concerns are performed. Any concerns raised by any PMA member or other designated relevant third party should be addressed by the group managing the CA equipment. When there are no remaining concerns, the Root or Subordinate CA Certificate with the requested modifications is issued. The old CA Certificate will not be revoked unless all issues related to the transition from the old CA Certificate to the new CA Certificate have been resolved.

4.8.4 Notification of New Certificate Issuance to Subscriber

See Section 4.3.2.

4.8.5 Conduct Constituting Acceptance of a Modified Certificate

See Section 4.4.1.

4.8.6 Publication of the Modified Certificate by the Authorized CA

See Section 4.4.2.

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

See Section 4.4.3.

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for Revocation

4.9.1.1 Permissive Revocation

A Subscriber can request revocation of his, her or its Certificate at any time for any reason (i.e., the Subscriber requests in writing that the CA revoke the Certificate). The CA may request revocation of an Administrative Certificate for an individual at any time for any reason. The CA may revoke a Certificate for any reason, including without limitation the failure of the Subscriber to meet its obligations under the CP, this CPS, or any other agreement, regulation, or law applicable to the Certificate that may be in force, including violating the provisions of the CA/B Forum Baseline Requirements. This includes revoking a Certificate when the CA suspects that a compromise of the corresponding Private Key has occurred.

The CA maintains a continuous 24x7 ability to accept and respond to revocation requests and related inquiries.

4.9.1.2 Required Revocation

A Subscriber will promptly request revocation of a Certificate whenever:

1. Any of the information in the Certificate changes or becomes obsolete;
2. The Subscriber notifies the CA that the original certificate request was not authorized and does not retroactively grant authorization;
3. The Private Key, or the media holding the Private Key, associated with the Certificate is known or suspected of being compromised.

The CA will revoke a Certificate whenever:

1. The Subscriber has failed to meet its material obligations under the CP, any applicable CPS, or any other agreement, regulation, or law that may be in force that is applicable to the Certificate, including applicable provisions of the CA/B Forum Baseline Requirements;
2. The CA obtains evidence that the Subscriber's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise or no longer complies with the requirements of Appendix A in the CA/B Forum Baseline Requirements;
3. The CA is made aware that a Subscriber has violated one or more of its material obligations under the Subscriber or Terms of Use Agreement;
4. The CA is made aware of any circumstance indicating that use of a FQDN or IP address 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);
5. The CA is made aware of a material change in the information contained in the Certificate;
6. The CA determines that any of the information appearing in the Certificate is inaccurate or misleading;
7. The CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Certificate;
8. The CA's right to issue Certificates under the CA/B Forum Baseline Requirements expires or is revoked or terminated, unless the CA has made arrangements to continue maintaining the OCSP Repository;
9. The CA is made aware of a possible compromise of the Private Key of the Subordinate CA used for issuing the Certificate;
10. Revocation is required by the CP, and/or the corresponding CPS;
11. The technical content or format of the Certificate presents an unacceptable risk to Application Software Suppliers or Relying Parties as determined by the CA or the CA/B Forum;
12. The CA determines that the Certificate was not properly issued in accordance with the CP and/or any applicable CPS; or
13. Knowledge or reasonable suspicion of misuse is obtained.

4.9.2 *Who Can Request Revocation*

The only persons permitted to request Revocation of a Certificate issued pursuant to the CP and this CPS are the Subscribers, the CA, or the RA.

In addition, an individual who is not the Subscriber may request revocation of a DV-SSL Certificate if the individual can demonstrate ownership or control over the device, and ownership or control over the domain. Likewise, an individual who is not the Subscriber can request revocation of an Administrative Certificate if the individual can demonstrate affiliation with the CA in a position of authority or responsibility for either the individual or the use of the Administrative Certificate.

The CA provide Subscribers, Relying Parties, Application Software Suppliers, and other third parties with clear instructions for reporting suspected Private Key Compromise, Certificate misuse, or other types of fraud, compromise, misuse, inappropriate conduct, or any other matter related to Certificates. The CA publicly discloses the instructions online at the ISRG website https://letsencrypt.org/.

4.9.3 *Procedure for Revocation Request*

DV-SSL Certificates can by revoked by requesting Revocation using an ACME client. Revocation requests via ACME must be signed be either the Private Key associated with the Certificate to be revoked, or the Subscriber's ACME account key.

If a Subscriber does not have access to the Private Key associated with the Certificate to be revoked or the relevant AMCE account key, the Subscriber may re-authenticate (successfully respond to challenges) for the domain and then request revocation using the new ACME account key associated with the domain to be revoked.

DV-SSL Certificates can also be revoked after a conclusive investigation of a Certificate, conducted in accordance with section 4.9.13, that is initiated by a report received via email. Instructions for filing such a report can be found in section 4.9.13.

The CA or RA, when the request is submitted via email, will document the reason for the request and archive this documentation.

If the Cryptomodule cannot be obtained from a Subscriber for an Administrative Certificate, then the Certificate(s) will be immediately revoked, expressing the reason code as "Key compromise." Promptly following Revocation, the CA updates the Certificate status in the Repository and updates the CRL. Alternatively, the CA may opt for not collecting any Cryptomodule due to logistical difficulties (e.g., Subscriber is terminated under unfriendly conditions, Subscriber is in a remote location, etc.) and instead always request Revocation of the Certificates as if the Cryptomodule was not obtained from the Subscriber. In these cases, the Revocation request will always result in a "Key compromise" code.

Revocation of CA, CSA Certificate
The CA will revoke a CA or CSA Certificate it has issued if the Private Key corresponding to the Public Key in the Certificate has been or is suspected to have been compromised. In any event, prior to taking such action, the highest level CA manager available will convene a meeting of management representatives (including representatives of the affected RAs and the PMA) to assess the situation and make an appropriate decision concerning a course of action.

General Guidance for All Situations not specifically addressed
Persons authenticating Revocation requests must balance the risk of an unauthorized request and the potential harm caused by revoking the Certificate against the harm caused by not revoking the Certificate.

Employees of the CA and RA are trained to expedite authentication and authorization checks on Revocation requests and to affect them on the CA as soon as possible.

4.9.4 *Revocation Request Grace Period*

There is no grace period for a Revocation request. All Participants are required to communicate a Certificate Revocation request as soon as it comes to their attention.

4.9.5 *Time within Which Authorized CA Must Process the Revocation Request*

DV-SSL Certificates are revoked within twenty-four hours of receiving a Certificate Revocation request.

Subordinate CA Certificates are revoked within seven days of receiving a Certificate Revocation request.

4.9.6 *Revocation Checking Requirements for Relying Parties*

Use of revoked Certificates could have damaging or catastrophic consequences. The matter of how often new Revocation data should be obtained is a determination to be made by the Relying Party, considering the risk, responsibility, and consequences for using a Certificate whose Revocation status cannot be guaranteed. If it is temporarily infeasible to obtain Revocation information, then the Relying Party must either reject use of the Certificate, or make an informed decision to accept the risk, responsibility, and consequences for using a Certificate whose authenticity cannot be guaranteed to the standards of the CP and this CPS.

The CA shall have no liability if a Relying Party does not obtain an OCSP response indicating that the Certificate is valid or fails to check the most recent CRL for Certificate Revocation.

4.9.7 *CRL Issuance Frequency*

CRLs issued for the Root Certificate are issued every thirty days. CRLs will be issued even if there are no changes or updates to be made, to ensure timeliness of information. CRLs issued for the Root Certificate

last for thirty days. If there are circumstances under which the CA will post early updates the CA will ensure that superseded CRLs are removed from the directory system upon posting of the latest CRL.

When CRLs are used to distribute status information:

- They are issued periodically, even if there are no changes to be made, to ensure timeliness of information; and
- Superseded Certificate status information is removed from the Repository system upon posting of the latest Certificate status information.

No CRLs are issued for Subordinate CAs. Instead Certificate status is available through OCSP validation.

4.9.8 Maximum Latency of CRLs

The CA publishes a CRL within twenty four hours of authenticating a Revocation request. Each CRL is published no later than the time specified in the nextUpdate field of the previously issued CRL for the same scope.

4.9.9 Online Revocation/Status Checking Availability

The CSA supports OCSP and provides online Certificate status information in digitally signed OCSP Responses for Certificates issued by CAs that are indicated in OCSP Requests submitted by Relying Parties. The OCSP Responder provides the most recent information available from the CA system's database. OCSP responses may be batch-signed based on current database status, in which case responses will be updated every four days, and the value of the nextUpdate is seven days. For certificates that change status through revocation, a new OCSP response will be signed and made available as part of the revocation process.

The CSA service is mandatory and Certificates include a pointer to the OCSP responder in the Authority Information Access extension. The CSA service is provided via CA-delegated trust model OCSP as specified in RFC 6960.

Each OCSP Responder is issued a Certificate signed by the same subordinate CA Private Key that signed the Certificates that will be validated by the OCSP Responder.

4.9.10 Online Revocation Checking Requirements

Use of revoked Certificates could have damaging or catastrophic consequences. The matter of how often new Revocation data should be obtained is a determination to be made by the Relying Party, considering the risk, responsibility, and consequences for using a Certificate whose Revocation status cannot be guaranteed.

4.9.11 Other Forms of Revocation Advertisements Available

The CA does not support any other method for obtaining Certificate status information than those described in Sections 4.9.7 and 4.9.9. The CA reserves the right to make other forms of Revocation advertisement available to Relying Parties.

4.9.12 Special Requirements Related to Key Compromise

When a CMA Certificate or Subscriber's Certificate is revoked because of compromise, or suspected compromise, of a Private Key, the revocation information will be available as soon as possible. In the case of a Subordinate CA, this information will be available within 24 hours as specified in Section 4.9.9. Practices followed in the case of a CA Private Key compromised are explained in Section 5.7.3 Practices followed in the case of a Subscriber's Private Key compromised are explained in Section 4.9.3

4.9.13 Certificate Problem Reporting, Investigation, and Response

The CA provides Subscribers, Relying Parties, application software suppliers and other third parties with clear instructions and contact information for reporting suspected Private Key compromise, Certificate misuse, or other types of fraud, compromise, misuse, inappropriate conduct, or any other matter related to

Certificates. These instructions are available online at the CA's website in the repository at https://letsencrypt.org/repository/. This page lists an e-mail address to contact the CA during business hours and to ensure reporting will be received 24/7.

Once a report is received by email, a CA trusted employee will file a ticket for the report including the details provided by the contact. The CA trusted employee will provide the following information for the report when possible:

1) Account number;
2) Name and contact information of the Individual/Organization reporting the Certificate;
3) Subscriber, Organization, and domain name;
4) Nature of the issue (illegal activity, Private Key compromise, etc.); and
5) When the issue was discovered.

Upon creating a record of the contact the following considerations are assessed to determine the appropriate action:

1) The nature of the alleged problem;
2) The number of Certificate problem reports received about a particular Certificate or Subscriber;
3) The entity making the complaint (for examplea security professional with good evidence of private key compromise should carry more weight than a complaint from a consumer alleging that he/she didn't receive the good they ordered); and
4) Relevant legislation.

Upon review, ISRG will determine whether Revocation or other action is warranted. If it is determined that Revocation is necessary, an official request will be authorized by the CA trusted employee to execute the specified action accordingly. When deemed necessary based on the content of the report and the findings by management, the CA will forward the complaint to law enforcement.

All email contact associated with the case must be saved and documented by the CA trusted employee and the CA.

4.9.14 *Circumstances for Suspension*

Suspension is not available for any Certificates.

4.9.15 *Who Can Request Suspension*

Suspension is not available for any Certificates.

4.9.16 *Procedures for Suspension Request*

Suspension is not available for any Certificates.

4.9.17 *Limits on Suspension Period*

No stipulation.

4.10 Certificate Status Services

The CA uses OCSP and CRLs to distribute status information. Specifics on how to obtain status information via CRL or OCSP are found in Sections 7.2 and 7.3 mainly.

4.10.1 Operational Characteristics

The CA validates the status of the Certificate indicated in a Certificate validation request message in accordance with RFC 6960.

4.10.2 Service Availability

The CA and CSA update information provided via an Online Certificate Status Protocol at least every four days. OCSP responses from this service have a maximum expiration time of seven days.

The Issued CA and CSA operate and maintain its OCSP capability with resources sufficient to provide a response time of ten seconds or less under normal operating conditions.

Revocation entries on an OCSP Response are not be removed until after the Expiry Date of the revoked Certificate.

The Repository does not include entries that indicate that a Certificate is suspended.

See Section 2.2.1.

4.10.3 Optional Features

No stipulation.

4.11 End of Subscription

4.11.1 Subscribers

A Subscriber may terminate its subscription to Certificate services by allowing the term of a Certificate to expire without Renewal.

Subscriber may also voluntarily revoke their Certificate as explained in Section 4.9.3. If a Subscriber terminates its Subscription during a Certificate's Validity Period, the Certificate is revoked.

Prior to the end of subscription, the CA or the RA will send the Subscriber notice of pending Certificate expiration, in the form of a renewal notification, when 20% of the certificate's lifetime remains, if a contact email address was provided.

4.12 Key Escrow and Recovery

4.12.1 Private Key Recovery

The CA does not provide the mechanisms (hardware, software, or procedural) that permit recovery of the Private Key of DV-SSL Certificates or Administrative Certificates.

4.12.2 Circumstances for Private Key Recovery

There are no circumstances for Private Key Recovery for Certificates because the Private Key is not held in escrow.

4.12.3 *Key Recovery Roles: Who Can Request Private Key Recovery*

There are no circumstances for Private Key Recovery for Certificates because the Private Key is not held in escrow.

4.12.4 *Procedure for Private Key Recovery Request*

4.12.4.1 *Automated Self-Recovery*

There are no circumstances for Private Key Recovery for Certificates because the Private Key is not held in escrow.

4.12.4.2 *Session Key Encapsulation and Recovery Policy and Practices*

There are no circumstances for Private Key Recovery for Certificates because the Private Key is not held in escrow.

5 Facility, Management, and Operational Controls

The CA and its associated RAs, CSAs, and Repositories maintain security controls to assure adequate security for all information processed, transmitted, or stored for the CA. This includes appropriate physical security controls to restrict access to the hardware and software (including the server, workstations, and any external cryptographic hardware modules or tokens) used in connection with providing CA services.

Adequate security means security commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of information. Systems and applications operate effectively and provide appropriate confidentiality, integrity, and availability.

No party may use any software, program, routine, query, device or manual process in an attempt to bypass security measures (including attempting to probe, scan or test vulnerabilities to breach security); access data the party is not authorized to access; interfere with the proper operation of the CA's systems (e.g., install or attempt to install malware); or overload, crash, or otherwise impose a disproportionately large load on the infrastructure supporting the CA's systems; except as part of a planned test authorized by the CA.

The CA, CSA, and RA equipment, including all Cryptomodules, are located in jurisdictions that have statutes against computer trespass and intrusion. In addition, US computer security legislation applies. Together, those laws generally forbid unauthorized use and access to CA computer equipment; however, legal advice should be obtained in specific cases.

For each system, an individual is the focal point for assuring that there is adequate security within the system, including ways to prevent, detect, and recover from security problems in those assigned security areas. The CA, CSA, and RA operations for Certificates are serviced by trusted personnel. All trusted personnel meet the requirements of the CP for Trusted Roles.

The CA has contracted with a third party (the "Contractor") for operation and management of its CA systems. The Contractor has extensive CA experience, has passed numerous WebTrust for CA audits, and has facilities and policies that meet the requirements of the CP and this CPS. Responsibility for facility, management, and operational controls remains with the CA.

5.1 Physical Controls

The CA, and all associated RAs, CMAs, and Repositories, provide appropriate physical security controls to restrict access to the hardware and software (including the server, workstations, and any external cryptographic hardware modules or tokens) used in connection with providing CA Services. Access to such hardware and software is limited to those personnel performing in a Trusted Role, as described in Section 5.2.1.

The CA implements a physical and environmental security program that addresses access controls, water exposure, fire safety, failure of supporting utilities, media storage, waste disposal, offsite backup capabilities, structural collapse, interception of data, and control of mobile and portable systems.

5.1.1 Site Location and Construction

The construction and location of the building housing the CA system has been designed to offer security protection mechanisms consistent with facilities used to house high value, sensitive information. The CA maintains both a primary facility and a disaster recovery site.

Primacy facility: The area in which the CA's primary datacenter resides is not prone to such environmental hazards as tornadoes, earthquakes, hurricanes, wildfires, etc. The building that houses the datacenter has been designed for environmental safety and security. It is constructed to Class-4 seismic

standards, exceeding the Class-3 earthquake zone in which it is located. To prevent water damage, the CA systems are located on an upper floor of the building, which is sited in an area where flooding is virtually nonexistent.

Disaster Recovery (DR) site: The (DR site) is located in an area geographically separated and diverse from the primary datacenter.

Site construction: The area in which the primary datacenter resides is not prone to such environmental hazards as tornadoes, earthquakes, hurricanes, wildfires, etc. The DR system resides in an unmarked concrete building that is not identified in any way as housing the CA equipment. The data processing area of the building is located on a raised level, at least 24 inches above the normal first-floor level, in an area with no windows.

5.1.2 *Physical Access*

The CA provides physical access controls designed to provide protections against unauthorized access to its system resources.

Primary facility: The CA system is housed in an unmarked secure datacenter. The building is located on fenced and guarded grounds. Access to the grounds is controlled through a programmable electronic passcard system. A guard post is within 50 feet of the gate entrance to the property, with a clear line of sight to the gate. Building entryways and passageways are under continuous recorded video surveillance. The facility is manned 24x7x365 and is never left unattended.

The staff members from the hosting facility perform frequent checks of the facility and data processing areas throughout each day, but cannot enter the CA's system area, known as the "Secure Room."

The area in which the CA systems are located, known as the Secure Room, is separated from the rest of the building interior by physical and visual barriers including walls and caging materials that go slab to slab. The Contractor's Security Office performs checks and reviews of the physical security integrity of the Secure Room to ensure that alarms, access points, ingress and egress access readers, safes containing Cryptomodules and activation materials, video surveillance equipment, storage containers, access logging equipment, and other items are functioning correctly. A record of these reviews is kept that describes the type of checks performed, the time, and the person who performed them. Records are kept for no less than one year and reviewed with external auditors annually as part of the CA's WebTrust for CA audit and other audits as described in Section 8.

Programmable electronic passcards are required for employee entrance to the foyer of the building, which serves as a mantrap. Entrance into the public and datacenter areas of the building requires two-factor authentication, including programmable electronic passcards; these passcards permit entry only into those datacenter areas authorized by the appropriate building tenants.

Employees are prohibited from permitting unknown or unauthorized persons to pass through doors, gates, and other entrances to restricted areas when accessing the facilities. Authorization for any persons, including hosting facility personnel, CA personnel, vendors, repair persons, or visitors, to enter the CA's Secure Room must be obtained in advance from the Contractor's Security Office or senior management.

Visitors are allowed within the fence only with authorization from the guard in the control center after properly identifying themselves, their purposes, and the persons they will visit. Also, visitors are only allowed to access the CA's or Contractor's areas after their visits' purposes and their identities have been verified; they have presented government-issued photo identification for entry into an electronic visitor log; and at least one Contractor Trusted Role employee escorts them. Visitors are not allowed in nonpublic areas of the building without escorts. For security purposes, CA personnel are subject to the same policies as visitors.

The CA Secure Room is physically secured with two-person, dual-factor authentication including biometrics. The room is also equipped with a 24x7x365 camera system that is monitored and reviewed by the Contractor's Security Office. Only previously authorized Contractor Trusted Role employees are granted access to the Secure Room. Such authorization is granted by the Contractor's CIO, or when so designated, by the Contractor's Security Office.

The Secure Room is required to be under 2-of-M person control at all times when individuals are present in the room. By policy, M is kept to the lowest number of Contractor's Trusted Role employees that still allows for enough personnel to cover the needs of the CA's diverse customer base. Two-person control is enforced through strict policy provisions, as well as through the biometric access system. At no time is any individual left alone in the Secure Room. Two approved Contractor Trusted Role employees accompany any additional personnel at all times.

Access to storage safes located inside the CA Secure Room is controlled through Separation of Duties and Multi-party Control. The safes have dual locks and require two Contractor Trusted Role employees for access; no single individual has the tools or information necessary to open a safe alone. All access to material inside the safes is documented through access logs. Any material placed into or removed from a safe is logged and signed for by two Contractor Trusted Role employees.

In addition to the electronic entry and exit logs generated by the biometrics access-control system, each entry into, and exit from, the Secure Room is logged with the individuals' names, entry and exit times, date, and reason for access. Prior to signing out and departing the Secure Room, the Contractor Trusted Role personnel accessing the Secure Room are required by policy to check that all physical protection is in place, that all sensitive materials are securely stored, and that the alarms are properly armed.

CA, CSA, and RA equipment is located inside locked computer cabinets within the Secure Room. Cabinet keys are accessible by the same number of Trusted Role employees who have access to the Secure Room. CA and CSA Cryptomodules are secured in the locked computer cabinets within the CA Secure Room when in use. When not in use, the Cryptomodules and activation materials are securely stored in the safes. The Contractor Security Office reviews the following on a periodic basis to determine if any Secure Room access violations have occurred:

- Written access logs;
- Video surveillance tapes; and
- Two-factor access logs, all of which are maintained by the Contractor's Security Office.

After review, all such logs are archived and kept securely offsite by the Contractor's Security Office for not less than one year.

DR site: The perimeter of the building is secured with surveillance cameras and intrusion sensors monitored by guards 24 hours a day, 365 days a year (24x7x365). The CA's DR area is separated from the rest of the data processing area and is enclosed on all sides, including top and bottom by substantial entry barriers including caging material. Visual barriers may also be erected if needed.

The staff of the DR facility performs checks of the facility several times a day, covering the facility's access points, cameras, and other aspects of a physical walk-through. A record is kept that describes the types of checks performed, the time, and the person who performed them. In addition, the Contractor Security Office performs checks of the CA's area upon each visit to the site, which are similar in nature and scope to the checks performed at the Primary site. Records are kept for not less than one year and reviewed with external auditors on an annual basis as part of the WebTrust for Certification Authorities audit.

CA personnel require authorization from the Contractor to access the building and to enter CA or Contractor areas within the building. In addition, computer rooms (such as the Secure Room where CA, RAs and Repositories systems are housed) are equipped with riot doors, fire doors, and other doors resistant to forcible entry.

Access to the building requires a programmable electronic passcard or permission from the building staff. Access to the area where the secure cage is requires two-factor authentication including electronic passcard.

The CA area requires two-person, two-factor authentication including biometrics for access. The CA area is equipped with a Contractor-owned 24x7x365 camera system that is maintained and reviewed as needed by the Contractor's Security Office. The area surrounding the CA area is also surveilled by building cameras that are constantly monitored by hosting company personnel. Only previously authorized Contractor Trusted Role employees are granted ongoing access to the CA area; all others are considered visitors and are subject to the visitor policies described above. Policies covering visitor access to the datacenter and the Secure Room apply to CA personnel as well.

CA equipment is located inside locked computer cabinets within the CA area. Cabinet keys are maintained by the same number of Contractor Trusted Role employees who have access to the CA area. Safes are present for the storage of highly sensitive material if they are needed at the site, which the same protections described for the primary site.

5.1.2.1 *Physical Access for RA Client-side Equipment*

RA processes are performed programmatically by equipment housed in the Secure Room, and are subject to the same protections at both the primary and DR sites.

5.1.3 *Power and Air Conditioning*

Primary facility: The facility is located less than one-half mile from a major power generation plant and substation, with power coming into the site over nonpublic lands. Additionally, the facility maintains its own UPS and backup generator, which are maintained and tested routinely. To protect against excessive temperatures, the building has an overcapacity heating/cooling tower, with redundant HVAC systems for backup.

DR site: The facility has high-capacity connections to the local power utility, backed up with a robust UPS and multiple backup generators, which are maintained and tested routinely. To protect against excessive temperatures, the building has overcapacity heating/cooling systems.

5.1.4 *Water Exposure*

Primary facility: To mitigate the risk of water damage, hosts, network equipment, and communications facilities for the CA system are housed on the second floor of the company's Datacenter. Equipment also sits on a raised computer room floor. All air handlers and other environmental equipment are located on the outside perimeter of the Datacenter. Restroom facilities and other building plumbing are not located directly above or below the areas hosting the systems, and are not immediately adjacent to the data room. The building's fire suppression system is also non-liquid. Therefore, the only water threat to systems is humidity control equipment that employs a water-based environmental maintenance system with plumbing that runs under the raised floor behind a concrete barrier that isolates it from the under-floor wiring and prevents the lines from being located under the system equipment. Water-sensing cable is located inside the concrete barrier and is capable of detecting moisture as small as a humidity change; when triggered, it alerts the Datacenter operations staff and pinpoints the area of concern on an annunciation panel.

DR site: The building site is located away from potential water hazards and is above the flood plain. The building itself contains subfloor curbing to prevent any water or moisture from affecting computer equipment or cabling. The building is also designed so that no water lines or plumbing fixtures exist directly above or below the datacenter areas. For further moisture protection, subfloor sensors alert the building staff if water or high moisture is detected.

5.1.5 *Fire Prevention and Protection*

Primary facility: The building has the following fire prevention and protection features and meets relevant fire codes:

- Fire-resistant and fire-retardant construction materials;
- Advanced chemical, smoke, and heat-based detection systems;
- Water-based sprinkler fire suppression in business suites;

- Inergen® or similar fire suppression systems (containing inert gas) in the data processing areas, including the Secure Room;
- 24x7x365 onsite operators with fire control console/panel access; and
- Seismic separation between the Secure Room and office space, which also serves as an interstitial gap to thwart fire spread.

DR site: In addition to fire-resistant construction, he building has a full complement of VESDA sensors that automatically alert both building staff and fire authorities if smoke is detected. The datacenter areas are also equipped with dry pipe sprinkler systems. Facility personnel are on site 24x7x365 to monitor the fire console and panel.

5.1.6 *Telecommunications Access and Media Storage*

Primary facility:

Telecommunications: Internet access is obtained from multiple providers through separate access points to the building and are routed exclusively to the IdenTrust CA system. Simultaneous failure of multiple lines is extremely unlikely, but if it should occur, the datacenter maintains additional lines from other providers that can be accessed in an emergency.

Media handling and storage: The CA and the Contractor adhere to a "clean desk" policy under which all hardcopy sensitive information is locked in file cabinets, desks, safes, or other furniture when it is not in use. Likewise, all workstation-based computer media (such as disks, tapes, or CD-ROMs) containing sensitive information is locked in similar enclosures when not in use or when not in a clearly visible and attended area.

For the most sensitive media – the key materials and associated items – the Secure Room contains multiple safes, which are also tightly controlled. All removal or additions to the safes are tracked with logs requiring two Contractor Trusted Role employees to sign them acknowledging such actions. Server-based computer media containing sensitive materials is stored both within the Secure Room and at an offsite location, as described below.

Offsite storage facility: The storage vault is a hardened site constructed of cement, steel and solid granite. Environment-related storage mechanisms include but are not limited to constant temperature and humidity, air circulation and filtration, prohibited storage of flammable items, ionization detectors, fire extinguishers, and independent power sources. The entrance is protected by multiple levels of security including gates, mantraps, and a 12,000-pound vault door.

There is only one point of ingress and egress for the facility and for the vault proper. Any attempt to use explosives to force the gates and vault door would be detected by heat detectors and seismic sensors that are connected to an alarm system. Card readers and sign-in logs are also utilized for physical access control and auditing.

An armed security force supports the vault. It is also under 24-hour electronic surveillance, and it is regularly patrolled by local law enforcement when not occupied. An armed guard escorts all persons entering the facility and the vault area proper. All access to the vault requires 24-hour advance notice

Records are maintained in a temperature and humidity controlled environment and the vault meets or exceeds all federal requirements for archival storage.

The most sensitive materials, including Cryptomodules, tokens, and password copies, are stored within locked mini-vaults and their combinations are under the CA's control. Other material is placed in metal boxes that are secured with locks, with keys maintained under the CA's normal two-person control procedures. As noted above, boxes contain no labels identifying them as belonging to the CA, or as containing sensitive materials; all labeling is generic so as not to reveal box contents.

Backup copies of PKI materials, including CA, CSA and CMS Cryptomodules and activation materials, are securely stored.

Shipment of materials to and from the off-site location is conducted via bonded couriers who are employees of the offsite facility. They do not have keys or combinations to the transport boxes and mini safes, and have no specific knowledge of box or safe contents.

DR site:

Telecommunications: Internet access is obtained from multiple providers through separate access points to the building and are routed exclusively to the IdenTrust CA system. Simultaneous failure of multiple lines is extremely unlikely, but if it should occur, the datacenter maintains additional lines from other providers that can be accessed in an emergency.

Media handling and storage: No paper-based media is used at the DR site. The same protections used for electronic media at the primary facility are in place at the DR site.

Offsite storage: Because it is designed for short-term recovery operation, the DR site has no provisions in place for offsite storage. Should longer-term operations be required, offsite storage contracts and procedures can be put in place quickly.

5.1.7 *Waste Disposal*

The CA policy prohibits any media from leaving organizational control that does contain or has contained sensitive data. Such media is destroyed as described below when it reaches end-of-life. The same policies and procedures apply to both the primary and DR sites, and to the CA and the Contractor organizations.

After it is no longer needed, all sensitive information is securely destroyed using procedures that are approved by the CA Security Office or Contractor senior management, and that are consistent with US federal regulations and guidelines. Employees are prohibited from destroying or disposing of potentially important records or information without specific management approval in advance.

All outdated or unnecessary copies of printed sensitive information are shredded using in-office equipment, or are disposed of in a secure waste receptacle that is shredded onsite by a bonded company that specializes in disposing of sensitive information, under the direct observation of a CA trusted employee or a Contractor Trusted Role employee.

When sensitive CA information is erased from a disk, tape, or other magnetic storage media, the erasure is followed by a repeated overwrite operation, using approved secure-delete programs.[1] This prevents the information from later being scavenged. Alternatively, degaussers, shredders, and/or other equipment and procedures approved by the CA's management or by the Contractor's Security Office are employed.

The Contractor's Security Office is contacted for assistance in disposing of media and equipment no longer being used by the CA, RA and Repository systems. Such media and equipment are stored at a level of security appropriate to the level of sensitivity of information contained in the media and equipment until they can be effectively sanitized or destroyed. Key materials, for example, are stored in a safe within the Secure Room, as described elsewhere.

Cryptomodules remain in locked safes within the Secure Room; sensitive backup tapes remain in the offsite secure location's vault prior to destruction. All Cryptomodules are zeroized after the keys on them are no longer needed. If zeroization procedures fail, then they are physically destroyed. Destruction techniques vary depending on the medium in question. Methods of destruction include:

- Zeroizing, then incinerating Cryptomodules, hard disks, and similar items;

[1] Recent US government guidelines stipulate that a single overwriting pass is sufficient to wipe newer-technology disks. Single- or multiple-wipe processes may be used at the CA's or Contractor's discretion.

- Zeroizing, securely erasing, or degaussing; then crushing Cryptomodules, hard disks, and similar items;
- Degaussing, then shredding, cutting, stretching, and/or otherwise destroying magnetic tapes; and
- Shredding paper.

5.1.8 *Offsite Backup*

The CA system is backed up at the primary datacenter, using specialized backup software, to a local backup server. These system backups provide the capability to recover from a system failure. Incremental backups are performed daily. Full system backups are performed every week. Backups are sent to the hardened, secure offsite storage vault described in Section 5.1.6 at least twice a week.

At least annually, backup tapes are consolidated and archive media is identified and stored in the offsite storage vault to satisfy the CA's data retention schedule. Components needed to restore the CA, RA and Repositories systems are stored in separate areas of the offsite vault, as described in Section 5.1.6.

Only those Contractor employees in Trusted Roles, and only with a need-to-know status as authorized by the Contractor's Security Office, are permitted ongoing access to the offsite storage facility, or to the materials stored there. When a request is made to deliver backup material to the CA's facilities, the request is made by a Contractor Trusted Role employee who has been previously authorized as a requestor and has been so identified to the offsite facility. That request is then verified via call-back procedures by a second Contractor Trusted Role employee who has been similarly authorized and identified to the facility to approve such requests. When key materials are delivered, they are received and signed for by two authorized Contractor Trusted Role employees.

Visitors to the offsite storage facility must be previously announced and authorized by the storage facility management before access is granted.

5.2 Procedural Controls

5.2.1 *Trusted Roles*

All employees, contractors, and consultants to the CA and RAs who have access to or control over cryptographic operations that may materially affect the Issuance, use, suspension, or Revocation of DV-SSL Certificates, including access to restricted operations of the CA and RA systems, and Repository must be previously designated as serving in Trusted Roles. Such personnel include, but are not limited to, the following:

- CA Administrator;
- CSA Administrator;
- PKI Director, Administrator, or Operator;
- Repository Administrator;
- Registration Authority or Validation Authority Administrator or Representative;
- Systems Administrator or Engineer;
- Network Administrator or Engineer;
- Security Officer;
- Auditor; and
- Risk Manager or Risk Management Committee member.

The functions and duties performed by these persons are separated and distributed so that one person alone cannot circumvent security measures or subvert the security and trustworthiness of the PKI. See Section 5.2.4.

The following subsections provide a detailed description of the responsibilities for each Trusted Role.

5.2.2 *Description of Roles*

5.2.2.1 *CA Administrator*

All Certificates issued under the CA Root Certificate, including the Root, are issued under the control of CA Operations management as operator and CA services provider. The responsibilities for CA functions are carried out by the CA's employees or authorized Contractors acting in their Trusted Roles and include administration and operation tasks described in the CP. The CA Administrator's responsibilities and operating procedures, as they relate to CA Operations, are as follows:

- Installation, configuration and maintenance of the CA software;
- Establishing and maintaining system accounts and configuring audit parameters;
- Installation and configuration of Repository software;
- Installation and configuration of the RA software (Internal RA only, if used for this PKI);
- Configuration of CRL parameters;
- Configuration of Certificate profiles;
- Cross-Certificate, Root CA Certificate, and Subordinate CA Certificate key management (performed under two person control); and
- Cross-certification paperwork and workflow of the Root CA and subordinate CAs by the other Bridges.

The CA Administrator will ensure that the Root CA Keys will not be used to sign Certificates except in the following cases:

- Self-signed Certificate to represent the Root CA itself;
- Certificates for CAs;
- Certificates for infrastructure purposes (e.g. administrative role Certificates, internal CA operational device Certificates, and OCSP Response verification Certificates); and
- Certificates issued solely for the purpose of testing products with Certificates issued by the Root CA.

The CA will maintain redundancy in the role of CA Administrators. For the CA PKI, at least two CA Administrators are maintained in case a primary CA Administrator is on vacation, sick leave, etc.

5.2.2.2 *CSA Administrator*

Within the CA, CA Administrators also carry out the responsibilities of the CSA Administrator. The CSA Administrator responsibilities and operating procedures performed by CA Administrators, as they relate to CSA Operation, are as follows:

- Installation, configuration, and maintenance of the CSA software;
- Generating and backing up CSA Keys (performed under two person control);
- Management of CSA Key and Certificate lifecycle, including renewal of OCSP Responder Certificates (performed under two person control);
- Establishing and maintaining system accounts and configuring audit parameters; and
- Operation of the CSA equipment.

5.2.2.3 *PKI Director, Administrator, or Operator*

The PKI Administrator operates and manages the portion of the CA system that creates Key Pairs and signs Certificates. Those named to PKI roles are responsible for the following:

5.2.2.4 *CSA Operator*

Within the CA, the CSA Operator functions are divided between the CSA Administrator and the System Administrator. See Section 5.2.4.7 for details on CSA Operator's tasks performed by the System Administrator.

5.2.2.5 CSA Auditor

Within the CA, the CSA Auditor functions are performed by the Security Officer. See Section 5.2.4.9 for details.

5.2.2.6 RA Administrator

The RA functions are performed programmatically for all DV-SSL Certificate applications except for those determined to be High Risk Applications. These are reviewed and needed RA functions are performed by a Validation Authority. In either case, the process is the same – to determine that the Applicant has legitimate control over the domain named in the Certificate application.

RA functions are administered by an RA Administrator, who has the following duties:

- Installation, configuration, and maintenance of software on the RA System;
- Generation and management of keys and the Certificate lifecycle of the RA System; and
- Secure operation and management of the RA System, including patch management, backup, system logging and physical and logical security.

RA Administrator functions are performed by the System Administrator with the exception of Key Management, which is performed by the CA Administrator. See Section 5.2.2.7 for details on RA Administrator tasks performed by the System Administrator.

5.2.2.7 System Administrator

The CA's System Administrators are responsible for RA and CA operations including the following:

- Installation and configuration of operating systems, and databases;
- Installation and configuration of applications and initial setup of new accounts;
- Performance of system backups, software upgrades, patches, and system recoverability;
- Secure storage and distribution of backups and upgrades to an off-site location
- Performance of the daily incremental database backups; and
- Administrative functions such as time services and maintaining the database.

5.2.2.8 Network Engineer

The CA's Network Engineers are and responsible for the following:

- Initial installation and configuration of the network routers and switching; equipment, configuration of initial host and network interface;
- Installation, configuration, and maintenance of firewalls, DNS and load balancing appliances;
- Creation of devices to support recovery from catastrophic system loss; and
- Changing of the host or network interface configuration.

5.2.2.9 Security Officer

The CA Security Officers are responsible for reviewing the audit logs recorded by CA, CSA and RA systems and actions of administrators and operators during the performance of some of their duties. They also perform and oversee compliance audits to ensure compliance of the PKI with this CPS.

A Security Officer reviews logs for events such as the following:

- Requests to and responses from the CA system;
- The Issuance of Certificates;
- Repeated failed actions;
- Requests for privileged information;
- Attempted access of system files, the CA databases or the RA database;
- Receipt of improper messages;
- Suspicious modifications;
- Performance of archive and delete functions of the audit log and other archive data as described in Sections 5.4 and 5.5 of this document;
- Administrative functions such as compromise reporting; and for SSL Certificates, performing quarterly self-audits to monitor Certificate Issuance quality described in Sections 8, 8.5.1 and 8.6.1 of this document.

The Security Officer also performs, or oversees, internal compliance audits to ensure that the CA, CSA, and RA systems are operating in accordance with this CPS; and in conjunction with the Operations Manager, authorizes use of activation data for administrative Cryptomodules used with CA software.

5.2.2.10 CA Auditor

Within the CA, the CA Auditor functions are performed by the Security Officer. See Section 5.2.2.9 for details.

5.2.2.11 Operations Manager

The Operations Manager performs the following duties:

- Provides internal audit oversight;
- Works closely with external auditors as needed;
- Handles approval/removal of other Trusted Role employees;
- Authorize use of activation data for administrative Cryptomodules used with CA software.

5.2.3 Number of Persons Required per Task

A list of the CA's Operations Managers (i.e., the CA's Chief Information Officer and other Operations designees below the CIO) is kept at all times as approved and authorized by the CA's Chief Operating Officer (COO), Chief Information Officer (CIO) or Chief Executive Officer (CEO). The Operations Manager performs the following duties:

- Provides internal audit oversight, and works closely with external auditors as needed;
- Handles approval/removal of Network, System and CA Administrators as well as other Trusted Role employees;
- Acts as custodian of activation data for administrative Cryptomodules used with CA software;

5.2.4 Identification and Authentication for Each Role

The vetting of personnel in Trusted Roles is found below in Sections 5.3.1 and 5.3.2. I&A for logical and physical access to CA system resources is described in this Section. In accordance with the CA's security policies, the CA personnel must first authenticate themselves before they are:

- Included in the access list for any component of the CA system;
- Included in the access list for physical access to a component of the CA system;
- Issued a Certificate for the performance of their Trusted Role;
- Given an account on a computer connected to the CA system; or
- Otherwise granted physical or logical access to a component of the CA system.

Each of these access methods (Certificates and system accounts) are:

- Directly attributable to the individual;
- Password/account password protected;
- Not shared; and
- Restricted to actions authorized for that role through the use of CA software, operating system and procedural controls.

If accessed across shared networks, CA operations are secured, using hardware Cryptomodules, strong system authentication, and encrypted secure connections.

5.2.5 *Separation of Roles*

The CA maintains strict separation-of-duties/multi-party controls for its Trusted Roles. These controls are audited annually by a third party auditor as part of the AICPA/CPA Canada and WebTrust Program for Certification Authorities audit described in Section 8.

Oversight of the CA's Trusted Roles is performed by the Risk Management Committee, Operations Management, the Human Resources Department, and Executive Management. The CA maintains a list of individuals performing each Trusted Role. The list is maintained by the highest-ranking Operations manager (i.e., CIO or Vice President of Operations) and, for audit purposes, the Security Office maintains a current copy of the list.

Roles requiring separation of duties include (but are not limited to):

CA/CSA Administrator. No person participating as the CA/CSA Administrator will assume the role of Security Officer, RA, System Administrator, Network Engineer or Operations Manager.

RA Administrator**.** An RA Administrator may not assume the Operations Manager, RA, System Administrator, Network Engineer, or Security Officer role.

System Administrator**.** A System Administrator may not assume the Security Officer, RA, CA/CSA Administrator or Operations Manager role.

Network **Engineer.** The Network Engineer may not assume the Security Officer, RA, CA/CSA Administrator or Operations Manager role

Security Officer. The Security Officer may not serve in any other Trusted Role (e.g. the roles of CA/CSA Administrator, RA, RA Administrator, Systems Administrator, or Network Engineer)

Operations Manager. The Operations Manager may not serve as CA/CSA Administrator, Systems Administrator, RA, or Network Engineer.

5.3 Personnel Controls

The CA and its RA, CMA, CSA, and Repository subcontractors implement personnel and management policies sufficient to provide reasonable assurance of the trustworthiness and competence of their employees and of the satisfactory performance of their duties in a manner consistent with the requirements of the CP.

Contractor personnel employed to perform functions for the CA pertaining to the CP and this CPS meet applicable requirements set forth in the CP, CPS, and System Security Plan (SSP).

The CA takes appropriate administrative and disciplinary actions against personnel who have performed actions involving the CA or its Repository not authorized in the CP and this CPS.

The following sections outline these controls.

5.3.1 *Background, Qualifications, Experience, and Security Clearance Requirements*

Personnel who administer or operate components of the CA, CSA and RA systems, are under the direct control of the CA and meet the following requirements:

- Successful completion of appropriate training programs as evidenced by Certificates of completion issued by the entity providing training;
- Demonstrated ability to perform duties, as indicated by annual performance reviews;

- Trustworthiness, as initially determined by a background investigation;
- No other duties that would interfere or conflict with the duties of their Trusted Role;
- Not previously relieved of duties in a Trusted Role for reasons of negligence or non-performance of duties, as indicated by employment records;
- Not convicted of a felony offense, as indicated by a criminal background check; and
- Appointed in writing by Operations Management or pursuant to written contract with the CA or in a certificate of incumbency, as evidenced by records maintained for such purpose by such organization.

5.3.2 *Background Check Procedures*

Persons appointed by the CA to serve in Trusted Roles have undergone a local and national criminal background check, and a financial status check through national credit bureau databases. Other checks are performed as described below for the purposes listed:

- Previous employers are contacted to determine that the person is competent, reliable and trustworthy;
- High schools, colleges and universities are contacted to verify the highest or most relevant degree;
- Residence checks are performed to determine that the person was and is a trustworthy neighbor;
- Driver's license records are checked through a commercial database to determine if the person has a record of serious or criminal violations; and
- A Social Security trace is performed to determine whether the person has a valid social security number. This check is required only if the country in which the duty is performed has social security number or similar identifier.
- A criminal history check is performed through a commercial database, to determine that the person has no previous felony convictions;
- A credit history check is performed through a commercial database to determine that the person has not committed any fraud and is financially trustworthy; and
- Professional references are contacted to determine that the person is competent, reliable, and trustworthy.

The period of investigation covers at least the last five years for employment, education, criminal, and references, and the last three years for places of residence. Regardless of the date of award, the highest educational degree is verified.

Background checks are renewed periodically. If the initial or subsequent background checks reveal a material misrepresentation by the individual, substantially unfavorable comments from persons contacted, a criminal conviction, or personal financial problems, then it is be brought to the attention of the Operations Manager and Security Officer who will evaluate the severity, type, magnitude, and frequency of the behavior or actions of the individual, and determine the appropriate action to be taken, which may include removal from a Trusted Role.

RAs are obligated by contract, this CPS and the CP to implement background check procedures equivalent to the ones explained above. To the extent that any of the foregoing cannot be met due to circumstances peculiar to that party, substantially similar procedures must be performed and may include background checks performed by government agencies or providers of such services in their jurisdictions.

5.3.3 *Training Requirements*

Personnel performing CA, CSA, RA and RA duties receive comprehensive training in security principles and procedures, PKI hardware and software used, and disaster recovery and business continuity procedures. Security awareness and training programs are developed and implemented in accordance with Federal laws, regulations, and guidelines and supporting security guidelines the CA maintains records of the training received by persons in Trusted Roles.

CA/CSA Administrator:

- Key Pair generation and Certificate Issuance, re-keying and Revocation for Root CAs and CSAs;
- Configuration and posting of Certificates and CRLs;

- Daily maintenance and other CA-, CSA-related administrative functions; and
- Initializing CA and CSA hardware.

System Administrator:
- Operating systems and software applications used within the PKI systems;
- Backup applications and procedures;
- Use of database tools including reporting and maintenance;
- Restriction for privileged system use; and
- Generation of audit data.

Network Engineer:
- Network architecture and equipment used in the PKI;
- Proper and secure configuration and switching for the network;
- Intrusion detection monitoring; and
- Requirements for securing network transmissions.

Security Officer:
- Security risk assessment and analysis;
- Security policies and guidelines;
- Computer attack trends, security threats and vulnerabilities;
- Physical security and physical Access Controls;
- Networks, distributed systems trust relationships, PKI and cryptosystems;
- Firewalls and other network security devices;
- Event logging and auditing; and
- Incident response and contingency planning.

Operations Management Personnel:
- Operating systems and software applications used within the PKI system;
- Network architecture; and
- Audit and risk management oversight.

5.3.4 *Retraining Frequency and Requirements*

Any significant change to the CA and RA systems requires that personnel receive additional training. Through change control processes (see Section 6.6.2), an awareness plan is prepared for any significant change to the systems (e.g., a planned upgrade of CA equipment, software or changes in procedures). All Trusted Role personnel undergo a retraining session once a year that includes a review of the applicable provisions of the CP and CPS under which they are operating, and a full review of all applicable policies and procedures.

Documentation identifying all personnel who received training and the level of training completed is maintained.

5.3.5 *Job Rotation Frequency and Sequence*

Job rotation is implemented when in the judgment of the CA's or RAs' management it is necessary to ensure the continuity and integrity of the CA's or RAs' ability to continually provide PKI-related services.

5.3.6 *Sanctions for Unauthorized Actions*

Failure of any employee or agent of the CA or an RA to comply with the provisions of the CP, this CPS, or Federal regulations, whether through negligence or malicious intent, will subject such individual to appropriate administrative and disciplinary actions, which may include termination as an employee or agent, and possible civil and criminal sanctions. Any person performing a Trusted Role who is cited by management for unauthorized actions, inappropriate actions, or any other unsatisfactory investigation results will be immediately removed from the Trusted Role pending management review. Subsequent to management review, and discussion of actions or investigation results with the employee, he or she may be

reassigned to the Trusted Role, transferred to a non-Trusted Role, or dismissed from employment as appropriate.

5.3.7 *Contracting Personnel Requirements*

Independent contractors who are assigned to perform Trusted Roles are subject to the duties and all requirements of the CP and this CPS, including the ones described elsewhere in this Section 5.3. Independent contractors are subject to sanctions stated in Section 5.3.6 for unauthorized actions or failure to comply with the provisions of the CP and this CPS.

5.3.8 *Documentation Supplied to Personnel*

CA and RA Personnel in Trusted Roles, including contractors, are provided with the documentation necessary to define and support the duties and procedures of the roles to which they are assigned. The CA provides a copy of the CP, relevant portions of this CPS, any relevant statutes, policies, and guidelines and all technical and operational documentation needed to maintain, and integrate with the CA or RA systems, as appropriate, as well as other relevant information to fulfill their tasks.

The information is available in print or online. The information provided consists of internal CA system and security documentation, the CA Policies and Procedures, discipline-specific books, treatises and periodicals, and other information developed by or supplied to the CA or the RA that is relevant to the role being performed.

5.4 Security Audit Logging Procedures

For the purposes of security audit, events related to operation of the CA PKI are recorded as described in this Section, whether the events are attributable to human action in any role or are automatically invoked by the equipment that is used to register Applicants; generate, sign and manage Certificates; and provide Revocation information.

Where possible, the audit data is automatically collected; when this is not possible, a logbook or other physical mechanism is used. All security logs, both electronic and non-electronic, are retained and maintained securely in accordance with the requirements of Section 5.5.2 and are made available during compliance audits.

5.4.1 *Types of Events Recorded*

All security auditing capabilities of the CA's systems required by the CP are enabled.

The CA, CSA, and RA equipment automatically record all significant events related to the operations of the equipment. Events recorded include those that occur to the routers, firewalls, at each host, within applications and databases, and all physical security check points.

The CA's staff manually record all significant events that are not logged by the equipment.

For events recorded, the minimum information logged includes the following items: type of event, time of occurrence, identity of the individual or system that logged the event, who caused the event, and a success or failure indication. For some types of events, these minimums may be expanded to include source or destination of a message, and the disposition of a created object (e.g., a filename).

Auditable Event	CA	CSA	RA
SECURITY AUDIT	**CA**	**CSA**	**RA**
Any changes to the audit parameters, e.g., audit frequency, type of event audited – The operating system and applications automatically record modifications made to audit parameters; including date and time of modification, type of event, success or failure indication and identification of user making modification.	X	X	X

Auditable Event	CA	CSA	RA
Any attempt to delete or modify the audit logs – The operating system automatically records all attempted modifications made to security audit configurations and files, including date and time of modification, type of event, success or failure indication and identification of user making modification.	X	X	X
Obtaining a third-party time-stamp	N/A	N/A	N/A
IDENTITY AND AUTHENTICATION	**CA**	**CSA**	**RA**
Successful and unsuccessful attempts to assume a role – The operating system and applications automatically record: date and time of attempted login, username asserted at time of attempted login, and success or failure indication, are automatically logged by the CA, CSA and RA.	X	X	X
The value of maximum authentication attempts is changed – The operating system logging facility automatically logs date and time, type of event, and identification of the user making modification(s). Changes in configuration files, security profiles, and administrator privileges are logged through a combination of automatic and manual logging. All changes are manually logged through change management procedures.	X	X	X
Maximum number of authentication attempts occurring during user login – Date and time of attempted login, username asserted at time of attempted login, and failures are recorded automatically by the operating system and application audit logs.	X	X	X
An administrator unlocks an account that has been locked as a result of unsuccessful authentication attempts – Date and time of event and identification of account holder and administrator are logged automatically by the operating system.	X	X	X
An administrator changes the type of authenticator, e.g., from a password to a biometric – Date and time, type of event, and identification of the user making the modification(s) are logged automatically by the operating system and manually through change management procedures. Changes in configuration files, security profiles and administrator privileges are logged through a combination of operating system and manual change management procedures.	X	X	X
LOCAL DATA ENTRY	**CA**	**CSA**	**RA**
All security-relevant data that is entered in the system – The system records the identity of the local operator performing local data entry so that the accepted data can be associated with the operator in the audit log.	X	X	X
REMOTE DATA ENTRY	**CA**	**CSA**	**RA**
All security-relevant messages that are received by the system – Date and time, digital signature/authentication mechanism, and message are automatically logged by the application.	X	X	X
DATA EXPORT AND OUTPUT	**CA**	**CSA**	**RA**
All successful and unsuccessful requests for confidential and security-relevant information – Date and time of attempted access, username or identity asserted at time of attempt, and record of success or failure, are logged through a combination of automatic and manual logging. Manual logging by the Security Office also collects the name of person reporting the event and the resolution.	X	X	X
KEY GENERATION	**CA**	**CSA**	**RA**
Whenever a CA generates a Key (not mandatory for single session or one-time use symmetric Keys) – The CA system automatically records all significant events related to CA operations, including Key generation and Certificate signing. Additionally, manual and audiovisual records of CA and CSA Key generation are created. RA Key and Certificate generation events are automatically recorded by the CA system.	X	X	-

Auditable Event	CA	CSA	RA
PRIVATE KEY LOAD AND STORAGE	**CA**	**CSA**	**RA**
The loading of Component Private Keys – A manual log of all physical access to production CA and CSA Cryptomodules is maintained by the CA, and the log records each action taken, the date and time the action was taken and the name of person who performed each action. A separate record of authorization to access Cryptomodules is also maintained which specifies date, time, reason for access and name of authorizing person.	X	X	N/A
All access to Certificate subject Private Keys retained within the CA for Key recovery purposes – Date and time, messages between the CA and the requesting component, and indicator of success or failure are automatically logged.	X	N/A	N/A
TRUSTED PUBLIC KEY ENTRY, DELETION AND STORAGE	**CA**	**CSA**	**RA**
All changes to the trusted Public Keys, including additions and deletions are automatically logged through the applications and manually through the CA's change management process and access authorization forms.	X	X	X
SECRET KEY STORAGE	**CA**	**CSA**	**RA**
The manual entry of secret Keys used for authentication – Use of secret Keys (PED Keys) for access to the CAs' and CSAs' Cryptomodules is recorded manually at the time of cryptographic Key use. The log records the action(s) taken, the date and time action was taken, and the name of the person who performed the action. A separate record of authorization to access Cryptomodules is also maintained which specifies date, time, reason for access, and name(s) of authorizing person.	X	X	N/A
PRIVATE AND SECRET KEY EXPORT	**CA**	**CSA**	**RA**
The export of private and secret Keys (Keys used for a single session or message are excluded) – Private and secret Key export involving the CA's Cryptomodules take place in accordance with the principles of Separation of Duties/Multi-party Control stated in Section 5.2.5. At the time of export a manual log records the action taken, date and time the action was taken, and the name(s) of person(s) who performed the action. Separate records of access to Cryptomodules are also maintained that specify the date, time, reason for access, and name of authorizing person.	X	X	N/A
CERTIFICATE REGISTRATION	**CA**	**CSA**	**RA**
All Certificate requests – Date and time of request, type of event, and request information are automatically logged by the application. This includes Issuance, renewal, and re-key requests as well as sender/requester DN, Certificate serial number, initial application, method of request (online, in-person), source of verification, name of document presented for identity proofing, all fields verified in the application, Certificate common name, new validity period dates, date and time of response and success or failure indication are automatically logged by the application, and all associated error messages and codes. Manual interactions with participants such as telephone or in person inquiries and results of verification calls will be logged manually in a logbook or in a computer-based recording/tracking system and include date/time, description of interaction and identity provided.	X	N/A	X
CERTIFICATE REVOCATION	**CA**	**CSA**	**RA**
All Certificate Revocation requests – Date and time of Revocation request, sender/requester DN, Certificate serial number, subject DN of Certificate to revoke, Subscriber's common name, Revocation reason, date and time of response and success or failure indication are automatically logged by the application; manual interactions with requestors such as telephone or in person inquiries and requests for Revocation are logged	X	N/A	X

Auditable Event	CA	CSA	RA
manually in a logbook or in a computer-based recording/tracking system. The date/time, description of interaction and identity provided are also recorded.			
CERTIFICATE STATUS CHANGE APPROVAL	**CA**	**CSA**	**RA**
The approval or rejection of a Certificate status change request – Identity of equipment operator who initiated the request, message contents, message source, destination, and success or failure indication are automatically logged by the application.	X	N/A	N/A
COMPONENT CONFIGURATION	**CA**	**CSA**	**RA**
Any security-relevant changes to the configuration of a component – Date and time of modification, name of modifier, description of modification, build information (i.e. size, version number) of any modified files and the reason for modification are manually logged during change management processes.	X	X	X
ACCOUNT ADMINISTRATION	**CA**	**CSA**	**RA**
Roles and users are added or deleted – Date and time, type of event, and identification of the user making modification(s) are logged automatically and manually. Changed roles are logged through a combination of automatic and manual logging. All changes are manually logged through change management procedures. Change management records capture date and time and type of change, reason for change of role, and authorization and approval records.	X	X	-
The access control privileges of a user account or a role are modified – Date and time, type of event, and identification of user making modification are logged automatically and manually. Changes in configuration files, security profiles and administrator privileges are logged through a combination of automatic and manual logging. All changes are manually logged through change management procedures. Change management records capture date and time and type of change, reason for modification and authorization and approval records.	X	X	-
CERTIFICATE PROFILE MANAGEMENT	**CA**	**CSA**	**RA**
All changes to the Certificate profile – Change management records capture date and time and type of change, reason for modification and authorization and approval records.	X	N/A	N/A
REVOCATION PROFILE MANAGEMENT	**CA**	**CSA**	**RA**
All changes to the Revocation profile – Change management records capture date and time and type of change, reason for modification and authorization and approval records.	X	N/A	N/A
CERTIFICATE REVOCATION LIST PROFILE MANAGEMENT	**CA**	**CSA**	**RA**
All changes to the Certificate Revocation list profile – Change management records capture date and time and type of change, reason for modification and authorization and approval records.	X	N/A	N/A
MISCELLANEOUS	**CA**	**CSA**	**RA**
Appointment of an individual to a Trusted Role – Date of the appointment, name of the appointee, and authorizing signature are manually logged.	X	X	X
Designation of personnel for multiparty control – Date of the appointment, name of the appointee and authorizing signature are manually logged.	X	-	N/A
Installation of the Operating System – Date and time of server installation, name of installer, and details of installation process are manually recorded during installation. The automatic security auditing capabilities of the underlying operating system hosting the software are	X	X	X

Auditable Event	CA	CSA	RA
enabled during installation. All changes are also manually logged through change management procedures.			
Installation of the PKI application – Date and time of installation, name of installer, and details of installation process are manually recorded during installation. All changes are also manually logged through change management procedures.	X	X	X
Installation of hardware Cryptomodules – A manual list of hardware Cryptomodules is maintained, and the list records action taken, date and time action was taken, and the name of person who performed the action.	X	X	X
Removal of hardware Cryptomodules – A manual list of hardware Cryptomodules is maintained, and the list records action taken, date and time action was taken, and the name of the person who performed action.	X	X	X
Destruction of Cryptomodules – A manual list of Cryptomodules is maintained, and the list records action taken, date and time action was taken, and the name of the person who performed the action.	X	X	X
System Startup – Date and time of system startup is automatically logged in the system's event log.	X	X	X
Logon attempts to PKI Applications – For CA, RA and CSA application access – the date and time of the event, type of event, identity of user accessing the system, and success or failure indication are automatically logged by the application.	X	X	X
Receipt of hardware / software – Kept manually in a database that records the hardware and software possessed, licensed or owned.	X	X	X
Attempts to set passwords – Date and time, identity of user, and success or failure indication of attempt to set password is kept automatically by the operating system/application or manually in a password change log.	X	X	X
Attempts to modify passwords – Date and time, identity of user, and success or failure indication of attempt to modify password is kept by the operating system/application or manually in a password change log.	X	X	X
Back up of the internal CA database – Date and time of the backup event and location of backup are kept manually in a backup log.	X	-	-
Restoration from back up of the internal CA database – Dates and times of restoration tests are kept in a disaster recovery log.	X	-	-
File manipulation (e.g., creation, renaming, moving) – the file system records the identity of the local operator who created or last modified the file so that the creation, renaming or moving of files can be associated with the operator is kept automatically by the operating system audit and logging facility.	X	-	-
Posting of any material to a Repository – Date and time of posting, transaction identifier and success or failure indication are automatically logged by the application. For CRL generation and publication to directory - Date and time of generation, DN of the CA and success or failure of publication of CRL is automatically logged by the application.	X	-	-
Access to the internal CA database – Date and time of login, username asserted at the time of attempted login, and success or failure indication, are automatically logged by the database audit log.	X	-	-
All Certificate compromise notification requests – Date and time of notification, identity of person making the notification, identification of entity compromised, and a description of the compromise are logged manually by the personnel who receive the notification (e.g. Help Desk, RA Operators, etc.) and by RA/RA Operators' system processing logs.	X	N/A	X
Loading Cryptomodules with Certificates – A manual log of all physical access to production CA and CSA tokens is maintained, and the log records action taken (including transferring Keys to or from and backing	X	X	N/A

Auditable Event	CA	CSA	RA
up the tokens), date and time action was taken and the name of the person who performed the action. A separate record of authorization to access tokens is also maintained which specifies date, time, reason for access, and name of authorizing person.			
Shipment of Cryptomodules – Receipt, servicing (e.g. Keying or other cryptologic manipulations), and shipping of modules are manually recorded for CA, CSA and RA production tokens. Recording contains information regarding action taken, (e.g. return, receipt), date and time action was taken, name of person performing action and reason for action.	X	X	N/A
Zeroizing Cryptomodules – A manual list of modules is maintained, and the list records action taken, date and time action was taken, name of person who performed action, name and role of person authorizing the action.	X	X	N/A
Re-key of the CA – CA, CSA and RA systems automatically record all significant events related to their respective operations, including Key generation for re-keying. Additionally, manual and audiovisual records of CA Key generation are created. RA re-keying and Certificate generation events are also automatically recorded by the CA system.	X	X	N/A
CONFIGURATION CHANGES TO THE PKI SERVERS INVOLVING	**CA**	**CSA**	**RA**
Hardware – All changes are manually logged through change management procedures.	X	X	X
Software – All changes are manually logged through change management procedures.	X	X	X
Operating System – All changes are manually logged through change management procedures.	X	X	X
Patches – All changes are manually logged through change management procedures.	X	X	X
Security Profiles – All changes are manually logged through change management procedures.	X	X	X
PHYSICAL ACCESS / SITE SECURITY	**CA**	**CSA**	**RA**
Personnel Access to room housing component – A manual recording of physical access to Secure Rooms is maintained through physical logs that include recording of date and time, person accessing the Secure Room, and reason for access.	X	-	-
Access to the component server – Logged through a combination of automatic and manual logs based upon the type of component and type of access.	X	X	-
Known or suspected violations of physical security – For any known or suspected violations of physical security - date/time, description of suspected event, name of person reporting the event and resolution are manually logged by the Security Office.	X	X	X
ANOMALIES	**CA**	**CSA**	**RA**
Software error conditions – Date and time of event, and description of event are automatically logged by the application reporting the event or by the operating system.	X	X	X
Software check integrity failures – Date and time of event, and description of event are automatically logged by the application reporting the event or by the operating system.	X	X	X
Receipt of improper messages – Date and time of event, and description of event are automatically logged by the application reporting the event or by the operating system.	X	X	X

Auditable Event	CA	CSA	RA
Misrouted messages – Date and time of event, and description of event are automatically logged by the application reporting the event or by the operating system.	X	X	X
Network attacks (suspected or confirmed) – Date/time, description of suspected event, name of person reporting the event and resolution are manually logged by a Security Officer.	X	X	X
Equipment failure – Date/time, description of suspected event, name of person reporting the event and resolution are manually logged by a Security Officer.	X	X	-
Electrical power outages – Date/time, description of suspected event, name of person reporting the event and resolution are manually logged by a Security Officer.	X	X	-
Uninterruptible Power Supply (UPS) failure – Date/time, description of suspected event, name of person reporting the event and resolution are manually logged by a Security Officer.	X	X	-
Obvious and significant network service or access failures – Date/time, description of suspected event, name of person reporting the event and resolution are manually logged by a Security Officer.	X	X	-
Violations of Certificate Policy – Date/time, description of suspected event, name of person reporting the event and resolution are manually logged by a Security Officer.	X	X	X
Violations of Certification Practice Statement – Date/time, description of suspected event, name of person reporting the event and resolution are manually logged by a Security Officer.	X	X	X
Resetting Operating System clock – Date/time, description of suspected event, name of person are automatically logged by the operating systems logging facility.	X	X	X

5.4.2 *Frequency of Processing Log*

The CA's Security Officers and System Administrators conduct reviews of all the audit log data through a combination of automated and manual means at least weekly. In order to ensure a thorough review of all data, the Security Officer selects all of CA, CSA, and RA logs for review and a minimum of 25% of other security audit data generated since the last review for each category of audit data.

The Security Officer uses automated tools to scan logs for specific conditions. The Security Officer then reviews the output and produces a written summary of findings when significant events that require documentation occur. The reviews include date, name of reviewer, description of event, details of findings and recommendations for remediation or further investigation if appropriate. Such reviews involve verifying that the log has not been tampered with, and then briefly inspecting all log entries, with a more thorough investigation of any alerts or irregularities in the logs. The reviews include CA, CSA and RA activities that are listed as recorded in Section 5.4.1. These reviews are made available to the CA's external auditor.

Restrictions are applied to the logs to prevent unauthorized access, deletion, or overwriting of data. Storage capability is monitored to ensure that sufficient space exists in order to prevent overflow conditions. Alerts are sent to a Security Officer if space available becomes inadequate.

The security audit logs are moved monthly to archive by Security Officer in accordance with Section 5.4.4.

5.4.3 *Retention Period for Audit Logs*

All security audit logs, both electronic and non-electronic, are retained and made available during compliance audits.

Audit log information generated on CA, CSA, and RA equipment is kept on the equipment until the information is moved to the off-site archive facility described in 4.1.2.2 the CA's Secure Registration Messaging Protocol. There are ninety days of active logs remaining on the equipment for analysis. The oldest is thirty days; e.g., logs dated between ninety and one-hundred and twenty days, are removed monthly to be archived by the Security Officer in accordance with Section 5.4.4. Electronic audit logs are deleted only after they have been backed up to archive media.

Only Security Officers are authorized to delete these logs and must first verify that the audit log data has been successfully backed up to archive media by checking hash values against the original and the backup copies.

5.4.4 *Protection of Audit Logs*

The security audit logs are written simultaneously to separate network locations to ensure their safety and security. No individual has the rights to modify or delete files in all three locations. Log storage capability is monitored by the operating systems at each location to ensure that sufficient space exists in order to prevent overflow conditions. Logs for the current and two prior months are retained on each server and on the logging hosts to aid in troubleshooting. Alerts are sent to the System Administrators and to the Security Office if it appears that the space available will become inadequate.

The integrity of each archived audit log is ensured by the use of a checksum. The Security Office oversees procedures governing the archiving of all audit logs to ensure that archived data is protected from modification, deletion, or premature destruction. Each month, audit data and review summaries no longer needed on the hosts are archived and moved to a secure offsite storage location as described in Section 5.1.8. As described previously, the audit logs and related materials are stored separately from the daily backups, and access to the offsite data is restricted to Security Officers.

5.4.5 *Audit Log Backup Procedures*

The CA makes a backup of each audit log monthly as described in Sections 5.5.3 and 5.5.4. Backup copies of the audit logs and audit summary data are transferred to the secure offsite location in locked containers separate from all other storage containers. They are also stored separately and can be retrieved only by the Security Office.

5.4.6 *Audit Collection System (Internal vs. External)*

Automated audit log collection systems are internal to the CA, CSA, RA, and Repository. These systems invoke audit processes at system startup, which cease only at system shutdown. Processes are enforced technically through the operating system and a secondary monitoring application.

As described in Section 5.5.4, audit log collection systems are configured such that security audit data logs are protected against loss (e.g., overwriting or overflow of automated log files).

5.4.7 *Notification to Event-Causing Subject*

The CA provides no notice to the event-causing entity (i.e., Subscriber or Device) that an event was audited.

5.4.8 *Vulnerability Assessments*

The Security Officers, System Administrators, and other operating personnel monitor attempts to violate the integrity of CA systems, including the equipment, physical location, and personnel. The audit logs are checked for anomalies that may indicate violations, and are reviewed by the Security Office for events including but not limited to repeated failed actions, attempts to acquire privileged access, requests for privileged information, attempted access of system files, and unauthenticated responses. The Security Office also checks for continuity of the security audit data. Reviews of the security audit logs are conducted by the Security Office in accordance with Section 5.5.2.

5.5 Records Archive

5.5.1 *Types of Events Archived*

The CA retains and archives all data through the life of the CA PKI Certificates. Archive records are maintained locally for at least three months and archived offsite for at least seven years and six months. The archive records are designed to be sufficiently detailed to establish the proper operation of the PKI, or the validity of any Certificate (including those revoked or expired) issued by the CA.

The CA maintains and archives that information and more in the following records, in either electronic or paper format. The use of electronic records is preferred, and paper records are digitized whenever possible.

- CA accreditation;
- Certificate Policy;
- Certificate Practices Statement;
- Contractual obligations and other agreements concerning operations of the CA;
- System and equipment configuration;
- Modifications and updates to system or configuration;
- Certificate requests;
- Record of re-key;
- Revocation requests;
- Subscriber I&A data as per Section 3.2.3;
- Documentation of receipt and Acceptance of Certificates;
- Export of Private Keys;
- Certificate Agreements;
- Documentation of loading, shipping, receipt and zeroizing of Cryptomodules;
- All Certificates issued or published;
- Security audit data in accordance with Section 5.4.1;
- All changes to the trusted Public Keys;
- All CRLs issued and/or published;
- All routine Certificate validation transactions;
- Other data or applications to verify archive contents;
- Documentation required by compliance auditors; and
- Subscriber encryption Private Keys that are archived/escrowed in accordance with this CPS.

5.5.2 *Retention Period for Archive*

Archive records are maintained locally for at least three months and archived offsite for at least seven years and six months.

The CA maintains copies of the applications that can read these types of files for at least the retention period.

5.5.3 *Protection of Archive*

Archived data is stored in a separate, offsite storage facility identified in Section 5.1.6. Records are uniquely identified. The media used for retaining the archived data is specifically chosen and tested to insure that the archived data will be conserved on the same media for the minimum retention period defined in Section 5.5.2.

The contents of the archive will not be released as a whole, except as required by law, as described in Section 9.3. Access to the offsite storage facility is strictly limited to individuals who have been authorized by the CA CIO, Vice President of Operations, or the Security Office. The CA maintains a list of people

authorized to access the archive records and makes this list available to its auditors during compliance audits. Certain sensitive materials are stored in a physically separate area within the offsite storage location, and access to the materials is limited to the CA's Security Officers. The CA's Security Office oversees procedures governing the archival of the audit log to ensure that archived data is protected from deletion or destruction during the data retention period.

The integrity of the electronic archive data is protected through multiple means, while also ensuring that no transfer of medium will invalidate the applied checksum and any attempt to modify the data will be evident. Repository information is archived in a human readable form. The CA maintains copies of the applications that can read these types of files for at least the retention period.

5.5.4 *Archive Backup Procedures*

The CA does not have a backup archival facility because three copies of each archive log are maintained in separate locations. All archive copies are stored in the offsite storage facility and are readily available within a short time in the event of loss or destruction of the primary Datacenter or Secure Room.

5.5.5 *Archive Collection System*

No stipulation.

5.5.6 *Procedures to Obtain and Verify Archive Information*

Upon proper request the CA will create, package and send copies of archived information. Archived information is provided and verified using the formats and media explained in Section 5.5. Access to archive data is restricted to authorized personnel in accordance with Sections 9.3 and 9.4.

Archived data is retrieved from secure storage using The CA's procedures for accessing archived material. Requested archived material is identified by inventory number, which was recorded for the materials when they were originally placed in the locked storage containers for archival. The request procedure requires two CA Trusted Role employees – a requestor and an approver – to complete the request for retrieval from the archive storage facility. Material is delivered to a predefined destination by a bonded courier employed by the storage facility. Identification of the receiving party is checked, a receipt is signed by the receiving party, and physical custody of the archive material is transferred back to the CA. The materials are stored in the Secure Room until they can be reviewed and/or copied in a forensically sound manner for the requestor. The materials are then returned to the archive storage facility.

5.5.7 *Long Term Information Preservation*

No stipulation.

5.6 Key Changeover

The CA provides for the extension and/or continuation of its self-signed root Certificates prior to their expiration through a Key rollover process involving signing the new Public Key with the old Private Key, and vice versa. Upon Key changeover, only the new Key is used for Certificate signing purposes. The older valid Certificate remains available to verify old signatures until all of the Certificates signed using the associated Private Key have also expired. The CA's signing Key has a validity period as described in Section 6.3.2.

When the CA re-keys its signature Private Key and thus generates a new Public Key, it will make it publicly known in the Repository and notify the PMA, RAs, and Subscribers that rely on its CA Certificate, that it has changed its Keys.

5.7 Compromise and Disaster Recovery

5.7.1 *Incident and Compromise Handling Procedures*

The CA maintains security incident response and compromise handling policies and procedures, as well as disaster recovery and business continuity plans. Such procedures and plans are available for onsite review by its auditors and major Authorized Relying Parties under appropriate non-disclosure agreements. Below is a synopsis of the incident response policies and procedures.

An initial goal of the incident response plan is to determine the degree and scope of the incident. This includes a determination of the cause or source of the incident (internal system failure or external malicious attack), and whether the immediate harm caused by the incident will be mild or severe. For all incidents, data is collected and analyzed to determine, among other things:

- Whether a crime has been committed, and if so, whether evidence can be collected that will be helpful to law enforcement;
- What data was disclosed or compromised, and whether there was a Key compromise; and
- What steps need to be taken immediately to mitigate further damage.

For anticipated threats, the CA maintains step-by-step procedures and task assignments for members of the incident response team, depending on the type of incident that is believed to have occurred.

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

The CA backs up essential information in near-real time to its disaster recovery site, which is located in a geographically separate area that is not subject to the same local or regional events as the primary site. The CA also performs tape backups of all its production CA systems daily. Backup tapes and backups of Cryptomodules are stored offsite in a secure location. In the event of a disaster in which the primary Datacenter becomes inoperative, the disaster recovery site can take over Certificate validation operations promptly, and can provide all other essential CA operations within 72 hours. If both principal and backup CA operations become inoperative, the CA's operations will be re-initiated on appropriate hardware using backup copies of software and Cryptomodules.

Re-initiation will occur according to one of the following contingencies:

- If the CA signature Keys are not destroyed, CA operations will be reestablished, giving priority to the ability to generate Certificate status information within the CRL Issuance schedule specified in Section 4.9.7.
- If the CA signature Keys are destroyed, CA operation will be reestablished as quickly as possible, giving priority to the generation of a new CA Key Pair and Certificate with new DN. The old CA Certificate will be revoked and notification will be placed on a CRL as specified in Section 4.9.3. New Certificates will be issued.

Subscribers will be notified and instructed via email, if provided, and a secure CA site (https://letsencrypt.org/) on how to remove the old Root CA from their Certificate stores and install the new root in their Certificate stores.

If a CA (i.e., Root or subordinate) cannot issue a CRL prior to the time specified in the next-update field of its currently valid CRL, then the Relying Parties and all CAs that have issued Certificates to the CA will be notified informally via telephone call immediately. This call will be followed formally by a Certificate-based communication if possible; otherwise, by a written letter sent via courier service.

A subordinate CA Certificate will be revoked if Revocation services are not reestablished within a reasonable period of time. The period of time will be established by the highest-ranking CA Operations manager and representatives from the CAs Risk Management Committee after analyzing the risk exposure at the time. However, the CA may be revoked at any time. As guidelines, this period should not exceed 18 hours after a Revocation has been requested of any Certificate issued under the CA; or 72 hours after the last CRLs next update, whichever occurs earlier.

When the Root CA Certificate is unable to issue a CRL, the highest-ranking CA Operations manager and representatives from the CA Risk Management Committee will establish the risk exposure and determine whether to stand up a new Root CA Certificate. If a CA has requested Revocation of its Certificate by the root, the risk exposure must be considered as high, and within an 18-hour period after the Revocation has been requested, the procedures described in a prior paragraph in this Section are used to revoke the old Root CA Certificate and to establish and promulgate the new Root CA Certificate.

5.7.3 *CA Private Key Compromise Procedures*

The CA has developed a Key Compromise plan to address the procedures that will be followed in the event of a compromise of the signature Private Key used by the CA to issue Certificates. The plan includes procedures for (and documentation of) revoking all affected Certificates it has issued, and promptly notifying all Subscribers and all Relying Parties.

If CA signature Keys are compromised or lost (such that compromise is possible even though not certain), the CA will:

- Immediately notify all CAs with whom it has cross-certified;
- Revoke all Certificates it has issued using that Key and provide appropriate notice; Generate a new CA Key Pair using appropriate procedures as outlined elsewhere in this CPS;
- Distribute its new CA Certificate using the reliable out-of-band means allowed by this CPS;
- Issue new CA Certificates to subordinate CAs in accordance with this CPS; and
- Ensure all CRLs are signed using the new Key.

The CA will investigate what caused the compromise or loss, and what measures have been taken to preclude recurrence.

Compromise of CA Private Key
In the event that any CA Private Key has been or is suspected to have been compromised, the highest-ranking CA Operations manager available will convene a meeting of management representatives to assess the situation and take appropriate action. CA Trusted Role personnel will implement the procedural steps and tasks that have been outlined for Key compromise in the security incident response plan, including:

- Quantifying the scope, extent and effects of the compromise;
- Revoking the Subordinate CA Certificate and ensuring that it is promptly included in a published CRL;
- Explaining the situation to all employees, and notifying all interested parties (either by Certificate-based communication, telephone, or written letter sent by courier service). Recipients of this communication will include:
    - The PMA;
    - All RAs; and
    - All Subscribers.

As soon as possible, the PMA will investigate the incident, and if necessary will forensically record and analyze the causes of the compromise.

A report will be prepared and delivered to the PMA concerning the causes of the compromise and what measures have been or will be taken to prevent a future recurrence.

After the factors leading up to the Key compromise can be satisfactorily addressed, the CA will generate a new Key Pair and Subordinate CA Certificate with a new DN, in accordance with CA Key generation ceremony procedures. The CA will issue new Subscribers Certificates; upon completing identity proofing processes outlined in Section 3.2, signing them with the new Subordinate CA Certificate; and will issue a new, blank CRL.

Any .p7c, .cer, or other PKCS#7 files that contain or refer to the Certificate, Public Key or corresponding Private Key will be replaced with new files to reflect that a new CA Certificate has been issued. All appropriate HTTP and LDAP pointers will be updated to ensure proper path construction and validation.

Compromise of the Root Private Key
When Revocation of the Root CA Certificate is required, in addition to the foregoing procedures, the CA will immediately notify all browsers that have that specified root. A new Root CA Key Pair, self-signed Root CA Certificate with new DN, and CRL will be generated in a Key generation ceremony consistent with the procedures of Section 6.1.1.

RAs are required by contract to facilitate the replacement of the revoked Root CA Certificate with the new Root CA Certificate in Subscriber and Relying Party applications. The CA will also notify all participants and browsers that the new Root CA Certificate is available in a secure area of the CA website (HTTPS) where it can be downloaded through a server-side encrypted session.

Cross-certified CAs will be asked to submit new Certificate requests.

The CA will notify all interested parties via email, telephone, or written letter sent by courier service. In addition, the CA will set up an informational secure site (https://) that establishes a server-side session.

Compromise of the CSA Key
OCSP Responder Certificates are issued with the nocheck extension (id-pkix-ocsp-nocheck) specifying that OCSP Responder Certificates are not checked by the Relying Party applications for the lifetime of the Certificate. If the CSA Signing Key has been or is suspected to have been compromised, then the highest-rank CA Operations manager available will convene a meeting of personnel involved in CSA operations to assess the degree and scope of the compromise. If it is determined that Private Keys were compromised, a new OCSP Responder Key Pair and Certificate will be immediately created (signed by the Subordinate CA Certificate) and installed in the OCSP Responder as soon as possible.

For any period of compromise, all signed validations for that period (during which the CSA Key was suspected to have been compromised) will be reviewed and either re-signed with a new Key.

5.7.4 *Business Continuity Capabilities after a Disaster*

The CA has a disaster recovery/business resumption plan in place (Business Continuity Plan or BCP) that allows the CA to reconstitute the CA within seventy-two hours of catastrophic failure. The CA's business continuity and disaster recovery plans allow for other nonessential systems to be brought into operation later than seventy-two hours.

If for any reason the CA installation is physically damaged and all copies of the CA signature Key are destroyed as a result, the CA will notify any applicable policy authorities. Relying Parties may decide of their own volition whether to continue to use Certificates signed with the destroyed Private Key pending reestablishment of CA operation with new Certificates.

5.8 CA or RA Termination

In the event that it is necessary for the CA or an RA to cease operation, all affected parties, will be notified of the planned termination, promptly and as far in advance as is commercially reasonable. A termination plan will be created and submitted to the PMA. The termination plan will propose methods of minimizing the disruption to the operations of all parties caused by the planned termination and also include provisions for the following:

Termination of RA
- Archival of all audit logs and other records prior to termination;

- Delivery of current operating records to a responsible successor RA that will provide Certificate Revocation services for the remaining terms of Certificates and accept the assignment of any related, contracted-for support services. Note that if the termination is for convenience, or other non-security related reason, and provisions have been made to continue compromise recovery, compliance and security audit, archive, Revocation, and data recovery services, then the Certificates approved by the RA not need to be revoked. However, all RA System and RA Certificates will be revoked;
- Refund of pro rata portions of Certificate fees and any payments for services that will not be delivered;
- Ensuring the transfer to, and preservation of, archived records by a responsible RA successor for the archive retention period specified in Section 5.5.2;
- Surrender and/or zeroization of Cryptomodules containing Private Keys in accordance with Section 6.2.9 and Revocation of all Certificates, if necessary; and
- If a successor RA will be assuming responsibilities for existing customers, provisions for such transition, e.g. replacement Certificates, customer relations, etc.

Termination of Root CA

In the event that the CA ceases operation, all Subscribers, RAs, CMAs, CSAs, Repositories, and Authorized Relying Parties will be promptly notified of the termination. Browsers will also be informed about the termination. All DV-SSL Certificates issued by the CA that reference the CP will be revoked no later than the time of termination. All current and archived CA identity proofing, Certificate, validation, Revocation, renewal, policy and practices, billing, and audit data will be transferred to the PMA (or designate) within twenty-four hours of the CA cessation and in accordance with the CP. Transferred data will not include any data unrelated to the CP. No Key recovery enabled Repository data will be co-mingled with this data.

6 Technical Security Controls

Technical controls are implemented to reduce the probability of threat to the CA system and its data's integrity. Since the CA assigns operation of the technical systems to a contracting organization, most of the controls in this section pertain to the Contractor, and are so noted.

The Contractor Security Office selects the mix of controls, technologies, and procedures that best fits the risk profile of the system. The CA and all other PKI Participants implement appropriate technical security controls.

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

Key Pairs for all Subscribers must be generated in such a way that the Private Key is not known by any person other than the Key holder.

6.1.1.1 CA Key Pair Generation

Cryptographic Keying material used by the CA to sign Certificates, CRLs or status information is generated in a FIPS-140 validated Cryptomodule. The CA's Cryptomodules meet FIPS 140-2 Level 3.

The CA and CSA Key generation ceremonies are performed in the Secure Room. The ceremony is scripted, video-recorded and witnessed. The ceremony is performed by personnel in Trusted Roles who use different security Keys at the appropriate time depending on whether Key generation, Certificate generation or a Cryptomodule backup/cloning operation is being performed. The scripts and video recording are made available to independent third party auditors during the annual audit for examination.

6.1.1.2 Subscriber Key Pair Generation

Key Pairs for Subscribers can be generated in either hardware or software. For Subscribers, validated software or hardware is used to generate pseudo-random numbers, Key Pairs, and symmetric Keys. Any pseudo-random numbers used for Key generation material is generated by a FIPS approved method.

Subscriber signature Private Keys will not be generated by the CA.

6.1.1.3 Private Key Delivery to Subscriber

The CA does not generate signature Private Keys for Subscribers.

The CA does not deliver Cryptomodules with Private Keys in them, instead Private Keys are generated in a blank Cryptomodule previously delivered to the Applicant/Subscribers through a postal method that allows tracking and confirmation delivery.

6.1.1.4 Public Key Delivery to Certificate Issuer

The Subscriber's Public Key is delivered to the CA in a secure and trustworthy manner. The delivery of the Public Key, in a PKCS#10 structure, binds the Private and Public Keys, through a digital signature, and is submitted to the CA during a server-authenticated SSL/TLS-encrypted session.

The Applicant requests that a certificate be issued by using a "certificateRequest" message, which contains a Certificate Signing Request (CSR) and a signature by the authorized key pair.

6.1.1.5 CA Public Key Delivery to Relying Parties

The CA ensures that Subscribers and Relying Parties receive and maintain the trust anchor(s) in a trustworthy fashion through a Cross-Certifying Entity. Methods implemented for this delivery may include:

(1) The Public Key may be delivered to Subscribers during the Certificate retrieval process for their own Subscriber's Certificates during the server-authenticated SSL/TLS-encrypted session as part of a message formatted in accordance with PKCS#7.

(2) The Public Key may also be delivered through the cryptographic container in the major browsers. The CA maintains a trust anchor for the program that is embedded in the browser through their CA Root programs in association with a Cross-Certifying Entity. This process requires both parties to fulfill specific requirements by the browser manufacturers including providing them with the trust anchor in a secure manner. Browsers distribute the trust anchor and any updates along with the standard distribution of their software in a secure manner.

(3) Relying Parties may also obtain the trust anchor(s) (e.g., Root CA) Certificates from the CA's and the Cross-Certifying Entities' secure web sites. An email or other communication may be sent to participants directing them to download the trust anchor(s) Certificate at an https:// website secured with a valid SSL Certificate that chains to one of the CA's Root Certificates in the browser through the Cross-Certifying Entity. Alternatively, Subscribers and Relying Parties may be directed to an http:// website that is not secured in which case, the CA will provide the hash or fingerprint via authenticated out-of-band sources (i.e., the CA phone support).

6.1.2 Key Sizes

All valid Root CA certificates contain Public Keys of at least 2048 –bit RSA Keys or at least 224-bit ECDSA Keys. Root CA Certificates issues on or after 12/31/10 contain Public 4096-bit RSA Keys or 256-bit ECDSA Keys.

All valid Subordinate CA Certificates contain at least 2048-bit RSA Keys or at least 224–bit ECDSA Keys. All Subscribers Certificates use at least 2048-bit RSA Keys or at least 224-bit ECDSA Keys

CAs issuing Certificates under will use the SHA-256 hash algorithm when generating digital signatures on Certificates, CRLs and OCSP responses.

6.1.3 Public Key Parameters Generation and Quality Checking

Cryptomodules and associated software platforms used by CAs and CSA have been validated as conforming to FIPS 186-4, and provide random number generation and on-board creation of at least 2048-bit Keys for RSA; and at least 224-bit Keys for ECDSA.

The CA ensures that the public exponent of the RSA Keys for a DV-SSL Certificates is in the range between 2 16+1 and 2256-1. The modulus are an odd number, not the power of a prime, and have no factors smaller than 752.

6.1.4 Key Usage Purposes (as per X509 v3 Key Usage Field)

The use of a specific Key is determined by the Key usage extension in the X.509 Certificate. Certificate Key Usage and Extended Key Usage fields are used in accordance with RFC 5280.

The CA sets the Key Usage bits for all Certificates in accordance with this section. For further details see Sections 7 and 10 which address Certificate profiles.

Root CA Certificates
All CA signature Private Keys are used only to sign Certificates and CRLs.
The following Key Usage values are present in the CA Certificates: (i) CRL Signature; (ii) Key Certificate Signature; and (iii) Digital Signature.

Subordinate CA Certificates

The following Key Usage values are present in the Subordinate CA Certificates: (i) CRL Signature; (ii) Key Certificate Signature, and (iii) Digital Signature.

The following Extended Key Usage values are present in the Subordinate Certificates: (i) Server authentication (ip-kp-serverAuth); and (ii) Client authentication (ip-kp-clientAuth).

DV-SSL Device Certificates
The following Key Usage values are present in the SSL Device Certificates: (i) Digital Signature; and (ii) Key Encipherment.

The following extended Key usage values are present: (i) Server Authentication (ip-kp-serverAuth); and (ii) Client Authentication (ip-kp-clientAuth).

OCSP Responder Certificates
The following Key Usage value is present in OCSP responder Certificates: (i) Digital Signature; and (ii) Non Repudiation.

The following Extended Key Usage value is present in OCSP Signing Certificates: (i) id-kp-OCSPSigning {1.3.6.1.5.5.7.3.9}.

Administrative Certificates
The following Key Usage value is present in human Administrative Certificates: (i) Digital Signature; and (ii) Non Repudiation.

6.2 Private Key Protection and Cryptomodule Engineering Controls

The CAs, RAs, CSAs, and CMAs each protects their Private Key(s) in accordance with the provisions of the CP and this CPS.

6.2.1 *Cryptomodule Standards and Controls*

The CA uses only FIPS 140-2 Level 3-validated hardware Cryptomodules for the CA, the OCSP (CSA) and backup Cryptomodules. These modules do not allow output of the private asymmetric Key to plaintext.

Administrative Certificate Subscribers will store their Certificates in at least FIPS 140-2 Level 1-validated software Cryptomodules. If a Subscriber uses a hardware Cryptomodule, it will be validated to at least FIPS 140-2 Level 2. These modules will not allow the user to export Key Pairs in plain text.

The installation, removal, and destruction of all Cryptomodules holding CA (i.e., Root or Subordinate CA) and CSA Keys is documented in writing, approved by management, witnessed, and video recorded.

6.2.2 *Private Key (n out of m) Multi-Person Control*

The CA and CSA signature Private Keys are stored in the Secure Room under multi-person control as discussed in section 5.1.2.1. The PIN Entry Device Keys (PED Keys) are kept in a separate safe. At least one CA Administrator and one System Administrator are required, along with the additional presence of a Security Officer, to retrieve and activate the CA or CSA signature Private Keys.

For purposes of disaster recovery, backups of CA and CSA signature Private Keys are made under two-person control and are stored in the Secure Room and in a secure off-site facility where two-person controls are implemented as explained in sections 5.1.6, 5.1.8 and 5.2.2.

This separation-of-duties/multi-party control prevents a single individual from gaining access to a CA or CSA signature Private Keys.

The individuals taking part in tasks that require two-person control and separation of duties principles are Trusted Roles within the CA. As such, their names are part of a list maintained within the Operations group and made available during audits (see section 5.2.7).

6.2.3 Private Key Escrow

6.2.3.1 Escrow of Authorized CA Signature Private Key

The CA does not escrow the CA Private Keys used to sign Certificates and CRLs.

6.2.3.2 Escrow of Authorized CA Encryption Keys

Not applicable.

6.2.3.3 Escrow of Subscriber Signature Private Keys

The CA does not escrow Subscriber's signature Private Keys. RAs are prohibited under the CP and this CPS from escrowing the signature Private Keys of Subscribers.

6.2.3.4 Escrow of Subscriber's Encryption Private Keys

Subscriber's encryption Private Keys may be escrowed to enable Key recovery. Encryption Private Key escrow is decided on an implementation specific basis.

6.2.4 Private Key Backup

6.2.4.1 Backup of CA Signature Private Keys

Under two-person control, the CA backs up CA Private Keys on cloned Cryptomodules in order to obviate the need to re-key in the case of hardware failure.

Two copies of the Root CA Certificate are created in separate Cryptomodules. Two copies of all other CAs are created in a shared Cryptomodule. All backup Cryptomodules are FIPS 140-2 level 3-validated.

The backup of all other CA Keys is performed during a ceremony that is scripted, video recorded and witnessed under the same controls used for the original Key generation. PED Keys are kept under two-person control as explained in section 5.1.2.1.

The CA stores the Root CA and all other CA Private Keys and one of the copies in the Secure Room. The second backup of the Root CA and all other CAs signature Private Keys are kept in a secure off-site facility. Access to these Private Keys is documented as explained in section 5.1.8.

When the Root CA and all other CAs Keys are no longer needed, the Cryptomodule containing them is zeroized in accordance with section 6.2.9.

The CA will not archive the Private Keys for any issuer that is not the CA. Those Private keys will be held exclusively by that issuer. If those keys are communicated to another party the CA will revoke the Certificates.

6.2.4.2 Backup of Subscriber's Signature Private Key

A Subscriber may optionally back-up his, her or its own Private Key. If so, the Key must be copied and stored in encrypted form and protected at a level no lower than stipulated for the primary version of the Key.

6.2.4.3 Backup of Subscriber's Key Management Private Keys

Encryption Private Keys may be backed up as long as they remain under the control of the Subscriber and are protected and used under conditions protected at a level no lower than stipulated for the primary version of the Key. This level of protection for the Encryption Private Key includes not backing it up in plain text outside of the module.

6.2.4.4 *Backup of CSA Private Key*

Under two-person control, the CA backs up CSA Private Keys on cloned Cryptomodules in order to obviate the need to re-key in the case of hardware failure.

Two copies of all CSAs are created in a shared Cryptomodule. All backup Cryptomodules are FIPS 140-2 Level 3-rated.

The backup of all other CSA Keys is performed during a ceremony that is scripted, video recorded and witnessed under the same controls used for the original Key generation. PED Keys are kept under two-person control as explained in section 5.1.2.1.

The CA stores the CSA Private Keys and one of the copies in the Secure Room. The second backup of the CSA signature Private Keys are kept in a secure off-site facility.

When the CSA Keys are no longer needed, the Cryptomodule containing them is zeroized in accordance with section 6.2.9.

6.2.5 *Private Key Archival*

Under no circumstances will the CA archive the signature Private Key of a Subscriber or its CA signature Private Keys.

Private Key Transfer into or from a Cryptomodule

CA and CSA Private Keys are generated on a FIPS 140-2 Level 3 validated Cryptomodule that allows for a "cloning" process that creates a copy of the Private Keys. The CA uses the cloning process to create one or more copies for purposes of business continuity. The CA Private Keys are backed up in accordance with section 6.2.4.1.

Administrative Certificate Subscriber's signature Private Keys are generated and kept inside of Cryptomodules.

6.2.6 *Private Key Storage on a Cryptomodule*

The CA and CSA Private Keys are stored in FIPS 140-2 level 3 Modules.

For Administrative Certificates held on hardware Cryptomodules, Subscriber's Private Keys are maintained in Cryptomodules evaluated at FIPS Level 2 and never appear in plaintext. For Subscribers using a software-based Cryptomodule, the module may store Private Keys in any form as long as the Keys are not accessible without an authentication mechanism.

6.2.7 *Method of Activating Private Keys*

CA and CSA Private Keys are activated by using activation data stored securely and separately from the Cryptomodules in which they are kept. Activation of the Private Key requires a PED Key to be connected to the module. The PED Keys and Cryptomodules are stored in separate safes. PED Keys and Cryptomodules are retrieved and used always under two-person control. The Private Key is activated by use of the PED Key during a ceremony.

Administrative Certificate Subscribers must protect their Private Key from unauthorized use with a strong password, whose constrains are consistent with a FIPS 140-2 module specification. Subscribers of Administrative Certificates are instructed to protect their Private Key from unauthorized use with a strong password.

Subscribers are obligated by contract, the CP and this CPS to authenticate to the module before the activation of the Private Key, as well as to protect the password or other data used to activate it from disclosure.

6.2.8 *Method of Deactivating Private Keys*

The CA and CSA Cryptomodules when active are not exposed to unauthorized access. The modules are maintained in the Secure Room that requires two-person control. In addition, the modules are enclosed in locked steel cabinets. When not in use, a module is deactivated via logout procedures, removed and stored in accordance with section 5.1.2.1.

Subscribers are notified of their obligation to not leave their Cryptomodules unattended or open to unauthorized access while active. Subscribers are required to deactivate the modules either by a manual logout or by configuring a passive timeout that does it automatically.

6.2.9 *Method of Destroying Private Keys*

Upon expiration or Revocation of a CA, CSA or RA System Certificate, or other termination of use of the signature Private Key, all copies of the signature Private Key are securely destroyed by CA personnel in Trusted Roles. When no longer needed, all Private Keys are destroyed in accordance with the FIPS 140-validated zeroize destruction method that is part of the Cryptomodule's design (Physical destruction of the Cryptomodule is not required).

Subscribers are notified of their obligation to destroy their signing Private Keys and are provided instructions on zeroizing, re-initializing or destroying the Cryptomodules when they are no longer needed, or when the Certificates to which they correspond are expired or revoked.

6.2.10 *Cryptomodule Rating*

Requirements for Cryptomodules are as stated above in section 6.2.1.

6.3 Other Aspects of Key Management

6.3.1 *Public Key Archival*

No stipulation.

6.3.2 *Certificate Operational Periods and Key Usage Periods*

All Certificates and corresponding Keys pairs have maximum Validity Periods in accordance with the following table:

Periods / Key Type	Certificate Lifetime	Key Usage Period
Root CA	20 years	20 years
Root OCSP	30 days	3 years
Intermediate CA	6 years	6 years
Intermediate OCSP	30 days	3 years
DV-SSL Certificates	Up 12 months	Up 12 months
CA Administrative Certificates	3 years	3 years

Subscriber Key Pairs must be replaced in accordance with the provisions of Section 3.3.1.

6.3.3 *Restrictions on Authorized CA's Private Key Use*

The CA implements a Root CA Certificate that is used only to sign subordinate CA Certificates and provide validation services (i.e., OCSP Certificate and CRLs). Subordinate CA Certificates issued by the CA are similarly used to sign Certificates and provide validation services only.

If the RA is an automated system, the Private Key and Certificate are only used for access control and communication protection between the RA and the CA.

The CA Signature Keys used to support non-repudiation are not escrowed.

6.4 Activation Data

6.4.1 *Activation Data Generation and Installation*

A pass-phrase, PIN or other activation data is used to protect access to the Private Keys used by the CA or Subscribers.

The CA uses a manually-held Key share PED and PED Keys to activate its Private Keys for CAs and CSAs. The activation data meets the requirements of FIPS 1402 Level 3. The PED and PED Keys are held in the Secure Room under the two-person controls to enforce Split-Knowledge Technique.

Administrative Certificate Subscribers are instructed to use strong passwords in accordance with the FIPS 140 guideline in accordance with the level of the Cryptomodule.

6.4.2 *Activation Data Protection*

Activation data for Cryptomodules used by CAs and CSAs are protected by keeping the PED Keys in separate safes inside of the Secure Room. Access to the Secure Room requires two individuals in Trusted Roles. Access to the content in the safe requires a password and a Key, each one held by a different individual to enforce Split-Knowledge Technique.

When activation data is in the form of a PIN or password, Subscribers are notified of their obligation to protect activation data as follows:

- It should be memorized, not written down;
- If written down, it must be secured at the level of the data that the associated Cryptomodule is used to protect, and will not be stored with the Cryptomodule; and
- Activation data must never be shared with or disclosed to another individual.

Alternatively, activation data could be biometric in nature.

6.4.3 *Other Aspects of Activation Data*

No stipulation.

6.5 Computer Security Controls

The CA operates a variety of commercial software and hardware systems to provide CA, CSA, RA, and Repository services. The CA operates these software systems on Solaris, UNIX, Linux and Windows platforms. These systems are regularly scanned for potential security compromises and software is run locally to prevent such compromises. Machines running on the Windows platform are for client interface purposes only.

6.5.1 *Specific Computer Security Technical Requirements*

For access to all of the CAs systems, user ID/password, cryptographic-module-based, and/or biometrics authentication schemes are used. The use and enforcement of password security are in accordance with The CA security policy and supporting security guidelines. The same policies and procedures apply to both the primary and DR sites, and to the CA and the Contractor organizations.

Users are required to identify themselves uniquely before being allowed to perform any actions on the system. The CA system internally maintains the identity of all users throughout their active sessions on the

system and is able to link actions to specific users. Identification data is kept current by adding new users and deleting former ones. User IDs that are inactive on the system for a specific period of time (e.g., three months) are disabled. The CA authenticates all data requests from the application.

The Contractor's System Security Plan (SSP) described the self-protection techniques for user authentication, any policies that provide for bypassing user authentication requirements, single-sign-on technologies (host-to-host authentication servers, user-to-host identifier, and group user identifiers), and any compensating controls.

The CA's accountability covers a trusted path between the user and the system. A trusted path is a secure means of communication between the user and the system. For example, when a user types in their account name and password, the user wants to be sure that it is the system that the user is talking to, not a malicious program that someone else has left running on the terminal.

Users are restricted to data files, processing capability, or peripherals, and type of access (read, write, execute, delete) to the minimum necessary for the efficient completion of their job responsibilities. The CA's physical access controls are designed and/or configured to provide least privilege.

The CA provides technical access controls designed to provide least privilege and protections against unauthorized access to the CA's system resources. Technical controls are developed and implemented in accordance with best industry practices, U.S. Federal law, and applicable regulations and guidelines. The CA or Contractor describes the technical security controls in the SSP.

The systems support a lock-out threshold if excessive invalid access attempts are input, and record when an administrator unlocks an account that has been locked as a result or unsuccessful authentication attempts. User IDs are revoked if a password attempt threshold failed login attempts is exceeded.

The CA systems are able to create, maintain, and protect from modification, unauthorized access, or destruction an audit trail of accesses to the resources it protects in accordance with Federal law, regulations, and guidelines. Activity-auditing capabilities are employed and enabled on all CA information systems to maintain a record of system activity by system or application processes and by users.

6.5.2 *Computer Security Rating*

No stipulation.

6.6 Life Cycle Technical Controls

6.6.1 *System Development Controls*

For commercial off-the-shelf software, the CA selects vendors that design and develop applications using formal development methodologies and as a consequence have received security certifications supporting their assertions.

The CA develops some PKI software components and standard development methodologies are used. Strict quality assurance is maintained throughout the process. Documentation is maintained supporting the process. Development and testing environments are maintained on separate servers in a separate network from the main operational environment with appropriate segregation rights restricting developers and testers from having access to production equipment.

When open source software is used, it is selected focusing on specific functionality, and it goes through unit and integration testing on a controlled environment. Then, when it is used in development the entire developed module goes through the standard change control process.

The CA has a process in place to minimize the likelihood of any component being tampered with vendors selected are chosen based on their reputation in the market, ability to deliver quality product, and likelihood

of remaining viable companies in the future. Controls ensure that management is involved in the vendor selection and purchase decision process. External purchasing paperwork will only generically identify the purpose for which the component will be used. CA, CSA, and RA hardware and software PKI components are shipped directly to a trusted employee using shipping providers that have shipment tracking mechanisms allowing continuous tracking. Tracking information is provided to the CA directly by the equipment vendor. Cryptomodules are received in tamper-evident containers. Cryptomodule's shipment specific information (e.g., Serial Number) is requested by the CA in order to confirm the content when it is received. Other major PKI components (i.e., servers) are shipped under standard conditions. At reception, a chain of custody is maintained from that point forward and information provided by the vendor during the purchase order process is used to confirm the correct equipment has been received.

The CA dedicates a PKI platform specifically to its PKI operations including the CA, CSA and RA functions. This includes server hardware, operating system software, Cryptomodule, and PKI application software. No non-PKI applications are installed on those PKI platforms.

The CA maintains controls to prevent malicious software from being loaded. CA, CSA and internal RA platforms are protected by a host-based Fault Integrity Checker that monitors files in the system weekly to alert of any unapproved changes and informs the System Administrator, CA Administrator and Security Officers enabling them to correct the situation. RAs are required to take reasonable care to prevent malicious software from being loaded on their equipment. Only applications required to perform the RA functions are loaded on an RA's computer, and all such software will be obtained from sources authorized by local policy. Data on RA equipment must be scanned for malicious code on first use and at least weekly afterward. Equipment updates are purchased or developed in the same manner as original equipment, and are installed by trusted and trained personnel in a defined manner.

6.6.2 *Security Management Controls*

The CA has mechanisms in place to control and monitor the configuration of its CA, CSA and RA systems. The CA installs its equipment and software in a controlled environment using a documented change control process. Software, when first loaded, is verified using file checksums provided by vendors at the file or file archive level. Upon installation time, and at least once every 24 hours, the integrity of the CA system must be validated.

Change control processes consist of a change control form that is processed, logged and tracked for any changes to CA, CSA and internal RA systems, firewalls, routers, software and other access controls. File modifications are controlled through the change control process. In this manner, the CA can verify whether a change to the system has been properly evaluated for risk mitigation and authorized by management. Hashes for CA, CSA systems files are recorded on installation and validated weekly thereafter as explained in the previous section. Host based intrusion detection is utilized to alert for changes to files. Notifications are monitored and are reviewed on a daily basis.

6.6.3 *Life Cycle Security Ratings*

No stipulation.

6.7 Network Security Controls

The CA implements a multi-tiered network utilizing the principles of defense in depth, such as multi-tiered security and redundancy. This infrastructure is comprised of firewalls, proxy servers, and intrusion detection systems.

Any accounts, port, protocols added to the firewall configurations is documented, authorized, tested and implemented in accordance with the System Security Plan and other relevant policies and procedures. Firewalls are configured with a minimum number of accounts. Only services and protocols required to support CA, CSA and RA functions are enabled. Firewalls and boundary control devices are configured to allow access only by the addresses, ports, protocols and commands required for the trustworthy provision of PKI services by such systems. The CA blocks all ports and protocols by default and open only the

minimum necessary ports to enable CA, CSA and RA functions. Any network software present on firewalls is required to their functioning. All CA, CSA, RA and Repository computer systems are located in a secure facility behind the previously mentioned multi-tiered infrastructure.

Remote access to the CA system is restricted to secure methods employing approved I&A as well as intrusion detection and unauthorized access monitoring.

If encryption is used to prevent unauthorized access to sensitive files as part of the system or application access control procedures, the following information is provided:

- The cryptographic methodology (e.g., secret Key and Public Key) used;
- If a specific off-the-shelf product is used, the name of the product;
- If the product and the implementation method meet Federal standards (e.g., Data Encryption Standard, digital signature Standard), include that information; and
- Cryptographic Key management procedures for Key generation, distribution, storage, entry, use, destruction, and archiving.

6.7.1 *Interconnections*

The CA system is connected to one network and is protected against known network attacks. The CA Root is kept offline and turned on under controlled conditions only when necessary for signing Subordinate CA Certificates.

6.8 Time Stamping

The CA's system clock time is derived from multiple trusted third party time sources in accordance with applicable requirements and is used to establish timestamps for the following:

- Initial validity time of a Certificate;
- Revocation of a Certificate;
- Posting of CRLs and CRL updates;
- OCSP Responses; and
- System audit journal entries.

System time for servers providing CA and CSA services are updated using the Network Time Protocol (NTP) to synchronize system clocks at least once every 60 minutes. Trusted external time sources operated by government agencies are used to maintain an average accuracy of one second or better.

Clock adjustments are auditable events listed with other events in the log available for auditors.

7 Certificate, CRL, and OCSP Profiles

7.1 Certificate Profiles

7.1.1 Version Number(s)

All Certificates issued under this policy conform to version 3 of ITU X.509

All Certificates issued under this policy will contain a non-sequential serial number with entropy of at least 20 bits

7.1.2 Certificate Extensions

This section shows all the extension supported in each of the Certificates issued under this policy

Root CA Certificate

- **basicConstraints.** This extension is present and marked critical. The cA value set to true. The pathLenConstraint field is not present.
- **keyUsage.** This extension is present and marked critical. The bit positions for keyCertSign and cRLSign are set.
- **subjectKeyIdentifier.** This extension is present and is marked non-critical. It contains the SHA-1 hash of the subjectPublicKey.

Subordinate CA Certificates:

- **authorityKeyIdentifier.** This extension is present and is marked non-critical. It contains the identifier defined in the subjectKeyIdentifier extension of the issuer CA certificate
- **subjectKeyIdentifier.** This extension is present and is marked non-critical. It contains the SHA-1 hash of the subjectPublicKey.
- **keyUsage.** This extension is present and marked critical. Bit positions for keyCertSign and cRLSign are set. When the Subordinate CA Private Key is used for signing OCSP responses, the digitalSignature bit is also set.
- **extkeyUsage.** This extension is optional and marked as critical when present. Subordinate CA Certificates issuing DV-SSL are technically constrained by including the values id-kp-serverAuth and id-kp-clientAuth.
  Subordinate CA Certificates issuing Administrative Certificates do not have this extension.
- **certificatePolicies.** This extension is present and marked non-critical. It includes the at least one policyIdentifier, a cPSuri and a userNotice.
- **basicConstraints.** This extension is present and marked critical. The cA value set to true. The pathLenConstraint field is present with a value of zero (0).
- **nameConstraints.** This extension is optional and marked non-critical if present. The excludedSubtrees field is present and the iPAddress field includes exclusions for all IPv4 and IPv6 IP addresses.

- **authorityInformationAccess.** This extension is present and marked non-critical. It contains the HTTP URL of the CA's OCSP responder (accessMethod= 1.3.6.1.5.5.7.48.1). It also contains the HTTP URL of the CA's certificate (accessMethod = 1.3.6.1.5.5.7.48.2).

- **cRLDistributionPoints.** This extension is present and marked non-critical. It contains the HTTP URL of the CA's CRL service.

DV-SSL Certificates:

- **authorityKeyIdentifier.** This extension is present and is marked non-critical. It contains the identifier defined in the subjectKeyIdentifier extension of the issuer CA certificate

- **subjectKeyIdentifier.** This extension is present and is marked non-critical. It contains the SHA-1 hash of the subjectPublicKey.

- **keyUsage.** This extension is present and marked critical. Bit positions for digitalSignature and keyEncipherment are set.

- **extkeyUsage.** This extension is present and marked non-critical. It includes the values id-kp-serverAuth and id-kp-clientAuth.

- **certificatePolicies.** This extension is present and marked non-critical. It includes the at least one policyIdentifier, a cPSuri and a userNotice.

- **subjectAltName.** This extension is present and marked non-critical. It includes at least one dNSName entry containing the Fully-Qualified Domain Name. No iPAddress entries are included.

- **authorityInformationAccess.** This extension is present and marked critical. It contains the HTTP URL of the CA's OCSP responder (accessMethod= 1.3.6.1.5.5.7.48.1). It also contains the HTTP URL of the CA's certificate (accessMethod = 1.3.6.1.5.5.7.48.2).

Administrative Certificates:

- **authorityKeyIdentifier.** This extension is present and is marked non-critical. It contains the identifier defined in the subjectKeyIdentifier extension of the issuer CA certificate

- **subjectKeyIdentifier.** This extension is present and is marked non-critical. It contains the SHA-1 hash of the subjectPublicKey.

- **keyUsage.** This extension is present and marked critical. Bit positions for digitalSignature and nonRepudiation are set.

- **certificatePolicies.** This extension is present and marked non-critical. It includes one policyIdentifier, a cPSuri and a userNotice.

- **subjectAltName.** This extension is present and marked non-critical. It includes the rfc822Name containing the email address of the Subscriber.

- **authorityInformationAccess.** This extension is present and marked critical. It contains the HTTP URL of the CA's OCSP responder (accessMethod= 1.3.6.1.5.5.7.48.1). It also contains the HTTP URL of the CA's certificate (accessMethod = 1.3.6.1.5.5.7.48.2).

OCSP Certificates:

In addition to the standard extensions, the following are included

- **authorityKeyIdentifier.** This extension is present and is marked non-critical. It contains the identifier defined in the subjectKeyIdentifier extension of the issuer CA certificate

- **subjectKeyIdentifier.** This extension is present and is marked non-critical. It contains the SHA-1 hash of the subjectPublicKey.

- **keyUsage.** This extension is present and marked critical. Bit positions for digitalSignature and nonRepudiation are set.

- **extkeyUsage.** This extension is present and marked non-critical. It includes the value id-kp-OCSPSigning.

- **subjectAltName.** This extension is present and marked non-critical. It includes the dNSName entry containing the Fully-Qualified Domain Name of the HTTP URL.

- **id-pkix-ocsp-nocheck.** This extension is present and marked non-critical. The value is NULL.

7.1.3 *Algorithm Object Identifiers*

The CA will use the following algorithms to sign Certificates, CRLs and OCSP responses

sha256WithRSAEncryption	{ iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1)pkcs-1(1) 11 }
ecdsa-with-SHA256	{iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2 (3) 2}

The CA will use the following algorithms to generate Keys:

rsaEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1}
id-ecPublicKey	{iso(1) member-body(2) us(840) ansi-x9-62(10045) public key-type (2) 1}

For certificates that contain an elliptic curve public key, the following named curves are used:

Curve P-256	ansip256r1 ::= { iso(1) member-body(2) us(840) ansi-X9-62(10045) curves(3) prime(1) 7 }
Curve P-384	ansip384r1 ::= { iso(1) identified-organization(3) certicom(132) curve(0) 34 }

7.1.4 *Name Forms*

The following table describes the name forms for the CA Certificates.

Identifier type:	*with data content of:*	*Indicates:*
Subject: CountryName (C)	**Root CA** The ISO 3166-1 two-letter code. In this case "US" **Subordinate CA** The ISO 3166-1 two-letter code. In this case "US"	**Root CA** That the Root Certificate is managed by a CA operated in the United States. **Subordinate CA** That the Subordinate CA Certificate is managed by a CA operated in the United States.

Identifier type:	*with data content of:*	*Indicates:*
Subject: OrganizationName (O)	**Root CA** The word "ISRG" **Subordinate CA** The word "ISRG"	**Root CA** That the Root CA is owned and operated by ISRG. **Subordinate CA** That the Subordinate CA is owned and operated by ISRG.
subject:CommonName (CN)	**Root CA** The alphanumeric text "ISRG Root CA *[n]*" **Subordinate CA** The alphanumeric text "ISRG DV-SSL CA *[m]*" Or "ISRG Admin CA *[m]*	**Root CA** The name of the Root CA. A progressively increasing number *[n]* is appended to indicate the instance of the Root CA Certificate. **Subordinate CA** The name of the Subordinate CA Certificate. A progressively increasing number *[m]* is appended to indicate the instance of the subordinate CA.
nameConstraint: excludedSubtrees: generalName:iPAddress	**Subordinate CA** Octet strings as specified in RFC791 for IP version 4, and RFC 2460 for IP version 6.	**Subordinate CA** The space of IP addressed for IP version 4 and IP version 6 that are excluded from issuance.

The following table describes the name forms for the DV-SSL Certificates.

Identifier type:	*with data content of:*	*Indicates:*
subject:CommonName (CN)	Alphanumeric text	The Fully Qualified Domain Name of the server being certified
subjectAltName:dNSName	Alphanumeric text expressed in IA5String data type	The Fully Qualified Domain Name(s) of the server being certified. No wildcard Domain Names are allowed under this policy.

The following table describes the name forms for the human Administrative Certificates.

Identifier type:	*with data content of:*	*Indicates:*
Subject: CountryName (C)	The ISO 3166-1 two-letter code. In this case "US"	The two-letter code indicating the country where the Subscribing Organization for Administrative Certificates is located
Subject: OrganizationName (O)	The word "ISRG"	The name of Subscribing Organization issuing the Administrative Certificate
subject: OrganizationUnitName (OU)	The words "Administrative Certificate"	The that these Certificates are issued for administrative purposes
subject:CommonName (CN)	Alphanumeric text	The Subscriber's name vetted in accordance with Section 3.2.2.1. Name format consist of first name, middle initial and last name each separated from the next by a space character. If middle initial is not present, first name and last name are separated by one space character.

subjectAltName: rfc822name	The e-mail address in the form prescribed by IETF RFC 2822	An e-mail address at which the Subscriber can receive messages via SMTP.

The following table describes the name forms for the Certificates used by OCSP Responders.

Identifier type:	*with data content of:*	*Indicates:*
Subject: CountryName (C)	The ISO 3166-1 two-letter code. In this case "US"	The two-letter code indicating the country where the Subscribing Organization for Administrative Certificates is located
Subject: OrganizationName (O)	The word "ISRG"	The name of Subscribing Organization issuing the Administrative Certificate
subject:CommonName (CN)	Alphanumeric text	The name of the OCSP Responder. The name is constructed based on the CA name and the words "OCSP Signer". For example, for the first Root CA the name would be "ISRG Root CA 1 OCSP Signer"
subjectAltName:dNSName	Alphanumeric text expressed in IA5String data type	The domain name of the OCSP Responder identified in the Certificate

7.1.5 Name Constraints

The Subordinate CA issuing DV-SSL Certificates is not allowed to use IP addresses. This is indicated by including the entire space of IP version 4 and IP version 6 address ranges in the excludedSubtres field of the NameConstrain extension.

The Certificate includes within excludedSubtrees an iPAddress GeneralName of 8 zero octets (covering the IPv4 address range of 0.0.0.0/0). The Certificate also includes within excludedSubtrees an iPAddress GeneralName of 32 zero octets (covering the IPv6 address range of 0:0:0:0:0:0:0:0/0).

7.1.6 Certificate Policy Object Identifier

Certificates issued under this policy assert the appropriate OID to the type of certificate (DV-SSL, Administrative) as specified in Section 1.2.2.

7.1.7 Usage of Policy Constraint Extension

This extension is not used in Certificates issued to CAs under this policy.

7.1.8 Policy Qualifiers, Syntax, and Semantics

Subordinate CA, DV SSL and Administrative Certificates include both the CPSuri and UserNotice policyQualifiers.

The CPSuri includes and IA5String with an HTTP URL to this CPS.

The UserNotice incorporates this CPS by reference and makes it binding to all participants. By using or otherwise relying on a Certificate, the Relying Party accepts and consents to not only the language in the UserNotice, but also to the applicability of this CPS including limitations of liability, disclaimers of warranties, applicable law, and other notices and disclosures made herein that may be determined to have been necessarily made within the Certificate.

Policy Qualifiers are populated as follows:
Policy Qualifier Id=CPS
Qualifier: http://*cp.letsencrypt.org/*

Policy Qualifier Id=User Notice
Qualifier Text = This Certificate may only be relied upon by Relying Parties and only in accordance with the Certificate Policy found at https://letsencrypt.org/repository/

7.1.9 *Processing Semantics for the Critical Certificate Policies Extension*

Not applicable, the Certificate Policies extension is marked non-critical.

7.2 CRL Profile

7.2.1 *Version Number(s)*

All CRLs issued under this policy conform to version 2 CRLs of ITU X.509

7.2.2 *CRL and CRL Entry Extensions*

This section shows all the extensions supported in each of the CRLs issued under this policy. CRLs are issued only by the Root CA.

- **authorityKeyIdentifier.** This extension is present and is marked non-critical. It contains the identifier defined in the subjectKeyIdentifier extension of the issuer CA certificate (Root CA Certificate)
- **CRLnumber.** This extension is present and is marked non-critical. It contains a monotonically increasing sequence number.

7.3 OCSP Profiles

Details for OCSP Responders Certificates are addressed in Section 7.1. Details about the OCSP requests and responses are specified below and in Section 10.

7.3.1 *Version Number(s)*

OCSP requests and responses conform to version 1.

7.3.2 *OCSP Extensions*

The nonce cryptographically binds a request and a response to prevent replay attacks. The nonce is included as one of the requestExtensions in requests; while in responses it would be included as one of the responseExtensions. In both the request and the response, the nonce will be identified by the object identifier id-pkix-ocsp-nonce, while the extnValue is the value of the nonce.

The nonce may be included in the response only if it is included in the request.

7.3.3 *OCSP Signature*

Clients requesting a Certificate status shall be able to process responses signed using RSA with SHA-256 (sha256WithRSAEncryption). Clients may optionally provide another signature algorithm. In this particular implementation, the other option is ECDSA with SHA-256 (ecdsa-with-SHA256). The mechanism for a client to express such preference is the PreferredSignatureAlgorithms (id-pkix-ocsp-pref-sig-algs) extension in its request.

If id-pkix-ocsp-pref-sig-algs is present in the request, the OCSP responder may sign the responses with an algorithm included in the request. The OCSP responder will select the signature algorithm using methods described RFC 6960 Section 4.4.7.2.1 and 4.4.7.2.2.

7.3.4 *OCSP Response for Non-issued Certificates*

When the OCSP responder receives a request for status of a certificate that has not been issued, then the responder will respond with an "unknown" status

8 Compliance Audits and Other Assessments

8.1 Frequency of Audit or Assessments

The CA has a regularly scheduled compliance audit mechanism in place to ensure that the requirements of the CP and CPS are implemented and enforced. The security policy describes how the security features and controls of the CA systems are to be tested and reviewed when significant modifications are made. Full or partial audit results may be released to the extent permitted by law, regulation, contract, or CA management.

The CA also conducts a separate internal audit to ensure the DV-SSL Certificates are adhering to requirements of the CP for quality Issuance. These are conducted quarterly on randomly selected 3 percent of the DV-SSL Certificates chosen from the period immediately after the prior audit. Results from these quarterly audits are saved and provided upon request to third-party auditors meeting the criteria in 8.2.

8.2 Identity and Qualifications of Assessor

To perform the compliance audit, the CA engages the services of a professional auditing firm having the following qualifications:

(1) Focus and experience. Auditing must be one of the firm's principal business activities. Moreover, the firm must have experience in auditing secure information systems and Public Key Infrastructures (PKI).

(2) Expertise: The firm must have a staff of auditors trained and skilled in the auditing of secure information systems. The staff must be familiar with PKI, certification systems, and the like, as well as internet security issues (such as management of a security perimeter), operations of secure Datacenters, personnel controls, and operational risk management. The staff must be large enough to have the necessary depth and range of expertise required to audit the CA's operations.

(3) Reputation: The firm must have a reputation for conducting its auditing business competently and correctly.

(4) Disinterest: The firm has no financial interest, business relationship, or course of dealing that could foreseeably create a significant bias for or against the CA (or the RA being audited).

(5) Rules and standards: The firm must conform to applicable standards, rules, and best practices promulgated by the American Institute of Certified Public Accountants (AICPA), the Chartered Professional Accountants of Canada (CPA Canada; formerly known as the Canada Institute of Chartered Accountants), the Institute of Chartered Accountants of England & Wales (ICAEW), the International Accounting Standards adopted by the European Commission (IAS), Information Systems Audit and Control Association (ISACA), the Institute of Internal Auditors (IIA), or another qualified auditing standards body, and must require its audit professionals to do the same.

Moreover, in auditing secure information systems, the independent firm should be guided by generally accepted standards for evaluating secure information systems such as ISO 27001, Annex B of ANSI X9.79, or ISO 21188. The auditing firm will also maintain professional liability/errors & omissions insurance with policy limits of at least one million US dollars in coverage. The engagement of the auditing firm takes the form of a contract obligating the firm to assign members of its professional auditing staff to perform the audit when required. While the audit is being performed, those staff must, by agreement, perform the audit as their primary responsibility.

In addition, the members of the firm's staff performing the audit are contractually subject to the following requirements:

(1) Professional qualifications: Each external auditing professional performing the audit must be a member of the AICPA, CPA Canada, ICAEW, ISSA, (ISC)2, IIA, or ISACA. In addition, at least one staff member must be qualified as a Certified Information Systems Auditor, AICPA Certified Information Technology Professional (CPA.CITP), or have another recognized information security auditing credential.

(2) Primary responsibility: The external auditing professional assigned by the auditing firm to take the lead in the audit must have the audit as his or her primary responsibility until the audit is completed. That staff member and the CA will agree on a project plan before beginning the audit to ensure that adequate staff, other resources, and time are provided.

(3) Conformity to professional rules: Each external professional active in auditing the CA must conform to the ethical and other professional rules of the AICPA, CPA Canada, ICAEW, ISSA, (ISC)2, IIA, or ISACA or those of the applicable other qualified auditing standards body.

(4) Professional background: The external professionals assigned to perform the audit must be trained to a standard generally accepted in the auditing field. They should also be familiar with PKI and other information security technologies and their secure operation. The CA's operations are audited to ensure that the CA conforms to its CP and CPS and familiarity with those documents is necessary for performing the audit for either the CA or for an RA. The CA expects that other PKI Participants will do the same as appropriate for their functions.

8.3 Assessor's Relationship to Assessed Entity

The CA's compliance auditors are representatives from independent security audit firms specializing in information systems and network security, and private, unaffiliated and nationally recognized accounting firms.

The CA has a contractual relationship with the auditing firm for performance of the audit, but otherwise, auditors are independent, unrelated entities having no financial interest in each other. Auditors maintain a high standard of ethics designed to ensure impartiality and the exercise of independent professional judgment, subject to disciplinary action by their licensing bodies. The auditor(s) have no other relationships with the CA or its officers and directors, including financial, legal, social or other relationships that would constitute a conflict of interest.

8.4 Topics Covered by Assessment

The CA's engagement of its auditors requires them to audit the CA's operations for conformity to the CP, this CPS and every Memorandum of Agreement (MOA) between the CA and other PKIs, if any.

8.5 Actions Taken as a Result of Deficiency

For audits of the CA's operations, if the auditor finds discrepancies between how the CA is designed or is being operated or maintained as a CA, the requirements of the CP or this CPS or any applicable MOAs, the following actions will be performed:

- The auditor will note the discrepancy;
- The auditor will notify the PMA about the discrepancy;
- The PMA will address any identified discrepancies with the CA; and
- The CA will correct any deficiencies noted during compliance reviews, as specified by the PMA including proposing a remedy and expected time for completion.

Also, if irregularities are found during OCC compliance audits, the OCC may require appropriate remedial action or terminate the CA's operations after appropriate notice to existing clients. The results of

compliance audits will not be made public except as described in section 8.6.Results of the C&A review will be made available to the PMA to approve or disapprove after due consideration.

8.5.1 *Actions Taken as a Result of Internal Audit Deficiency*

If the quarterly internal DV-SSL audit shows discrepancies between Certificates and the requirements of the CP and this CPS, the following actions will be performed:

- The Security Officer will note the discrepancy;
- The Security Officer will notify the CIO about the discrepancy;
- The CIO will address any identified discrepancies with the CA;
- The CA will correct any deficiencies noted during compliance reviews, as specified by the Security Officer including proposing a remedy and expected time for completion.

8.6 Communication of Results

The results of the CA's compliance audit and the C&A are fully documented, and reports resulting from it are submitted to the PMA within thirty calendar days of the date of their completion. Such reports will identify the CP and CPS used in the assessment including their dates and version numbers.

The CA posts its auditor's WebTrust for CA certification on its web site in accordance with applicable AICPA audit-reporting standards. Audit information that might pose an immediate threat of harm to Program Participants or that could potentially compromise the future security of the CA's operations is not made publicly available.

8.6.1 *Communication of Internal Audit Results*

The results of the CA's internal Certificate Issuance quality audit for DV-SSL Certificates for the CA are fully documented, and reports resulting from it are submitted to management for review within 30 calendar days of the date of their completion by the Security Office. Such reports will identify the CP and CPS used in the assessment including their dates and version numbers.

9 Other Business and Legal Matters

9.1 Fees

9.1.1 Certificate Issuance or Renewal Fees

ISRG does not charge any fees for certificate issuance or renewal.

9.1.2 Certificate Access Fees

No stipulation.

9.1.3 Revocation or Status Information Access Fee

ISRG does not charge any fees for certificate revocation or for checking the validity status of an issued certificate using a CRL or OSCP.

9.1.4 Fees for Other Services

No stipulation.

9.1.5 Refund Policy

ISRG collects no fees, and so provides no refunds.

9.2 Financial Responsibility

9.2.1 Insurance Coverage

No stipulation.

9.2.2 Other Assets

No stipulation.

9.2.3 Insurance or Warranty Coverage for End-entities

No stipulation.

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

The CA will not collect confidential business information from Subscribers.

9.3.2 Information not within the Scope of Confidential Information

Not applicable.

9.3.3 Responsibility to Protect Confidential Information

ISRG employees, agents, and contractors are responsible for protecting confidential information and are bound by ISRG's policies with respect to the treatment of confidential information or are contractually obligated to do so. Employees receive training on how to handle confidential information.

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

ISRG follows the privacy policy posted on its website (https://letsencrypt.org/repository/) when handling personal information.

9.4.2 Information Treated as Private

The privacy policy posted on ISRG's website (https://letsencrypt.org/repository/) identifies information that ISRG treats as private.

9.4.3 Information not Deemed Private

The privacy policy posted on ISRG's website (https://letsencrypt.org/repository/) identifies information that ISRG does not treat as private.

9.4.4 Responsibility to Protect Private Information

ISRG employees and contractors are subject to policies or contractual obligations requiring them to comply with ISRG's privacy policy (https://letsencrypt.org/repository/) or contractual obligations at least as protective of private information as ISRG's privacy policy.

9.4.5 Notice and Consent to use Private Information

ISRG follows the privacy policy posted on its website (https://letsencrypt.org/repository/) when using personal information.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

ISRG may disclose personal information if compelled to do so by court order or other compulsory legal process, provided that ISRG will oppose such disclosure with all legal and technical tools reasonably available to ISRG.

9.4.7 Other Information Disclosure Circumstances

ISRG may disclose personal information under other circumstances that are described in the privacy policy posted on its website (https://letsencrypt.org/repository/).

9.5 Intellectual Property Rights

ISRG and/or its business partners own the intellectual property rights in ISRG's services, including the certificates, trademarks used in providing the services, and this CPS. Certificate and revocation information are the property of ISRG. ISRG grants permission to reproduce and distribute certificates on a non-exclusive and royalty-free basis, provided that they are reproduced and distributed in full. Private Keys and Public Keys remain the property of the Subscribers who rightfully hold them.

Notwithstanding the foregoing, third party software (including open source software) used by ISRG to provide its services is licensed, not owned, by ISRG.

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

Except as expressly stated in this CPS or in a separate agreement with a Subscriber, ISRG does not make any representations or warranties regarding its products or services. ISRG represents and warrants, to the extent specified in this CPS, that:

1. ISRG complies, in all material aspects, with the CP and this CPS,
2. ISRG publishes and updates CRLs and OCSP responses on a regular basis,
3. All certificates issued under this CPS will be verified in accordance with this CPS and meet the minimum requirements found herein and in the CA/B Forum Baseline Requirements, and
4. ISRG will maintain a repository of public information on its website.

9.6.2 RA Representations and Warranties

Each RA represents and warrants that:

1. The RA's certificate issuance and management services conform to the ISRG CP and this CPS,
2. Information provided by the RA does not contain any false or misleading information,
3. Translations performed by the RA are an accurate translation of the original information, and

4. All certificates requested by the RA meet the requirements of this CPS.

ISRG's agreement with the RA may contain additional representations and warranties.

9.6.3 *Subscriber Representations and Warranties*

1. Each Subscriber warrants to ISRG and the public-at-large that Subscriber is the legitimate registrant of the Internet domain name that is, or is going to be, the subject of the ISRG certificate issued to Subscriber, or that Subscriber is the duly authorized agent of such registrant.
2. Each Subscriber warrants to ISRG and the public-at-large that either (a) Subscriber did not obtain control of such domain name as the result of a seizure of such domain name, or (b) such domain name had no ongoing lawful uses at the time of such seizure.
3. Each Subscriber warrants that all information in the ISRG certificate issued to Subscriber regarding Subscriber or its domain name is accurate, current, reliable, complete, and not misleading.
4. Each Subscriber warrants that all information provided by Subscriber to ISRG is accurate, current, complete, reliable, complete, and not misleading.
5. Each Subscriber warrants that Subscriber rightfully holds the Private Key corresponding to the Public Key listed in the ISRG certificate issued to Subscriber.
6. Each Subscriber warrants that Subscriber has taken all appropriate, reasonable, and necessary steps to secure and keep Subscriber's Private Key secret.
7. Each Subscriber warrants that Subscriber will not use ISRG certificates issued to Subscriber to attack, defraud or intercept the traffic of others.

9.6.4 *Relying Party Representations and Liability*

Each Relying Party represents and warrants that, prior to relying on an ISRG certificate, it:

1. Obtained sufficient knowledge on the use of digital certificates and PKI,
2. Studied the applicable limitations on the usage of certificates and agrees to ISRG's limitations on its liability related to the use of certificates,
3. Has read, understands, and agrees to this CPS,
4. Verified both the ISRG certificate and the certificates in the certificate chain using the relevant CRL or OCSP,
5. Will not use an ISRG certificate if the certificate has expired or been revoked, and
6. Will take all reasonable steps to minimize the risk associated with relying on a digital signature, including only relying on an ISRG certificate 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 unauthorized reliance on a certificate is at a party's own risk.

9.6.5 *Representations and Warranties of Other Participants*

No stipulation.

9.7 Disclaimer of Warranties

ISRG CERTIFICATES AND SERVICES ARE PROVIDED "AS-IS." ISRG DISCLAIMS ANY AND ALL WARRANTIES OF ANY TYPE, WHETHER EXPRESS OR IMPLIED, INCLUDING AND WITHOUT LIMITATION ANY IMPLIED WARRANTY OF TITLE, NON-INFRINGEMENT, MERCHANTABILITY, OR FITNESS FOR A PARTICULAR PURPOSE, IN CONNECTION WITH ANY ISRG SERVICE OR ISRG CERTIFICATE.

9.8 Limitations of Liability

ISRG DOES NOT ACCEPT ANY LIABILITY FOR ANY LOSS, HARM, CLAIM, OR ATTORNEY'S FEES IN CONNECTION WITH ANY CERTIFICATES. ISRG WILL NOT BE LIABLE FOR ANY DAMAGES, ATTORNEY'S FEES, OR RECOVERY, REGARDLESS OF WHETHER SUCH DAMAGES ARE DIRECT, CONSEQUENTIAL, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, PUNITIVE, OR COMPENSATORY, EVEN IF ISRG HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THIS LIMITATION ON LIABILITY APPLIES IRRESPECTIVE OF THE THEORY OF LIABILITY, I.E., WHETHER THE THEORY OF LIABILITY IS BASED UPON CONTRACT, WARRANTY, INDEMNIFICATION, CONTRIBUTION, TORT, EQUITY, STATUTE OR REGULATION, COMMON LAW, OR ANY OTHER SOURCE OF LAW, STANDARD OF CARE, CATEGORY OF CLAIM, NOTION OF FAULT OR RESPONSIBILITY, OR THEORY OF RECOVERY. THIS DISCLAIMER IS INTENDED TO BE CONSTRUED TO THE FULLEST EXTENT ALLOWED BY APPLICABLE LAW.

WITHOUT WAIVING OR LIMITING THE FOREGOING IN ANY WAY, ISRG DOES NOT MAKE, AND ISRG EXPRESSLY DISCLAIMS, ANY WARRANTY REGARDING ITS RIGHT TO USE ANY TECHNOLOGY, INVENTION, TECHNICAL DESIGN, PROCESS, OR BUSINESS METHOD USED IN EITHER ISSUING CERTIFICATES OR PROVIDING ANY OF ISRG'S SERVICES. EACH SUBSCRIBER AFFIRMATIVELY AND EXPRESSLY WAIVES THE RIGHT TO HOLD ISRG RESPONSIBLE IN ANY WAY, OR SEEK INDEMNIFICATION AGAINST ISRG, FOR ANY INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS, INCLUDING PATENT, TRADEMARK, TRADE SECRET, OR COPYRIGHT.

9.9 Indemnification of the CA

9.9.1 Indemnification by CAs

The CA does not provide any indemnification except as described in Section 9.9.1 of the Certificate Policy.

9.9.2 Indemnification by Subscribers

Each Subscriber will indemnify and hold harmless ISRG and its directors, officers, employees, agents, and affiliates from any and all liabilities, claims, demands, damages, losses, costs, and expenses, including attorneys' fees, arising out of or related to: (i) any misrepresentation or omission of material fact by Subscriber to ISRG, irrespective of whether such misrepresentation or omission was intentional, (ii) Subscriber's violation of the Subscriber Agreement, (iii) any compromise or unauthorized use of an ISRG certificate or corresponding Private Key, or (iv) Subscriber's misuse of an ISRG certificate. If applicable law prohibits Subscriber from providing indemnification for another party's negligence or acts, such restriction, or any other restriction required by law for this indemnification provision to be enforceable, shall be deemed to be part of this indemnification provision.

9.9.3 Indemnification by Relying Parties

To the extent permitted by law, each Relying Party shall indemnify ISRG, its partners, and any cross-signed entities, and their respective directors, officers, employees, agents, and contractors against any loss, damage, or expense, including reasonable attorney's fees, related to the Relying Party's (i) breach of any service terms applicable to the services provided by ISRG or its affiliates and used by the Relying Party, this CPS, or applicable law; (ii) unreasonable reliance on a certificate; or (iii) failure to check the certificate's status prior to use.

9.10 Term and Termination

9.10.1 Term

This CPS and any amendments to this CPS are effective when published to the ISRG 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 with a newer version.

9.10.3 *Effect of Termination and Survival*

ISRG will communicate the conditions and effect of this CPS's termination via the ISRG Repository. The communication will specify which provisions survive termination. At a minimum, all responsibilities related to protecting confidential information will survive termination. All Subscriber Agreements remain effective until the certificate is revoked or expired, even if this CPS terminates.

9.11 Individual Notices and Communications with Participants

ISRG accepts notices related to this CPS at the locations specified in Section 1.5.2 of this CPS. Notices are deemed effective after the sender receives a valid and digitally signed acknowledgment of receipt from ISRG. If an acknowledgement of receipt is not received within five days, the sender must resend the notice in paper form to the street address specified in Section 1.5.2 of this CPS using either a courier service that confirms delivery or via certified or registered mail with postage prepaid and return receipt requested. ISRG may allow other forms of notice in its Subscriber Agreements.

9.12 Amendments

9.12.1 *Procedure for Amendment*

This CPS is reviewed at least annually and may be reviewed more frequently. Amendments are made by posting an updated version of the CPS to the online repository. Controls are in place that are designed to reasonably ensure that this CPS is not amended and published without the prior authorization of the ISRG PMA.

9.12.2 *Notification Mechanism and Period*

ISRG posts CPS revisions to its Repository. ISRG does not guarantee or set a notice-and-comment period and may make changes to this CPS without notice.

9.12.3 *Circumstances under Which OID Must Be Changed*

The ISRG PMA is solely responsible for determining whether an amendment to the CPS requires an OID change.

9.13 Dispute Resolution Provisions

Any claim, suit or proceeding arising out of this CPS or any ISRG product or service must be brought in a state or federal court located in San Jose, California. ISRG may seek injunctive or other relief in any state, federal, or national court of competent jurisdiction for any actual or alleged infringement of its, its affiliates, or any third party's intellectual property or other proprietary rights.

9.14 Governing Law

The laws of the state of California, United States of America, govern the interpretation, construction, and enforcement of this CPS and all proceedings related to ISRG products and services, including tort claims, without regard to any conflicts of law principles. The United Nations Convention for the International Sale of Goods does not apply to this CPS.

9.15 Compliance with Applicable Law

This CPS is subject to all applicable laws and regulations, including United States restrictions on the export of software and cryptography products.

9.16 Miscellaneous Provisions

9.16.1 *Entire Agreement*

ISRG contractually obligates each RA to comply with this CPS and applicable industry guidelines. ISRG also requires each party using its products and services to enter into an agreement that delineates the terms associated

with the product or service. If an agreement has provisions that differ from this CPS, then the agreement with that party controls, but solely with respect to that party. Third parties may not rely on or bring action to enforce such agreement.

9.16.2 *Assignment*

Any entities operating under this CPS may not assign their rights or obligations without the prior written consent of ISRG. Unless specified otherwise in a contract with a party, ISRG does not provide notice of assignment.

9.16.3 *Severability*

If any provision of this CPS is held invalid or unenforceable by a competent court or tribunal, the remainder of the CPS will remain valid and enforceable. Each provision of this CPS that provides for a limitation of liability, disclaimer of a warranty, or an exclusion of damages is severable and independent of any other provision.

9.16.4 *Enforcement*

ISRG may seek indemnification and attorneys' fees from a party for damages, losses, and expenses related to that party's conduct. ISRG's failure to enforce a provision of this CPS does not waive ISRG's right to enforce the same provision later or right to enforce any other provision of this CPS. To be effective, waivers must be in writing and signed by ISRG.

9.16.5 *Force Majeure*

ISRG is not liable for any delay or failure to perform an obligation under this CPS to the extent that the delay or failure is caused by an occurrence beyond ISRG's reasonable control. The operation of the Internet is beyond ISRG's reasonable control.

9.17 Other provisions

No stipulation.

10 Certificate Profiles

10.1 Root CA Certificate Profile

Field	Value
Version	V3 (2)
Serial Number	Must be unique. 20 bits of entropy
Issuer Signature Algorithm	sha256 WithRSAEncryption {1 2 840 113549 1 1 11}
Issuer Distinguished Name	cn = ISRG Root X *[n]* o = Internet Security Research Group c = US *[n]:* instance of the ISRG Root CA (e.g., ISRG Root X 1, ISRG Root X 2, etc.)
Validity Period	Up to 25 years expressed in UTC format
Subject Distinguished Name	cn = ISRG Root X *[n]* o = Internet Security Research Group c = US *[n]:* Iteration of the ISRG Root CA (e.g., ISRG Root X 1, ISRG Root X 2, etc.)
Subject Public Key	4096 bit RSA key modulus, rsaEncryption {1 2 840 113549 1 1 1}
Extension	**Value**
Subject Key Identifier	C = no; keyIdentifier is SHA-1 hash of subjectPublicKey
Key Usage	C = yes; keyCertSign cRLSign
Basic Constraints	C = yes; cA=True Path Length Constraint is not present

10.2 Subordinate CA Certificates

10.2.1 DV-SSL Subordinate CA Certificate (for RSA and ECDSA) Profile

This profile presents the Subordinate CA Certificates issued by the ISRG Root.

Field	Value
Version	V3 (2)
Serial Number	Must be unique. 20 bits of entropy
Issuer Signature Algorithm	sha256 WithRSAEncryption
Issuer Distinguished Name	Derived from Issuer Certificate
Validity Period	Up to 8 years expressed in UTC format

Field	Value
Subject Distinguished Name	cn = Let's Encrypt Authority X[m] *[m]* o = Let's Encrypt c = US *[m]:* Iteration of the Domain Validated SSL CA (e.g., Let's Encrypt Authority 1, Let's Encrypt Authority 2, etc.)
Subject Public Key	2048 bit RSA key modulus, rsaEncryption (for RSA subordinate CA) Or namedCurve P-256, id-ecPublicKey (for ECDSA subordinate CA)
Extension	**Value**
Authority Key Identifier	C = no; keyIdentifier is the identifier defined in the subjectKeyIdentifier extension of the Root CA Certificate
Subject Key Identifier	C = no; keyIdentifier is SHA-1 hash of subjectPublicKey
Key Usage	C = yes; keyCertSign cRLSign digitalSignature
Extended Key Usage	C = no; TLS Server Authentication TLS Client Authentication
Certificate Policies	C = no; CAB Forum Domain Validated (2.23.140.1.2.1) ISRG Domain Validated (TBD) [1] Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: *[Pointer to this CPS]* [2] Policy Qualifier Info: Policy Qualifier Id=User Notice Qualifier: Notice Text= <User Notice text from Section 7.1.8>
Basic Constraints	C = yes; cA=True Path Length Constraint is zero
Authority Information Access	C = no; [1]accessMethod = {1.3.6.1.5.5.7.48.1} accessLocation = (URL for OCSP responder) [2] accessMethod = {1.3.6.1.5.5.7.48.2} accessLocation = (HTTP URL for location of .p7c file with CA certificate)
CRL Distribution Points	C = no; [1] CRL HTTP *(HTTP ULR location of crl file containing the CRL issued by the Root CA)*

10.2.2 *DV-SSL Subordinate CA Certificate (for RSA and ECDSA) Profile from Cross-Certification*

This profile presents the Subordinate CA Certificates product of the cross-certification with the IdenTrust Root CA in the browsers.

Field	**Value**
Version	V3 (2)
Serial Number	Must be unique. 20 bits of entropy
Issuer Signature Algorithm	sha256 WithRSAEncryption
Issuer Distinguished Name	cn = DST Root CA X3 o = Digital Signature Trust Co.
Validity Period	6 years expressed in UTC format
Subject Distinguished Name	cn = ISRG RSA DV-SSL CA *[m]*, or cn = ISRG ECC DV-SSL CA *[m]* o = ISRG c = US *[m]:* Iteration of the Domain Validated SSL CA (e.g., ISRG RSA DV-SSL CA 1, ISRG RSA DV-SSL CA 2, ISRG ECC DV-SSL CA 1, ISRG ECC DV-SSL CA 2, etc.)
Subject Public Key	2048 bit RSA key modulus, rsaEncryption (for RSA subordinate CA) Or namedCurve P-256, id-ecPublicKey (for ECDSA subordinate CA)
Extension	**Value**
Authority Key Identifier	C = no; keyIdentifier is the identifier defined in the subjectKeyIdentifier extension of the Root CA Certificate
Subject Key Identifier	C = no; keyIdentifier is SHA-1 hash of subjectPublicKey
Key Usage	C = yes; keyCertSign cRLSign digitalSignature
Extended Key Usage	C = no; TLS Server Authentication TLS Client Authentication
Certificate Policies	C = no; CAB Forum Domain Validated (2.23.140.1.2.1) ISRG Domain Validated (TBD) [1] Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: *[Pointer to this CPS]* [2] Policy Qualifier Info: Policy Qualifier Id=User Notice Qualifier: Notice Text= <User Notice text from Section 7.1.8>
Basic Constraints	C = yes; cA=True Path Length Constraint is zero

Field	Value
Name Constraints	C = no; excludedSubtree IP:0.0.0.0/0.0.0.0 IP:0:0:0:0:0:0:0:0/0:0:0:0:0:0:0:0
Authority Information Access	C = no; [1]accessMethod = {1.3.6.1.5.5.7.48.1} accessLocation = (TBD -URL for OCSP responder from IdenTrust) [2] accessMethod = {1.3.6.1.5.5.7.48.2} accessLocation = (TBD- HTTP URL for location of .p7c file with CA certificate from IdenTrust)
CRL Distribution Points	C = no; [1] CRL HTTP *(TBD = HTTP ULR location of crl file containing the CRL issued by the Root CA from IdenTrust)*

10.2.3 *Administrative Subordinate CA Certificate Profile*

Field	Value
Version	V3 (2)
Serial Number	Must be unique. 20 bits of entropy
Issuer Signature Algorithm	sha256 WithRSAEncryption
Issuer Distinguished Name	Derived from Issuer Certificate
Validity Period	6 years expressed in UTC format
Subject Distinguished Name	cn = ISRG Admin CA *[m]* o = ISRG c = US *[m]:* Iteration of the Admin CA (e.g., ISRG Admin CA 1, ISRG Admin CA 2, etc.)
Subject Public Key	2048 bit RSA key modulus, rsaEncryption {1 2 840 113549 1 1 1}
Extension	**Value**
Authority Key Identifier	C = no; keyIdentifier is the identifier defined in the subjectKeyIdentifier extension of the issuing CA Certificate
Subject Key Identifier	C = no; keyIdentifier is SHA-1 hash of subjectPublicKey
Key Usage	C = yes; keyCertSign cRLSign digitalSignature

Field	Value
Certificate Policies	C = no; ISRG Administrative Certificate (TBD) [1] Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: *[Pointer to this CPS]* [2] Policy Qualifier Info: Policy Qualifier Id=User Notice Qualifier: Notice Text= <User Notice text from Section 7.1.8>
Basic Constraints	C = yes; cA=True Path Length Constraint is zero
Authority Information Access	C = no; [1]accessMethod = {1.3.6.1.5.5.7.48.1} accessLocation = (TBD -URL for OCSP responder) [2] accessMethod = {1.3.6.1.5.5.7.48.2} accessLocation = (TBD- HTTP URL for location of .p7c file with CA certificate)
CRL Distribution Points	C = no; [1] CRL HTTP *(TBD = HTTP ULR location of crl file containing the CRL issued by the Root CA)*

10.3 DV-SSL and Human Administrative Certificate Profiles

10.3.1 DV-SSL Certificate Profiles

Field	Value
Version	V3 (2)
Serial Number	128 bits, of which the first 8 compose a unique identifier for each intermediate, the next 56 compose a sequentially increasing serial number, and the last 64 are random, with at least 20 bits of entropy
Issuer Signature Algorithm	sha256 WithRSAEncryption (for RSA subordinate CA) or ecdsa-with-SHA256 (for ECDSA subordinate CA)
Issuer Distinguished Name	Unique X.500 CA DN. Derived from Issuer Certificate
Validity Period	Up to 365 days. Time is expressed in UTC format
Subject Distinguished Name	Unique X.500 subject DN cn = <Fully Qualified Domain Name>

Field	Value
Subject Public Key	2048 bit RSA key modulus, rsaEncryption Or namedCurve P-256, id-ecPublicKey
Extension	**Value**
Authority Key Identifier	C = no; keyIdentifier is the identifier defined in the subjectKeyIdentifier extension of the Root CA Certificate
Subject Key Identifier	C = no; keyIdentifier is SHA-1 hash of subjectPublicKey
Key Usage	C = yes; digitalSignature keyEncipherment
Extended Key Usage	C = no; TLS Server Authentication TLS Client Authentication
Certificate Policies	C = no; CAB Forum Domain Validated (2.23.140.1.2.1) ISRG Domain Validated (TBD) [[1] Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: *[Pointer to this CPS]* [2] Policy Qualifier Info: Policy Qualifier Id=User Notice Qualifier: Notice Text= <User Notice text from Section 7.1.8>
Subject Alternative Name	C = no; DNSName=<Fully Qualified Domain Name or Names>
Authority Information Access	C = no; [1]accessMethod = {1.3.6.1.5.5.7.48.1} accessLocation = (TBD -URL for OCSP responder) [2] accessMethod = {1.3.6.1.5.5.7.48.2} accessLocation = (TBD- HTTP URL for location of .p7c file with CA certificate)

10.3.2 *Human Administrative Certificate Profile*

Field	Value
Version	V3 (2)
Serial Number	non-sequential Certificate serial number that exhibit at least 20 bits of entropy
Issuer Signature Algorithm	sha256 WithRSAEncryption
Issuer Distinguished Name	Unique X.500 CA DN. Derived from Issuer Certificate
Validity Period	Up to 365 days. Time is expressed in UTC format

Field	Value
Subject Distinguished Name	Unique X.500 subject DN cn = <firsname middleinitial lastname> o = ISRG ou = Administrative Certificate c = US
Subject Public Key	2048 bit RSA key modulus, rsaEncryption
Extension	**Value**
Authority Key Identifier	C = no; keyIdentifier is the identifier defined in the subjectKeyIdentifier extension of the Root CA Certificate
Subject Key Identifier	C = no; keyIdentifier is SHA-1 hash of subjectPublicKey
Key Usage	C = yes; digitalSignature nonRepudiation
Certificate Policies	C = no; ISRG Administrative Certificate (TBD) [1] Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: *[Pointer to this CPS]* [2] Policy Qualifier Info: Policy Qualifier Id=User Notice Qualifier: Notice Text= <User Notice text from Section 7.1.8>
Subject Alternative Name	C = no; rfc822Name=<Subscriber's validated email>
Authority Information Access	C = no; [1]accessMethod = {1.3.6.1.5.5.7.48.1} accessLocation = (TBD -URL for OCSP responder) [2] accessMethod = {1.3.6.1.5.5.7.48.2} accessLocation = (TBD- HTTP URL for location of .p7c file with CA certificate)

10.4 OCSP and CRL Profiles

10.4.1 Root CA OCSP Responder Profile

Field	Value
Version	V3
Serial Number	Unique Serial Number
Issuer Signature Algorithm	sha256 WithRSAEncryption
Issuer Distinguished Name	Derived from Issuer Certificate
Validity Period	Up to 5 years

Field	Value
Subject Distinguished Name	cn = ISRG OCSP Root X *[n]* o = Internet Security Research Group c = US *[m]:* Iteration of the Root CA
Subject Public Key	2048 bit RSA key modulus, rsaEncryption Or namedCurve P-256, id-ecPublicKey
Extension	**Value**
Authority Key Identifier	C = no; keyIdentifier is the identifier defined in the subjectKeyIdentifier extension of the Issuer CA certificate
Subject Key Identifier	C = no; keyIdentifier is SHA-1 hash of subjectPublicKey
Key Usage	C = yes; digitalSignature nonrepudiation
Extended Key Usage	C = no; id-kp-OCSPSigning {1.3.6.1.5.5.7.3.9}
No Check	C = no; id-pkix-ocsp-nocheck, {1 3 6 1 5 5 7 48 1 5} value is NULL

10.4.2 *DV-SSL Subordinate CA OCSP Responder Profile*

Field	Value
Version	V3
Serial Number	Unique Serial Number
Issuer Signature Algorithm	sha256 WithRSAEncryption or ecdsa-with-SHA256
Issuer Distinguished Name	Derived from Issuer Certificate
Validity Period	30 days
Subject Distinguished Name	cn = ISRG RSA DV-SSL CA *[m]* OCSP Signer, or cn = ISRG ECC DV-SSL CA *[m]* OCSP Signer o = ISRG c = US *[m]:* Iteration of the RSA DV-SSL CA, *or* Iteration of the ECC DV-SSL CA
Subject Public Key	2048 bit RSA key modulus, rsaEncryption Or namedCurve P-256, id-ecPublicKey
Extension	**Value**
Authority Key Identifier	C = no; keyIdentifier is the identifier defined in the subjectKeyIdentifier extension of the Issuer CA certificate
Subject Key Identifier	C = no; keyIdentifier is SHA-1 hash of subjectPublicKey

Field	Value
Key Usage	C = yes; digitalSignature nonrepudiation
Extended Key Usage	C = no; id-kp-OCSPSigning {1.3.6.1.5.5.7.3.9}
Subject Alternative Name	C = no; dNSName = TBD- DNS Name for the OCSP Responder
No Check	C = no; id-pkix-ocsp-nocheck, {1 3 6 1 5 5 7 48 1 5} value is NULL

10.4.3 *Administrative Subordinate CA OCSP Responder Profile*

Field	Value
Version	V3
Serial Number	Unique Serial Number
Issuer Signature Algorithm	sha256 WithRSAEncryption {1 2 840 113549 1 1 11}
Issuer Distinguished Name	Derived from Issuer Certificate
Validity Period	30 days
Subject Distinguished Name	cn = ISRG Admin CA *[m]* OCSP Signer o = ISRG c = US *[m]:* Iteration of the Admin CA
Subject Public Key	2048 bit RSA key modulus, rsaEncryption {1 2 840 113549 1 1 1}
Extension	**Value**
Authority Key Identifier	C = no; keyIdentifier is the identifier defined in the subjectKeyIdentifier extension of the Issuer CA certificate
Subject Key Identifier	C = no; keyIdentifier is SHA-1 hash of subjectPublicKey
Key Usage	C = yes; digitalSignature nonrepudiation
Extended Key Usage	C = no; id-kp-OCSPSigning {1.3.6.1.5.5.7.3.9}
Subject Alternative Name	C = no; dNSName = TBD- DNS Name for the OCSP Responder
No Check	C = no; id-pkix-ocsp-nocheck, {1 3 6 1 5 5 7 48 1 5} value is NULL

10.4.4 *OCSP Request Format*

Field	Value
Version	V1
Requestor Name	Not Required
Request List	List of Certificates

Field	Value
Signature	Not Required
Request Extension	**Value**
Preferred Signature Algorithm id-pkix-ocsp-pref-sig-algs	Optional List of preferred signature algorithm by client

10.4.5 *OCSP Response Format*

Field	Value
Version	V1
Response Status	Successful | Malformed Request | Internal Error | Try Later
Response Type	Id-pkix-ocsp-basic
Responder ID	Hash of the Responder Public Key
Produced At	Date and Time when the response was produced
List of Responses	Each response includes Certificate identifier, Certificate status, thisUpdate and NextUpdate For both the Root CA and Subordinate CA response, NextUpdate = thisUpdate + 7 days
Signature	sha256 WithRSAEncryption or ecdsa-with-SHA256
Certificates	Applicable Certificates issued to the OCSP Responder
Extension	**Value**
Nonce	Octet String value of the nonce if nonce extension is present in the request

10.4.6 *Root CA CRL Profile*

Field	Value
Version	V2
Signature Algorithm	sha256 WithRSAEncryption
Issuer Distinguished Name	Derived from Root CA Certificate
ThisUpdate	The date and time when the Certificate revocation list was issued.
NextUpdate	ThisUpdate + 30 days
RevokedCertificates	This field contains the following subfields: userCertificate contains a subfield containing an integer revocationDate contains a date and time specified as UTCtime Reason Code is an enumerated integer between zero and five. The invalidityDate extension is not used.
CRL Extension	**Value**
Authority Key Identifier	C = no; keyIdentifier is the identifier defined in the subjectKeyIdentifier extension of the Root CA certificate
CRLnumber	The serial number of this CRL in an incrementally increasing sequence of CRLs.