Internet Security Research Group (ISRG)

Certificate Policy

Version 1.2

Updated May 5, 2016
Approved by ISRG Policy Management Authority

ISRG

Web Site: https://letsencrypt.org

Copyright Notice

Internet Security Research Group
1 Letterman Drive, Suite D4700
San Francisco, CA 94129

Table of Contents

Change History

Date	Changes / Authors	Version
05 May 2015	Original Authors: Shelley Johnson, Warren Brunson	1.0
09 September 2015	Added DV SSL OID, added/corrected a number of policy URIs, clarifications to Procedure for Revocation Request, substantial changes to all of Section 9 regarding legal matters, other minor fixes/improvements Authors: Josh Aas	1.1
05 May 2016	Add info about tlsFeature extension, serialNumber in Subject Distinguished Name field.	1.2

1 Introduction

1.1 Overview

This ISRG Certificate Policy (CP) contains the business, technical, and legal requirements for governing the life cycle events of Domain Validated SSL Certificates (DV-SSL) and CA Administrative Certificates, including approval, issuance, usage, validation, revocation, and renewal.

This CP applies to the Certification Authority (CA), Policy Management Authority (PMA), Certificate Manufacturing Authority (CMA), Certificate Status Authority (CSA), Registration Authority (RA), Repository, Applicants, Subscribers, and Relying Parties[1].

This document also contains the policies ISRG uses to meet the requirements of the CA/Browser Forum (CA/B Forum), including the CA/B Forum Baseline Requirements for the Issuance and Management of Publicly Trusted Certificates (CA/B Forum Baseline Requirements) version 1.1.9, as published on August 4, 2014, at https://cabforum.org and the CAB Forum Network Requirements published on January 1, 2013, at https://cabforum.org/network-security/.

Should any inconsistency arise between the provisions of this CP and the CA/B Forum Baseline Requirements, the CA/B Forum Baseline Requirements take precedence.

This CP is used along with other documents – most notably, the Certification Practice Statement (CPS) – to govern the operation of the ISRG PKI.

This Certificate Policy and its corresponding Certification Practice Statement are structured in accordance with RFC 3647 format and shall be publicly disclosed and available online on a 24x7 basis.

1.2 Document Name and Identification

1.2.1 Alphanumeric Identifier

The alphanumeric identifier (i.e., the title) for this CPS is the "ISRG Certificate Practices Statement, May 5 2016" or “isrg-cps-v2016 5 5”.

1.2.2 Object Identifier

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

DV SSL Certificate (1.3.6.1.4.1.44947.1.1.1) and (2.23.140.1.2.1) – issued to Subscribers that demonstrate control of a domain in accordance with Section 3.2.2.

Administrative CA Certificates (Not Currently in Use) – used solely for the management and operation of the PKI, including device Certificates, individual certificates for Administrators, and others as needed.

[1] One legal entity may perform two or more of these functions.

Subordinate CA Certificate (2.23.140.1.2.1) – issued by the Root CA Certificate in accordance with Section 7 of this CP.

Other Types – as allowed by this Policy and upon approval of the PMA.

The Certificate profiles for these Certificates may be found in appendices and in Section 7, which are subject to modification from time to time.

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 Applicants who 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

The management of ISRG has established a Policy Management Authority (PMA). The purpose of the PMA is to establish, monitor, and maintain the integrity of this policy and associated public key infrastructures (PKIs).

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, version 1.1.9.

1.3.3 Registration Authorities (RAs)

The CA shall be ultimately responsible for all Certificates it issues. However, under this 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 this 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.

1.3.4 Applicants/Subscribers

In addition to other responsibilities of Applicant/Subscriber set forth in this 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 this Policy and only in a manner consistent with this Policy.

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 this 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 this Policy, Relying Parties must comply with applicable terms and conditions of this 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 this Policy, a Relying Party is obligated to:

1. Ensure that the Certificate and intended use are appropriate under the provisions of this 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 this 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 this Policy. Except to the extent otherwise specified in this 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

The CA will remain ultimately responsible for the manufacture of DV-SSL Certificates. However, the CA may subcontract manufacturing and administrative functions to third party Certificate Manufacturing Authorities (CMAs) who agree to be bound by this Policy.

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 this Policy, but the CA remains responsible for the performance of those services in accordance with this 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 this 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 this 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 shall not be used for any function or purposes described below in this Section.

1. 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; and
    e. Any other system whose failure could lead to injury, death, or environmental damage.
2. Transactions in which applicable law prohibits the use of digital signatures for such transactions.
3. Transactions that are otherwise prohibited by law.
4. 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); and
    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.)
5. Any use other than those explicitly allowed under Section 1.4.1.

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 may approve cross-certification to other Certificate Policies. The CA must inform Subscribers of the uses allowed within the cross-certified PKI. Any cross-certification to external CPs will only be done after approval by the PMA or its designee.

If the CA is cross-certifying with another external party, it cannot 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 Document*

This Policy is owned by ISRG and is administered by the PMA.

1.5.2 *Contact Person*

Questions regarding the implementation and administration of this Policy 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 Policy*

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

1.5.4 *CPS Approval Procedures*

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

1.6 Definitions and Acronyms

Capitalized terms used in this Policy have the following meanings:

1.6.1 *Definitions*

Accept or Acceptance: An act that triggers rights and obligations of an Applicant with respect to its Certificate 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; (ii) 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.

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 Beneficiaries: Each of the following:

- Subscribers;
- All Application Software Suppliers with which a Root CA to which the CA is a Subordinate CA has entered into a contract for the inclusion of such Root CA's Root Certificate in software distributed by such Application Software Supplier; and
- All Relying Parties who have formed Reasonable Reliance with respect to a Valid Certificate.

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 based on this Policy.

Certificate Policy (CP): 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. This document is a Certificate 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 Policy to establish the allowed format and contents of data fields within DV-SSL and Administrative Certificates issued under this Certificate Policy, which identify the CA, the Subscriber, the Validity Period of the Certificate, and other information that identifies the Subscriber.

Certificate Revocation List: 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 Revocation List capabilities.

Certification Authority (CA): 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 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 demonstrating control over a Domain by the Applicant or Subscriber.

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 (FQDN): 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; which is accessible only from Security Zones; and which is separated from Security Zones and Operations Zones by a perimeter. High-Security Zones are monitored 24 hours a day, 7 days a week (24x7) by security staff, other personnel, and/or 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 the Root Zone Database of the Internet Assigned Numbers Authority (IANA).

ISRG Certificate: A Certificate issued pursuant to this Policy.

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 (for example, 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 (OCSP): 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, RAs, CMAs, CSAs, and Repositories participating in the PKI defined by this Policy.

Policy: This Certificate Policy.

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, 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 such as browsers.

Qualified Auditor: A natural person or Legal Entity that meets the requirements of Section 8 (Auditor Qualifications).

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.

Reasonable Reliance: For purposes of this Policy, a Relying Party's decision to rely on an ISRG Certificate will be considered "Reasonable Reliance" if he, she, or it:

- Has entered into a Relying Party Agreement and agreed to be bound by the terms and conditions of this Policy;
- 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 this Policy 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 the 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).

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.

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.

Root Certificate Authority: The top level Certification Authority whose Root Certificate is distributed by Application Software Suppliers and that issues Subordinate CA Certificates. The Root CA also protects the CA Private Signing Key.[2]

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.

[2] The CA/B Forum Baseline Requirements define a Root CA as a "top level Certification Authority whose Root Certificate is distributed by Application Software Providers and that issues Subordinate CA Certificates." The definition used for this Policy does not include the requirement for distribution by Application Software Providers, which include browser makers.

A Security Zone should be monitored 24 hours a day and 7 days a week by security staff or 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 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 within the ISRG 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.

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.

Trustworthy System: Computer hardware, software, and procedures that are (i) 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

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
FQDN	Fully Qualified Domain Name
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 Repositories

The CA and CSA shall be responsible for maintaining an online 24x7 Repository that application software can use to automatically check the current status of all unexpired Certificates issued by the CA. The CA and CSA shall support an OCSP capability using the GET method for each Certificate issued.

The Repository shall not include entries that indicate that a Certificate is suspended. Suspension is not permitted under this Certificate Policy.

2.2 Publication of Certification Information

2.2.1 Publication of CA Information

Each CA and CSA will operate or cause the operation of one or more secure online Repositories that are available to Relying Parties and that contain (i) issued Certificates; (ii) an online Certificate status database (or both); (iii) the CA's CA Certificate for its CA Private Signing Key; (iv) past and current versions of the CA's CPS; (v) a copy of this Policy; and (vi) other relevant information relating to Certificates.

2.2.2 Interoperability

The CA shall 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).

2.3 Time or Frequency of Publication

The Certificates in this Policy shall be published following Acceptance by the Applicant (who is thereafter a Subscriber) in accordance with the procedure specified in Section 4.3. If the CA elects to publish CRLs, the CRLs will be published as specified in Section 4.10.

2.4 Access Controls on Repositories

The CA will not impose any access controls on

- This Policy;
- The CA's CA Certificate; or
- Past and current versions of the CA's CPS.

The CA and CSA may impose access controls on Certificates and Certificate status information, in accordance with provisions of this Policy.

3 Identification and Authentication

3.1 Naming

3.1.1 Types of Names

By issuing the Certificate, the CA represents that it followed the requirements set forth in the following Sections to verify that, as of the Certificate's issuance date, all of the Subject information was accurate. For Certificates other than DV-SSL, The CA shall generate and sign Certificates that contain non-null Distinguished Names (DNs). CAs shall not include a Domain Name in a Subject attribute except as specified below. Certificates may also include alternative name forms.

For CA (Root and Subordinate)
All CAs shall include non-null Subject or Issuer DNs.

For the Root CA Certificate, the Issuer DN shall include the name of the organization and country that operates the CA at the time of issuance. The issuer DN may include the common name of the CA that clearly identifies it. This common name can be expressed as a sequence of words, or as all the components of the CA's Registered Domain Name.

The Issuer and Subject DN for a Root CA Certificate will be the same. The Issuer DN of a subordinate CA shall be its Issuer's subject DN.

For DV-SSL
The Issuer DN of a DV-SSL Certificate shall be its Issuer's subject DN.

CAs shall include FQDNs or IP Addresses of the Device in the subject Alternative Name extension. The Subject Alternative Name extension may contain more than one instance of the name form. CAs may include a FQDN or IP Address in the subject DN for backwards compatibility, but this name shall be also included in the Subject Alternative Name extension.

Wildcard names are not permitted.

CA shall not issue a Certificate with a subjectAlternativeName extension or Subject commonName field containing a Reserved IP Address or Internal Name.

If the subject Domain Component field is populated, this field must contain a label from a Domain Name. The domainComponent fields for each Domain Name must be in a single ordered sequence containing all labels from the Domain name. The labels must be encoded in the reverse order to the on-wire representation of domain names in the DNS protocol, so that the label closest to the root is encoded first. The CA must ensure that the certificate is issued with the consent of, and according to procedures established by, the owner of each Domain Name.

CAs shall not include the address, locality, province/state, or postal code fields if the verified name of organization is not present.

CAs may include the two-letter ISO 3166-1 country code associated with the location of the Subject, as long as it is verified in accordance Section 3.2.2.4.

Any additional attribute in the subject DN may be populated as long as the information has been verified by the CA. Optional attributes shall not contain metadata indicating that the value is absent, incomplete or not applicable.

For human Administrative Certificates
The issuer DN of an administrative Certificate shall be its issuer's subject DN.

The subject DN shall include the Applicant's full name, the CA organization's name, sub-organization, and the two-letter ISO 3166-1 country code associated with the location of the Applicant, and the words "Administrative Certificate." The Subject Alternative Name extension will include the Applicant's verified email.

For device Administrative Certificates (e.g. OCSP Signers)
The Issuer DN of an administrative Certificate shall be its issuer's Subject DN.

The Subject DN may include the common name of the Device. This common name can be expressed as a sequence of words, or as all the components of the CA's Registered Domain Name. In addition, the CA organization's name, and the two-letter ISO 3166-1 country code associated with the location of the Device.

The Subject Alternative Extension shall include the Device's FQDN.

3.1.2 Need for Names To Be Meaningful

The contents of each Certificate Subject Alternative Name extension must have an association with the authenticated name of the Subscriber. A Certificate issued for an electronic device must include the authenticated name of the electronic device.

An Administrative Certificate issued to an individual must contain the authenticated common name – a combination of first name, surname, and optionally initials.

3.1.3 Anonymity or Pseudonymity of Subscribers

The subject name used for DV-SSL Certificates shall be the Subscriber's authenticated domain name. Each Subscriber must have a clearly distinguishable and unique X.501 Distinguished Name ("DN") in the Certificate subject name field and in accordance with RFC 5280. The DN must be in the form of an X.501 printable string and must not be blank.

3.1.4 Rules for Interpreting Various Name Forms

The CA may defer to a naming authority for guidance on name interpretation and subordination.

3.1.5 Uniqueness of Names

The Subject Name listed in a Certificate shall be unambiguous and unique for all Certificates issued by the CA and shall conform to X.500 standards for name uniqueness.

If necessary, additional numbers or letters may be appended to the real name to ensure the name's uniqueness within the domain of Certificates issued by the CA for Administrative Certificates. No wildcard name forms shall be allowed. Each name shall be unique and for a single unique entity.

3.1.6 Recognition, Authentication, and Role of Trademarks

3.1.6.1 Name Claim Dispute Resolution Procedure

The CA should reserve the right to make all decisions regarding Subscriber names in Certificates. A party requesting a Certificate may 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 may be done by signing the request with the Private Key. The CA shall establish 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.

3.2.2 Authentication of Domains and Administrative Certificates

The issuance of a DV-SSL or Administrative Certificate will be based on I&A performed by the CA or RA using procedures that shall be documented in the CPS. The number and types of identification documents (IDs), the process documentation and the authentication requirements for issuance of a DV-SSL Certificate are listed below.

3.2.2.1 Acceptable Forms of Identification Documents for Applicants

For DV-SSL Certificates and for administrative Certificates issued for devices, the CA shall provide 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 control shall be consistent with the relevant CA/B Forum Baseline Requirements. For domain ownership, the validation shall consist of comparison of the Applicant's submitted information with a domain registration database; for example, through a WHOIS inquiry.

For Administrative Certificates issued to individuals, the CA shall provide a secure means of validating the identity of the Applicant; such means shall include satisfactory proof of organizational affiliation with the Human Resources department of the CA.

The requirements for renewal of Certificates shall be the same as those above.

3.2.2.2 Performance of Electronic Identification

For each Name listed in a DV-SSL Certificate, the CA shall confirm that, as of the date the Certificate was issued, the Applicant (or the Applicant's Parent Company, Subsidiary Company, or Affiliate, collectively referred to as "Applicant" for the purposes of this Section) either is the Domain Name Registrant or has control over the FQDN by:

1. Confirming the Applicant as the Domain Name Registrant directly with the Domain Name Registrar;
2. Communicating directly with the Domain Name Registrant using an address, email, or telephone number provided by the Domain Name Registrar;
3. Communicating directly with the Domain Name Registrant using the contact information listed in the WHOIS record's "registrant," "technical," or "administrative" field;
4. Communicating with the Domain's administrator using an email address created by pre-pending "admin," "administrator," "webmaster," "hostmaster," or "postmaster" in the local part, followed by the at-sign ("@"), followed by the Domain Name, which may be formed by pruning zero or more components from the requested FQDN;
5. Relying upon a Domain Authorization Document;
6. Having the Applicant demonstrate practical control over the FQDN by making an agreed-upon change to information found on an online Web page identified by a uniform resource identifier containing the FQDN; or
7. Using any other method of confirmation, provided that the CA maintains documented evidence that the method of confirmation establishes that the Applicant is the Domain Name Registrant or has control over the FQDN to at least the same level of assurance as those methods previously described.

Note: For purposes of determining the appropriate domain name level or Domain Namespace, the registerable Domain Name is the second-level domain for generic top-level domains (gTLD) such as .com, .net, or .org, or, if the Fully Qualified Domain Name contains a 2 letter Country Code Top-Level Domain (ccTLD), then the domain level is whatever is allowed for registration according to the rules of that ccTLD.

If the CA relies upon a Domain Authorization Document to confirm the Applicant's control over a FQDN, then the Domain Authorization Document must substantiate that the communication came from either the Domain Name Registrant (including any private, anonymous, or proxy registration service) or the Domain Name Registrar listed in the WHOIS. The CA must verify that the Domain Authorization Document was either (i) dated on or after the certificate request date or (ii) used by the CA to verify a previously issued certificate and that the Domain Name's WHOIS record has not been modified since the previous certificate's issuance.

3.2.2.3 gTLD Domain Validation

The CA will not issue Certificates containing a new gTLD under consideration by ICANN. Prior to issuing a Certificate containing an Internal Name with a gTLD that ICANN has announced as under consideration to make operational, the CA will provide a warning to the applicant that the gTLD may soon become resolvable and that, at that time, the CA will revoke the Certificate unless the applicant promptly registers the domain name.

Within 30 days after ICANN has approved a new gTLD for operation, as evidenced by publication of a contract with the gTLD operator on [www.ICANN.org] each CA must (1) compare the new gTLD against the CA's records of valid certificates and (2) cease issuing Certificates containing a Domain Name that includes the new gTLD until after the CA has first verified the Subscriber's control over or exclusive right to use the Domain Name in accordance with the CA/B Forum Baseline Requirements.

Within 120 days after the publication of a contract for a new gTLD is published on [www.icann.org], the CA must revoke each Certificate containing a Domain Name that includes the new gTLD unless the Subscriber is either the Domain Name Registrant or can demonstrate control over the Domain Name.

3.2.2.4 Country Name Field Validation

If the subject:countryName field is present, then the CA will verify the country associated with the Subject using one of the following: (a) the IP Address range assignment by country for either (i) the web site's IP address, as indicated by the DNS record for the web site or (ii) the Applicant's IP address; (b) the ccTLD of the requested Domain Name; (c) information provided by the Domain Name Registrar; or (d) a method identified in the CA/B Forum Baseline Requirements. The CA will implement a process to screen proxy servers in order to prevent reliance upon IP addresses assigned in countries other than where the Applicant is actually located.

3.2.2.5 IP Address Validation

The CA will not issue certificates for IP Addresses.

*3.2.3 **Non-Verified Subscriber Information***

Information that is not verified in accordance with the appropriate I&A outlined in Section 3 of this CP and the corresponding CPS, shall not be placed in a Certificate.

3.2.4 Validation of Authority

For DV-SSL Certificates, demonstration of control over the device and domain may be conducted electronically and if used shall consist of validation of the information presented as described above. If the Applicant cannot demonstrate control, validation of authority will be verified through a check to an alternative source as listed in Section 3.2.2.

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

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

3.2.4.1 Verification against the Denied List

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

3.2.4.2 Verification against High Risk Certificate Requests

The CA shall develop, maintain, and implement 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.

3.2.4.3 Data Source Accuracy

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

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

This Policy allows for cross-certification with other PKIs. Criteria for cross-certification includes review and approval of this 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. 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 demonstrating control of the device and affiliation with the domain, as described in Section 3.2.2 above.

When issuing this type of Certificate, the CA shall conform to the following standards:

1. The “Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates,” version 1.1.9, published at http://www.cabforum.org. In the event of any inconsistency between this CP and those requirements, the requirements will take precedence over this document. This type of Certificate can only be issued by an CA that can ensure accomplishment of the I&A required by this Section; and
2. The CA/B Forum Network requirements.

Throughout this CP and the corresponding CPS, references from either document will be specified to indicate which requirements were satisfied with the content.

3.2.7 *Authentication of Other Certificates*

This policy has no stipulation for other Certificates.

3.3 Identification and Authentication (I&A) for Rekey and Renewal

3.3.1 *Identification and Authentication for Rekey Requests*

Rekey is not supported by this policy.

3.3.2 *Identification and Authentication for Rekey after Revocation*

Rekey is not supported by this policy.

3.3.3 *Certificate Renewal*

Renewing a Certificate means creating a new Certificate with the same name, Public Key, and authorizations as the old one, but a new Validity Period and a new serial number. A Certificate may be renewed without performing I&A if:

- It has not been revoked;
- The Key Pair has not reached the end of its validity;
- The Private Key has not been compromised;
- The data used for the renewal has not reached more than 39 months in age; and
- The Subscriber name and attributes are correct.

3.3.4 *Certificate Update*

Certificate update is not permitted under this Policy.

3.3.5 *Renewal or Update of Affiliated Individual’s Certificate*

Renewal or update of the Administrative Certificate of an affiliated individual will require that the affiliation between the affiliated individual and his or her sponsoring organization still exists.

3.4 I&A for Revocation and Suspension Requests

A Subscriber may request revocation of his, her, or its Certificate at any time for any reason. The CA, when faced with such a request, must adopt authentication mechanisms that balance the need to prevent unauthorized requests against the need to quickly revoke Certificates When a revocation request is electronically submitted, the identity of the requestor may be authenticated on the basis of the digital signature used to submit the message. If the request is signed using the Private Key corresponding to the requestor’s Public Key, such a request shall be accepted as valid.

Revocation requests submitted by other than digitally signed request shall require verification of the requestor's identity if the Revocation is meant for an Administrative Certificate or control of the device or domain for a DV-SSL Certificate. This can be done through completing a verification of the same information provided during initial registration, or other alternative information that was used during that process.

Suspension of an SSL Certificate shall not be permitted as per the requirements listed in the CA/B Forum Baseline Requirements Section 13.2.7.

4 Certificate Life Cycle Operational Requirements

4.1 Certificate Application

This Policy endorses the following procedures for satisfying the security requirements of this PKI. The following steps are required when applying for a Certificate: (i) establish identity of subject (per Section 3); (ii) obtain a Key Pair for each Certificate required; (iii) prove to the CA that the Public Key forms a functioning Key Pair with the Private Key held by the Subscriber; and (iv) provide a point of contact for verification of any roles or authorizations requested.

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

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

The CA obtains any additional documentation that it determines necessary to meet the requirements.

Prior to the issuance of a Certificate, the CA shall obtain from the Applicant a certificate request in a form prescribed by the CA and that complies with this policy and the CA/B Forum Baseline Requirements. One certificate request may 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 may be made, submitted, and/or signed electronically.

The certificate request must 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 Who Can Submit a Certificate Application

An application for a DV-SSL Certificate may be made by an individual acting on behalf of himself or herself, or by an individual acting on behalf of an organization. Applications may also be generated by machines acting on behalf or individuals or organizations.

An application for an individual's Administrative Certificate may be made by the individual acting on behalf of himself or herself; or by an individual acting on behalf of another, as long as that individual can demonstrate organizational affiliation and authority to do so.

4.1.2 Enrollment Process and Responsibilities

Applicants will complete a Certificate application and provide requested information in a form prescribed by the CA in accordance with this Policy. An Applicant must also enter into a Certificate Agreement with the CA. All applications are subject to review, approval, and acceptance by the CA.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

For domain-validated device Certificates, the CA shall validate the Applicant's ownership of, or 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 shall be conform to the requirements as listed in Section 3.2.2.2, "Electronic Identification."

For Administrative Certificates issued to individuals, the CA shall provide a secure means of validating the identity of the Applicant; such means shall include satisfactory proof of identity from the Human Resources Department of the CA and proof of organizational affiliation with the CA.

The requirements for renewal of Certificates shall be the same as those above.

The certificate request may include all factual information about the Applicant to be included in the Certificate, and such additional information required from the Applicant as is necessary for the CA to comply with this Policy, the corresponding CPS, and the CA/B Forum Baseline Requirements. In cases where the certificate request does not contain all the necessary information about the Applicant, the CA shall obtain the remaining information from the Applicant or, having obtained it from a reliable, independent, third-party data source, confirm it with the Applicant. The CA shall establish and follow a documented procedure for verifying all data requested for inclusion in the Certificate by the Applicant.

4.2.2 Approval or Rejection of Certificate Applications

Certificate applications shall 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.

4.2.3 Time to Process Certificate Application

The time required to process a Certificate application shall be consistent with the time requirement for acceptance or rejection.

4.3 Certificate Issuance

After all application and approval processes identified in this Policy are completed, the CA will: (i) issue the requested Certificate; (ii) notify the Applicant of the Certificate's issuance; and (iii) make the Certificate available to the Applicant for Acceptance. The procedures for notifying the Applicant of the Certificate's issuance, and the procedure used to deliver or make the Certificate available to the Applicant must be secure and confidential, and must comply with the applicable portions of the CA/B Forum Baseline Requirements.

4.3.1 CA Actions during Certificate Issuance

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

1. The Applicant's agreement to the Certificate Agreement; or
2. The Applicant's agreement to the Terms of Use agreement.

The CA shall implement a process to ensure that each Certificate Agreement 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 may be 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 Certificate Agreement or Terms of Use Agreement.

Nothing in the Certificate Agreements may waive or otherwise lessen the obligations of the Subscriber as set forth in this Policy.

4.3.2 *Notification to Subscriber by the CA of Issuance of the Certificate*

Notification of Certificate issuance to others may be effected by publication of the Certificate in a recognized Repository.

4.4 Certificate Acceptance

An Applicant's Acceptance of its Certificate will be a precondition to its use of such Certificate. The CA will define in its agreements with Applicants and Subscribers (or in its CPS, if incorporated by reference in its agreements with Applicants and Subscribers) the procedure(s) that constitute(s) Acceptance by an Applicant. By Accepting a Certificate, the Applicant / Subscriber warrants that all of the information provided by it (and by its sponsoring organization, where applicable) and included in the Certificate, and all representations made by the Applicant (and by its sponsoring organization, where applicable) as part of the application and I&A process, are true and not misleading.

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.

4.4.2 *Publication of the Certificate by the CA*

The CA and CSA shall publish the Certificates issued as described in Section 4.3 in a publicly accessible Repository.

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

Notification of Certificate issuance to others may be done by publication of the Certificate in a recognized Repository.

4.5 Key Pair and Certificate Usage

Certificates may not be used for purposes counter to the principles and applications outlined in this Policy.

4.5.1 *Subscriber Private Key and Certificate Usage*

Use of the Private Key corresponding to the Public Key in the Certificate shall only be permitted after Subscriber has agreed to the Certificate Agreement and accepted the Certificate. The Certificate shall be used lawfully in accordance with the Certificate Agreement, the terms of this CP, and the relevant CPS. Certificate use must be consistent with the KeyUsage field extensions included in the Certificate.

Subscribers shall protect their private keys from unauthorized use and shall discontinue use of the Private Key following expiration or revocation of the Certificate. Parties other than the Subscriber shall not archive the Subscriber Private Key except as set forth in Section 4.12.

4.5.2 *Relying Party Public Key and Certificate Usage*

Relying Parties shall rely on a Certificate only for those uses specified in the KeyUsage field of the Certificate. Relying Parties shall not rely on a Certificate that has been revoked or that has expired.

If any of the Certificates in the Certificate Chain have been revoked, the Relying Party is solely responsible to investigate whether prior reliance on the Certificate is reasonable. If circumstances indicate that additional assurance is required, the Relying party must obtain such assurances before using the Certificate. Any such reliance is made solely at the risk of the Relying Party.

Assuming that the use of the Certificate is appropriate, Relying Parties shall 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 shall specify the mechanism(s) used to determine the validity of a Certificate (e.g., OCSP), and shall acquire, process, and use this information in accordance with their obligations as Relying Parties.

4.6 Certificate Renewal

4.6.1 Circumstance for Certificate Renewal

A certificate may be renewed if:
1. It has not been revoked for reasons of key compromise; and
2. It has not yet reached its expiry date; and
3. The renewal period is in force; and
4. No information contained within the certificate, including the Public Key, has changed.

4.6.2 Who May Request Renewal

Only the Subscriber may request a Certificate Renewal. For DV-SSL Certificates, this may be 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 may be verified. For Administrative Certificates, this may be done electronically or by other means in which the Subscriber's identity and affiliation with the CA may be verified.

4.6.3 Processing Certificate Renewal Requests

All Renewal requests shall be validated by the CA to ensure that the circumstances for Renewal are met. Such validation shall be in compliance with the CA/B Forum Baseline Requirements.

4.6.4 Conduct Constituting Acceptance of a Renewal Certificate

As with Acceptance of any other Certificate the following conduct constitutes acceptance of a Renewal Certificate:
- 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.

4.6.5 Publication of the Renewal Certificate by the CA

The CA and CSA shall publish the Certificates issued in a publicly accessible Repository.

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

The notification procedures used by the CA shall be the same as with a new Certificate.

4.7 Certificate Rekey

4.7.1 Circumstances for Certificate Rekey

Rekey is not supported by this policy.

4.7.2 Who May Request a Rekey

Rekey is not supported by this policy.

4.7.3 Processing Certificate Rekeying Requests

Rekey is not supported by this policy.

4.7.4 Notification of New Certificate Issuance to Subscriber

Rekey is not supported by this policy.

4.7.5 Conduct Constituting Acceptance of a Rekeyed Certificate

Rekey is not supported by this policy.

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

Rekey is not supported by this policy.

4.8 Modification

Modifying a Certificate means creating a new Certificate that has the same or a different key, a different serial number, and differs in one or more fields, from the old Certificate.

The CA shall authenticate the request for the Certificate modification using the same means for the initial I&A in Section 3.2.

If the CA needs to modify the Root CA Certificate to update its Private Signature Key and generates a new Public Key, the new trust anchor shall be provided to all CAs, RAs, and Subscribers.

4.8.1 Circumstances for Certificate Modification

A Certificate may be modified at the request of a Subscriber that can fulfill the I&A requirements of Section 3.2 at any time during the life of the Certificate.

4.8.2 Who May Request Certificate Modification

The Subscriber may request the modification of their Certificate. The CA or RA shall verify any requested changes for the modification of the Subscriber Certificate.

4.8.3 Processing Certificate Modification Requests

The Certificate modification process shall be in accordance with Certificate Issuance and I&A as specified in Section 3.2. The CA or RA shall validate any changes in the Subscriber authorizations in the Certificate most specifically the FQDN as listed in DV-SSL Certificates.

4.8.4 Notification of New Certificate Issuance to Subscriber

See Section 4.3.2.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

See Section 4.4.1.

4.8.6 Publication of the Modified Certificate by the CA

See Section 4.4.2.

4.8.7 Notification of Certificate Issuance by the 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 may 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 (or any sponsoring organization, where applicable) to meet its obligations under this Policy, the applicable 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 shall maintain a continuous 24x7 ability to accept and respond to revocation requests and related inquiries.

4.9.1.2 Required Revocation

A Subscriber or Subordinate CA will promptly request revocation of a Certificate whenever:

1. Any of the information in the Certificate changes or becomes obsolete;
2. The Subscriber or Subordinate CA 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 may revoke a Certificate whenever:

1. The Subscriber or Subordinate CA has failed to meet its material obligations under this Policy, 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. Knowledge or reasonable suspicion of compromise is obtained;
3. The CA obtains evidence that the Subscriber's or Subordinate CA's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise or no longer complies with the requirements of Appendix A in the CA/B Forum Baseline Requirements;
4. The CA is made aware that a Subscriber or Subordinate CA has violated one or more of its material obligations under the Subscriber or Terms of Use Agreement;
5. 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);
6. The CA is made aware of a material change in the information contained in the Certificate;
7. The CA determines that any of the information appearing in the Certificate is inaccurate or misleading;
8. The CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Certificate;
9. 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;
10. The CA is made aware of a possible compromise of the Private Key of the Subordinate CA used for issuing the Certificate;
11. Revocation is required by this Certificate Policy and/or the corresponding Certification Practice Statement;
12. 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;
13. The CA determines that the Certificate was not properly issued in accordance with this Policy and/or any applicable CPS; or
14. Knowledge or reasonable suspicion of misuse is obtained.

4.9.2 Who Can Request Revocation

As described in Section 4.9.1 above, either the Subscriber or the CA may request revocation. The CA may summarily revoke Certificates within its domain.

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 domain, or the associated private key. Likewise, an individual who is not the Subscriber may 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 shall 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 shall publicly disclose the instructions through a readily accessible online means.

4.9.3 Procedure for Revocation Request

Certificate revocation requests should be communicated to the CA promptly, as described in this Policy.

Subscribers may request revocation by contacting the CA, electronically or otherwise, and providing adequate proof of identification in accordance with this Policy or an equivalent method.

Individuals who are not Subscribers may request revocation if adequate proof of the items listed in Section 4.9.2 is possessed.

4.9.3.1 Procedure for Investigating Certificate Problem Reports

The CA shall begin the investigation of a Certificate Problem Report within twenty-four hours of receipt, and decide whether revocation or other appropriate action is warranted based on at least the following criteria:

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 example a security professional with good evidence of private key compromise should carry more weight than a complaint from a consumer alleging that she didn’t receive the goods she ordered); and
4. Relevant legislation.

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

4.9.4 Revocation Request Grace Period

This Policy makes no stipulation regarding a Revocation request grace period.

4.9.5 Time within which CA must Process a Revocation Request

The CA shall revoke a Certificate as quickly as practical after receipt of a proper revocation request and confirmation of the authority of the person requesting revocation. The CA shall not suspend a Certificate in accordance with applicable CA/B Forum Baseline Requirements. Promptly following revocation of a

Certificate, the CA and CSA shall update the online Certificate database Repository and reporting mechanisms (e.g., OCSP). All revocation requests and the resulting actions taken by the CA will be archived.

4.9.6 Revocation Checking Requirements for Relying Parties

Use of revoked Certificates could have damaging or catastrophic consequences in certain applications. Therefore, before relying on a Certificate, a Relying Party must conduct a validation request in accordance with the method and procedures established by the CA (see Section 4.10). 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 of using a Certificate whose authenticity cannot be guaranteed to the standards of this Policy.

4.9.7 CRL Issuance Frequency

The CA, or CSA shall maintain CRL and OCSP Certificate status reporting mechanisms in accordance with the provisions of CAB/F Baseline Requirement 13.2.2. CRL reporting mechanisms will be used only for status reporting on Subordinate CA certificates. For all Subscriber Certificates, including DV-SSL and individual Administrative Certificates, OCSP or similar reporting mechanisms will be used.

CRL updating shall occur at intervals of no more than 12 months, or within 24 hours of a Subordinate CA Certificate revocation.

4.9.8 Maximum Latency of CRLs

CRLs issued in accordance with this Policy shall have resources sufficient to provide a response time of 10 seconds or less under normal operating conditions.

4.9.9 Online Revocation/Status Checking Availability

If OCSP validation is employed, the CA and CSA will validate online, near-real-time the status of the Certificate indicated in a properly formatted Certificate validation request message.

4.9.10 Online Revocation Checking Requirements

Relying Parties who rely on an online Certificate status database must (i) validate a Certificate with such database before relying on the Certificate, and (ii) log the validation request. Failure to do so negates the ability of the Relying Party to claim that it acted on the Certificate with reasonable reliance.

4.9.11 Other Forms of Revocation Advertisements Available

A CA may also use other methods to publicize revoked Certificates.

4.9.12 Special Requirements Rekey Compromise

This Policy makes no special requirements regarding Rekey compromise.

4.9.13 Circumstances for Suspension

This Policy does not allow for Certificate Suspension.

4.9.14 Who can Request a Suspension

See Section 4.9.2.

4.9.15 Procedure for Suspension Request

This Policy does not allow for Certificate Suspension.

4.9.16 Limits on Suspension Period

No stipulation.

4.10 Certificate Status Services

4.10.1 Operational Characteristics

The CA and the CSA shall make revocation information for Subordinate Certificates and Subscriber Certificates available in accordance with the CA/B Forum Baseline Requirements Appendix B.

If the Subscriber Certificate is for a high-traffic FQDN, the CA may rely on stapling, in accordance with [RFC4366], to distribute its OCSP responses. In this case, the CA shall ensure that the Subscriber "staples" the OCSP response for the Certificate in its TLS handshake. The CA shall enforce this requirement on the Subscriber either contractually, through the Subscriber or Terms of Use Agreement, or by technical review measures implement by the CA.

OCSP responses conform to RFC2560 and/or RFC5019. OCSP responses shall either:

1. Be signed by the CA that issued the Certificates whose revocation status is being checked, or
2. Be signed by an OCSP Responder whose Certificate is signed by the CA that issued the Certificate whose revocation status is being checked.

In the latter case, the OCSP signing Certificate MUST contain an extension of type id-pkix-ocsp-nocheck, as defined by RFC2560.

4.10.2 Service Availability

The CA and CSA shall update information provided via an Online Certificate Status Protocol at least every 4 days. OCSP responses from this service must have a maximum expiration time of 10 days.

The Issued CA and CSA shall operate and maintain its OCSP capability with resources sufficient to provide a response time of 10 seconds or less under normal operating conditions.

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

If the OCSP responder receives a request for status of a certificate that has not been issued, then the responder shall not respond with a "good" status. The CA and CSA will monitor the responder for such requests as part of its security response procedures.

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

4.10.3 Optional Features

4.11 End of Subscription

No stipulation.

4.12 Key Escrow and Recovery

If an Administrative Key Pair is used for both signature and confidentiality purposes, recovery of the Private Key is prohibited unless the CA provides mechanisms (hardware, software, or procedural) that permit recovery of the Private Key while protecting it from being used to impersonate the Subscriber.

This Policy does not permit the escrow of Private Keys.

4.12.1 Key Escrow and Recovery Policy and Practices

This Policy does not permit the escrow of Subscriber Private Keys,

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

No stipulation.

5 Facility, Management, and Operational Controls

5.1 Physical Controls

The CA, and all RAs, CMAs, CSAs and Repositories, will implement 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 will be limited to those personnel performing in Trusted Roles as described in Section 5.2.1. Access will be controlled through the use of electronic access controls, mechanical combination locksets, deadbolts, or other physical protections of equivalent or greater strength. Such access controls must be manually or electronically monitored for unauthorized intrusion at all times.

5.1.1 Site Location and Construction

The site(s) for the CA's server(s) must be located and constructed to satisfy the requirements for a High-Security Zone, as described in Section 1.6. These requirements include:

1. Location in a geographic area that is relatively free from multiple natural hazards;
2. Building construction that protects against or mitigates physical security and environmental hazards;
3. Multiple levels of security for the facility, with security increasing in areas closer to the CA key materials and associated equipment;
4. The ability to store sensitive information and materials in secured containers within a High-Security Zone as described in Section 1.6;
5. The ability to physically restrict access to CA key materials and associated equipment to personnel previously identified on an approved access list, and electronically or manually logged;
6. The ability to protect Hardware Cryptomodules physically, through site protection;
7. The ability to physically enforce dual- or multiple-person requirements for access to CA key materials, servers, and associated equipment;
8. The requirement that Trusted Role Employees of the CA and the RA must not leave their workstations unattended when the cryptography is in an unlocked state (i.e., when the PIN or password has been entered);
9. The protection of workstations that contain Private Keys on hard drives through physical security or protection with an appropriate access control product; and
10. The ability to enforce constant escort and supervision of all persons entering the restricted area(s) who are not on the approved access list.

The site(s) for RA activities must satisfy the requirements for an Operations Zone as described in Section 1.6. These requirements include:

1. Location within a site that meets the requirements for an Operations Zone or more secure zone as described in Section 1.6;
2. The ability to physically restrict access to RA workstations to personnel previously identified on an approved access list;
3. The ability to physically restrict access to Cryptomodules to personnel previously identified on an approved access list; and
4. The ability to store Cryptomodules and other sensitive information (including personally identifiable information, or PII) in a physically secured container within an area meeting Operations Zone or Security Zone requirements.

5.1.2 Physical Access

The physical access controls for the CA's servers and related equipment must accomplish the following:

1. Protect CA equipment at all times from unauthorized access;

2. Restrict access from one area of the facility to another, or from one security zone to another, using physical or electronic constraints (e.g., physically locked doors, programmable electronic badge systems, biometrics systems);
3. Restrict access to CA key materials, servers, and related equipment to those personnel on a preapproved access list;
4. Provide for constant monitoring of the site by electronic means (e.g., recorded video surveillance, motion detectors with logs and alarms), and by personnel with defined security duties;
5. Provide for physical security checks of the facility containing the CA's servers and related equipment at regular intervals to ensure that the area is protected against unauthorized access, with records maintained of each such check showing when it was performed, who performed it, and the results of the check;
6. Provide for physical security checks of the High-Security Zones, including areas where CA Cryptomodules and other key materials are stored, at regular intervals, with records maintained of each such check showing when it was performed, who performed it, and the results of the check;
7. Provide for electronic or manual logs of persons accessing the CA's Cryptomodules, servers, and related equipment.

The physical controls for RA equipment and working areas must accomplish the following:

1. Protect RA equipment such as workstations from unauthorized access, use, or removal, including placing the workstations and work areas in Operations or Security Zones as described in Section 1.6;
2. Protect associated Cryptomodules from unauthorized access use, or removal, including providing locked containers in secure areas for storing Cryptomodules that are not in use.

5.1.3 Power and Air Conditioning

Facilities that house the CA equipment must be supplied with power and air conditioning sufficient to create a reliable operating environment. In addition, personnel areas within the facility must be supplied with sufficient utilities to satisfy operational, health, and safety needs. The CA equipment will have power and air conditioning backup capabilities sufficient to automatically lock out input, finish any pending actions, and record the state of the equipment in the event a failure of one of these systems results in an equipment shutdown. The revocation systems will be supported by uninterruptible power supplies and sufficient backup power generation, or by automatic failover to a secondary processing site.

5.1.4 Water Exposures

CA equipment must be installed such that it is not in danger of exposure to water; e.g., on elevated floors. Moisture detectors must be installed in areas susceptible to flooding. CA operators who have sprinklers for fire control will have a contingency plan for recovery should the sprinklers malfunction or cause water damage outside of the fire area.

5.1.5 Fire Prevention and Protection

Facilities that house the CA equipment must be supplied with automatic fire extinguishing system(s) that will be installed in accordance with local code. The CA will have a contingency plan that accounts for damage by fire.

5.1.6 Media Storage

Media must be stored so as to protect it from accidental damage (e.g., by water, fire, or electromagnetic fields). Media that contains audit, archive, or backup information must be stored in a location separate from the CA equipment.

5.1.7 Waste Disposal

Normal office waste must be removed or destroyed in accordance with best business practices. Media used to collect or transmit information must be destroyed, such that the information is unrecoverable, prior to disposal.

5.1.8 Off-site Backup

System backups sufficient to recover from system failure will be made on a periodic schedule, as described in the CPS. At least one backup copy will be stored at an offsite location separate from the CA equipment. The backup will be stored at a site with physical and procedural controls commensurate to that of the operational CA system.

5.2 Procedural Controls

5.2.1 Trusted Roles

A Trusted Role is one whose incumbent performs functions that could introduce security problems if carried out improperly, whether by accident or malice. The people selected to fill Trusted Roles must be careful and above reproach as described in the next Section. The functions performed in Trusted Roles form the basis of trust in the entire PKI.

5.2.2 Number of Persons Required per Task

The CA must utilize commercially reasonable practices to ensure that one person acting alone cannot circumvent safeguards.

The CA must ensure that no single individual may gain access to Subscriber Private Keys stored by the CA. At a minimum, procedural or operational mechanisms must be in place for key recovery, such as a Split-Knowledge Technique, to prevent the disclosure of the Encryption Key to an unauthorized individual. Multi-user control is also required for CA Key generation, as outlined in Section 6.2.2. All other duties associated with CA roles may be performed by an individual operating alone. The CA must ensure that any verification process it employs provides for oversight of all activities performed by privileged CA role holders.

To best ensure the integrity of the CA equipment and operation, it is recommended that wherever possible a separate individual be identified for each Trusted Role. The separation provides a set of checks and balances over the CA operation. The CA requires that employees of the CA and RA and contractors to observe the principle of "least privilege" when accessing Certificate systems, or when configuring access privileges on them. Furthermore, the CA must implement a process that disables all privileged access by an individual to Certificate systems within 24 hours following termination of the individual's employment or contracting relationship with the CA or Delegated Third Party.

Under no circumstances will the incumbent of a CA Trusted Role perform his or her own auditor function.

5.2.3 Identification and Authentication for Each Role

Each person performing a CA role must have his or her identity and authorization verified before being (i) included in the access list for the CA site; (ii) included in the access list for physical access to the CA system; (iii) given a Certificate for the performance of a CA Trusted Role; or (iv) given an account on the PKI system. Each of these Certificates and accounts (with the exception of CA signing Certificates) must (i) be directly attributable to an individual; (ii) not be shared; and (iii) be restricted to actions authorized for that role through the use of CA software, operating system and procedural controls. When accessed across shared networks, CA operations must be secured, using mechanisms such as token-based strong authentication and encryption.

5.2.4 Roles Requiring Separation of Duties

Policy and control procedures are implemented by the CA to ensure segregation of duties based upon job responsibilities. The most sensitive tasks must require multiple Trusted Role personnel to be present; such tasks include access to and management of CA private key material, as well as cryptographic hardware and software. The requirement for multiple Trusted Role personnel must be enforced throughout the lifecycles of CA materials from initial receipt and inspection through final logical or physical destruction.

In addition, the CA must segregate roles performing the following duties:

- Identification and validation of information in Certificate Applications;
- Acceptance, rejection, or other processing of Certificate Applications, revocation requests, and key recovery or renewal requests;
- Issuance and revocation of Subscriber Certificates;
- Loading of a CA into a production environment;
- Generation, issuance, or destruction of CA certificates;
- Handling of Subscriber information;
- Duties generally required of a Security Officer; and
- Audits of CA systems.

5.2.4.1 Activities Requiring Multiple Individuals

The following activities require two or more individuals to be present:

- Physical access to the CA computing environment including associated network equipment;
- Physical access to the Cryptomodules containing CA Keys;
- Physical access to the activation material associated with the Cryptomodules containing CA Keys;
- Physical access to the equipment containing CA root and Subordinate Certificates used to issue Subscriber Certificates;
- Activities involving the creation or backup of Root Certificates or Subordinate Certificates, or the signing of OCSP materials;
- Activities involving the receiving of new Cryptomodules; and
- Activities involving the decommissioning or destruction of Cryptomodules.

5.3 Personnel Controls

5.3.1 Background, Qualifications, Experience, and Security Clearance Requirements

CAs, RAs, CSAs, and CMAs will formulate and follow 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 manner consistent with this Policy.

5.3.2 Background Check Procedures

CAs will conduct an appropriate investigation of all personnel who serve in Trusted Roles prior to their employment and thereafter as necessary or as stipulated in organization policy, to verify their trustworthiness and competence in accordance with the requirements of this Policy and the CA's personnel practices or equivalent. Personnel who fail an initial or subsequent investigation will not serve or continue to serve in a Trusted Role.

5.3.3 Training Requirements

The CA must ensure that all personnel performing managerial duties with respect to the operation of the CA and RAs receive suitable training in (i) CA/RA security principles and mechanisms; (ii) security awareness; (iii) all PKI software versions in use on the CA system; (iv) duties they are expected to perform; and (v) disaster recovery and business continuity procedures.

5.3.4 Retraining Frequency and Requirements

The requirements of Section 5.3.3 must be kept current to accommodate changes in the CA system. Refresher training must be conducted as required.

5.3.5 Job Rotation Frequency and Sequence

This Policy makes no stipulation regarding frequency or sequence of job rotation.

5.3.6 Sanctions for Unauthorized Actions

In the event of actual or suspected unauthorized action by a person performing duties with respect to the operation of the CA or RA, the CA should suspend his or her access to the CA system.

5.3.7 Independent Contractor Requirements

The CA must ensure that contractor access to the CA site is in accordance with Section 5.1.1.

5.3.8 Documentation Supplied to Personnel

Documentation sufficient to define duties and procedures for each role will be provided to the personnel filling that role.

5.4 Audit Logging Procedures

5.4.1 Types of Events Recorded

The CA and each Delegated Third Party shall record details of the actions taken to process a certificate request and to issue a Certificate, including all information generated and documentation received in connection with the certificate request, the time and date, and the personnel involved. The CA shall make these records available to its Qualified Auditor as proof of the CA's compliance with the CP, CPS, and the CA/B Forum Baseline Requirements.

The CA will record events related to CA servers and related equipment and applications, at a minimum including events that relate to the proper and secure function of the CA system, and the certificate life cycle items listed in Section 5.5.1. Events may be attributable to human action (in any role) or may be automatically invoked by the equipment. At a minimum, the information recorded will include the type of event, and the date and time the event occurred, the source of the event, and the success or failure of a requested action.

Where possible, the audit data will be collected by automated means; when this is not possible, a logbook, paper form, or other physical mechanism will be used. Audit processes will be invoked at system startup, and will cease only at system shutdown. Should it become apparent that an automated audit system has failed and that redundant audit systems are not sufficient to provide needed audit logs, the affected component(s) will cease CA-related operations until the audit capability can be restored. If it is unacceptable to cease CA operation, other means will be employed to maintain audit capability.

5.4.2 Frequency of Log Review and Processing

The CA must ensure that its audit logs are reviewed by Trusted Role CA personnel at least weekly and all significant events are explained in an audit log summary. Such reviews may include both electronic and manual means, and may 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 Trusted Role employee will validate the integrity of logging processes and ensure that monitoring, logging, alerting, and log-integrity-verification functions are operating properly (an in-house or third-party audit log reduction and analysis tool may be used). Supporting manual and electronic logs from the CA and RA should be compared where any action is deemed suspicious. Actions taken following these reviews must be documented.

5.4.3 Retention Period for Audit Logs

The information generated on the CA equipment will be kept on the CA equipment until the information is moved to an appropriate archive facility. Deletion of the audit log from the CA equipment will be performed by a person performing a Trust Role other than CA Operator. This Trusted Role will be identified in the CA's CPS. Audit logs shall be retained as archive records in accordance with Section 5.5.2.

5.4.4 Protection of Audit Logs

The audit log, to the extent possible, will not be open for reading or modification by any human, or by any automated process other than those that perform audit processing. Audit logs that have not been archived must not be deleted. Any entity that does not have modification access to the audit log may archive it (note that deletion requires modification access). Audit data to be archived shall be moved to a safe, secure storage location separate from the CA equipment.

5.4.5 Audit Log Backup Procedures

Audit logs and audit summaries shall be backed up or copied if in manual form.

5.4.6 Audit Collection System (Internal vs. External)

This Policy makes no requirement for the audit log collection system to be external to the CA equipment. The audit process shall run independently of the CA Operator and will not in any way be under the control of the CA Operator.

The CA shall identify those Certificate Systems under the control of the CA or Delegated Third Party Trusted Roles capable of monitoring and logging system activity and enable those systems to continuously monitor and log system activity.

5.4.7 Notification to Event-Causing Subject

Where an event is logged by the audit collection system no notice need be given to the individual, organization, device or application that caused the event.

5.4.8 Vulnerability Assessments

Events recorded by the audit process will be logged, in part, to monitor system vulnerabilities. The CA must ensure that a vulnerability assessment is performed, and reviewed, with remediation or mitigations performed in a timely manner, at least once yearly, or following examination of log events that show attempts or suspected attempts to breach the system.

The CA must undergo or perform a vulnerability scan for the following additional reasons:
1. Within one week of receiving a request from the CA/Browser Forum;
2. After any system or network changes that the CA determines are significant; and

3. At least once per quarter, on public and private IP addresses identified by the CA or Delegated Third Party as the CA's or Delegated Third Party's Certificate systems.

The CA must also undergo a penetration test on itself and each Delegated Third Party's Certificate Systems on at least an annual basis and after infrastructure or application upgrades or modifications that the CA determines are significant. The CA will also record evidence that each vulnerability scan and penetration test was performed by a person or entity (or collective group thereof) with the skills, tools, proficiency, code of ethics, and independence necessary to provide a reliable vulnerability scan or penetration test.

Should the CA or the CA discover a critical vulnerability during a penetration test not previously addressed by the CA's vulnerability correction process, the following must be completed within 96 hours:

1. The CA must remediate the critical vulnerability;
2. If remediation of the critical vulnerability within 96 hours is not possible, create and implement a plan to mitigate the Critical Vulnerability, giving priority to:
    a. Vulnerabilities with high CVSS scores, starting with the vulnerabilities the CA determines are the most critical (such as those with a CVSS score of 10.0) and
    b. Systems that lack sufficient compensating controls that, if the vulnerability were left unmitigated, would allow external system control, code execution, privilege escalation, or system compromise; or
3. Document the factual basis for the CA's determination that the vulnerability does not require remediation because:
    a. The CA disagrees with the NVD rating,
    b. The identification is a false positive,
    c. The exploit of the vulnerability is prevented by compensating controls or an absence of threats; or
    d. Other similar reasons.

5.4.8.1 Risk Assessment

The CA's security program must include an annual Risk Assessment that:

1. Identifies foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of any Certificate Data or Certificate Management Processes;
2. Assesses the likelihood and potential damage of these threats, taking into consideration the sensitivity of the Certificate Data and Certificate Management Processes; and
3. Assesses the sufficiency of the policies, procedures, information systems, technology, and other arrangements that the CA has in place to counter such threats.

5.5 Records Archive

5.5.1 Types of Events Archived

CA archive records must be detailed enough to establish the validity of a signature and of the proper operation of the PKI. At a minimum, the following data will be recorded and archived:

5.5.1.1 Certificate Issuance

- Applicant's name as it appears in the Certificate's "Common Name" field
- Method of application (i.e., online, in-person, etc.)\
- For each data element accepted for proofing, including electronic forms:
    - Name of document presented for identity proofing
    - Issuing authority
    - Date of issuance
    - Date of expiration
    - All fields verified

- Source of verification (i.e., which databases used)
- Method of verification (i.e., online, in-person)
- Date/time of verification
- Name of the RA
- All associated error messages and codes
- Date/time of process completion
- Date/time of Certificate download/Acceptance

5.5.1.2 Certificate Validation

- Certificate serial number
- Certificate status with reason code
- All associated error messages and codes
- Date/time of all Certificate validation requests
- Date/time of transmission of Certificate status request responses

5.5.1.3 Certificate Revocation

- Date/time
- Name of the RA
- Subscriber's common name
- Reason code for revocation request
- Certificate serial number
- All associated verification request and revocation data

5.5.1.4 Certificate Renewal

- Certificate serial number
- Certificate common name
- New Validity Period dates
- Date/time of completion of renewal process
- All associated renewal data

5.5.1.5 Security events

- Successful and unsuccessful PKI system access attempts;
- PKI and security system actions performed;
- Security profile changes;
- System crashes, hardware failures, and other anomalies;
- Firewall and router activities; and
- Entries to and exits from the CA facility.

5.5.2 ***Retention Period for Archive***

Archive records will be kept for a period of at least seven years and six months without any loss of data. If the original media cannot retain the data for the required period, a mechanism to periodically transfer the archived data to new media will be defined by the archive site. Software applications required to make the archive data readable by humans will also be maintained for as long as necessary. The CA shall retain all documentation relating to Certificate requests and the verification thereof, and all Certificates and revocation thereof, for aforementioned period of seven years and six months after any Certificate based on that documentation ceases to be valid. The CA shall make these audit logs available to its Qualified Auditor upon request.

5.5.3 ***Protection of Archive***

Archived logs will be written to media that cannot be modified afterwards. Only authorized Trusted Role individuals, as defined in Section 5.2.4, may retrieve archived logs from storage. No unauthorized individual will be able to write to, modify, or delete the archive. However, archived records may be moved to another medium. The contents of the archive will not be released as a whole, except as required by law or by lawful order of a judicial body with appropriate jurisdiction. Records of individual transactions may be released upon request of any entities involved in the transaction or their legally recognized agents. Archive media will be stored in a separate, safe, secure storage facility under conditions equivalent to or stronger than the security of the CA system and the information it contains.

5.5.4 Archive Backup Procedures

Adequate backup procedures must be in place so that in the event of the loss or destruction of the primary records, a complete set of backup copies will be available in a timely manner.

5.5.5 Requirements for Time-Stamping of Records

Certificate validations will be time-stamped using time from a trusted source such as an NTP server.

5.5.6 Archive Collection System

No stipulation.

5.5.7 Procedures to Obtain and Verify Archive Information

Procedures to obtain and verify archive information and procedures detailing how to create, package, and send the archive information will be published in the CA procedures handbook or CPS. Only authorized users will be allowed to access the archive. During any inspections required by this Policy, the inspector will verify the integrity of the archives.

5.5.8 Long Term Information Preservation

No stipulation.

5.6 Key Changeover

A Subscriber may only apply to renew his, her, or its Certificate within three months prior to the expiration of one of the Keys, provided the previous Certificate has not been revoked. A Subscriber, the CA, or the RA may initiate this renewal process. Automated key renewal is permitted. The CA must ensure that the details of this process are indicated in its CPS or other publicly available document. Subscribers without valid keys must be re-authenticated by the CA in the same manner as the initial registration. Where a Subscriber's Certificate has been revoked as a result of non-compliance, the CA must verify that any reasons for non-compliance have been addressed to its satisfaction prior to issuing a new Certificate. Keys may not be renewed using an expired key.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

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

The CA must have in place an appropriate disaster recovery and business resumption plan. The plan must set up and render operational a facility located in a geographically diverse area that is capable of providing CA Services in accordance with this Policy within 72 hours of an emergency. The plan will include a complete and periodic test of readiness for the recovery facility. The plan will be referenced within the CPS or other appropriate documentation that is publicly available as described previously.

5.7.3 CA Private Key Compromise Procedures

In the event of the compromise or suspected compromise of the CA's Private Signing Key, the CA must immediately notify all CAs with whom it has cross-certified. In the event of the compromise or suspected compromise of any other Participant's Signing Key, the Participant must notify the CA immediately. The CA must ensure that its CPS or other publicly available document and appropriate agreements contain provisions outlining the means it will use to provide notice of compromise or suspected compromise.

In the event of the compromise of a CA's CA Private Signing Key, the CA must revoke all Certificates issued using that key and provide appropriate notice. After addressing the factors that led to Key Compromise, the CA may (i) generate a new CA Signing Key Pair; and (ii) reissue Certificates to all Subscribers and ensure all OCSP responders are signed using the new key.

5.7.4 Business Continuity Capabilities After a Disaster

In the event that the CA declares a disaster (generally defined as the unplanned cessation of services), the CA will maintain continuity of validation services sufficient to maintain a service level of 99.5 percent uptime except for scheduled maintenance windows. The CA will re-establish continuity of certificate life cycle services within 72 hours of the disaster declaration.

The CA shall document business continuity and disaster recovery procedures designed to notify and reasonably protect Application Software Suppliers, Subscribers, and Relying Parties in the event of a disaster, security compromise, or business failure. The CA shall make the business continuity plan and security plan available to the CA's auditors upon request. The CA shall annually test, review, and update these procedures.

The business continuity plan will include:
1. The conditions for activating the plan;
2. Emergency procedures;
3. Fallback procedures;
4. Resumption procedures;
5. A maintenance schedule for the plan;
6. Awareness and education requirements;
7. The responsibilities of the individuals;
8. Recovery time objective (RTO);
9. Regular testing of contingency plans.
10. The CA's plan to maintain or restore the CA's business operations in a timely manner following interruption to or failure of critical business processes;
11. A requirement to store critical cryptographic materials (i.e., secure cryptographic device and activation materials) at an alternate location;
12. Designation of acceptable system outage and recovery times;
13. Designation of the frequency of backup procedures for essential business information and software;
14. The distance of recovery facilities to the CA's main site; and
15. Procedures for securing CA facilities to the extent possible during the period of time following a disaster and prior to restoring a secure environment either at the original or a remote site.

5.7.5 Customer Service Center

This Policy makes no stipulation as to the existence and function of a human-staffed Customer Service Center.

5.7.5.1 User Agent Verification

The CA shall host test web pages that allow Application Software Suppliers to test their software with Subscriber Certificates that chain up to each publicly trusted Root Certificate. At a minimum, the CA shall host separate web pages using Subscriber Certificates that are (i) valid, (ii) revoked, and (iii) expired.

5.8 CA or RA Termination

In the event that the CA ceases operation, all Subscribers, CMAs, CSAs, Relying Parties will be promptly notified of the termination. In addition, all CAs with which cross-certification agreements are current at the time of cessation will be promptly informed of the termination. All Certificates issued by the CA that reference this Policy must 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 seven days of CA cessation and in accordance with this Policy. Transferred data will not include any data unrelated to this Policy. No key recovery enabled repository data will be co-mingled with this data.

6 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 Key Generation Ceremony

For CA Root Keys that are for the operator of the Root CA or an Affiliate of the Root CA, the CA shall:
1. Prepare and follow a Key generation script; and
2. Have a Qualified Auditor witness the Root CA Key Pair generation process or record a video of the entire Root CA Key Pair generation process.

In all cases the CA shall:
1. Generate the keys in a physically secured environment described in Section 5.1;
2. Generate the CA keys using personnel in trusted roles under the principles of multiple person control and Split Knowledge;
3. Generate the CA keys within Cryptomodules meeting the applicable technical and business requirements as described in Section 6.1;
4. Log its CA key generation activities as described in Section 5.5.1; and
5. Maintain effective controls to provide reasonable assurance that the Private Key was generated and protected in conformance with the procedures described in Section 6.2.

.

6.1.2 Private Key Delivery to Subscriber

In most cases, a Private Key will be generated by and remain within the Cryptomodule for which it is intended. If this does not occur, then the CA must securely deliver the Private Key to the Subscriber. Accountability for the location and state of the Cryptomodule must be maintained until delivery and possession occurs and the Subscriber acknowledges receipt of the Key to the CA or the RA. If the Key is generated by the system for which it is intended as described above, the key will be stored by and used by that system and no further action is required. If the key must be extracted for use by other applications or in other locations, a protected data structure (such as defined in [PKCS#12]) will be used. The resulting file may be kept on a magnetic medium or transported electronically. See Section 6.4.1.

6.1.3 Public Key Delivery to CA

Public Keys shall be delivered to the CA in a secure and trustworthy manner, such as a Certificate request message. Delivery may also be accomplished via non-electronic means, such as CD or other storage medium sent via registered mail or courier. Any other methods used for Public Key delivery will be stipulated in a CPS.

The Public Key corresponding to the CA's CA Private Signing Key may be delivered to Subscribers and Relying Parties in an online transaction in accordance with IETF PKIX Part 3, or other appropriate mechanism.

6.1.4 Key Sizes

All valid certificates shall contain Public Keys of at least 2048 bits for RSA or at least 224 bits for ECDSA and a digest algorithm of SHA-256.

CA Root Certificates shall contain Public Keys of at least 3072 bits for RSA or at least 256 bits for ECDSA and a digest algorithm of SHA-256.

6.1.5 *Public Key Parameters Generation and Quality Checking*

The CA shall generate Digital Signature Algorithm (DSA) parameters in accordance with FIPS 186-3.

RSA: The CA shall confirm that the value of the public exponent is an odd number equal to 3 or more. Additionally, the public exponent should be in the range between 216+1 and 2256-1. The modulus should also have the following characteristics: an odd number, not the power of a prime, and have no factors smaller than 752.

DSA: Although FIPS 800-57 says that domain parameters may be made available at some accessible site, compliant DSA certificates must include all domain parameters. This is to insure maximum interoperability among relying party software. The CA must confirm that the value of the Public Key has the unique correct representation and range in the field, and that the key has the correct order in the subgroup.

ECC: The CA should confirm the validity of all keys using either the ECC full Public Key validation routine or the ECC partial Public Key validation routine.

6.1.6 *Key Usage Purposes (as per X509 v3 Key Usage Field)*

Keys contained in a DV-SSL Certificate may be used for SSL activities, including digital signature, key encipherment, and client and server authentication. Keys contained in an Administrative Certificate may be used for digital signature, and nonrepudiation.

CA Private Signing Keys are the only Keys permitted to be used for signing Certificates, CRLs, and OCSP responders. The Certificate Key Usage field must be used in accordance with PKIX-1 Certificate, CRL and OCSP Profiles. At least one of the following Key Usage values must be present in all Certificates: (i) digital signature, or (ii) Non-Repudiation. One of the following additional values must be present in CA Certificate-signing Certificates: (i) Key Cert Sign, (ii) CRL Sign, or (iii) digital signature. The use of a specific Key is determined by the Key usage extension in the X.509 Certificate. This restriction is not intended to prohibit use of protocols like the Secure Sockets Layer that provide authenticated connections using Key management Certificates.

6.2 Private Key Protection and Cryptomodule Engineering Controls

Each Subscriber and PKI Service Provider must protect its Private Key(s) in accordance with the provisions of this Policy.

6.2.1 *Cryptomodule Standards and Controls*

The standard for Cryptomodules for Subscribers and CA Administrative Certificates is FIPS140-2. Cryptomodules for Subscribers and Administrative Certificates must be validated to FIPS140-2 Level 2 or better. Cryptomodules for OCSP and other administrative devices must be validated to FIPS140-2 Level 2 or better.

The CA shall protect its Private Key in a system or device that has been validated as meeting at least FIPS-140-2 Level 3 or an appropriate Common Criteria Protection Profile or Security Target, EAL 4 or higher.

The CA shall encrypt its Private Key with an algorithm and key-length that, according to the state of the art, are capable of withstanding cryptanalytic attacks for the residual life of the encrypted key or key part.

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

The CA Private Key shall be backed up, stored, and recovered only by personnel in trusted roles using at least two-person control in a physically secured environment. The CA Private Keys shall be under a minimum of two-person control for all activities described in Section 5.2.4. In addition, the CA shall change authentication keys and passwords for any privileged account or service account on a Certificate System whenever a person's authorization to administratively access that account on the Certificate System is changed or revoked; and lock out account access to Certificate Systems after no more than five failed access attempts, provided that this security measure is supported by the Certificate System and does not weaken the security of this authentication control.

6.2.3 Private Key Escrow

Private Key escrow is not allowed under this Policy.

6.2.4 Private Key Backup

A Subscriber may optionally back up his, her, or its own Private Key for DV-SSL and Administrative Certificates. If this is done, 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.

The CA Private Key shall be backed up, stored, and recovered only by personnel in Trusted Roles using at least two-person control in a physically secured environment.

6.2.5 Private Key Archival

Private Keys shall not be archived.

6.2.6 Private Key Transfer into or from a Cryptomodule

CA and Issuer CA Private Keys must be generated by and kept within a Cryptomodule. In the event that a Private Key is to be transported from one Cryptomodule to another, the Private Key must be encrypted during transport. CA and Issuer CA Private Keys must never exist in plain text form outside the Cryptomodule boundary.

6.2.7 Private Key Storage on a Cryptomodule

No stipulation beyond that specified in FIPS-140-2.

6.2.8 Method of Activating Private Keys

A Subscriber must be authenticated to its Cryptomodule before the activation of the Private Key. For CA and Subordinate CA Certificates, it shall be through the use of an electronic device. For Subscribers and Administrative CA Certificate users, this authentication may be in the form of a password. When deactivated, Private Keys must be kept in encrypted form only.

6.2.9 Method of Deactivating Private Keys

Cryptomodules that have been activated must not be left unattended or otherwise open to unauthorized access. After use, they must be deactivated, using, for example, a manual logout procedure or a passive timeout. When not in use, hardware Cryptomodules should be removed and stored, unless they are within the Subscriber's sole control.

6.2.10 Method of Destroying Private Keys

Private Keys should be destroyed when they are no longer needed, or when the Certificates to which they correspond expire or are revoked. For software Cryptomodules, this can be done by overwriting the data. For tokens, this will likely be accomplished by executing a "zeroize" command. Physical destruction of hardware is not required.

6.3 Other Aspects of Key Management

6.3.1 *Public Key Archival*

This Policy makes no stipulation regarding the archiving of Subscriber Public Keys.

6.3.2 *Certificate Operational Periods and Key Usage Periods*

All Certificates and corresponding keys shall have maximum Validity Periods not to exceed the following:

Key Type	Certificate Lifetime	Key Usage Period
Root CA	25 years	25 years
Root OCSP	30 days	3 years
Intermediate CA	8 years	8 years
Intermediate OCSP	30 days	3 years
DV-SSL Certificates	Up to 39 months	Up to 39 months
CA Administrative Certificates	3 years	3 years

Certificates and keys must not be used after the expiration of the Validity Periods indicated in this Section.

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

The Private Key used by the CA for issuing Certificates will be used only for signing such Certificates and, optionally, CRLs or other validation services responses (i.e. OCSP).

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

Root CA Private Keys shall not be used to sign Certificates except in the following cases:
1. Self-signed Certificates to represent the Root CA itself;
2. Certificates for Subordinate CAs and Cross Certificates;
3. Certificates for infrastructure purposes (e.g. administrative role certificates, internal CA operational device certificates, and OCSP Response verification Certificates); and
4. Certificates issued solely for the purpose of testing products with Certificates issued by a Root CA.

6.4 Activation Data

6.4.1 *Activation Data Generation and Installation*

A passphrase, PIN or other activation data shall be used to protect access to the Private Key of the CA Root Certificates, Subscribers, and CA Administrative Certificates.

For CA Root, Subordinate CA, and CSA Certificates, activation data shall be generated automatically. For DV-SSL and CA Administrative Certificates, the activation data may be user-selected.

For CA Administrative Certificates, if the activation data must be transmitted to the Subscriber, it shall be via a channel of appropriate protection, and distinct in time and place from the associated Cryptomodule. If this is not done by hand, the Subscriber should be advised of the date sent, method of sending, and expected delivery date of any activation data. As part of the delivery method, end entities should acknowledge receipt of the Cryptomodule and activation data. In addition, end entities should also receive (and acknowledge receipt of) information regarding the use and control of the Cryptomodule. See Section 6.1.2

6.4.2 Activation Data Protection

If written down, activation data must be secured at the level of the data that the associated Cryptomodule is used to protect, and must not be stored with the Cryptomodule. Activation data must never be shared.

6.4.3 Other Aspects of Activation Data

This Policy makes no stipulation on the life of activation data; however, it should be changed periodically to decrease the likelihood that it has been discovered. CAs may define activation data requirements in their CPSs or Certificate Agreements.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

All CA servers must include the following functionality either provided by the operating system or through a combination of operating system, PKI application, and physical safeguards:

1. Control of access to CA services and PKI roles;
2. Enforced separation of duties for PKI roles;
3. Identification and authentication of PKI roles and associated identities;
4. Object re-use or separation for CA random access memory;
5. Use of cryptography for session communication and database security;
6. Archival of CA and End-Entity history and audit data;
7. Audit of security related events;
8. Self-test of security related CA services;
9. Trusted path for identification of PKI roles and associated identities;
10. Recovery mechanisms for Keys and the CA system; and
11. Enforcement of domain integrity boundaries for security critical processes.

6.5.2 Computer Security Rating

The CA's equipment will meet and be operated to a Common Criteria EAL 4 rating or higher, or equivalent security as measured by another generally recognized standard. The CA's equipment operating at this rating will, as a minimum, implement:

1. Self-protection;
2. Process isolation;
3. Discretionary access control;
4. Object reuse controls;
5. Individual I&A; and
6. Protected audit records.

6.6 Life Cycle Technical Controls

CA equipment (hardware and software) procured to operate a PKI (including equipment for any RA, CMA, or CSA) will be purchased in a fashion to reduce the likelihood that any particular copy was tampered with; for instance, by random selection.

CA equipment will be protectively packaged and delivered via an accountable method. Tamper-evident packaging will be used or equipment will be hand-carried from a controlled procurement environment to the installation site. Equipment procured prior to registration as the CA will be deemed to satisfy this requirement. The CA equipment will be dedicated to administering a key management infrastructure. It will not have installed applications or component software that is not part of the CA configuration. Where possible, equipment such as servers will be wiped clean of any factory-installed software, and then reimaged to hardened standards using trusted software repositories. Cryptomodules will be zeroized before first use. Equipment updates will be purchased or developed in the same manner as original equipment, and will be installed by trusted and trained personnel in a defined manner.

6.6.1 *System Development Controls*

The CA must use software that has been designed and developed with the following standards: .

- For commercial off-the-shelf software, the software shall be designed and developed under a formal, documented development methodology;
- Where open source software has been utilized, the applicant shall demonstrate that security requirements were achieved through software verification & validation and structured development/lifecycle management.

The design and development process must provide sufficient documentation to support third party security evaluation of the CA components and be supported by third party verification of process compliance and on-going assessments to influence security safeguard design and minimize residual risk.

6.6.2 *Security Management Controls*

A formal configuration management methodology must be used for installation and ongoing maintenance of the CA system. The CA software, when first loaded, must provide a method for the CA to verify that the software on the system (i) originated from the software developer; (ii) has not been modified prior to installation; and (iii) is the version intended for use. The CA must provide a mechanism to periodically verify the integrity of the software, and to control and monitor the configuration of the CA system.

The CA must also apply recommended security patches to Certificate Systems within six months of the security patch's availability, unless the CA documents that the security patch would introduce additional vulnerabilities or instabilities that outweigh the benefits of applying the security patch. The CA will also review all system accounts at least every 90 days and deactivate any accounts that are no longer necessary for operations.

6.6.3 *Life Cycle Security Controls*

The CA must restrict remote administration or access to an issuing system, Certificate Management System, or security support system except when (i) the remote connection originates from a device owned or controlled by the CA or Delegated Third Party and from a pre-approved external IP address, (ii) the remote connection is through a temporary, non-persistent encrypted channel that is supported by multi-factor authentication, and (iii) the remote connection is made to a designated intermediary device (a) located within the CA's network, (b) secured in accordance with Section 6.5 and the CA/B Forum Baseline Requirements, and (c) that mediates the remote connection to the Issuing system.

6.7 Network Security Controls

CA equipment should be connected to no more than two network domains at a time. CA equipment intended to connect to more than one network classification domain will have procedures defined in a CPS, or other document made available to its auditors, that prevent information from one domain from reaching another (e.g., equipment shutdown, removable hard drives, switching the network connection). CA equipment may operate through a network guard insofar as it does not circumvent the function of the guard.

Protection of CA equipment will be provided against known network attacks. Use of appropriate boundary controls will be employed. All unused network ports and services will be turned off. Any network software present on the CA equipment will be necessary to the functioning of the CA application. Root CA equipment will be stand-alone (off-line) configurations.

The CA must maintain a network environment that protects the Private Keys, Root Certificates, and Subordinate CA Certificates from compromise or misuse.

1. Networks will be segmented in order to provide multiple levels of protection to the CA Certificates;
2. Networks will use firewalls and/or other inbound traffic protections to reject or restrict unauthorized traffic;
3. Networks will use intrusion detection and/or other monitoring systems to notify administrators and security personnel of attempts at unauthorized access;
4. Access to CA servers and CA Keys must be through approved applications;
5. Access to Applicant and Subscriber data must be monitored and logged, and must be traceable back to an individual; and
6. Networks will have an implemented detection and prevention controls under the control of the CA or Delegated Third Party Trusted Roles to protect Certificate Systems against viruses and malicious software

6.8 Time Stamping

All audit events will be time-stamped using NTP-validated time, which corresponds to the times on all network components being logged.

7 Certificate, CRL, and OCSP Profiles

7.1 Certificate Profiles

The CA shall populate the issuer field of each Certificate issued after the adoption of the CA/B Forum Baseline Requirements in accordance with the specifications within this Section. All other optional attributes, when present within the subject field, must contain information that has been verified by the CA. Optional attributes must not contain metadata such as '.', '-', and ' ' (space) characters, and/or any other indication that the value is absent, incomplete, or not applicable. By issuing the Certificates as per the guidelines in this Section, the CA verifies that the subject information was accurate.

7.1.1 Version Number(s)

The CA must issue X.509 Version 3 Certificates.

7.1.2 Certificate Extensions

Rules for the inclusion, assignment of value, and processing of extensions are summarized in the profiles Appendix A of the CA/B Forum Baseline Requirements. Use of Certificate extension shall comply with RFC 5280 and the requirements below provided for compliance with the CA/B Forum Baseline Requirements.

The CA shall generate non-sequential Certificate serial numbers that exhibit at least 20 bits of entropy.

The CA shall not issue a Certificate that contains a keyUsage flag, extendedKeyUsage value, Certificate extension, or other data not specified in below or in the profiles unless the CA is aware of a reason for including the data in the Certificate, in such case, this modification must be noted in the CPS.

CAs shall not issue a Certificate with:

- Extensions that do not apply in the context of the public Internet (such as an extendedKeyUsage value for a service that is only valid in the context of a privately manage d network), unless:
  - Such value falls within an OID arc for which the Applicant demonstrates ownership, or
  - The Applicant can otherwise demonstrate the right to assert the data in a public context; or
  - Semantics that, if included, will mislead a Relying Party about the certificate information verified by the CA (such as including extendedKeyUsage value for a smart card, where the CA is not able to verify that the corresponding Private Key is confined to such hardware due to remote issuance).

Root CA Certificate:

- **basicConstraints.** This extension must appear as a critical extension. The cA field must be set true. The pathLenConstraint field should not be present.

- **keyUsage.** This extension must be present and must be marked critical. Bit positions for keyCertSign and cRLSign must be set. If the Root CA Private Key is used for signing OCSP responses, then the digitalSignature bit must be set.

- **certificatePolicies.** This extension should not be present.

- **extendedKeyUsage.** This extension must not be present.

Subordinate CA Certificates:

- **certificatePolicies.** This extension must be present and should not be marked critical. certificatePolicies:policyIdentifier (Required)

  The following fields may be present if the Subordinate CA is not an Affiliate of the entity that controls the Root CA.
  certificatePolicies:policyQualifiers:policyQualifierId (Optional)
  - id-qt 1 [RFC 5280].

  certificatePolicies:policyQualifiers:qualifier:cPSuri (Optional)
  - HTTP URL for the Root CA's Certificate Policies, Certification Practice Statement, Relying Party Agreement, or other pointer to online policy information provided by the CA.

- **cRLDistributionPoints.** This extension must be present and must not be marked critical. It must contain the HTTP URL of the CA's CRL service.

- **authorityInformationAccess.** With the exception of stapling, which is noted below, this extension must be present. It must not be marked critical, and it must contain the HTTP URL of the CA's OCSP responder (accessMethod = 1.3.6.1.5.5.7.48.1). It should also contain the HTTP URL of the CA's certificate (accessMethod = 1.3.6.1.5.5.7.48.2). See Section 13.2.1 of the CA/B Forum Baseline Requirements for details. The HTTP URL of the CA's OCSP responder may be omitted, provided that the Subscriber "staples" the OCSP response for the Certificate in its TLS handshakes [RFC4366].

- **basicConstraints.** This extension must be present and must be marked critical. The cA field must be set true. The pathLenConstraint field may be present.

- **keyUsage.** This extension must be present and must be marked critical. Bit positions for keyCertSign and cRLSign must be set. If the Subordinate CA Private Key is used for signing OCSP responses, then the digitalSignature bit must be set.

- **nameConstraints (optional).** If present, this extension should be marked critical. Non-critical Name Constraints are an exception to RFC 5280 (4.2.1.10), however, they may be used until the Name Constraints extension is supported by Application Software Suppliers whose software is used by a substantial portion of Relying Parties worldwide.

- **extkeyUsage (optional).** For Subordinate CA Certificates to be technically constrained in line with Section 9.8, then either the value id-kp-serverAuth or id-kp-clientAuth, or both values, must be present. Other values may be present. If present, this extension should be marked non-critical. Generally Extended Key Usage will only appear within Subscriber certificates (as highlighted in RFC 5280 (4.2.1.12)), however, Subordinate CAs may include the extension to further protect relying parties until the use of the extension is consistent between Application Software Suppliers whose software is used by a substantial portion of Relying Parties worldwide.

DV-SSL Certificates:

- **certificatePolicies.** This extension must be present and should not be marked critical. certificatePolicies:policyIdentifier (Required)
  - A Policy Identifier, defined by the issuing CA, that indicates a Certificate Policy asserting the issuing CA's adherence to and compliance with these Requirements.

  The following extensions may be present:
  - certificatePolicies:policyQualifiers:policyQualifierId (Recommended)
    - id-qt 1 [RFC 5280].
  - certificatePolicies:policyQualifiers:qualifier:cPSuri (Optional)
    - HTTP URL for the Subordinate CA's Certification Practice Statement, Relying Party Agreement or other pointer to online information provided by the CA.

- **cRLDistributionPoints.** This extension may be present. If present, it must not be marked critical, and it must contain the HTTP URL of the CA's CRL service.

- **authorityInformationAccess.** With the exception of stapling, which is noted below, this extension must be present. It must not be marked critical, and it must contain the HTTP URL of the issuing CA's OCSP responder (accessMethod= 1.3.6.1.5.5.7.48.1). It should also contain the HTTP URL of the issuing CA's certificate (accessMethod = 1.3.6.1.5.5.7.48.2).

The HTTP URL of the issuing CA's OCSP responder may be omitted provided that the Subscriber "staples" OCSP responses for the Certificate in its TLS handshakes [RFC4366].

- **basicConstraints** (optional). If present, the cA field must be set false.

- **keyUsage (optional)** If present, bit positions for keyCertSign and cRLSign must not be set.

- **extKeyUsage (required).** Either the value id-kp-serverAuth [RFC5280] or id-kp-clientAuth[RFC5280] or both values must be present. id-kp-emailProtection [RFC5280] may be present. Other values should not be present.

- **tlsFeature (optional)** This extension defined by RFC 7633 may be present, and not marked critical, if requested by Subscriber.

7.1.3 Algorithm Object Identifiers

Certificates under this Policy will use the following OIDs for signatures:

sha256WithRSAEncryption	{ iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1)pkcs-1(1) 11 }
sha384WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha384WithRSAEncryption(12)}
sha512WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha512WithRSAEncryption(13)}
ecdsa-with-SHA256	{iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2 (3) 2}
ecdsa-with-SHA384	{iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 3}
ecdsa-with-SHA512	{iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 4}

Certificates under this Policy shall use the following OIDs for identifying the algorithm for which the subject key was generated:

id-dsa	{ iso(1) member-body(2) us(840) x9-57(10040) x9cm(4) 1 }
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}
id-ecDH	{iso(1) identified-organization(3) certicom(132) schemes(1) ecdh(12)}

For certificates that contain an elliptic curve public key, the parameters shall be specified as one of the following named curves.

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 }

Curve P-521	ansip384r1 ::= { iso(1) identified-organization(3) certicom(132) curve(0) 35 }

7.1.4 *Name Forms*

Every DN must be in the form of an X.501 printable string.

Where required as set forth in Section 3.1.1, the subject and issuer fields of the Certificate shall be populated with an X.500 Distinguished Name. Distinguished Names shall be composed of standard attribute types, such as those identified in RFC 5280.

For attribute values, All CA Distinguished Names (in various fields, e.g., Issuer, Subject, Subject Alternative Name, Name constraints) shall be encoded as printable strings. Any subscriber DN portion to which name constraints apply to shall be encoded as printable string. Other portions of the subscriber DN shall be encoded as printable strings, if possible. If a portion cannot be encoded as a printable string, then and only then shall it be encoded using a different format and that format shall be UTF8.

For domain component attribute values: All domain component attribute values shall be encoded as an IA string.

7.1.5 *Name Constraints*

For a Subordinate CA Certificate to be considered Technically Constrained, the certificate must include an Extended Key Usage (EKU) extension specifying all extended key usages for certificates that the Subordinate CA Certificate is authorized to issue.

If the Subordinate CA Certificate includes the id-kp-serverAuth extended key usage, then the Subordinate CA Certificate must include the Name Constraints X.509v3 extension with constraints on dNSName, iPAddress and DirectoryName as follows:

- For each dNSName in permittedSubtrees, the CA must confirm that the Applicant has registered the dNSName or has been authorized by the domain registrant to act on the registrant's behalf in line with the verification practices of Section 3.2.2.
- For each iPAddress range in permittedSubtrees, the CA must confirm that the Applicant has been assigned the iPAddress range or has been authorized by the assigner to act on the assignee's behalf.
- For each DirectoryName in permittedSubtrees the CA must confirm the Applicants and/or Subsidiary’s Organizational name and location such that Subscriber certificates issued from the subordinate CA Certificate will be in compliancy with 3.1.1.

If the Subordinate CA Certificate is not allowed to issue certificates with an iPAddress, then the Subordinate CA Certificate must specify the entire IPv4 and IPv6 address ranges in excludedSubtrees. The Subordinate CA Certificate must include within excludedSubtrees an iPAddress GeneralName of 8 zero octets (covering the IPv4 address range of 0.0.0.0/0). The Subordinate CA Certificate must also include within excludedSubtrees an iPAddress GeneralName of 32 zero octets (covering the IPv6 address range of :0:0:0:0:0:0:0:0/0). Otherwise, the Subordinate CA Certificate MUST include at least one iPAddress in permittedSubtrees.

If the Subordinate CA is not allowed to issue certificates with dNSNames, then the Subordinate CA Certificate MUST include a zero-length dNSName in excludedSubtrees. Otherwise, the Subordinate CA Certificate must include at least one dNSName in permittedSubtrees.

7.1.6 *Certificate Policy Object Identifier*

Certificates issued under this policy shall assert the appropriate OID with which it was issued, as defined in Section 1.2.2.

7.1.7 Usage of Policy Constraints Extension

No stipulation.

7.1.8 Policy Qualifiers, Syntax, and Semantics

The issuing CA shall populate the policyQualifiers user notice field of Subordinate CA Certificates if it is not an Affiliate of the entity that controls the Root CA. The issuing CA may populate the policyQualifier CPSuri field with the URI of the CA's CPS.

The issuing CA should populate the policyQualifiers user notice field of DV-SSL and administrative Certificates. The issuing CA may populate the policyQualifier CPSuri field with the URI of the CA's CPS.

When populated, the userNotice field should contain text substantially similar to the following:

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 not marked critical when present.

7.2 CRL Profile

If utilized, CRLs will be issued in the X.509 version 2 format. The CPS or other publicly available document will identify the CRL extensions supported and the level of support for these extensions.

7.2.1 Version Number(s)

The issuing CA must issue X.509 version two (2) CRLs in accordance with the PKIX Certificate and CRL Profile.

7.2.2 CRL and CRL Entry Extensions

All Subscriber PKI software must correctly process all CRL extensions identified in the Certificate and CRL profile in Section 10. The CPS or other publicly available document will identify must define the use of any extensions supported by the issuing CA, its RAs and end entities.

7.3 OCSP Profile

OCSP Signers shall sign responses using algorithms designated for CRL signing. Section 10 contains the profile for an OCSP certificate signer, OCSP request, and responses.

7.3.1 Version Number(s)

See OCSP request and responses in Section 10.

7.3.2 OCSP Extensions

See OCSP request and responses in Section 10.

8 Compliance Audits and Other Assessments

8.1 Frequency of Audit or Assessments

A CA will undergo a review and approval process by the PMA to demonstrate compliance with this Policy. This Policy makes no stipulation as to the exact frequency of compliance inspections, but inspections for re-certification will be required any time a significant change in CA operations is made.

In any event, the CA, RAs, CSAs, and CMAs must certify annually that they have at all times during the period in question complied with the requirements of this Policy. The CA, RAs, and CMAs must also state any periods of non-compliance with this Policy and provide reasons for non-compliance. The period during which the CA issues Certificates shall be divided into an unbroken sequence of audit periods. An audit period must not exceed one year in duration. Whichever scheme is chosen, it must incorporate periodic monitoring and/or accountability procedures to ensure that its audits continue to be conducted in accordance with the requirements of the scheme.

8.1.1 Internal Self-Assessment Audits

During the period in which the CA issues Certificates, it shall monitor adherence to its Certificate Policy, Certification Practice Statement and the CA/B Forum Baseline Requirements and strictly control its service quality by performing self-audits on at least a quarterly basis against a randomly selected sample of the greater of one certificate or at least 3 percent of the Certificates issued by it during the period commencing immediately after the previous self-audit sample was taken.

8.2 Identity and Qualifications of Assessor

Subject to further qualifications identified in Section 9, Compliance Inspectors must (i) have qualifications in accord with best commercial practice; (ii) perform CA or Information System Security inspections as their primary responsibility; and (iii) be familiar with the CA's practices.

The CA's audit shall be performed by a Qualified Auditor. A Qualified Auditor means a natural person, legal entity, or group of natural persons or legal entities that collectively possess the following qualifications and skills:

1. Independence from the subject of the audit;
2. The ability to conduct an audit that addresses the criteria specified in an eligible audit scheme as specified in the CA/B Forum Baseline Requirements;
3. Individuals who have proficiency in examining Public Key Infrastructure technology, information security tools and techniques, information technology and security auditing, and the third-party attestation function;
4. Accreditation in accordance with ETSI TS 119 403, or accredited to conduct such audits under an equivalent national scheme, or accredited by a national accreditation body in line with ISO 27006 to carry out ISO 27001 audits or licensed by WebTrust;
5. Bound by law, government regulation, or professional code of ethics; and
6. Except in the case of an internal government auditing agency, maintains professional liability/errors & omissions insurance with policy limits of at least one million US dollars in coverage.

8.3 Assessor's Relationship to Assessed Entity

The Compliance Inspector(s) and CA must have a contractual relationship for the performance of the inspection, or be sufficiently separated organizationally from the CA to provide an unbiased, independent evaluation.

8.4 Topics Covered by Assessment

Inspections will be substantially similar to (i) the American Institute of Certified Public Accountants' ("AICPA's") Service Organization Control 2 Report; (ii) AICPA/CICA WebTrust for Certification Authorities (CA WebTrust); and/or (iii) any other appropriate standards as determined by the PMA.

SOC 2 and CA WebTrust are performed by an accredited public accountant or nationally-recognized accounting firm. Inspections must follow any guidelines adopted by the PMA, including whether the CA's practices comply with the technical, procedural and personnel policies and practices outlined in this Policy.

8.5 Actions Taken as a Result of Deficiency

CA inspection results must be submitted to the CA's regulator or licensing body where applicable, and the PMA. If irregularities are found, the CA must submit a report to its regulator or licensing body and the PMA as to any action the CA will take in response to the inspection report. Where the CA fails to take appropriate action in response to the inspection report, the CA's regulator, licensing body or the PMA may (i) indicate the irregularities, but allow the CA to continue operations until the next programmed inspection; (ii) allow the CA to continue operations for a maximum of thirty (30) days pending correction of any problems prior to revocation; (iii) downgrade the assurance level of any Certificates issued by the CA (including Cross Certificates); or (iv) revoke the CA's Certificate. Any decision regarding which of these actions to take will be based on the severity of the irregularities.

Any remedy may include permanent or temporary CA cessation, but all relevant factors must be considered prior to making a decision. A special audit may be required to confirm the implementation and effectiveness of the remedy. The CA will post any appropriate results of an inspection, in whole or in part, so that it is accessible for review by Subscribers and relying parties. The manner and extent of the publication will be defined by the CA.

8.6 Communication of Results

The audit report shall state explicitly that it covers the relevant systems and processes used in the issuance of all Certificates that assert one or more of the policy identifiers listed in the CA/B Forum Baseline Requirements in Section 9.3.1. The CA shall make the audit report publicly available. The CA is not required to make publicly available any general audit findings that do not impact the overall audit opinion. The CA shall make its Audit Report publicly available no later than three months after the end of the audit period. In the event of a delay greater than three months, and if so requested by an Application Software Supplier, the CA shall provide an explanatory letter signed by the Qualified Auditor.

9 Other Business and Legal Matters

9.1 Fees

9.1.1 Certificate Issuance or Renewal Fees

No stipulation.

9.1.2 Certificate Access Fees

No stipulation.

9.1.3 Revocation or Status Information Access Fee

No stipulation.

9.1.4 Fees for Other Services

No stipulation.

9.1.5 Refund Policy

No stipulation.

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

No stipulation.

9.3.2 Information Not Within the Scope of Confidential Information

No stipulation.

9.3.3 Responsibility to Protect Confidential Information

No stipulation.

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

No stipulation.

9.4.2 Information Treated as Private

No stipulation.

9.4.3 Information not Deemed Private

No stipulation.

9.4.4 *Responsibility to Protect Private Information*

No stipulation.

9.4.5 *Notice and Consent to use Private Information*

No stipulation.

9.4.6 *Disclosure Pursuant to Judicial or Administrative Process*

No stipulation.

9.4.7 *Other Information Disclosure Circumstances*

No stipulation.

9.5 Intellectual Property Rights

No stipulation.

9.6 Representations and Warranties

9.6.1 *CA Representations and Warranties*

By issuing a Certificate, the CA makes the certificate warranties listed herein to the following Certificate Beneficiaries:

- The Subscriber that is a party to the Subscriber or Terms of Use Agreement for the Certificate;
- All Application Software Suppliers with whom the Root CA has entered into a contract for inclusion of its Root Certificate in software distributed by such Application Software Supplier; and
- All Relying Parties who reasonably rely on a Valid Certificate.

The CA represents and warrants to the Certificate Beneficiaries that, during the period when the Certificate is valid, the CA has complied with these Requirements and its Certificate Policy and/or Certification Practice Statement in issuing and managing the Certificate.

The Certificate Warranties specifically include, but are not limited to, the following:

1. Right to Use Domain Name or IP Address. That, at the time of issuance, the CA: (i) implemented a procedure for verifying that the Applicant either had the right to use, or had control of, the Domain Name(s) and IP address(es) listed in the Certificate's subject field and subjectAltName extension (or, only in the case of Domain Names, was delegated such right or control by someone who had such right to use or control); (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in this Certificate Policy and/or the corresponding Certification Practice Statement.

2. Authorization for Certificate. That, at the time of issuance, the CA: (i) implemented a procedure for verifying that the Subject authorized the issuance of the Certificate and that the Applicant Representative is authorized to request the Certificate on behalf of the Subject; (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in this Certificate Policy and/or the corresponding Certification Practice Statement.

3. Accuracy of Information. That, at the time of issuance, the CA: (i) implemented a procedure for verifying the accuracy of all of the information contained in the Certificate (with the exception of the subject:organizationalUnitName attribute); (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in this Certificate Policy and/or the corresponding Certification Practice Statement.

4. No Misleading Information. That, at the time of issuance, the CA: (i) implemented a procedure for reducing the likelihood that the information contained in the Certificate's subject:organizationalUnitName attribute would be misleading; (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in this Certificate Policy and/or the corresponding Certification Practice Statement.

5. Identity of Applicant. That, if the Certificate contains Subject Identity Information, the CA: (i) implemented a procedure to verify the identity of the Applicant in accordance with Section 3.2; (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in this Certificate Policy and/or the corresponding Certification Practice Statement.

6. Subscriber Agreement. That, if the CA and Subscriber are not Affiliated, the Subscriber and CA are parties to a legally valid and enforceable Subscriber Agreement that satisfies the CA/B Forum Baseline Requirements, or, if the CA and Subscriber are Affiliated, the Applicant Representative acknowledged and accepted the Terms of Use.

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

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

The Root CA SHALL be responsible for the performance and warranties of the Subordinate CA, for the Subordinate CA's compliance with these Requirements, and for all liabilities and indemnification obligations of the Subordinate CA under these Requirements, as if the Root CA were the Subordinate CA issuing the Certificates.

By issuing a Certificate, the CA represents that it followed the procedure set forth this Policy and its Certification Practice Statement to verify that, as of the Certificate's issuance date, all of the Subject Information was accurate.

By issuing a Subordinate CA Certificate, the CA represents that it followed the procedure set forth in this Policy and/or its Certification Practice Statement to verify that, as of the Subordinate CA Certificate's issuance date, all of the Subject Information was accurate.

The CA represents that all Certificates containing a policy identifier indicating compliance with the CA/B Forum Baseline Requirements are issued and managed in accordance with the CA/B Forum Baseline Requirements.

Every Subordinate CA shall represent, in its Certificate Policy and/or Certification Practice Statement, that all Certificates containing a policy identifier indicating compliance with the CA/B Forum Baseline Requirements are issued and managed in accordance with the CA/B Forum Baseline Requirements.

9.6.2 RA Representations and Warranties

No stipulation.

9.6.3 Subscriber Representations and Warranties

The CA SHALL require, as part of the Subscriber or Terms of Use Agreement, that the Applicant make the commitments and warranties in this section for the benefit of the CA and the Certificate Beneficiaries.

Prior to the issuance of a Certificate, the CA SHALL obtain, 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 SHALL implement 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 MAY be 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.

The Subscriber 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 following obligations and warranties:

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.

9.6.4 Relying Party Representations and Warranties

No stipulation.

9.6.5 Representations and Warranties of Other Participants

No stipulation.

9.7 Disclaimer of Warranties

No stipulation.

9.8 Limitations of Liability

For delegated tasks, the CA and any Delegated Third Party MAY allocate liability between themselves contractually as they determine, but the CA SHALL remain fully responsible for the performance of all parties in accordance with these Requirements, as if the tasks had not been delegated.

If the CA has issued and managed the Certificate in compliance with these Requirements and this Policy and/or corresponding Certification Practice Statement, the CA MAY disclaim liability to the Certificate Beneficiaries or any other third parties for any losses suffered as a result of use or reliance on such Certificate beyond those specified in the CA's Certificate Policy and/or Certification Practice Statement. If the CA has not issued or managed the Certificate in compliance with these Requirements and its Certificate Policy and/or Certification Practice Statement, the CA MAY seek to limit its liability to the Subscriber and to Relying Parties, regardless of the cause of action or legal theory involved, for any and all claims, losses or damages suffered as a result of the use or reliance on such Certificate by any appropriate means that the CA desires. If the CA chooses to limit its liability for Certificates that are not issued or managed in compliance with these Requirements or its Certificate Policy and/or Certification Practice Statement, then the CA SHALL include the limitations on liability in the CA's Certificate Policy and/or Certification Practice Statement.

9.9 Indemnities

9.9.1 Indemnification by CAs

Notwithstanding any limitations on its liability to Subscribers and Relying Parties, the CA understands and acknowledges that the Application Software Suppliers who have a Root Certificate distribution agreement in place with the Root CA do not assume any obligation or potential liability of the CA under these Requirements or that otherwise might exist because of the issuance or maintenance of Certificates or reliance thereon by Relying Parties or others. Thus, except in the case where the CA is a government entity, the CA SHALL defend, indemnify, and hold harmless each Application Software Supplier for any and all claims, damages, and losses suffered by such Application Software Supplier related to a Certificate issued by the CA, regardless of the cause of action or legal theory involved. This does not apply, however, to any claim, damages, or loss suffered by such Application Software Supplier related to a Certificate issued by the CA where such claim, damage, or loss was directly caused by such Application Software Supplier's software displaying as not trustworthy a Certificate that is still valid, or displaying as trustworthy (1) a Certificate that has expired, or (2) a Certificate that has been revoked (but only in cases where the revocation status is currently available from the CA online, and the application software either failed to check such status or ignored an indication of revoked status).

9.9.2 Indemnification by Subscribers

No stipulation.

9.9.3 Indemnification by Relying Parties

No stipulation.

9.10 Term and Termination

9.10.1 Term

No stipulation.

9.10.2 Termination

No stipulation.

9.10.3 Effect of Termination and Survival

No stipulation.

9.11 Individual Notices and Communications with Participants

No stipulation.

9.12 Amendments

9.12.1 Procedure for Amendment

No stipulation.

9.12.2 Notification Mechanism and Period

No stipulation.

9.12.3 Circumstances under Which OID Must Be Changed

No stipulation.

9.13 Dispute Resolution Provisions

No stipulation.

9.14 Governing Law

No stipulation.

9.15 Compliance with Applicable Law

No stipulation.

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

No stipulation.

9.16.2 Assignment

No stipulation.

9.16.3 Severability

If a court or government body with jurisdiction over the activities covered by the CA/B Forum Baseline Requirements determines that the performance of any mandatory requirement is illegal, then such requirement is considered reformed to the minimum extent necessary to make the requirement valid and legal. This applies only to operations or certificate issuances that are subject to the laws of that jurisdiction. The parties involved SHALL notify the CA/Browser Forum of the facts, circumstances, and law(s) involved, so that the CA/Browser Forum may revise these Requirements accordingly.

9.16.4 Enforcement

No stipulation.

9.16.5 Force Majeure

No stipulation.

9.17 Other Provisions

No stipulation.

10 Certificate Profiles

10.1 Root CA Certificate

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	As stipulated in Section 7.1.3
Issuer Distinguished Name	cn= ISRG Root X [*n*], o= Internet Security Research Group, C=US where [*n*] in an integer starting in 1 and represents the instance of the Root CA. For example, ISRG Root X1, ISRG Root X2, etc.
Validity Period	Up to 25 years. Dates expressed in UTC format. See Section 6.3.2.
Subject Distinguished Name	Same as issuer DN
Subject Public Key Information	As stipulated in Section 6.1.4
Issuer's Signature	As stipulated in Section 7.1.3
Extensions	
Subject Key Identifier	Not Critical. Required. Octet String (20 byte SHA-1 hash of the binary DER encoding of the Root CA public key information)
Key Usage	Critical. Required. keyCertSign, cRLSign
Extended Key Usage	Not Present
Private Key Usage Period	Not Present
Private Key Usage Period	Not Present
Certificate Policies	Not Present
Subject Information Access	Not Present
Policy Mapping	Not Present
Subject Alternative Name	Not Present
Issuer Alternative Name	Not Present
Subject Directory Attributes	Not Present
Basic Constraints	Critical. Required. cA=True, pathLength constraint absent
Policy Constraints	Not Present
CRL Distribution Points	Not Present

10.2 Subordinate CA Certificate

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	As stipulated in Section 7.1.3
Issuer Distinguished Name	Derived from the Issuer subject DN
Validity Period	Up to 8 years. Dates expressed in UTC format. See Section 6.3.2.
Subject Distinguished Name	cn= Let's Encrypt Authority X[*m*], o=Let's Encrypt, C=US where *m* in an integer starting in 1 and represents the instance of the subordinate CA. For example the initial instances of the subordinate CA for DV-SSL would be Let's Encrypt Authority X1, Let's Encrypt Authority X12, etc.
Subject Public Key Information	As stipulated in Section 6.1.4
Issuer's Signature	As stipulated in Section 7.1.3
Extensions	

Authority Key Identifier	Not Critical. Required. Octet String (20 byte SHA-1 hash of the binary DER encoding of the Root CA public key information)
Subject Key Identifier	Not Critical. Required. Octet String (20 byte SHA-1 hash of the binary DER encoding of the Subordinate CA public key information)
Key Usage	Critical. Required. digitalSignature, keyCertSign, cRLSign
Extended Key Usage	Not Critical. Optional id-kp-serverAuth, id-kp-clientAuth
Private Key Usage Period	Not Present
Certificate Policies	Not Critical. Required. One or more policy OIDS from Section 1.2.2 as appropriate. Required, a user notice qualifier Optional, a CPS's HTTP URI
Subject Information Access	Not Present
Policy Mapping	Not Present
Subject Alternative Name	Not Present
Issuer Alternative Name	Not Present
Subject Directory Attributes	Not Present
Basic Constraints	Critical. Optional. cA=True, pathLength=0
Policy Constraints	Not Present
Name Constraints	Not Critical[3]. Optional. As stipulated in Section 7.1.5
Authority Information Access	Not Critical. Required. The HTTP URL of the Issuing CA's OCSP responder MAY be omitted, provided that the Subscriber "staples" the OCSP response for the Certificate in its TLS handshakes. If present, contains the HTTP URI of the CA's OCSP responder, and the HTTP URI of the CA's Certificate
CRL Distribution Points	Not Critical. Required. Contains HTTP URI to CRL

10.3 **DV-SSL Certificate**

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	As stipulated in Section 7.1.3
Issuer Distinguished Name	Derived from the Issuer subject DN
Validity Period	Up to 39 months. Dates expressed in UTC format. See Section 6.3.2.
Subject Distinguished Name	One or more of the following optional elements is required: Optional, cn= Server's FQDN or IP Address, Optional, C=two letter ISO code Optional, serialNumber=certificate's serial number
Subject Public Key Information	As stipulated in Section 6.1.4
Issuer's Signature	As stipulated in Section 7.1.3
Extensions	

[3] Non-critical Name Constraints are an exception to RFC 5280 (4.2.1.10), however, they may be used until the Name Constraints extension is supported by Application Software Suppliers whose software is used by a substantial portion of Relying Parties worldwide. This is compliant with Baseline Requirements Appendix B (2).

Authority Key Identifier	Not Critical. Required. Octet String (20 byte SHA-1 hash of the binary DER encoding of the Subordinate CA public key information)
Subject Key Identifier	Not Critical. Required. Octet String (20 byte SHA-1 hash of the binary DER encoding of the public key information)
Key Usage	Critical. Optional. digitalSignature, keyEncipherment
Extended Key Usage	Not Critical. Required. id-kp-serverAuth, id-kp-clientAuth
Private Key Usage Period	Not Present
Certificate Policies	Not Critical. Required. Contains one or more policy OIDS from Section 1.2.2 as appropriate. Recommended, a user notice qualifier Optional, a CPS's HTTP URI
Subject Information Access	Not Present
Policy Mapping	Not Present
Subject Alternative Name	Not Critical. Required. At least one dNSName=FQDN;
Issuer Alternative Name	Not Present
Subject Directory Attributes	Not Present
Basic Constraints	Not Present
Policy Constraints	Not Present
Name Constraints	Not Present
Authority Information Access	Not Critical. Required. The HTTP URL of the Issuing CA's OCSP responder MAY be omitted, provided that the Subscriber "staples" the OCSP response for the Certificate in its TLS handshakes.If present, contains the HTTP URI of the CA's OCSP responder, and the HTTP URI of the CA's Certificate
CRL Distribution Points	Not Critical, Optional. Contains HTTP URI to CRL
TLS Feature	Not Critical, Optional. Present if requested by subscriber.

10.4 **Human Administrative Certificate**

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	As stipulated in Section 7.1.3
Issuer Distinguished Name	Derived from the Issuer subject DN
Validity Period	Up to 3 years. Dates expressed in UTC format. See Section 6.3.2.
Subject Distinguished Name	cn= [Applicant's Full name], O=[CA's organization Name], OU= Administrative Certificate, C=two letter ISO code
Subject Public Key Information	As stipulated in Section 6.1.4
Issuer's Signature	As stipulated in Section 7.1.3
Extensions	
Authority Key Identifier	Not Critical. Required. Octet String (20 byte SHA-1 hash of the binary DER encoding of the Subordinate CA public key information)
Subject Key Identifier	Not Critical. Required. Octet String (20 byte SHA-1 hash of the binary DER encoding of the public key information)
Key Usage	Critical. Optional. digitalSignature, nonRepudiation
Extended Key Usage	Not Present
Private Key Usage Period	Not Present
Certificate Policies	Not Critical. Required. Contains administrative policy OID from Section 1.2.2 as appropriate. Recommended, a user notice qualifier Optional, a CPS's HTTP URI
Subject Information Access	Not Present
Policy Mapping	Not Present
Subject Alternative Name	Not Critical. Required. RFC822= Applicant's email address
Issuer Alternative Name	Not Present
Subject Directory Attributes	Not Present
Basic Constraints	Not Present
Policy Constraints	Not Present
Name Constraints	Not Present
Authority Information Access	Not Critical. Required. Not present if the OCSP responses are stapled. If present, contains the HTTP URI of the CA's OCSP responder, and the HTTP URI of the CA's Certificate
CRL Distribution Points	Not Critical, Optional. Contains HTTP URI to CRL

10.5 **OCSP Responder Certificate(s)**

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	As stipulated in Section 7.1.3
Issuer Distinguished Name	Derived from the Issuer subject DN
Validity Period	Up to 5 years. Dates expressed in UTC format. See Section 6.3.2.
Subject Distinguished Name	cn= [OCSP Server Name], O= [Organization Managing OCSP], C=two letter ISO code

Subject Public Key Information	As stipulated in Section 6.1.4
Issuer's Signature	As stipulated in Section 7.1.3
Extensions	
Authority Key Identifier	Not Critical. Required. Octet String (20 byte SHA-1 hash of the binary DER encoding of the CA (either the Root CA or Subordinate CA) public key information)
Subject Key Identifier	Not Critical. Required. Octet String (20 byte SHA-1 hash of the binary DER encoding of the public key information)
Key Usage	Critical. Optional. digitalSignature,
Extended Key Usage	Not Critical. Required. id-kp-OCSPSigning
Certificate Policies	Not Critical. Optional. All the certificate policies, from Section 1.2.2, under which the CA issues Certificates.
Subject Alternative Name	Not Critical. Required. OCSP responder' URL
No Check	Not Critical. Required. id-pkix-ocsp-nocheck
Authority Information Access	Not Critical. Optional. Pointer to the CA Certificate
Basic Constraints	Critical. Optional. cA=False

10.6 Root CRL

Field	CRL Value
Version	V2 (1)
Issuer Signature Algorithm	As stipulated in Section 7.1.3
Issuer Distinguished Name	Derived from the Issuer subject DN cn= ISRG Root CA [*n*], o= ISRG, C=US where [*n*] in an integer starting in 1 and represents the instance of the Root CA. For example, ISRG Root CA 1, ISRG Root CA 2, etc.
thisUpdate	Time and date expressed in UTC format.
nextUpdate	Time and date expressed in UTC format. ThisUpdate + (up to) 12 months
Revoked Certificates List	0 or more 2-tuple of certificate serial number and revocation date (UTC Format)
Issuer's Signature	As stipulated in Section 7.1.3
CRL Extensions	
CRL Number	Integer
Authority Key Identifier	Not Critical. Required. Octet String (20 byte SHA-1 hash of the binary DER encoding of the CA public key information)
CRL Extensions	
Invalidity Date	Optional
Reason Code	Must be present if one of the following: Key Compromise, CA Compromised, Affiliation Changed, Superseded, and Cessation of Operations. Absent Otherwise.

10.7 **Subordinate CRL (Optional)**

Field	CRL Value
Version	V2 (1)
Issuer Signature Algorithm	As stipulated in Section 7.1.3
Issuer Distinguished Name	cn= ISRG [*Type*] CA [*m*], o= ISRG, o=TBD, C=US where *Type* represents the type of certificate issued from the CA. where *m* in an integer starting in 1 and represents the instance of the subordinate CA. For example the initial instances of the subordinate CA for DV-SSL would be ISRG DV-SSL CA 1, ISRG DV-SSL CA 2, etc.
thisUpdate	Time and date expressed in UTC format.
nextUpdate	Time and date expressed in UTC format. ThisUpdate + (up to) 7 days
Revoked Certificates List	0 or more 2-tuple of certificate serial number and revocation date (UTC Format)
Issuer's Signature	As stipulated in Section 7.1.3
CRL Extensions	
CRL Number	Integer
Authority Key Identifier	Not Critical. Required. Octet String (20 byte SHA-1 hash of the binary DER encoding of the CA public key information)
CRL Extensions	
Invalidity Date	Optional
Reason Code	Must be present if one of the following: Key Compromise, Affiliation Changed, Superseded, and Cessation of Operations. Absent Otherwise.

10.8 **OCSP Request Format**

Field	Expected Value
Version	V1 (0)
Requester Name	Not Required
Request List	List of Certificates
Signature	Not Required
Extensions	**Not Required**

10.9 **OCSP Response Format**

Field	Expected Value
Response Status	Successful | Malformed Request | Internal Error | Try Later
Response Type	id-pkix-ocsp-basic
Version	V1 (0)
Responder ID	Hash of Responder Public Key
Produced At	Generalized Time
List of Responses	Each response will contain Certificate identifier, Certificate status[4], thisUpdate, nextUpdate
Signature Algorithm	As stipulated in Section 7.1.3

[4] Certificate Status. If the Certificate is revoked, the OCSP Responder will provide revocation time and revocation reason

Signature	Present
Certificates	Applicable Certificates issued to the OCSP Responder
Extensions	**Not Required**
Nonce	Will be present if nonce extension is present in the request.