Combined Certificate Policy and Certification Practice Statement

ICANN Certificate Authority

Version 1.0

Root Zone KSK Operator Policy Management Authority

28 May 2026

Table of Contents

1 INTRODUCTION

1.1 Overview

This combined Certificate Policy (CP) and Certification Practice Statement (CPS) describes the policies and practices employed by the Internet Corporation for Assigned Names and Numbers (ICANN) in operating its Public Key Infrastructure (PKI). It covers certificate lifecycle services including issuance, management, and revocation, and defines the operational, procedural, and technical controls implemented by the ICANN Certificate Authority (CA).

The ICANN CA is operated solely to support ICANN's role as the DNSSEC Root Zone Key Signing Key (KSK) Publisher and Manager. Its function is to issue and manage certificates related to the signing of the DNS Root Trust Anchors file. The CA does not provide certificate services to the public or for commercial purposes, and all issued certificates are used within a strictly controlled and restricted trust environment.

1.2 Document name and identification

This document is the CP/CPS for ICANN Certificate Authority.

Corresponding policy OID: 1.3.6.1.4.1.42139.1.1

The following revisions have been made:

Date	Changes	Version
2017-03-31	Initial version (draft)	n/a
2026-05-28	First formal release; major update	1.0

1.3 PKI participants

1.3.1 Certification authorities

Trust in this PKI originates from the ICANN Root CA, which issues certificates to designated end-entities. These end-entity certificates are used to digitally sign the DNS Root Trust Anchors file. The PKI consists of two Root CAs (a legacy root and a current active root) and their corresponding end-entity certificates.

CA Type	Distinguished Name	Key Pair Type and Parameters	Cert SHA-256 Fingerprint	Validity Period	Usage
Root CA (Legacy)	O=ICANN, OU=ICANN Certification Authority, CN=ICANN Root CA, C=US	RSA 2048 bit, e=65537	AE:E8:99:06:D7:CC:60:C5:E1:51:F3:BB:92:3A:BF:8A:1B:28:DC:85:5D:5E:21:27:CB:52:4E:AD:4A:AD:60:3D	Not Before: Dec 23 04:19:12 2009 GMT, Not After : Dec 18 04:19:12 2029 GMT	Retained for validation purposes. No longer used for new signing operations, but still validates the corresponding end-entity certificate
End Entity (Legacy)	O=ICANN, CN=DNSSEC Trust Anchor Verification, emailAddress=dnssec@iana.org Issuer: O=ICANN, OU=ICANN Certification Authority, CN=ICANN Root CA, C=US	RSA 2048 bit, e=65537	2C:A1:3F:66:11:A5:68:30:02:17:7B:42:90:A2:6E:A7:ED:A9:EE:EA:65:18:EF:A5:D6:3A:27:A2:A6:75:B6:7F	Not Before: Mar 15 21:49:35 2023 GMT, Not After : Mar 13 21:49:35 2029 GMT	Continues to sign versions of the DNS Root Trust Anchors file
Root CA (Current)	C=US, O=ICANN, OU=ICANN Certification Authority, CN=ICANN Root CA v2	RSA 4096 bit, e=65537	D8:EE:E1:B7:42:08:B8:16:3E:1C:2B:99:0F:82:DD:9F:75:22:36:BA:13:0C:92:93:9E:77:28:EA:46:4E:BF:C3	Not Before: Mar 20 21:04:26 2025 GMT, Not After : Mar 20 21:04:26 2045 GMT	Currently active trust anchor used to issue the current end-entity certificate

End Entity (current)	C=US, OU=ICANN, CN=DNSSEC Trust Anchor Verification v2, emailAddress=dnssec@iana.org Issuer: C=US, O=ICANN, OU=ICANN Certification Authority, CN=ICANN Root CA v2	RSA 4096 bit, e=65537	87:CF:3A:83:8C:92:74:1D:CC:3C:B2:B7:67:ED:28:05:02:14:9C:B4:F1:FF:05:FD:F8:95:13:2F:D2:71:6B:ED	Not Before: Mar 20 21:07:57 2025 GMT, Not After : Mar 20 00:00:00 2045 GMT	Actively used to sign the DNS Root Trust Anchors file

1.3.2 Registration authorities

The Registration Authority (RA) functions and responsibilities are performed by ICANN.

1.3.3 Subscribers

Subscribers to the ICANN CA are internal services with a legitimate business need for authentication and encryption services. All subscribers are internal to ICANN.

1.3.4 Relying parties

The relying parties of certificates issued by the ICANN CA are entities establishing encrypted communication or verifying the authenticity or integrity of data signed using an issued certificate.

1.4 Certificate usage

CA certificates are only used for CA functions, while end-entity certificates may not be used for CA functions.

Other certificate usage restrictions are indicated in the Key Usage attributes in the applicable certificate profile, as per section 7.1.

1.5 Policy administration

This CP/CPS is subject to periodic review and updates by the Policy Management Authority (PMA). The PMA is responsible for the management of the CP/CPS and should be considered as the point of contact for all matters related to the CP/CPS.

1.5.1 Organization administering the document

Internet Corporation for Assigned Names and Numbers
12025 Waterfront Drive, Suite 300
Los Angeles
CA 90094
United States of America

1.5.2 Contact person

Root Zone KSK Operator Policy Management Authority.

Internet Corporation for Assigned Names and Numbers

12025 Waterfront Drive, Suite 300
Los Angeles
CA 90094
United States of America

Phone: +1 (424) 254-5300

Email: root-ksk-pma@iana.org

1.5.3 Person determining CP/CPS suitability for the policy

The Policy Management Authority is responsible for determining the CP/CPS suitability and compliance with the business requirements and any applicable policy.

1.5.4 CP/CPS approval procedures

Amendments to this CP/CPS are made by the Policy Management Authority (PMA). Amendments will either be in the form of a document containing an amended form of the CP/CPS or an update. Updates supersede any designated or conflicting provisions of the referenced version of the CP/CPS.

The PMA reserves the right to amend the CP/CPS without notification for amendments that are not material, including without limitation corrections of typographical errors, changes to URLs, and changes to contact information. The PMA's decision to designate amendments as material or non-material is within the PMA's sole discretion. Proposed amendments to the CP/CPS will appear in the Practices Updates and Notices section of the Repository, which is located at:

https://www.iana.org/dnssec/procedures

Proposed amendments to the CP/CPS are solicited from the community by the PMA. If the PMA considers such an amendment desirable and proposes to implement the amendment, the PMA will provide public notice of such amendment in accordance with this section.

Should the PMA determine that material amendments to the CP/CPS are necessary immediately to stop or prevent a breach of the security of any portion of it, the PMA is entitled to make such amendments by publication in the Repository. Such amendments will be effective immediately upon publication.

1.6 Definitions and acronyms

1.6.1 Definitions

Hardware Security Module (HSM): A type of secure cryptoprocessor aimed at managing cryptographic keys and cryptographic operations while providing physical protection of the private keying material through mechanisms to detect and protect against tampering.

Key Management Facilities (KMF): High security location where cryptographic materials are stored, and cryptographic operations are performed.

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

Public Key Infrastructure (PKI): The architecture, organization, techniques, practices, and procedures that collectively support the implementation and operation of a public key cryptographic system.

1.6.2 Acronyms

CBO	Cryptographic Business Operations
FIPS	Federal Information Processing Standards
HSM	Hardware Security Module
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
ISO	International Organization for Standardization
OID	Object Identifier
PMA	Policy Management Authority
S/MIME	Secure/Multipurpose Internet Mail Extensions
SHA	Secure Hash Algorithm

1.6.3 References

CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates: https://cabforum.org/working-groups/server/baseline-requirements/documents/

[RFC3647] “Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework”, November 2003, https://www.rfc-editor.org/info/rfc3647

[RFC5280] “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile”, May 2008, https://www.rfc-editor.org/info/rfc5280

1.6.4 Conventions

All dates and times in this document are represented in Coordinated Universal Time (UTC) using the YYYY-MM-DD HH:MM:SS format unless otherwise specified.

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

The CP/CPS is published in the repository section of the IANA web site at:

https://www.iana.org/dnssec/procedures

The ICANN Root CA certificates and applicable certificate revocation lists (CRLs) are available at:

https://data.iana.org/root-anchors/

2.2 Publication of certification information

Certificates for valid Certificate Authorities (CAs) are published in the repository.

2.3 Time or frequency of publication

All information designated for publication in the repository will be published as soon as operationally feasible following its approval or generation.

2.4 Access controls on repositories

Information published in the repository is publicly accessible information. Read-only access to this information is unrestricted. ICANN has implemented logical and physical security measures to prevent unauthorized persons from adding, deleting, or modifying repository entries.

3 IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of names

All certificates in the PKI use the X.500 Distinguished Name (DN) format to identify subjects and issuer.

Certificates may additionally include the following attributes:

- Country (C)
- Organization (O)
- Organization Unit (OU)
- Common Name (CN)
- E-Mail Address (E)

3.1.2 Need for names to be meaningful

Subscribers' certificate naming follows standards and conventions to allow the relying party to determine the identity of the individual, function, or organization that is the subject of the certificate.

3.1.3 Anonymity or pseudonymity of subscribers

No stipulation.

3.1.4 Rules for interpreting various name forms

Name forms are interpreted as described in the applicable certificate profiles, as per section 7.1.

3.1.5 Uniqueness of names

Each Distinguished Name is required to be unique per subscriber within the naming domain of the specific CA.

3.1.6 Recognition, authentication, and role of trademarks

No stipulation.

3.2 Initial identity validation

3.2.1 Method to prove possession of private key

The certificate applicant must prove possession of the private key by providing a PKCS#10 compliant certificate signing request. This establishes that the certificate applicant holds or controls the private key corresponding to the enclosed public key.

3.2.2 Authentication of organization identity

Not applicable. All subscribers are internal to ICANN.

3.2.3 Authentication of individual identity

Not applicable. All subscribers are internal to ICANN.

3.2.4 Non-verified subscriber information

Not applicable.

3.2.5 Validation of authority

Authority to request certificates are verified through the processes described in 3.2.2 and 3.2.3 respectively.

3.2.6 Criteria for interoperation

No stipulation.

3.3 Identification and authentication for re-key requests

Any request to change a certified key is processed as a new certificate request, and authentication is carried out in terms of section 3.2.2 and 3.2.3 respectively.

3.4 Identification and authentication for revocation request

Identification of the entity requesting revocation will be made by available means and as thoroughly as the situation requires. If the subject is unable to authenticate using the certified key pair, the subject may be authenticated by demonstrating ability to read received e-mail to the e-mail address given at the time of application.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate Application

4.1.1 Who can submit a certificate application

Only internal ICANN staff with legitimate business needs may apply for an end-entity certificate.

4.1.2 Enrollment process and responsibilities

Authorized applicants shall submit the application in the form of a Certificate Signing Request in PKCS#10 format, providing proof-of-possession of private key and supplying the accompanying attributes which should be certified.

The application is verified by CA operations staff, using the appropriate means as per 3.2.

After the application has been approved, the Certificate Signing Request will be processed, and the end-entity certificate will be issued.

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

ICANN shall perform identification and authentication of all required subscriber information as described in section 3.2,

4.2.2 Approval or rejection of certificate applications

Cryptographic Business Operations (CBO) staff may approve or reject any end-entity Certificate Signing Request based on the result of the validation process.

The processing of CA Certificate Signing Requests is approved or rejected by the PMA.

4.2.3 Time to process certificate applications

Certificate Signing Requests will be processed within a reasonable time of receipt. There is no time stipulation to complete processing of an application.

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

Once the Certificate Signing Request has been approved, ICANN will generate a Certificate based on the information in the Certificate Signing Request provided by the subscriber. ICANN will add the appropriate key usage extensions to the Certificate at the time of issuance.

4.3.2 Notification to subscriber by the CA of issuance of certificate

Subscribers are notified of certificate issuance and are provided the issued certificate.

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

The act of installing the issued certificate and using it with the subscribers' key pair constitutes acceptance.

4.4.2 Publication of the certificate by the CA

CA certificates are published at the repository web site per section 2.1. Subscribers' certificates are not published by the CA.

4.4.3 Notification of certificate issuance by the CA to other entities

Not applicable.

4.5 Key pair and certificate usage

4.5.1 Subscriber private key and certificate usage

Subscribers may use their certificate and private key in compliance with the subscriber agreement (when applicable) and as constrained by the key usage extensions of the certificate.

4.5.2 Relying party public key and certificate usage

After having made the appropriate revocation checks, relying parties may use the certificates and public keys as constrained by the key usage extensions of the certificate.

4.6 Certificate renewal

Any request to renew a certificate is processed as a new certificate request as per section 4.1-4.4.

4.7 Certificate re-key

Any request to change a certified key is processed as a new certificate request as per section 4.1-4.4. In addition, if the current private key is lost or compromised, the subscriber must request revocation as per section 4.9.

4.8 Certificate modification

Any request to modify a certificate is processed as a new certificate request as per section 4.1-4.4. In addition, if current certificate information is invalid, the subscriber must request revocation as per section 4.9.

4.9 Certificate revocation and suspension

4.9.1 Circumstances for revocation

Subscribers are obliged to promptly request revocation in the event of a suspected or known compromise of subjects' private key or if the certificate information is no longer valid.

In addition, ICANN may revoke a certificate at its own discretion if ICANN suspects or is made aware the subscribers' key has been compromised, if the subscriber has violated material obligations under the subscriber agreement, if the certified information is invalid or if CA operations are terminated.

4.9.2 Who can request revocation

The subscriber or a delegate of the subscriber may request revocation.

4.9.3 Procedure for revocation request

The subscriber shall submit revocation requests using any of the means available through the repository web site (section 2.1). The request will be verified and expedited and a CRL will be published as soon as practically possible and within the time frames set forth in section 5.7.4.

4.9.4 Revocation request grace period

Revocations are effective immediately after they have been processed.

4.9.5 Time within which CA must process the revocation request

No stipulation.

4.9.6 Revocation checking requirement for relying parties

Relying parties are required to make the appropriate revocation checks before accepting a certificate as valid.

4.9.7 CRL issuance frequency (if applicable)

CRLs are issued for certificates where revocation is supported. CRLs are published on an as-needed basis and reissued whenever a revocation occurs, or more frequently if operationally required.

This CA does not follow a fixed CRL publication interval unless specified in the applicable certificate profile.

4.9.8 Maximum latency for CRLs (if applicable)

As per section 4.9.7.

4.9.9 On-line revocation/status checking availability

No on-line certificate status checking service is provided.

4.9.10 On-line revocation checking requirements

Not applicable.

4.9.11 Other forms of revocation advertisements available

No stipulation.

4.9.12 Special requirements regarding key compromise

No stipulation.

4.9.13 Circumstances for suspension

Suspension of certificates is not supported within the PKI.

4.9.14 Who can request suspension

Not applicable.

4.9.15 Procedure for suspension request

Not applicable.

4.9.16 Limits on suspension period

Not applicable.

4.10 Certificate status services

No other certificate status checking service is provided other than the publishing of the CRLs.

4.11 End of subscription

The subscription is ended by either:

- allowing the certificate to expire without renewing that certificate

- revoking the certificate without replacing the certificate

4.12 Key escrow and recovery

Subscriber private keys are maintained under CA control; no third-party escrow is used.

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1 Physical controls

Physical security controls, which support the security requirements of this CP/CPS, have been implemented.

5.1.1 Site location and construction

PKI operations are conducted within a physically protected environment that deters, prevents, and detects any unauthorized use of, access to, or disclosure of sensitive information and systems, whether covert or overt.

5.1.2 Physical access

CA systems are protected by a minimum of four tiers of physical security, with access to lower tiers required before gaining access to higher tiers. Progressively more restrictive physical access controls to each tier are applied. Unauthorized access becomes increasingly difficult as one reaches higher tiers.

Sensitive PKI operational activity and any activity related to the lifecycle of the CA keys occur within these restrictive physical tiers.

Physical access is automatically logged and video recorded. All tiers enforce individual access control through the use of two-factor authentication. Unescorted personnel, including visitors or employees without specific authorization, are not allowed into such secured areas. The physical security system includes additional controls for tiers used for key management activity which serves to protect storage of Hardware Security Modules (HSMs) and keying material.

Areas used to create and store cryptographic material enforce dual access control, each through the use of two-factor authentication. HSMs are protected through the use of tamper-evident bags, locked safes, cabinets and containers. Access to HSMs and keying material is restricted in accordance with the requirements for segregation of duty. The opening and closing of cabinets or containers in these tiers is logged for auditing purposes.

5.1.3 Power and air conditioning

The KMF is equipped with a UPS backup power system that provides limited, temporary access to electric power. The air conditioning systems are managed by the building's central controls, which regulate temperature and relative humidity.

5.1.4 Water exposures

Reasonable precautions have been taken to minimize the risk of water exposure to the PKI systems.

5.1.5 Fire prevention and protection

Reasonable precautions have been taken to prevent fires or other damaging exposure to flame or smoke. The fire prevention and protection measures have been designed to comply with local fire safety regulations.

5.1.6 Media storage

All media containing production data, software, audit records or backup information are stored within the facilities or in a secure off-site storage facility with appropriate physical and logical access controls designed to limit access to authorized personnel and protect such media from accidental damage (e.g., flooding, extreme temperatures and fire).

5.1.7 Waste disposal

Sensitive documents and materials are shredded before disposal. Media used to collect or transmit sensitive information are rendered unreadable before disposal. Cryptographic devices are physically destroyed or zeroized in accordance with the manufacturers' guidance prior to disposal. Other waste is disposed of in accordance with the normal waste disposal and recycling requirements.

5.1.8 Off-site backup

Routine backups of critical system data, audit log data, and other sensitive information are performed. Off-site backup media are stored in a physically secure.

5.2 Procedural controls

5.2.1 Trusted roles

The categories of personnel identified in this section are considered as Trusted Persons having a Trusted Role. A Trusted Person may only possess one Trusted Role. Persons seeking to become Trusted Persons by obtaining a Trusted Role must successfully complete the screening requirements set out in this CP/CPS.

Trusted Persons include all employees, contractors, and consultants that have access to or control operations that may materially affect:

- Generation and protection of the private component of the CA keys.
- Secure export or import of any public components.

Trusted roles include, but are not limited to:

- Ceremony Administrator
- Internal Witnesses
- Crypto Officers

- Safe Security Controllers
- System Administrator

5.2.2 Number of persons required per task

Rigorous control procedures have been established which enforces segregation of duties based on roles to ensure that multiple Trusted Persons are required to perform sensitive tasks.

Access to and management of cryptographic hardware is based on the principle of successive barriers in three tiers, requiring at least six trusted persons from four different roles. These barriers are as follows:

Tier 5: Physical access to the safe room requires one person from the Key Ceremony Administrator role in combination with one person from the Internal Witness roles.

Tier 6: Physical access to HSMs and activation material, requires one out of two of the Safe Controllers, in addition to the Trusted Persons required at Tier 5 and 7.

Tier 7: Activation of an HSM requires three out of seven Crypto Officers to extract activation material from a set of safe deposit boxes installed within the safe (Tier 6), using their physical key. Backup and restoration of the contents of a HSM requires at least five out of seven Crypto Officers.

Other internal control procedures are designed to ensure that at a minimum two Trusted Persons are required to perform any sensitive task.

5.2.3 Identification and authentication for each role

For all personnel seeking to become Trusted Persons, verification of identity is performed through a check of well-recognized forms of identification (e.g., passports and driver's licenses). Identity is further confirmed through the background checking procedures described in section 5.3 of this CP/CPS. It is ensured that personnel have achieved the Trusted Person status and approval has been given before these personnel are:

- Issued access devices and granted access to the required facilities, or
- Issued electronic credentials to access and perform specific functions on the CA systems.

5.2.4 Roles requiring separation of duties

Tasks requiring separation of duties include (but are not limited to) the generation, use and destruction of CA key material.

Personnel fulfilling the roles of auditors may also not participate in the operations or multi-person control of the CA systems.

5.3 Personnel controls

5.3.1 Qualifications, experience, and clearance requirements

Personnel seeking to become Trusted Persons are required to present proof of the requisite background, qualifications, and experience needed to perform their prospective job responsibilities competently and satisfactorily.

Background checks are repeated at least every 5 years for personnel holding Trusted Roles.

5.3.2 Background check procedures

All personnel with access to any cryptographic components used with the CA systems are required to pass a background check extending back at least five years.

Prior to commencement of engagement in a Trusted Role, background checks are conducted that include the following:

- Confirmation of previous employment
- Checking of professional references
- Confirmation of the highest or most relevant educational degree obtained
- Checking of credit/financial records to the extent allowed by national laws for the individual's country of residence

The factors revealed in a background check that may be considered grounds for rejecting candidates for Trusted Roles, or for taking action against an existing Trusted Person generally include, but are not limited to:

- Misrepresentations made by the candidate or Trusted Person
- Highly unfavorable or unreliable professional references
- Indications of a lack of financial responsibility

Reports containing such information are evaluated by the Human Resources function and security personnel, who determine the appropriate course of action in light of the type, severity, and frequency of the behavior uncovered by the background check.

Such actions may include measures up to and including the cancellation of offers of employment made to candidates for Trusted Roles or the termination of existing Trusted Persons. The use of information revealed in a background check to take such actions is subject to the applicable federal, state, and local laws.

5.3.3 Training requirements

Personnel are provided with training when hired, as well as the requisite on-the-job training needed to perform their duties competently and satisfactorily.

The training programs are tailored to the individuals' responsibilities and include the following as relevant:

- Basic PKI concepts
- Job responsibilities
- Use and operation of deployed hardware and software
- Security and operational policies and procedures
- Incident and compromise reporting and handling
- Disaster recovery and business continuity procedures

The training programs are periodically reviewed and enhanced as necessary.

5.3.4 Retraining frequency and requirements

Refresher training and updates are provided to personnel to the extent and frequency required to ensure that such personnel maintain the required level of proficiency to perform their job responsibilities competently and satisfactorily.

5.3.5 Job rotation frequency and sequence

The responsibility to execute the tasks of respective Trusted Role will be distributed evenly over the set of the appointed personnel.

Other positions are rotated and replaced as needed.

5.3.6 Sanctions for unauthorized actions

Appropriate disciplinary actions are taken for unauthorized actions with respect to this CP/CPS and/or other violations of security policies and procedures. Disciplinary actions may include measures up to and including termination and are commensurate with the frequency and severity of the unauthorized actions.

5.3.7 Independent contractor requirements

In limited circumstances, independent contractors or consultants may be used to fill Trusted Roles. Any such contractor or consultant is held to the same functional and security criteria that apply to any employees in a comparable role. Independent contractors and consultants who have not completed or passed the background check procedures specified in the CP/CPS section 5.3 are permitted access to secure facilities only to the extent they are escorted and directly supervised by Trusted Persons at all times.

5.3.8 Documentation supplied to personnel

Employees are provided the requisite training and other documentation needed to perform their job responsibilities competently and satisfactorily.

5.4 Audit logging procedures

5.4.1 Types of events recorded

Specific auditing events related to CA key life cycle management events, including:

- Key generation, cloning, storage, recovery, archival, and destruction
- Exporting of public key components

CA signing and key management events, including:

- Receipt and validation of Certificate Signing Requests
- Key activation
- Successful or unsuccessful processing of certificate signing requests

Security-related events, including:

- Assignment and revocation of credentials
- Successful and unsuccessful system access attempts
- Key and security system actions performed by trusted personnel
- Security sensitive files or records read, written or deleted
- Security profile changes
- System crashes, hardware failures and other anomalies
- Facility visitor entry and exit
- System changes and maintenance updates
- Incident response handling

Log entries include the following elements:

- Date and time of the entry
- Identity of the entity making the journal entry
- Type of entry
- Other events as appropriate

5.4.2 Frequency of processing log

Audit logs are examined after each key ceremony for significant security and operational events. In addition, audit logs are reviewed for suspicious or unusual activity in response to alerts generated based on irregularities and incidents within the CA systems. Audit log processing consists of a review of the audit logs and documentation for all significant events in an audit log summary. Audit log reviews include a verification that the log has not been tampered with and an investigation of any alerts or irregularities in the logs. Actions taken based on audit log reviews are also documented.

5.4.3 Retention period for audit log

All audit data collected in terms of section 5.4.1 is retained on-site for at least one year after creation and then archived for at least 10 years after its initial creation.

The media holding the audit data and the applications required to process the information are maintained to ensure that the archived data can be accessed for the time period set forth in this CP/CPS.

5.4.4 Protection of audit log

Audit logs are kept off-line and protected with an audit log handling procedure that includes mechanisms to protect the log files from unauthorized viewing, modification, deletion, or other tampering.

Only authorized Trusted Persons are able to obtain direct access to the audit information.

5.4.5 Audit log backup procedures

Electronic archives of the audit information are backed up and stored at an off-site secure facility after each key ceremony. Copies of paper-based records are also stored off-site and are maintained in the same manner.

5.4.6 Audit collection system (internal vs. external)

Automated audit data is generated and recorded at the application and operating system level. Manually generated audit data is recorded by the Ceremony Administrator on paper.

After each completed Key Ceremony, the audit log information is collected by the Ceremony Administrator at the generating host and copied onto at least two portable media. Electronic copies of paper-based documents are also made.

5.4.7 Notification to event-causing subject

No notice is required to be given to the individual, organization, device, or application causing a log event.

5.4.8 Vulnerability assessments

Events in the audit process are logged, in part, to monitor system vulnerabilities. Vulnerability assessments are performed manually as part of the audit log review process after each key ceremony.

Contacts are maintained with relevant parties within the security community to share the latest security-related information which may affect the PKI operations. Continuous vulnerability assessments are made based on this information.

5.5 Records archival

Archive records are retained as per section 5.4.3.

5.6 Key changeover

Certificate Authorities will stop issuing certificates as the operational period of its respective key pair expires in accordance with 6.3.2. The key changeover of a root CA will be managed such that it will allow significant time overlap between the old key and a new key, to enable a seamless roll-over for any relying parties. Entities affected by a key changeover will be notified prior to the event.

5.7 Compromise and disaster recovery

5.7.1 Incident and compromise handling procedures

If an event is detected that has led to, or could have led to a security compromise of any of the systems security mechanisms, an investigation will be performed in order to determine the source and nature of the incident. If the incident is suspected to have compromised the private component of an active CA key, the emergency roll-over procedures will be enacted as described in section 5.7.3.

Otherwise, the scope, severity and damage of the incident will be assessed and a plan to remedy the effect will be developed and implemented. The plan will also include measures to prevent the event from reoccurring.

The incident handling procedures include reporting of all events to the Policy Management Authority (PMA).

5.7.2 Computing resources, software, and/or data are corrupted

In the event of the corruption of computing resources, software, and/or data, this occurrence will cause the incident handling procedures to be enacted. Such procedures require appropriate escalation, incident investigation, and incident response. If necessary, the key compromise or disaster recovery procedures will be enacted, as described in section 5.7.3 and 5.7.4.

5.7.3 Entity private key compromise procedures

Emergency key roll-over procedures have been established to ensure readiness for key compromise situations. Upon the suspected or known compromise of a CA private key, ICANN will:

- Assess the situation and cease using the compromised materials

- Notify stakeholders of any emergency as soon as possible using the channels stipulated in Section 2.1
- Develop an action or implementation plan with approval from the PMA
- Revoke all Certificates signed with the compromised Key
- New certificates will be re-issued to all Entity CAs in accordance with Section 4.3

ICANN will also investigate and report to the PMA what caused the compromise or loss, and what measures have been taken to preclude recurrence.

5.7.4 Business continuity capabilities after a disaster

A business continuity and IT disaster recovery plan has been developed, implemented and tested. The plan has been designed to mitigate the effects of natural, man-made, or technological disasters or other disasters that require temporary or permanent cessation of CA operations. The business continuity and IT disaster recovery plans are in place to address the restoration of information systems services and key business functions. These plans address:

- Roles and responsibilities in the event of a disaster
- Fallback procedures for restoring business-critical processes within acceptable times
- Resumption procedures for restoring normal operations
- The criteria for activating the plan

Capabilities are maintained to restore or recover essential operations within 96 hours following a disaster with support for at minimum the following functions:

- Communication with the stake holders
- Generation and publication of CA keys
- Signing and publication of Certificate Revocation Lists (CRLs)
- Ability to process Certificate Signing Requests

The business continuity and IT disaster recovery plans have been designed to provide full recovery within one week at any backup site following an incident or disaster occurring at the primary site. These plans are regularly tested, validated, and updated to be operational in the event of any incident or disaster. Results of such tests are reviewed and kept for audit and planning purposes.

5.8 CA or RA termination

A CA operations termination plan has been developed, in the event that the roles and responsibilities of the CA operator must transition to other entities or cease. A transition will be coordinated with the receiving operator to execute any transition in a secure and transparent manner.

6 TECHNICAL SECURITY CONTROLS

6.1 Key pair generation and installation

6.1.1 Key pair generation

All CA keying materials are generated in pre-planned key generation ceremonies in accordance with the requirements of the CP/CPS. The activities performed in each key generation ceremony are recorded, dated, and signed by the Ceremony Administrator. These records are kept for audit and tracking purposes as required in section 5.4.3.

6.1.2 Private key delivery to subscriber

Private keys are generated by the subscriber.

6.1.3 Public key delivery to certificate issuer

Public keys are provided to the certificate issuer in PKCS#10-formatted Certificate Signing Requests.

6.1.4 CA public key delivery to relying parties

The public component of a CA key pair will be distributed in a secure fashion to preclude substitution attacks.

Acceptable methods for delivery and validation of CA certificates include, but are not limited to:

- Publication of CA certificates in the repository
- Proof distributed via separate channels to vendors for inclusion of CA certificates into vendors' products

6.1.5 Key sizes

Key pairs are required to be of sufficient length to prevent others from determining the key pair's private component using crypto-analysis or brute force during the period of expected utilization of such key pairs.

The Root CA and all intermediate CAs’ key pairs are RSA keys with a modulus size of 2048, or 4096 bits.

6.1.6 Public key parameters generation and quality checking

For all RSA keys, key generation and validation shall be performed in accordance with the requirements of FIPS 186-5.

Quality checking will also include validating the size of the public exponent to be both resource efficient and secure.

6.1.7 Key usage purposes (as per X.509 v3 key usage field)

CA	X509v3 Key Usage
ICANN Root CA	*Digital Signature, Non Repudiation, Key Encipherment, Data Encipherment, Key Agreement, Certificate Sign, CRL Sign*

6.2 Private Key Protection and Cryptographic Module Engineering Controls

All cryptographic functions involving the private component of a CA certificate are performed within the HSM; that is, the private component will not be exported from the HSM except in encrypted form for purposes of key distribution and backup.

6.2.1 Cryptographic module standards and controls

CA private keys are stored in a Hardware Security Module (HSM) certified at a minimum of FIPS 140-2 or FIPS 140-3 level 3 or higher.

6.2.2 Private key (n out of m) multi-person control

Technical and procedural mechanisms have been implemented that require the participation of multiple trusted individuals to perform sensitive cryptographic operations. Access to Private Keys requires N out of M trusted individuals. No single person has all the activation data needed for accessing any of the CA Private Keys.

6.2.3 Private key escrow

Private keys are not escrowed.

6.2.4 Private key backup

Backups of the CA Private Key are maintained in a physically secure location, and are never stored unencrypted outside of the Hardware Security Module (HSM). When keys are transferred to other media for backup and disaster recovery purposes, the keys are transferred and stored in an encrypted form. Backed up keys are never stored in a plain text form outside of the cryptographic module.

6.2.5 Private key archival

Private keying materials are not archived after its operational time period has expired.

6.2.6 Private key transfer into or from a cryptographic module

CA key pairs are generated on the hardware security modules in which the keys will be used. In addition, the contents of the HSM is distributed to a set of spare HSMs for routine recovery and disaster recovery purposes. When key pairs are distributed to another hardware security module, these key pairs are transported between modules in encrypted form.

6.2.7 Private key storage on cryptographic module

Private CA keys are stored within a Hardware Security Module (HSM) that is tamper resistant and certified at a minimum level of FIPS 140-2 or FIPS 140-3 level 3 or higher. The only operation which extracts private keying material is the distribution between HSMs as described in 6.2.4 and 6.2.6.

6.2.8 Method of activating private key

The CA private key will be activated using three out of seven Crypto Officer controlled hardware credentials. These credentials are used in accordance with the manufacturer's documentation.

6.2.9 Method of deactivating private key

The CA private keys may be deactivated via offline procedure on the applicable HSM using three out of seven crypto officer controlled hardware credentials.

Alternatively, the CA private keys may be deactivated upon system shutdown.

6.2.10 Method of destroying private key

As required, any CA private keys are destroyed in a manner that reasonably ensures that there are no residual remains of the keys that could lead to the reconstruction of the keys.

If a functional HSM is being decommissioned, the HSMs zeroization function and the vendor-provided declassification procedure of the HSMs are used to ensure complete destruction of any private and secret keys, configuration and log information.

If a non-functional HSM is decommissioned, a physical destruction and recycling procedure will be followed to ensure there are no remains of private and secret keys, configuration or log information.

If a private key shall be removed from a HSM which is not being decommissioned, the private key will be destroyed using the HSM's delete command.

When performed, private key destruction activities are logged as part of a key ceremony.

6.2.11 Cryptographic Module Rating

As per section 6.2.1.

6.2.12 Applicability of CA Key Controls to End-Entity Certificates

The private key associated with the end-entity certificate used to sign the DNS Root Trust Anchors file resides within the same Hardware Security Module (HSM) as the Root CA private keys. As such, all technical, procedural, and operational controls applicable to the CA private keys, including those defined in sections 6.2.1 through 6.2.11, also apply to the end-entity certificate's private key.

This includes, but is not limited to:

- Storage within a FIPS 140-2 or FIPS 140-3 Level 3 or higher certified HSM
- Multi-person (n out of m) control for key access and activation
- Key backup, transfer, and destruction procedures
- Use of key ceremonies for all operations involving access to the private key
- Access control mechanisms
- Activation data generation and handling

No operations involving the end-entity private key are performed outside of the secure and audited HSM environment. All signatures made using this private key are conducted under the same ceremony-based process required for Root CA key operations.

6.3 Other aspects of key pair management

6.3.1 Public key archival

Public CA keys and CA certificates will be retained in accordance with section 5.4.3 for at least 10 years after their operational periods have expired.

6.3.2 Certificate operational periods and key pair usage periods

Root CA certificates will have a validity period of 20 years. The operational period for the Root CA key pair will expire 15 years after generation. After the operational period, the private component of the key pair will only be used for signing revocation lists.

End-entity certificates will have a maximum validity time of 20 years, but in no case shall their validity extend beyond the expiration date of the issuing CA certificate.

6.4 Activation data

6.4.1 Activation data generation and installation

Activation data for protection of CA private keys contained within the hardware security modules (HSM) is generated by the HSM in the initialization phase, where it is split and stored on hardware credentials in accordance with the requirements of section 6.2.2.

6.4.2 Activation data protection

Crypto Officers credentials needed to access activation data are protected from unauthorized disclosure via physical access control mechanisms.

6.4.3 Other aspects of activation data

When required, hardware credentials containing activation data will be decommissioned using methods that protect against the compromise of the activation data and unauthorized use of any of the private keys protected by the activation data.

6.5 Computer security controls

6.5.1 Specific computer security technical requirements

Procedures have been established to ensure that the systems maintaining CA software components and data are trustworthy and secure from unauthorized access.

6.5.2 Computer security rating

No stipulation.

6.6 Life cycle technical controls

6.6.1 System development controls

PKI Software is developed in-house or by consultants using standard software development methodologies. Hardware is procured through a managed process leveraging industry standard vendors. Quality assurance is maintained throughout the process through a series of testing and management approvals prior to implementation.

6.6.2 Security management controls

An Information Security Management System (ISMS) has been implemented, based on the principles of ISO/IEC 27001. Fundamental to the information security and risk management process is the monitoring, analyzing and improving of the ISMS, which is scoped to include CA operations.

6.6.3 Life cycle security controls

The CA system is designed to require a minimum of maintenance. Updates critical to the security and operations of the CA system will be applied after formal testing and approval.

Critical hardware components of the CA system will be procured directly from the manufacturer and transported in tamper-evident bags to their destination in the KMF. Any hardware will be decommissioned well before the specified maximum life expectancy.

6.7 Network security controls

No parts of the CA systems making use of the HSMs are connected to any communications network. Required materials are transferred manually using portable media and physically brought into the Key Management Facility.

The production networks supporting the CA operations are logically segregated into separate security zones using firewalls, which limits the nature and source of network activities to pre-defined application processes.

6.8 Time-stamping

Time will be derived through a manual procedure before each key ceremony. The ceremony administrator will manually set the signer system clock and the wall clock to current UTC time drawn from a reliable time source.

Time derived from the procedure will be used for timestamping of:

- electronic and paper based audit log records
- certificate expiration and inception times

Asserted times are required to be accurate within three minutes.

Other components supporting CA operations which are connected to communications networks are required to be synchronized to a reliable time source and continuously monitored for potential time skew.

7 CERTIFICATE, CRL, AND OCSP PROFILES

7.1 Certificate profile

Certificates conform with RFC 5280, Internet X.509 Public Key Infrastructure Certificate and CRL Profile. Certificate extensions and their criticality, as well as cryptographic algorithm object identifiers, are populated according to the IETF RFC 5280 standards.

Issuing CA Certificate profile:

Field	Value
Version	*3*
Serial Number	*Unique number*
Signature Algorithm	*sha256WithRSAEncryption, or sha512WithRSAEncryption*
Issuer	*C=US, O=ICANN, and a meaningful CN*
Not Before	*Date by which the CA certificate is valid*
Not After	*Date by which the CA certificate expires*
Subject	*CA Distinguished Name (DN)*
Public Key	*CA's Public Key (RSA 2048, or 4096)*
Certificate Policy (optional)	*1.3.6.1.4.1.42139.1.1*
CRL Distribution Points (optional)	*https://data.iana.org/root-anchors/*
Basic Constraints	*CA True (critical)*
Key Usage	*Digital Signature, Non Repudiation, Key Encipherment, Data Encipherment, Key Agreement, Certificate Sign, CRL Sign (critical)*

End-entity Certificate profile:

Field	Value
Version	*3*
Serial Number	*Unique number per Issuing CA*
Signature Algorithm	*sha256WithRSAEncryption, or sha512WithRSAEncryption*
Issuer	*CA Distinguished Name (DN)*
Not Before	*Date by which the certificate is valid*
Not After	*Date by which the certificate expires*
Subject	*C=US, OU=ICANN, and a meaningful CN and email*

Public Key	*Subjects Public Key (RSA 2048, or 4096)*
Certificate Policy (optional)	*1.3.6.1.4.1.42139.1.1*
CRL Distribution Points (optional)	https://data.iana.org/root-anchors/
Basic Constraints	*CA False*
Key Usage	*Digital Signature, Key Encipherment (critical)*
Extended Key Usage	*E-mail Protection (critical)*

7.2 CRL profile

Field	Value
Version	*2*
Signature Algorithm	*sha256WithRSAEncryption, or sha512WithRSAEncryption*
Issuer	*CA Distinguished Name (DN)*
Effective Date	*Date by which the CRL is effective*
Next Update	*Date by which next CRL will be issued*
Revoked Certificates	*Listing of revoked certificates*

7.3 OCSP profile

No OCSP service is provided for the ICANN CA.

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1 Frequency or circumstances of assessment

No stipulation.

8.2 Identity/qualifications of assessor

No stipulation.

8.3 Assessor's relationship to assessed entity

No stipulation.

8.4 Topics covered by assessment

The scope of the compliance audit includes all PKI-related security controls, such as key management, infrastructure and administrative controls, CA certificate life cycle management, and practice disclosures.

8.5 Actions taken as a result of deficiency

With respect to compliance audits of the CA operations, significant exceptions or deficiencies identified during the compliance audit will result in a determination of actions to be taken by the PMA.

8.6 Communication of results

No stipulation.

8.7 Self-Audits

Although no formal audit schedule is stipulated, the CA operations are subject to periodic internal reviews to ensure adherence to the CP/CPS and associated security policies. Key aspects monitored include:

- Enforcement of key management and hardware security controls
- Verification of operational procedures for certificate management
- Validation of access controls and multi-person activation requirements
- Regular review of hardware security modules and physical security measures

Significant non-compliance or deficiencies identified during reviews will prompt corrective actions coordinated by the PMA to maintain the integrity and trustworthiness of the CA.

9 OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

No stipulation.

9.2 Financial Responsibility

No stipulation.

9.3 Confidentiality of Business Information

No stipulation.

9.4 Privacy of Personal Information

No stipulation.

9.5 Intellectual Property Rights

No stipulation.

9.6 Representations and Warranties

No stipulation.

9.7 Disclaimers of Warranties

No stipulation.

9.8 Limitations of Liability

No stipulation.

9.9 Indemnities

No stipulation.

9.10 Term and Termination

No stipulation.

9.11 Individual Notices and Communications

No stipulation.

9.12 Amendments

No stipulation.

9.13 Dispute Resolution

No stipulation.

9.14 Governing Law

No stipulation.

9.15 Compliance with Applicable Law

No stipulation.

9.16 Miscellaneous Provisions

No stipulation.

9.17 Other Provisions

No stipulation.