Certificate Policy (CP)

Notarize, Inc. (Proof.com)
Effective Date: 15-July-2025
Document Version: V.1.2

Table of Contents

1. INTRODUCTION

1.1. Overview

1.1.1. Certificate Policy

This Certificate Policy (CP) defines the procedural and operations requirements for the Proof public key infrastructure (PKI) system. In addition, this CP applies to all PKI Participants that request, issue, manage, and validate digital certificates and time stamp tokens (TSTs) from this Proof PKI system.

This CP is consistent with the Internet Engineering Task Force (IETF) Request for Comments (RFC) 3647: Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework (RFC 3647) standard. In accordance with this standard, this CP is organized into sections to cover security requirements and practices. Proof also uses “Not Applicable” or “No Stipulation” terms for sections that do not apply to this Proof PKI system.

Moreover, this CP addresses requirements from the current versions of the following policies, guidelines, and practices:

- WebTrust Principles and Criteria for Certification Authorities
- WebTrust Principles and Criteria for Certification Authorities - Network Security
- Certificate Authority/Browser Forum Baseline Requirements for Issuance and Management of Publicly-Trusted TLS Server Certificates
- Certificate Authority/Browser Forum Network and Certificate System Security Requirements
- Adobe Approved Trust List Technical Requirements
- Coalition for Content Provenance and Authenticity Technical Specification

Proof continuously tracks changes to the above policies, guidelines, and practices and updates this CP accordingly. In addition, Proof produces other documents about this Proof PKI system including, but not limited to, the Certification Practices Statement (CPS), privacy policies, and standard operating procedures (SOPs).

This CP does not apply to the PKI Participants involved with other Proof PKI systems that are considered private. Proof has defined different CPs and PKI-related documents for those Proof PKI systems.

The Proof Root CA R1 conforms to the current version of CA/B Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates published at https://www.cabforum.org. In the event of any inconsistency between this document and those Requirements, those Requirements take precedence over this document.

1.1.2. Digital Certificates

The Proof PKI system issues digital certificates to individuals as a means to assert their digital identity in electronic transactions (*e.g.*, digitally signing documents). Proof registers individuals in this Proof PKI system. Once registered, Proof performs identity verification of the individuals. Next, Proof creates certificate requests and issues individual certificates. When the individual certificates are about to expire, Proof issues new individual certificates. Further, Proof allows individuals to revoke their individual certificates due to errors; changes to their identity data (*e.g.*, last name changed due to marriage or divorce); or no longer required.

Moreover, the Proof PKI system issues certificates to legal entities as a way to assert their digital identity in electronic transactions (*e.g.*, digitally sealing documents). Proof requires registered and vetted individuals to request organizational certificates.

Proof issues individual and organizational certificates in compliance with the IETF RFC 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List Profile (RFC 5280) standard to cryptographically bind data from Subscribers with public keys from asymmetric key pairs.

1.1.3. Validation Services

The Proof PKI system offers a couple of validation methods to Relying Parties to find the current status (*e.g.*, good, revoked, etc.) of CA, individual, and organizational certificates. The first validation method, online certificate status protocol (OCSP), provides OCSP responses with the current status to OCSP requests sent by the Relying Parties. The second validation method, certificate revocation lists (CRLs), are files that contain serial numbers of all revoked CA, individual, and organizational certificates which have not expired yet.

1.1.4. System Availability

The Proof PKI system and repositories shall be maintained with resources to have commercially reasonable availability for access at all times.

1.2. Document Name And Identification

1.2.1. Certificate Policy Name

The official document name shall be the Proof Certificate Policy. The PMA shall approve all changes to this CP and shall maintain the following version control in Appendix C | Change History.

1.2.2. Proof Object Identifiers

Proof shall register the following Object Identifier (OID) arc, joint-ISO-CCIT (2) country (16) USA (840) US-company (1) Proof (63693), with the Internet Assigned Numbering Authority (IANA):

OID	Description
2.16.840.1.63693	Proof Assigned OID Arc
2.16.840.1.63693.1	Security
2.16.840.1.63693.1.1	PKI
2.16.840.1.63693.1.1.1	Proof Certificate Policy
2.16.840.1.63693.1.1.1.1	Identity Validated
2.16.840.1.63693.1.1.1.2	Organization Validated

Additionally, Proof shall assert the appropriate OIDs in the Certificate Policy extension of the CA, individual, and organizational certificates issued from this Proof PKI system.

1.3. PKI Participants

1.3.1. Policy Management Authority

Proof shall establish a Policy Management Authority (PMA) to govern the Proof PKI system that includes the Root, Intermediate, and Issuing CAs. The PMA shall have the following responsibilities:

- Represent the interests of Proof
- Draft and update this CP in accordance with applicable laws, regulations, policies, guidelines, and requirements
- Approve a CPS and related policies
- Supervise the conformance of the Proof PKI with this CP and CPS

The Proof policies shall be designed to ensure the Proof PKI system complies, in all material respects, with applicable United States (US) laws and regulations for electronic signatures; international standards; and program requirements such as WebTrust CA and and Network Security Requirements; Certificate Authority/Brower Forum (CA/B) TLS Baseline and Network Security Requirements; Coalition for Content Provenance and Authenticity (C2PA) Technical Specification; and Adobe Approved Trust List (ATL) Technical Requirements.

1.3.2. Certification Authority

Proof shall be the Certification Authority (CA) for this Proof PKI system. The CA shall have the following responsibilities:

- Create Root, Intermediate, and Issuing CA certificates in the CA systems
- Issue individual and organizational certificates in a timely manner from the CA systems
- Manage CA, organizational, and individual certificates which may involve rekeys, renewals, and revocations in the CA systems

- Operate Validation Authority (VA) systems that provide status (*e.g.*, valid, revoked, etc.) of CA, individual, and organizational certificates to Relying Parties via CRL or OCSP methods
- Publish CA certificates, CRLs, and PKI documents (*e.g.*, CP, RPA, etc.) on publicly-available web sites

1.3.3. Registration Authorities

Proof shall be the Registration Authority (RA) for this Proof PKI system. The RA shall have the following responsibilities:

- Confirm qualification requirements defined in CP Section 5.3.1
- Retain documentation in accordance with CP Section 5.3.2
- Authenticates Subscribers to RA system
- Approve certificate and revocation requests submitted by Subscribers in RA system
- Notify Subscribers about imminent expiry of individual or organizational certificates

The RA may delegate some or all of the responsibilities to Delegated Third Parties except for CP Sections 3.2.2.4 and 3.2.2.5. In this case, the Delegated Third Party shall produce and submit a Registration Practice Statement (RPS) that documents procedures to meet the delegated responsibilities. Once submitted, Proof shall review and approve the RPS. Further, Proof shall require the Delegated Third Party to obtain and maintain a WebTrust for RA audit annually.

1.3.4. Subscribers

Subscribers shall be any natural persons that receive individual certificates from the Proof PKI system and are legally bound by the applicable terms and conditions.

Note: Before completing identity verification and certificate issuance processes, the Subscribers are known as Applicants. After the certificates are issued, the Applicants become Subscribers.

1.3.5. Sponsors

Sponsors shall be any representatives of legal entities that receive organizational certificates from the Proof PKI system and are legally bound by the applicable terms and conditions.

Note: Before completing identity verification and certificate issuance processes, the Sponsors are known as Applicants. After the certificates are issued, the Applicants become Sponsors.

1.3.6. Relying Parties

Relying Parties may be any natural persons or legal entities that rely on individual or organizational certificates issued by this Proof PKI system. Further, Relying Parties may be any natural persons or legal entities that rely on digital signatures based on digital certificates or TSTs issued by the Proof PKI system.

Relying Parties may check the status of CA, individual, and organizational certificates via the CRL or OCSP methods.

1.3.7. Application Software Suppliers

Application Software Suppliers may include software or software-as-a-server (SaaS) vendors (*e.g.*, Adobe Acrobat, Mozilla, etc.) that trust CA, individual, and organizational certificates issued by the CA.

1.3.8. Other Participants

No stipulations.

1.4. Certificate Usage

1.4.1. Appropriate Certificate Uses

Digital certificates issued under this CP shall only be used as designated by the selected values in the Key Usage and Extended Key Usage extensions.

The Relying Parties should evaluate the associated risks of their environments and decide whether to accept digital certificates issued under this CP.

1.4.2. Prohibited Certificate Uses

Digital certificates issued under this CP shall not be used for any other purposes other than the selected values in the Key Usage and Extended Key Usage extensions.

1.5. Policy Administration

1.5.1. Organization Administering the Document

This CP and relevant documents referenced herein shall be approved and maintained by the PMA.

1.5.2. Contact Person

Any questions about this CPS shall be addressed by the PMA which may be reached at either pma@proof.com or mailed to the following address:

Notarize Inc. (*d.b.a.* Proof.com)
ATTN: Proof PMA
867 Boylston St.
Boston, MA 02116

Note: See CP Section 4.9.3.4 for instructions on how to submit Certificate Problem Reports.

1.5.3. Person Determining CPS Suitability for the Policy

The PMA shall determine the suitability and applicability of this CP. Moreover, the PMA shall ensure the conformance of the CPS to this CP. Also, the PMA shall evaluate and act on audit results by an independent auditor as specified in CP Section 8.0.

1.5.4. CP Approval Procedures

The PMA shall approve the CP and any amendments. Amendments shall be made by either updating the entire CP or by publishing an addendum. The PMA shall also decide whether a CP amendment requires notice or an OID change as defined in CP Sections 9.10 and 9.12.

1.6. Definitions and Acronyms

See Appendix A | Definitions and Appendix B | Acronyms and Abbreviations.

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1. Repositories

The CA shall maintain repositories that allow public access to Proof policies, agreements, CA certificates, and revocation data.

While the publicly available CA certificates and revocation data shall be available in a security repository, the Proof policies and agreements shall be accessible in the legal repository located at:

- **Security Repository:** https://crl.proof.com, https://ocsp.proof.com
- **Legal Repository:** https://www.proof.com/legal/general-terms

The repositories shall be maintained with resources to ensure commercially-reasonable availability for access at all times.

2.2. Publication Of Certification Information

The CA shall publish the following information in publicly-available repositories:

- Public CA certificates including Root, Intermediate, and Issuing CAs
- CRLs with revocation data about public CA, individual, and organizational certificates
- PKI documents including CP, RPA, and applicable terms and conditions

Further, the CA shall include valid uniform resource identifiers (URIs) as distribution points for the above information in CA, individual, and organizational certificates. Relying Parties may use the URIs to access this information.

2.3. Time Or Frequency Of Publication

The CA shall publish new versions of Proof policies and agreements in the legal repository within seven (7) days of approval. Further, the CA shall update the public CA certificates as soon as possible after issuance in the security repository and before distribution to trusted root programs (*e.g.*, Adobe ATL, C2PA, etc.)

Moreover, the CA shall update the CRLs in the repositories for public Root and Intermediate CAs at least annually or upon revocation of an Intermediate or Issuing CA. The CA shall publish new CRLs for Issuing CAs at least every seven (7) days.

Note: The CA shall remove expired CA, individual, and organizational certificates from CRLs.

2.4. Access Controls On Repositories

The CA shall configure all repositories to be publicly-available with unrestricted read access. Also, the CA shall implement security controls to ensure the integrity and availability of all repositories including, but not limited to, preventing unauthorized write access and protecting against distributed denial of service attacks (DDoS).

3. IDENTIFICATION AND AUTHENTICATION

3.1. Naming

3.1.1. Types Of Names

The CA shall have non-null values for the Common Name (CN) attribute within the Subject and Issuer Distinguished Name (DN) extensions of CA, individual, and organizational certificates. While the CA may include additional attributes (*e.g.*, Country, Organization, etc.) in DN extensions. the CA shall verify all values for attributes in DN extensions. All attributes shall be in compliance with the International Telecommunication Union (ITU) X.500: Open Systems Interconnection (ITU X.500) standard.

3.1.2. Need For Names To Be Meaningful

The CA shall verify and include meaningful representation of names for natural persons or legal entities in the CN or Organization (O) attributes of Subject and Issuer DN extensions of CA, individual, and organizational certificates.

3.1.3. Anonymity Or Pseudonymity Of Subscribers

The CA may use pseudonyms for legal entities that have “doing business as” (*d.b.a.*) names in the CN or O attributes of Subject DN extension of CA, individual, and organizational certificates.

3.1.4. Rules For Interpreting Various Name Forms

The DN shall be interpreted based on the ITU X.500, Abstract Syntax Notation One (ASN.1), and IETF RFC 822: Standard for the Format of ARPA Internet Text Messages (RFC 822) standards.

3.1.5. Uniqueness Of Names

The CA shall ensure name uniqueness based on a combination of attributes in the Subject DN extension of CA, individual, and organizational certificates.

Note: Name uniqueness is not violated when there are multiple certificates issued to the same natural person or organization.

3.1.6. Recognition, Authentication, And Role Of Trademarks

The CA shall verify the right of legal entities to use trade names, trademarks, service names, and *d.b.a.* names submitted by Applicants in the certificate requests.

Note: The CA may revoke any CA, individual, and organizational certificate that was issued based on information deemed to violate CP Section 3.16. As part of the certificate request process, Applicants agree that their certificate request does not contain any information that infringes or

interferes upon the rights of any third parties in any jurisdiction with regards to trade names, trademarks, service names, *d.b.a.* names, or any other intellectual property rights.

3.2. Initial Identity Validation

3.2.1. Method To Prove Possession Of Private Key

The CA shall generate and store the private keys for CA certificates on hardware security modules (HSMs) rated at FIPS 140-2 Level 3. Since the CA has possession of the private keys, the CA shall not perform any proof-of-possession.

Also, the CA shall require Subscribers or Sponsors to generate and store the private keys for individual or organizational certificates on HSMs rated at least FIPS 140-2 Level 2. If the Subscribers or Sponsors generate their own private keys, the CA shall verify proof-of-possession by checking the digital signatures on certificate signing requests (CSRs) submitted by Subscribers and Sponsors. If the CA creates and stores the private keys on behalf of Subscribers and Sponsors in their HSMs, the CA shall not perform any proof- of-possession because the CA has possession of the private keys.

3.2.2. Authentication Of Organization Identity

The CA shall verify all legal entity information for O and CN attributes in the Subject DN extension of CA certificates against Reliable Data Sources (*e.g.*, Secretary of State offices, business-to-business contact services, etc.). The PMA shall authorize the Reliable Data Sources.

If the CA includes legal entity information for CN or O attributes in the Subject DN extension of individual certificates, the CA shall verify this information against the Reliable Data Sources .

3.2.3. Authentication Of Individual Identity

The CA shall verify the personally identifiable information (PII) of Proof personnel as specified in the associated CPS which submit CA Naming Forms to create Proof CAs.

The RA shall verify the PII of Subscribers or Sponsors requesting individual or organizational certificates as specified in the associated CPS. The Subscribers shall include any natural persons for individual certificates and Sponsors for organization certificates.

The RA shall validate the PII of Subscribers or Sponsors in accordance with the associated CPS.

The PMA may authorize Delegated Third Parties to perform identity verification responsibilities.

3.2.4. Non-Verified Subscriber Information

The RA shall only utilize verified PII for the C, O, and E attributes in the Subject DN extension of individual or organizational certificates in the production environment. However, RA may use non-verified PII for these attributes in the non-production environments (*e.g.*, development, test, etc.).

3.2.5. Validation Of Authority

The RA shall contact executives at legal entities to validate Sponsors are authorized to request organizational certificates on behalf of the legal entities.

If the RA includes legal entity names for the O attribute in the Subject DN extension of individual certificates, the RA shall maintain a list of approvers for the legal entities authorized to approve natural persons requesting individual certificates.

3.2.6. Criteria For Interoperation

No stipulations.

3.3. Identification And Authentication For Rekey Requests

The CA shall require the PMA to approve CA Revocation Forms to revoke existing CAs and CA Naming Forms to create new CA certificates.

The RA shall provide Subscribers or Sponsors with one of the following rekey options before expiration or revocation of the individual or organizational certificates:

- Submit rekey requests to retain the same values for all attributes in the Subject DN extension of individual or organizational certificates
- Revoke existing and submit certificate requests for individual and organizational certificates

If the Subscribers or Sponsors need to rekey individual or organizational certificates after expiration or revocation, the RA shall require Subscribers or Sponsors to login, with multifactor authentication, to the RA system in order to submit certificate requests for new individual or organizational certificates.

3.3.1. Identification And Authentication For Routine Rekey

The RA shall require Subscribers or Sponsors to login with multifactor authentication to the RA system in order to submit revocation requests to revoke existing individual or organizational certificates and certificate requests to issue new individual or organizational certificates.

3.3.2. Identification And Authentication For Rekey after Revocation

The RA shall require Subscribers or Sponsors to login with multifactor authentication to the RA system in order to submit certificate requests for new individual or organizational certificates.

3.4. Identification And Authentication For Revocation Requests

The CA shall require the PMA to approve CA Revocation Forms to revoke CA certificates.

The RA shall require Subscribers or Sponsors to login with multifactor authentication to the RA system to submit revocation requests for their unexpired individual or organizational certificates.

If the CA receives revocation requests from other parties (*e.g.*, certificate problem reports, Relying Parties, etc.), the CA shall investigate these requests. If there is just cause to revoke the individual or organizational certificates, the CA shall submit and approve the revocation requests in the RA system.

4. CERTIFICATE LIFE CYCLE OPERATIONAL REQUIREMENTS

4.1. Certificate Application

4.1.1. Who May Submit A Certificate Application

The Applicants shall meet one of the following requirements to submit certificate requests:

- Any individual who is the subject of the individual digital certificate
- Any authorized representative of a legal entity for organizational certificates
- Any authorized personnel for CA certificates
- Any authorized representative of the RA

The RA shall ensure Applicants are not included on denied persons or business lists maintained by the US Federal government. Further, the RA shall ensure the natural persons or legal entities are not located in a sanctioned country under US Federal laws and regulations.

4.1.2. Enrollment Process And Responsibilities

The CA shall ensure the RA verifies the PII and legal entity information in accordance with this CP and associated CPS and RPS (if applicable) before issuing CA, individual, and organizational certificates.

The RA shall require the Applicants to provide sufficient PII, legal entity information, and documentation for the RA to perform the required verification.

4.2. Certificate Application Processing

4.2.1. Performing Identification And Authentication Functions

The CA or RA shall identify and verify the Applicants in accordance with this CP and associated CPS and RPS (if applicable). Moreover, the CA or RA may use previously collected and verified PII and legal entity information up to 398 days to issue CA, individual, and organizational certificates (*e.g.*, renewals, rekeys, etc.). Additionally, the CA or RA shall have and follow a High Risk Certificate Request procedure to address unique situations and ensure proper verifications.

4.2.2. Approval Or Rejection Of Certificate Applications

The CA or RA shall reject any certificate applications under the following conditions:

- Incomplete PII or legal entity information
- PII or legal entity information that cannot be verified

Additionally, the CA or RA may reject any certificate applications on a reasonable basis that includes, but is not limited to, one of the following conditions:

- Correlation with previously rejected certificate applications
- Correlation with previously revoked CA, individual, and organizational certificates

- Presence on denied persons or business lists
- Located in a sanctioned country under US laws and regulations

4.2.3. Time To Process Certificate Applications

The CA or RA shall process certificate applications in commercially reasonable timeframes, but the CA or RA shall not be responsible for delays caused by actions or inactions by Applicants in response to missing or incorrect PII or legal information. Also, the CA or RA shall not be responsible for events outside their control (*e.g.,* Applicant experiences issues with liveness check, legal entity executives do not respond to verification requests, etc.).

4.3. Certificate issuance

4.3.1. CA Actions During Certificate Issuance

The CA shall verify the authenticity of certificate requests before issuing any CA, individual, and organizational certificates.

Also, the CA shall require two (2) person control to issue direct commands to any offline CA certificates (e.g., Root, Intermediate, etc.) to create new Intermediate or Issuing CAs as well as generate CRLs

Further, the CA shall implement a linting process to check conformity of the to-be-signed individual or organizational certificates.

4.3.2. Notification To Subscriber By The CA of Issuance Of Certificate

The CA or RA shall notify the natural persons or legal entities about the issuance of CA, individual, and organizational certificates by a reliable method (*e.g.*, email, Slack message, etc.) within a reasonable timeframe.

4.4. Certificate Acceptance

4.4.1. Conduct Constituting Certificate Acceptance

The CA shall display a preview of individual or organizational certificates to Subscribers or Sponsors before issuing these certificates. The Subscribers or Sponsors shall accept the preview in order for the CA to issue these certificates.

Additionally, the CA shall consider CA certificates to be accepted if the Subscribers or Sponsors do not object within two (2) business days.

4.4.2. Publication Of The Certificate By The CA

The CA shall publish CA certificates in the security repository. However, the CA shall not publish individual or organizational certificates in a public repository.

4.4.3. Notification Of Certificate Issuance By The CA To Other Entities

The CA shall notify the trusted root programs about CA certificates to be included in trust lists. Also, the CA shall notify the RA about the issuance of individual or organizational certificates.

4.5. Key Pair and Certificate Usage

4.5.1. Subscriber Private Key And Certificate Usage

The CA shall require Subscribers or Sponsors to protect the private keys as specified in the applicable terms and conditions. If the CA stores key pairs on behalf of natural persons or legal entities, the CA shall generate, store, and protect the new key pairs. Moreover, the CA shall require Subscribers or Sponsors to use multifactor authentication to access and use these key pairs.

Also, the CA shall require Subscribers or Sponsors to use individual, and organizational certificates lawfully in accordance with the applicable terms and conditions.

4.5.2. Relying Party Public Key And Certificate Usage

The CA shall require Relying Parties to utilize CA, individual, and organizational certificates in accordance with the applicable terms and conditions in order to make any claims against the warranties.

In addition, the CA shall require Relying Parties to utilize software compliant with RFC 5280 and RFC 3161. Further, the Relying Parities shall be responsible for validating the status of CA, individual, and organizational certificates based on the CRLs and OCSP provided by the CA.

4.6. Certificate Renewal

4.6.1. Circumstance For Certificate Renewal

The CA may renew CA, individual, and organizational certificates by extending the value for the Not After attribute and issuing new certificates under the following conditions:

- The associated public keys have not exceeded the values in Not After attribute
- The associated private Keys have not been compromised.
- The certificates have not been revoked
- The PII or legal entity information for Subscribers or Sponsors remains valid and accurate
- If required, the PII or legal entity information for Subscribers or Sponsors is revalidated by the CA

The Subscribers or Sponsors should renew CA, individual, and organizational certificates before exceeding the values in the Not After attribute.

4.6.2. Who May Request Renewal

The CA shall require Subscribers or Sponsors to meet one of the following requirements to submit renewal requests:

- Any individual who is the subject of the individual digital certificate
- Any authorized representative of a legal entity for organizational certificates
- Any authorized personnel for CA certificates
- Any authorized representative of the RA

4.6.3. Processing Certificate Renewal Requests

The CA may require confirmation of previously verified PII and legal entity information for Subscribers or Sponsors to process renewal requests. Further, the CA may need to re-validate the PII and legal entity information for Subscribers or Sponsors after 398 days since the previous verification.

4.6.4. Notification Of Renewal Certificate Issuance To Subscriber

The CA or RA shall notify the natural persons or legal entities about the renewal of CA, individual, and organizational certificates by a reliable method (*e.g.*, email, Slack message, etc.) within a reasonable timeframe.

4.6.5. Conduct Constituting Acceptance Of A Renewal Certificate

The CA shall display a preview of individual or organizational certificates to Subscribers or Sponsors in the RA system before renewing the certificates. The Subscribers or Sponsors shall accept the preview in order for the CA to renew these certificates.

4.6.6. Publication Of The Renewal Certificate By The CA

The CA shall publish the renewed CA certificates in the security repository. However, the CA shall not publish renewed individual or organizational certificates in a public repository.

4.6.7. Notification Of Certificate Renewal By The CA To Other Entities

The CA shall notify the trusted root programs about the renewed CA certificates to update the trust lists. Also, the CA shall notify the RA about the renewal of individual or organizational certificates.

4.7. Certificate Rekey

4.7.1. Circumstance For Certificate Rekey

The CA may rekey CA, individual, and organizational certificates by using new key pairs and re-issuing these certificates under the following conditions:

- The associated public keys have not exceeded the values in Not After attribute
- The associated private Keys have not been compromised.
- The certificates have not been revoked
- The PII or legal entity information for Subscribers or Sponsors remains valid and accurate
- If required, the PII or legal entity information for Subscribers or Sponsors is revalidated by the CA

The Subscribers or Sponsors should rekey CA, individual, and organizational certificates before exceeding the values in the Not After attribute.

4.7.2. Who May Request Certification Of A New Public Key

The Subscribers or Sponsors shall meet one of the following requirements to submit rekey requests:

- Any individual who is the subject of the individual digital certificate
- Any authorized representative of a legal entity for organizational certificates
- Any authorized personnel for CA certificates
- Any authorized representative of the RA

4.7.3. Processing Certificate Rekeying Requests

The CA may require confirmation of previously verified PII and legal entity information for Subscribers or Sponsors to process rekey requests. Further, the CA may need to re-validate the PII and legal entity information for Subscribers or Sponsors after 398 days since the previous verification.

4.7.4. Notification Of New Certificate Issuance To Subscriber

The CA or RA shall notify the natural persons or legal entities about the rekey of CA, individual, and organizational certificates by any reliable method within a reasonable timeframe.

4.7.5. Conduct Constituting Acceptance of a Rekeyed Certificate

The CA shall display a preview of the individual or organizational certificates to Subscribers or Sponsors in the RA system before re-keying the certificates. The Subscribers or Sponsors shall accept the preview in order for the CA to rekey these certificates.

4.7.6. Publication Of The Rekeyed Certificate By The CA

The CA shall publish rekeyed CA certificates in the security repository. However, the CA shall not publish rekeyed individual or organizational certificates in a public repository.

4.7.7. Notification Of Certificate Issuance By The CA To Other Entities

The CA shall notify the trusted root programs about the rekeyed CA certificates to update the trust lists. Further, the CA shall notify the RA about the rekey of individual or organizational certificates.

4.8. Certificate Modification

4.8.1. Circumstance For Certificate Modification

The CA may modify CA, individual, and organizational certificates by updating attributes in these certificates, but using same key pairs and issue new certificates under the following conditions:

- The associated public keys have not exceeded the values in Not After attribute
- The associated private Keys have not been compromised.
- The certificates have not been revoked
- The PII or legal entity information for Subscribers or Sponsors remains valid and accurate
- If required, the PII or legal entity information for Subscribers or Sponsors is revalidated by the CA

The Subscribers or Sponsors should modify CA, individual, and organizational certificates before exceeding the values in the Not After attribute.

4.8.2. Who May Request Certificate Modification

The Subscribers or Sponsors shall meet one of the following requirements to submit modification requests:

- Any individual who is the subject of the individual digital certificate
- Any authorized representative of a legal entity for organizational certificates
- Any authorized personnel for CA certificates
- Any authorized representative of the RA

4.8.3. Processing Certificate Modification Requests

The CA may require confirmation of previously verified PII and legal entity information for Subscribers or Sponsors to process modification requests. Further, the CA may need to re-validate the PII and legal entity information for Subscribers or Sponsors after 398 days since the previous verification.

Additionally, the CA shall determine whether the CA, individual, or organizational certificates have been used to digitally sign objects (*e.g.*, PDF files, media content, etc.). If the certificates have digitally signed objects, the CA shall revoke the current and issue new CA, individual, or organizational certificates with new key pairs and modified certificate content. If the certificates have not digitally signed objects, the CA shall delete the current and issue new CA, individual, or organizational certificates with same key pairs and modified certificate content.

4.8.4. Notification Of Modified Certificate Issuance To Subscriber

The CA or RA shall notify the natural persons or legal entities about the modifications to CA, individual, and organizational certificates by any reliable method within a reasonable timeframe.

4.8.5. Conduct Constituting Acceptance Of Modified Certificate

The CA shall display a preview of individual or organizational certificates to Subscribers or Sponsors before modifying these certificates. The Subscribers or Sponsors shall accept the preview in order for the CA to rekey these certificates.

4.8.6. Publication Of The Modified Certificate By The CA

The CA shall publish the modified CA certificates in the security repository, but the CA shall not publish modified individual or organizational certificates.

4.8.7. Notification Of Certificate Modification By The CA To Other Entities

The CA shall notify the trusted root programs about the modified CA certificates to update the trust lists. Further, the CA shall notify the RA about the modification of individual or organizational certificates.

4.9. Certificate Revocation And Suspension

The CA may revoke CA, individual, and organizational certificates for many reasons (*e.g.*, private key compromise, incorrect PII, etc.). The revocation process changes the status of these certificates from valid to revoked. This process adds the values for Serial Number attribute of the

revoked certificates to CRLs and returns a revoked status in OCSP responses. Once the revoked certificates expire, this process removes the revoked certificates from the CRLs.

The CA shall not support suspended status for CA, individual, and organizational certificates.

4.9.1. Circumstances For Revocation

The CA shall revoke any individual or organizational certificates within 24 hours in accordance with one of the following conditions with revocation reason codes (CRLReason) as defined in RFC 5280:

- The Subscriber or Sponsor submits electronic or written revocation requests, but does not specify a reason (CRLReason 0: unspecified)
- The Subscriber or Sponsor notifies the CA that the original certificate request was not authorized and does not retroactively grant authorization (CRLReason 9: privilegeWithdrawn)
- The CA obtains evidence that the private keys corresponding to public keys in certificates have been compromised (CRLReason 1: keyCompromise)
- The CA becomes aware of a demonstrated or proven method to easily compute the private keys based on the corresponding public keys (CRLReason 1: keyCompromise)
- The CA obtains evidence the verified domain names for mailboxes managing email address is no longer valid (CRLReason 4: superceded)

The CA should revoke any individual or organizational certificates within 24 hours, but no later than five (5) business days, in accordance with one of the following conditions with revocation reason codes:

- The CA becomes aware that the certificate no longer complies with this CP (CRLReason 4: superceded)
- The CA obtains evidence that the certificate was either misused or used other than the intended purposes (CRLReason 9: privilegeWithdrawn)
- The Subscriber or Sponsor breached a material obligation under this CP, CPS, or relevant agreement (CRLReason 9: privilegeWithdrawn)
- The CA receives notification that the legal entity name has changed or the Subscriber or Sponsor is no longer affiliated with the legal entity (CRLReason 9: privilegeWithdrawn)
- The CA confirms any circumstances indicating the Subscriber or Sponsor no longer has legal rights to the mailbox for the E attribute in the Subject DN extension of the certificate (CRLReason 5: cessationOfOperations)
- The CA confirms that there has been a material change to the information in the certificate (CRLReason 9: privilegeWithdrawn)
- The CA becomes aware that the certificate contains either misleading or inaccurate information (CRLReason 9: privilegeWithdrawn)
- The CA has clear evidence the specific method to generate the private key is flaws (CRLReason 1: keyCompromise)
- The CA revokes the certificate for another reason (CRLReason 0: unspecified)

The CA shall revoke a CA or certificate within seven (7) days after receiving and confirming one or more of the following actions:

- The legal entity submits electronic or written revocation requests, but does not specify a reason (CRLReason 0: unspecified)
- The legal entity notifies the CA that the original certificate request was not authorized and does not retroactively grant authorization (CRLReason 9: privilegeWithdrawn)
- The CA becomes aware that the private key for CA certificate has been compromised (CRLReason 1: keyCompromise)
- The CA obtains evidence that the CA certificate was either misused or used other than the intended purposes (CRLReason 9: privilegeWithdrawn)
- The CA confirms that the CA certificate was not issued in accordance with this CP, CPS, or relevant agreement (CRLReason 9: privilegeWithdrawn)
- The CA confirms that there has been a material change to the information in the CA certificate (CRLReason 9: privilegeWithdrawn)
- The CA determines that the CA certificate contains either misleading or inaccurate information (CRLReason 9: privilegeWithdrawn)
- The CA receives notification that the legal entity name has changed or the Subscriber is no longer affiliated with the legal entity (CRLReason 9: privilegeWithdrawn)
- The CA ceases operations for any reason and has not arranged for another CA to provide revocation support (CRLReason 5: cessationOfOperations)
- The CA revokes the CA certificate for another reason (CRLReason 0: unspecified)

4.9.2. Who May Request Revocation

The CA shall accept revocation requests from authorized Subscribers, Sponsors, RAs, or Delegated Third Parties in the RA system. Further, the CA shall allow Application Software Suppliers to submit manual revocation requests. Lastly, the CA shall allow other entities to submit certificate problem reports about suspected issues. In these cases, the CA may revoke the certificates.

The CA may revoke certificates of its own volition without reason even if no entity requested revocation.

4.9.3. Procedure For Revocation Request

4.9.3.1. CA Revocation Request

The CA shall provide a process for authorized Proof personnel to request revocation of CAs through CA Revocation Forms.

4.9.3.2. Subscriber Revocation Request

The CA shall provide a process for Subscribers or Sponsors to request revocation of their own individual certificates. Also, the CA shall define a process for legal entities to request revocation of their CA or organizational certificates. Once received, the CA shall confirm the authenticity of the revocation requests.

4.9.3.3. RA Revocation Request

The CA shall establish a process for the RAs or Delegated Third Parties to request revocation of individual or organizational certificates. Once received, the CA shall verify the authenticity of the revocation requests.

4.9.3.4. Certificate Problem Report

The CA shall allow any entity (*e.g.,* Relying Parties, Application Software Suppliers, etc.) to submit a certificate problem report about the following conditions:

- Suspected Private Key compromise
- Certificate misuse
- Other types of fraud, compromise, misuse, or inappropriate conduct
- Any other matters related to the certificate

The entities shall send emails to digital-certificates@proof.com to report problems with the certificates.

The CA shall investigate the certificate problem reports and notify Subscribers or Sponsors as well as entities with status of the investigation. If the CA finds sufficient evidence, the CA shall revoke the certificates.

4.9.3.5. Application Software Supplier Revocation Request

The CA shall develop a process for Application Software Suppliers to request revocation of CA, individual, and organizational certificates. Once received, the CA shall investigate these requests. If the CA finds sufficient evidence, the CA shall revoke the certificates

4.9.4. Revocation Request Grace Period

The CA may allow a grace period for Subscribers, Sponsors, RAs, and Delegated Third Parties to withdraw the revocation requests.

4.9.5. Time Within Which CA Must Process The Revocation Request

4.9.5.1. Revocation Request

The CA shall process revocation requests as defined in CP Section 4.9.1.

4.9.5.2. Certificate Problem Report

The CA shall investigate certificate problem reports as defined in CP Section 4.9.1. Also, the CA shall provide preliminary reports about the investigation findings to the reporting entities as well as the Subscribers or Sponsors of the certificates in question within 24 hours.

During the investigations, the CA shall determine whether to revoke the certificates or take other appropriate actions. If the CA decides to revoke the certificates, the CA shall set revocation dates based on the following criteria:

- The nature of the alleged problem (scope, context, severity, magnitude, risk of harm)
- The consequences of revocation (direct and collateral impacts to Subscribers and Relying Parties)
- The number of certificate problem reports received about the certificates in question as well as the Subscribers and Sponsors
- The reporting entity that submitted the certificate problem reports
- Any relevant legislation

At the end of the investigations, the CA shall send final reports about the investigation findings to the reporting entities as well as the Subscribers or Sponsors of the certificates in question.

4.9.6. Revocation Checking Requirement For Relying Parties

The Relying Parties should verify each certificate in the certificate chain in accordance with relevant RFC standards which may include:

- Checking values for attributes in Issuer DN and Subject DN extensions chain as expected
- Confirming values for attributes in Key Usage and Extended Key Usage extensions meet intended use
- Verifying values in attributes in Certificate Policy extension meet expected policies
- Validating certificates have not exceeded values in Not After attribute
- Checking CRLs or OCSP to ensure certificates are not revoked

4.9.7. CRL Issuance Frequency

4.9.7.1. Offline CA Certificates

The CA shall produce CRLs for offline CA certificates at least once every 12 months. If the CA revokes Intermediate or Issuing CA certificates, the CA shall generate and publish new CRLs within 24 hours of revocation.

4.9.7.2. Online CA Certificates

The CA shall create CRLs for online CA certificates at least once every seven (7) days. Further, the values for the NextUpdate attribute shall not be more than ten (10) days beyond the values for the thisUpdate attribute.

4.9.8. Maximum Latency for CRLs (if applicable)

The CA shall publish CRLs in the security repository within a commercially reasonable time after creation.

4.9.9. Online Revocation/Status Checking Availability

The CA may provide OCSP support for CA, individual, and organizational certificates. Also, the CA shall ensure OCSP responses conform to the RFC 6960: X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP standard. In addition, the CA shall sign

the OCSP responses by either the CA certificates that issued these certificates or OCSP responder certificates signed by the same CA certificates that issued these certificates.

4.9.10. Online Revocation Checking Requirements

The Relying Parties should check the current status of certificates via CRL or OCSP before relying on these certificates.

If the CA provides OCSP for CA certificates, the CA shall update information provided in OCSP responses at least every 12 months and within 24 hours of revoking a CA certificate.

If the CA enables OCSP for individual or organizational certificates, the CA shall ensure:

- OCSP responses shall have a validity period greater than or equal to eight (8) hours
- OCSP responses shall have a validity interval less than or equal to ten (10) days
    - If OCSP responses have a validity interval less than 16 hours, then the CA shall update information in OCSP responses before reaching the half way point of the validity interval (*e.g.*, OCSP responses with a 12 hour validity interval must update information no later than every six (6) hours).
    - If OCSP responses have a validity interval greater than 16 hours, then the CA shall refresh the information in the OCSP responses at least eight (8) hours before reaching the value in NextUpdate attribute and no later than four (4) days after the value in the thisUpdate attribute (*e.g.*, OCSP responses with a 48 hour validity interval must refresh information no later than every 40 hours, OCSP responses with a seven (7) day validity interval must update information no later than every four (4) days, etc.)

The CA shall not provide OCSP responses with good status for certificates which have not been assigned values for the Serial Number attribute (*a.k.a.*, unused) or certificates not issued by this CA.

4.9.11. Other Forms Of Revocation Advertisements Available

The CA may use alternative methods to publish revoked certificates based on the following conditions:

- The alternative methods are described in the CPS
- The alternative methods provide authentication and integrity services
- The alternative methods meet CRL issuance and latency requirements as defined in CP Sections 4.9.5, 4.9.7, and 4.9.8

4.9.12. Special Requirements Related To Key Compromise

The CA shall use commercially reasonable efforts to notify Relying Parties and Application Software Suppliers about suspected or confirmed compromise of private keys.

The Entity shall use the Certificate Problem Report as defined in CP Section 4.9.3.3 to provide evidence of a Private Key Compromise based on one of the following methods:

- Submission of the compromised Private Key itself
- Submission of a CSR signed by the compromised Private Key

In addition, the Entity shall include a valid email address in the Certificate Problem Report to get confirmation and updates.

4.9.13. Circumstances For Suspension
The CA may suspend individual certificates.

4.9.14. Who May Request Suspension
The CA may offer the ability for Subscribers to suspend individual certificates.

4.9.15. Procedure For Suspension Request
The CA may provide a process for Subscribers to request suspension of their own individual certificates. Once received, the CA shall confirm the authenticity of the suspension requests.

4.9.16. Limits On Suspension Period
The CA may allow individual certificates to be suspended for up to six (6) months.

4.10. Certificate Status Services

4.10.1. Operational Characteristics
The CA shall provide current status of CA, individual, and organizational certificates through CRL and/or OCSP. In addition, the CA shall remove revoked certificates that have expired from the CRL and/or OCSP.

Moreover, the CA shall have a value for the URI attribute in Certificate Distribution Point (CDP) extension of these certificates (except for the Root CA certificates) to allow Relying Parties to download the CRLs. Also, the CA may include a value for the URLs in the Authority Information Access (AIA) extension of these certificates to let Relying Parties send OCSP requests and receive OCSP responses.

4.10.2. Service Availability
The CA shall maintain sufficient resources to provide responses in under ten (10) seconds for the current status of CA, individual, and organizational certificates. Also, the CA shall have 24x7x365 capability to respond to certificate problem reports. Where appropriate, the CA shall forward these reports to law enforcement or revoke the certificates in question.

4.10.3. Optional Features
No stipulation.

4.11. End Of Subscription
The CA shall allow Subscriber and Sponsors to end their subscriptions by either revoking or not renewing their individual or organizational certificates. Further, legal entities may end their subscription by either revoking or not renewing their CA certificates.

4.12. Key Escrow And Recovery

4.12.1. Key Escrow And Recovery Policy And Practices

The CA shall not escrow the private keys for CA certificates or any certificates with the Non-Repudiation values in the Key Usage extension of these certificates.

4.12.2. Session Key Encapsulation And Recovery Policy And Practices

The CA may offer session key encapsulation. If the CA provides session key encapsulation, the CA shall define the practices in the CPS.

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1. Physical Controls

5.1.1. Site Location And Construction

The CA shall operate infrastructure (*e.g.*, servers, networks, etc.) for the Proof PKI system in secure data centers with appropriate physical security controls to protect against interference or damage. Also, the CA shall implement appropriate physical security controls to protect HSMs that are in use, in transit, or in storage.

5.1.2. Physical Access

The CA shall have appropriate physical access controls to prevent unauthorized access to infrastructure for the Proof PKI system. The CA shall have physical controls that include, but are not limited to:

- Multifactor authentication to physically access infrastructure for the Poof PKI system via physical key cards and biometric readers
- Video surveillance on a 24x7x365 basis of the infrastructure for Proof PKI system
- Full time security guards on a 24x7x365 basis to log and monitor physical access
- Multi-person controls to activate and use HSMs

Also, the CA shall electronically monitor physical access logs at the secure data centers for unauthorized access to the Proof PKI system.

5.1.3. Power And Air Conditioning

The CA shall ensure the secure data centers have sufficient backup power and heating, ventilation, and air conditioning (HVAC) to ensure the infrastructure for the Proof PKI system may finish any pending operations before a system shutdown due a lack of power or air conditioning.

5.1.4. Water Exposure

The CA shall ensure the secure data centers protect the infrastructure for the Proof PKI system from damage due to water exposure.

5.1.5. Fire Prevention And Protection

The CA shall ensure the secure data centers protect the infrastructure for the Proof PKI system from fire with automatic fire suppression systems designed to protect electronic infrastructure.

5.1.6. Media Storage

The CA shall securely handle and store media to protect against unauthorized access, damage, or theft.

5.1.7. Waste Disposal

The CA shall shred and dispose of all paper documents or printed materials with confidential information in a secure manner. In addition, the CA shall wipe, zeroize, or overwrite data on electronic media

5.1.8. Offsite Backup

The CA shall backup and/or replicate data in Proof PKI system from the primary data center to at least one other geographically-separated data center based on the business continuity plans. Further, the CA shall ensure the other data center(s) have the commensurate physical protections and controls to the primary data center.

5.2. Procedural Controls

5.2.1. Trusted Roles

The PMA shall define and approve Trusted Roles that separates the CA and RA responsibilities to multiple personnel to prevent circumventing the security controls or subverting the trustworthiness of Proof PKI system. Moreover, the PMA may define and approve additional Trusted Roles to segregate responsibilities for the Proof PKI system.

5.2.2. Number Of Persons Required Per Task

The CA shall have security controls to ensure segregation of duties based on job roles. In addition, the CA shall require two-person control for critical CA functions which include, but are not limited to:

- Activating and using the HSMs
- Producing. backing up, and recovering key pairs for CA certificates
- Creating and managing offline CA certificates
- Generating CRLs for offline CA certificates
- Issuing OCSP responses from CA certificates
- Archiving and deleting CA audit logs

5.2.3. Identification And Authentication For Each Role

The CA shall require personnel in Trusted Roles to use multifactor authentication to access the Proof PKI system.

5.2.4. Roles Requiring Separation Of Duties

The PMA shall assign personnel to the Trusted Roles. Further, the PMA may assign personnel to multiple Trusted Roles, but, the PMA shall not allow personnel that have internal audit responsibilities to be assigned to any other Trusted Roles.

5.3. Personnel Controls

5.3.1. Qualifications, Experience, And Clearance Requirements

The CA shall verify the PII and trustworthiness of all personnel at Proof. Further, the CA shall specify the qualifications and experience for positions in Trusted Roles. Also, the CA shall assess whether candidates for these positions can perform responsibilities competently and satisfactorily.

5.3.2. Background Check Procedures

The CA shall conduct background checks, subject to local laws, on all personnel to verify PII, employment history, criminal and driving records, and educational levels.

5.3.3. Training Requirements

The CA shall provide comprehensive training to personnel in Trusted Roles to ensure understanding of the following items:

- Trusted roles and responsibilities
- Basic PKI concepts
- Security awareness
- Applicable policies and procedures

5.3.4. Retraining Frequency And Requirements

The CA shall require personnel in Trusted Roles to maintain required skill levels to perform their assigned responsibilities. Moreover, the CA shall provide periodic training to reinforce those skills levels and reflect any relevant changes impacting the Proof PKI system.

5.3.5. Job Rotation Frequency And Sequence

The CA may have personnel in Trusted Roles change job functions. In these cases, the CA shall minimize impacts due to these job changes.

5.3.6. Sanctions For Unauthorized Actions

The CA shall enforce administrative or disciplinary actions, up to and including termination and criminal sanctions, for personnel that fail to comply with this CP whether through negligence or malicious intent.

5.3.7. Independent Contractor Requirements

The CA shall subject independent contractors to the same qualification, background checks, training, and sanctions as specified in CP Sections 5.3.1, 5.3.2, 5.3.3, 5.3.4, and 5.3.6.

5.3.8. Documentation Supplied To Personnel

The CA shall give personnel in Trusted Roles with relevant documentation required to perform their job responsibilities. Also, the CA shall periodically update the relevant documentation to accurately reflect the Proof PKI system, operations, or security measures.

5.4. Audit Logging Procedures

5.4.1. Types Of Events Recorded

The CA shall enable audit logging processes in the Proof PKI system and Delegated Third Party systems to collect audit logs about system actions and security events. Moreover, the CA shall ensure the Proof PKI system or Delegated Third Party systems invoke the audit logging processes at system start up and only ends at system shut down. Further, the CA shall prevent circumvention of the audit logging processes.

Additionally, the CA shall capture, at a minimum, the following information in the audit logs:

- System action or security event description
- System action or security event date and time
- System action result
- User or service account that triggered system action or security event

If the Proof PKI system or Delegated Third Party systems do not support automated audit logging, the CA shall implement manual SOPs to record system actions and security events.

Finally, the CA shall make the audit logs available to the Qualified Auditors for inspection.

5.4.1.1. System Actions For CA Certificates

The CA shall capture, at a minimum, the following system actions in audit logs for CA certificates:

- Key generation, backup, storage, recovery, archival, and destruction
- Submission of certificate, renewal, rekey, and revocation requests
- Approval or denial decision for certificate, renewal, rekey, or revocation requests
- Issuance and revocation of CA certificates
- HSM life cycle management events
- Generation of CRLs
- Signature of OCSP responses
- Introduction of new certificate profiles
- Retirement of existing certificate profiles

5.4.1.2. System Actions For Individual And Organizational Certificates

The CA shall capture, at a minimum, the following system actions in audit logs for individual and organizational certificates:

- All verification actions as defined in CP Sections 3.1 and 3.2
- Submission of certificate, renewal, rekey, and revocation requests

- Approval or denial decision for certificate, renewal, rekey, and revocation requests
- Issuance and revocation of individual and organizational certificates
- Generation of CRLs
- Signature of OCSP responses

5.4.1.3. Security Events

The CA shall capture, at a minimum, the following security events in the audit logs:

- Successful and unsuccessful system access attempts
- PKI and security system actions performed
- Security profile changes
- Installation, update, or removal of infrastructure and applications
- System crashes, infrastructure failures, or other anomalies
- Firewall rule changes
- Physical access to data data centers

5.4.2. Frequency Of Processing Log

The CA shall collect and forward audit logs from the Proof PKI system and Delegated Third Party systems to a security event and incident management (SIEM) system at least daily. Further, the CA shall configure the SIEM to process audit logs upon receipt to identify any security incidents.

5.4.3. Retention Period For Audit Log

The CA shall retain audit logs in the archive for, at a minimum, two (2) years related to the following:

- CA certificate and HSM life cycle system actions as specified in CP Sections 5.4.1.1
- Individual and organizational certificate system actions as defined in CP Section 5.4.1.2
- Security events as described in CP Section 5.4.1.3

5.4.4. Protection Of Audit Log

The CA shall implement automated monitoring processes to continuously monitor the collection of audit logs from the Proof PKI system and Delegated Third Party systems as well as processing of audit logs by the SIEM. Further, the CA shall ensure the processes check the tamper-evident seals and time stamps on the audit logs. If the processes discover any anomalies, irregularities, or malicious activities, the CA shall produce security incidents and notify appropriate personnel in Trusted Roles as per the security incident process defined in CP Section 5.7.1.

Moreover, the CA shall configure the SIEM and have SOPs to protect archived audit logs from destruction before the end of the retention period by ensuring only authorized personnel in Trusted Roles have read only access and may archive audit logs.

5.4.5. Audit Log Backup Procedures

The CA shall backup and/or replicate data in the SEIM from the primary data center to at least one other geographically-separated data center based on the business continuity plans. Also, the

CA shall ensure the other data center(s) have the commensurate security controls to the primary data center.

5.4.6. Audit Collection System (Internal Versus External)

The CA may deploy an internal SIEM system or use a third-party service as the SIEM system. If the SIEM fails, the CA shall notify the PMA to determine whether to suspend CA and RA operations until the issues have been remediated.

5.4.7. Notification To Event-Causing Subject

No stipulation.

5.4.8. Vulnerability Assessments

The CA shall conduct risk assessments at least annually to identify known internal and external threats that may result in unauthorized access, disclosure, misuse, alteration, or destruction of data in the Proof PKI system and Delegated Third Party systems. Also, the CA shall determine the likelihood and potential damage of these threats. Moreover, the CA shall perform internal audits as specified in CP Section 8.7 to assess the effectiveness of security controls against these threats.

Further, the CA shall perform vulnerability scans at least quarterly to identify known vulnerabilities on the Proof PKI system and Delegated Third Party systems. In addition, the CA shall engage an independent third party vendor to hold penetration tests on the Proof PKI system and Delegated Third Party systems. The CA shall identify, review, prioritize, and remediate findings discovered from these vulnerability scans and penetration tests to maintain integrity of the Proof PKI system and Delegated Third Party systems.

5.5. Records Archival

5.5.1. Types Of Records Archived

The CA shall archive legal entity and PII verification results for Proof personnel along with the Subscribers and Sponsors of individual certificates. In addition, the CA shall archive certificate, renewal, rekey, and revocation requests. Further, the CA shall archive documents about the Proof PKI system and Delegated Third Party systems. Lastly, the CA shall archive audit logs.

5.5.2. Retention Period For Archive

The CA shall retain archived data in accordance with the following schedule:

- Legal entity and PII verification results shall be retained for the entire validity period of CA, individual, and organizational certificate plus two (2) years
- Certificate, renewal, rekey, and revocation requests shall be kept for the entire validity period of CA, individual, and organizational certificate plus two (2) years
- System documentation for Proof PKI system and Delegated Third Party systems shall be retained for two (2) years
- Audit logs shall be kept for two (2) years

5.5.3. Protection Of Archive

The CA shall protect the data in archives from unauthorized access, changes, substitution, or destruction by restricting access to personnel in Trusted Roles and encrypting the data at-rest. Further, the CA shall monitor the archive for unauthorized access or changes.

5.5.4. Archive Backup Procedures

The CA shall backup and/or replicate data in the archives from the primary data center to at least one other geographically-separated data center based on the business continuity plans. Also, the CA shall ensure the other data center(s) have the commensurate security controls to the primary data center.

5.5.5. Requirements For Time Stamping Of Records

The CA shall include date and time stamps for all system actions (*e.g.*, uploading data, viewing data, etc.) in the archives. Further, the CA shall ensure the time stamps are derived from trusted time sources.

5.5.6. Archive Collection System (Internal Or External)

The CA may deploy an internal archive system or leverage a third-party service as the archive system.

5.5.7. Procedures To Obtain And Verify Archive Information

The CA shall periodically update, delete, and verify data in the archives manually or automatically. Also, the CA shall restrict access to the archives to authorized personnel in Trusted Roles. Further, the CA shall have SOPs about updating, deleting, and verifying data in the archives.

5.6. Key Changeover

The CA shall periodically change the key pairs for CA, individual, and organizational certificates as specified in the associated CPS Section 5.6.

5.7. Compromise And Disaster Recovery

5.7.1. Incident And Compromise Handling Procedures

The CA shall have security incident processes to identify, analyze, respond, remediate, and recover from security incidents in the Proof PKI system and Delegated Third Party systems. Additionally, the CA shall prepare a business continuity plan to declare and recover from potential disasters that compromise data or impact secure data centers. Further, the CA shall notify Subscribers, Sponsors, Relying Parties, Other Participants, and Application Software Suppliers in the event of disasters, data compromises, or business failures. Finally, the CA shall perform tabletop exercises to test security incident and business continuity processes at least every 12 months.

5.7.2. Recovery Procedures If Computing Resources, Software, And/Or Data Are Corrupted

The CA shall include recovery options in the business continuity plans to promote alternative secure data centers to be the primary data centers and restore data from backups.

5.7.3. Recovery Procedures After Key Compromise

The CA shall include recovery options in the business continuity plan to address suspected or confirmed compromise, loss, or destruction of the private keys for CA certificate. Further, the CA shall add recovery options in the business continuity plans to handle theoretical or actual compromise of the parameters or algorithms used to generate the private keys for CA certificates.

If the private keys for CA certificate are compromised, the CA shall investigate the security incidents as specified in CP Section 5.7.1 and may take the following steps:

- Revoke all individual and organizational certificates issued by CA certificates
- Revoke CA certificates
- Generate new key pairs on HSMs
- Sign CA certificates with new key pairs
- Send notifications

5.7.4. Business Continuity Capabilities After A Disaster

The CA shall restore the Proof PKI system and Delegated Third Party systems in accordance with recovery time objectives (RTOs) and recovery point objectives (RPOs) as per the business continuity plans in cases of disasters, data compromises, or business failures.

5.8. CA Or RA Termination

The CA shall send timely notice about termination of CA or RA responsibilities to all affected Subscribers, Sponsors, Relying Parties, Other Participants, and Application Software Suppliers.

If the CA decides to transfer these responsibilities to another CA, the CA shall create migration plans and share the transfer details with all affected Subscribers, Sponsors, Relying Parties, Other Participants, and Application Software Suppliers.

If the CA opts to stop issuing or renewing certificates, the CA shall send timely notice that allows affected Subscribers, Sponsors, Relying Parties, Other Participants, and Application Software Suppliers to switch to another CA. At the end of the notice period, the CA shall perform the following tasks at the end of the notice period:

- Revoke all valid CA, individual, and organizational certificates
- Destroy the private keys for the CA certificates.
- Publish the final CRLs in the security repository

6. TECHNICAL SECURITY CONTROLS

6.1. Key Pair Generation And Installation

6.1.1. Key Pair Generation

The CA shall generate all key pairs (*a.k.a.*, public/private keys) on HSMs validated by NIST to comply with US NIST Federal Information Processing Standards (FIPS) 140-2: Security Requirements for Cryptographic Modules standard.

Note: US NIST has published the FIPS 140-3 standard which supersedes FIPS 140-2 standard, but many HSM vendors are waiting for the NIST Cryptographic Module Validation Program (CMVP) to review their applications for FIPS 140-3 certificates. The CA will use HSMs with FIPS 140-3 certificates where possible.

6.1.1.1. CA Certificates

The CA shall create key pairs on HSMs rated at FIPS 140-2 Level 3 for CA certificates. Further, the PMA shall authorize key ceremonies with personnel in Trusted Roles to follow key ceremony scripts to activate the HSMs and generate key pairs. Also, the CA shall require M of N to activate HSMs and enforce multi-person controls to perform CA operations. Additionally, the CA shall have Qualified Auditors either witness the key ceremonies or examine videos and attestations from the key ceremonies.

6.1.1.2. Individual And Organizational Certificates

The CA may generate and host key pairs on behalf of Subscribers and Sponsors for individual and organizational certificates. If the CA hosts the key pairs, the CA shall generate the key pairs on HSMs rated at FIPS 140-2 Level 2.

Additionally, the CA may allow Sponsors to generate key pairs and submit CSRs for organizational certificates. In this case, the CA shall require the Sponsor to produce the key pairs on HSMs rated at FIPS 140-2 Level 2.

6.1.2. Private Key Delivery To Subscriber

The CA shall grant access to Subscribers and Sponsors to use their private keys. Also, the CA shall require Subscribers and Sponsors to use multifactor authentication.

6.1.3. Public Key Delivery To Certificate Issuer

The CA shall deliver the public keys to Subscribers and Sponsors in the Public Key extension of individual and organizational certificates.

6.1.4. CA Public Key Delivery To Relying Parties

The CA shall deliver the public keys for CA certificates to Relying Parties in secure manners that preclude substitution attacks.

6.1.5. Key Sizes

The CA may use the following Rivest, Shamir, and Adleman (RSA) or elliptical curve cryptography (ECC) key sizes for certificates:

Certificate	Digest Algorithm	RSA Modulus Size (Bits)	ECC Curve
Root CA Certificate	SHA-256, SHA-384, or SHA-512	2048, 3072, or 4096	P-256, P-384, or P-521
Intermediate CA Certificate	SHA-256, SHA-384, or SHA-512	2048, 3072, or 4096	P-256, P-384, or P-521

Issuing CA Certificate	SHA-256, SHA-384, or SHA-512	2048, 3072, or 4096	P-256, P-384, or P-521
Individual Certificate	SHA-256, SHA-384, or SHA-512	2048, 3072, or 4096	P-256, P-384, or P-521
Organizational Certificate	SHA-256, SHA-384, or SHA-512	2048, 3072, or 4096	P-256, P-384, or P-521

The CA shall ensure all RSA key pairs have a modulus size, in bits, evenly divisible by eight (8).

6.1.6. Public Key Parameters Generation And Quality Checking

The CA shall confirm public key exponents for RSA keys are an odd number equal to three (3) or more. In addition, the CA shall perform parameter quality checking in accordance with the US NIST FIPS 186-5: Digital Signature Standard (DSS). Further, the CA should verify the validity of ECC keys using either ECC Full Public Key Validation Routine or ECC Partial Public Key Validation Routine in accordance with US NIST SP 800-56A Rev. 3: Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography standard.

6.1.7. Key Usage Purposes (As Per X.509 V3 Key Usage Field)

The CA shall include the Key Usage extension in CA, individual, and organizational certificates to technically limit usage in software applications compliant with the RFC 5280 standard.

Additionally, the CA shall only allow the private keys for Root CA certificates to sign the following types of certificates:

- Self-signed Root CA certificates
- Intermediate or Issuing CA certificates
- OCSP Responder certificates or OCSP responses

6.2. Private Key Protection And Cryptographic Module Engineering Controls

6.2.1. Cryptographic Module Standards And Controls

The CA shall generate, store, and protect private keys on HSMs that have obtained FIPS 140-2 certificates. In particular, the CA shall use the following HSMs for the certificates:

Certificate	HSM Rating
CA Certificates	FIPS 140-2 Level 3
Individual Certificates	FIPS 140-2 Level 2
Organizational Certificates	FIPS 140-2 Level 2
OCSP Responder Certificates	FIPS 140-2 Level 2

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

The CA shall require quorums (*a.k.a.*, M of N) to activate and use the HSMs. Moreover, the CA shall implement multi-person controls to perform CA operations involving the HSMs.

6.2.3. Private Key Escrow

The CA shall not escrow the private keys from the HSMs.

6.2.4. Private Key Backup

The CA shall backup private keys from the HSMs under multi-person controls. Moreover, the CA shall encrypt backups on HSMs and store backups in geographically-separated locations based on the business continuity plans.

6.2.5. Private Key Archival

The CA shall not archive private keys.

6.2.6. Private Key Transfer Into Or From A Cryptographic Module

The CA shall only allow private keys to be exported from HSMs for migration to other HSMs or backups. In addition, the CA shall encrypt the backups at rest. Further, the CA shall import the encrypted backups into HSMs for use.

The CA shall not permit the private keys to be in plain text outside of the HSMs.

6.2.7. Private Key Storage On Cryptographic Module

The CA shall store private keys on HSMs as specified in CP Section 6.2.1.

6.2.8. Method Of Activating Private Key

The CA shall implement multi-person controls to perform CA operations involving HSMs. Also, the CA shall meet the quorums to activate the HSMs storing the private keys for CA certificates.

Further, the CA shall require Subscribers and Sponsors to login with multifactor authentication to create sessions with the HSMs hosting the private keys for individual and organizational certificates.

6.2.9. Method Of Deactivating Private Key

The CA shall deactivate the private keys of CA certificates and securely store the HSMs when not in use. Further, the CA shall protect the HSMs when not in use from interference, damage, or unauthorized access.

6.2.10. Method Of Destroying Private Key

The CA shall implement multi-person controls to perform all CA operations involving HSMs which includes destroying private keys for CA certificates.

In addition, the CA shall destroy the private keys after the expiration of individual or organization certificates.

6.2.11. Cryptographic Module Rating

The CA shall ensure the HSMs have valid FIPS certificates as specified in CP Section 6.2.1.

6.3. Other Aspects Of Key Pair Management

6.3.1. Public Key Archival

The CA shall archive public keys for CA, individual, and organizational certificates as specified in CP Section 5.5.

6.3.2. Certificate Operational Periods And Key Pair Usage Periods

The CA shall set the following maximum validity periods for certificates and key pairs:

Certificate	Maximum Validity	Key Pairs	Maximum Validity
Root CA Certificates	25 Years	Root CA Key Pairs	25 Years
Intermediate CA Certificates	20 Years	Intermediate CA Key Pairs	20 Years
Issuing CA Certificates	10 Years	Issuing CA Key Pairs	10 Years
Individual Certificates	3 Years	Individual Key Pairs	3 Years
Organizational Certificates	3 Years	Organizational Key Pairs	3 Years

The CA shall not issue individual or organizational certificates with an expiration period that exceeds the Issuing CA certificates.

6.4. Activation Data

6.4.1. Activation Data Generation And Installation

The CA shall generate activation data (*e.g.*, key pairs, passwords, etc.) with sufficient strength to protect key pairs on HSMs against loss, theft, modification, modification, unauthorized access, or unauthorized use.

If the CA uses passwords as activation data for HSMs, the CA shall ensure the passwords comply with the CA/B Forum Network and Certificate System Requirements.

6.4.2. Activation Data Protection

The CA shall implement cryptographic and security controls to protect activation data from unauthorized access or use.

6.4.3. Other Aspects Of Activation Data

The CA shall ensure only personnel in Trusted Roles have access to activation data for HSMs.

6.5. Computer Security Controls

6.5.1. Specific Computer Security Technical Requirements

The CA shall configure the Proof PKI system which includes CA, RA, and VA systems to meet the following technical requirements:

- Configured, maintained, and secured using industry best practices
- Operated on trustworthy software
- Regularly scanned for malicious code and protected against spyware and viruses
- Updated with recommended security patches within six (6) months of the security patch's availability, unless documented testing determines that the security patch would introduce additional vulnerabilities

In addition, the CA shall configure the Proof PKI system to perform the following security tasks:

- Verify identity of users before permitting access
- Use multifactor authentication to access systems
- Manage privileges of users and limit users to assigned roles
- Generate and archive audit records for all transactions
- Enforce domain integrity boundaries for critical security processes
- Support recovery from system failure

6.5.2. Computer Security Rating

No stipulation.

6.6. Life Cycle Technical Controls

6.6.1. System Development Controls

The CA shall implement the following security controls for the software development life cycle (SDLC):

- Follow a documented SDLC process for software development related to Proof PKI system
- Obtain infrastructure and software for the Proof PKI system in a manner that reduces risks of tampering, falsification, or modification
- Maintain integrity of software throughout the SDLC and deployment processes
- Ensure the CA system has dedicated infrastructure, databases, software, and networks for CA operations

If the CA uses third-party software for linting, the CA should install the latest version that is no more than three (3) months from the general availability (GA) release.

6.6.2. Security Management Controls

The CA shall have security controls to establish, update, and monitor the baseline configurations for all infrastructure and software for the Proof PKI system. If the CA detects unauthorized

modifications to the baseline configurations, the CA shall investigate the security incidents as specified in CP Section 5.7.1.

6.6.3. Life Cycle Security Controls
No stipulation.

6.7. Network Security Controls
The CA shall implement security controls to protect all CA, RA, and VA operations in the Proof PKI system which includes:

- Segment networks into zones based on functional or logical relationships
- Apply security controls to all infrastructure and software within the same zones
- Manage data flow and secure communications within and between networks and zones
- Configure network infrastructure to only allow services, ports, and protocols required for CA, RA, and VA operations
- Ensure secure communications between Subscribers and RA system as well as RA system to CA system
- Grant and log access by personnel in Trusted Roles to networks and zones
- Monitor networks and zones for potential security incidents

6.8. Time Stamping
The CA shall ensure the accuracy of trusted time sources is within three (3) minutes for all time stamping operations. Further, the CA may use network time protocol (NTP) or cryptographically-based for the time stamps.

7. CERTIFICATE, CRL, AND OCSP PROFILES

7.1. Certificate Profile

7.1.1. Version Number(s)
The CA shall configure the CA system to issue CA, individual, and organizational certificates based on X.509 Version 3 in the RFC 5280 standard.

7.1.2. Certificate Extensions
The CA shall configure the CA system to include extensions based on RFC 5280 standard, C2PA technical standard, and Adobe ATL technical requirements in CA, individual, and organizational certificates.

Further, the CA shall configure extensions of CA certificates based on CA/B Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates standard.

7.1.3. Algorithm Object Identifiers
The CA shall specify one of the following object identifiers (OIDs) for the Signature Algorithm attribute in CA, individual, and organizational certificates:

OID	Dot Notation	ASN.1 Notation
sha256WithRSAEncryption	1.2.840.113549.1.1.11	{ iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha256WithRSAEncryption(11) }
sha384WithRSAEncryption	1.2.840.113549.1.1.12	{ iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha384WithRSAEncryption(12) }
sha512WithRSAEncryption	1.2.840.113549.1.1.13	{ iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha512WithRSAEncryption(13) }
ecdsa-with-SHA256	1.2.840.10045.4.3.2	{ iso(1) member-body(2) us(840) ansi-x962(10045) signatures(4) ecdsa-with-SHA2(3) ecdsa-with-SHA256(2) }
ecdsa-with-SHA384	1.2.840.10045.4.3.3	{ iso(1) member-body(2) us(840) ansi-x962(10045) signatures(4) ecdsa-with-SHA2(3) ecdsa-with-SHA384(3) }
ecdsa-with-SHA512	1.2.840.10045.4.3.4	{ iso(1) member-body(2) us(840) ansi-x962(10045) signatures(4) ecdsa-with-SHA2(3) ecdsa-with-SHA512(4) }

In addition, the CA shall include one of the OIDs for the Algorithm attribute in the Public Key Information extension of the CA, individual, and organizational certificates to indicate elliptical curve (EC) used for the key pair:

OID	Dot Notation	ASN.1 Notation
rsaEncryption	1.2.840.113549.1.1.1	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) rsaEncryption(1)}
ecPublicKey	1.2.840.10045.2.1	{ iso(1) member-body(2) us(840) ansi-x962(10045) keyType(2) ecPublicKey(1) }

Moreover, the CA shall include one of the OIDs for the Parameter attribute in the Public Key Information extension of the CA, individual, and organizational certificates to indicate type of key pair created by the CA, Subscriber, or Sponsor:

OID	Dot Notation	ASN.1 Notation
scep256r1 (*a.k.a.*, P-256, prime256v1)	1.2.840.10045.3.1.7	{ iso(1) member-body(2) us(840) ansi-x962(10045) curves(3) prime(1) prime256v1(7) }
scep384r1 (*a.k.a.*, P-384)	1.3.132.0.34	{ iso(1) identified-organization(3) certicom(132) curve(0) ansip384r1(34) }

scep521r1 (*a.k.a.*, P-521)	1.3.132.0.34	{ iso(1) identified-organization(3) certicom(132) curve(0) ansip521r1(35) }

Note: RSA based key pairs have null values for the Parameter attribute.

7.1.4. Name Forms

The CA shall include C, O, and CN attributes in the Issuer DN extension of CA, individual, and organizational certificates. Additionally, the CA shall populate C, O, and CN attributes in the Subject DN extension of CA and organizational certificates. Further, the CA shall have the C and CN attributes in the Subject DN extension of individual certificates. Moreover, the CA may include the O attribute in the Subject DN extension of individual certificates.

In addition, the CA shall populate the Serial Number attribute of CA, individual, and organizational certificates.

The CA shall not add symbols (*e.g.*, dash "-", space " ", etc.) for any attributes in the Subject or Issuer DN extensions that may indicate the value is absent, incomplete, or not applicable. Further, the CA shall not include the Organizational Unit (OU) attribute in the Issuer or Subject DN extensions.

7.1.5. Name Constraints

The CA may include the Permitted Sub Tree and Excluded Sub Tree attributes in the Naming Constraints extension (if applicable).

7.1.6. Certificate Policy Object Identifier

The CA shall add OIDs registered by Proof in the Certificate Policy extension of CA, individua,l and organizational certificates.

7.1.7. Usage Of Policy Constraints Extension

No stipulation.

7.1.8. Policy Qualifiers Syntax and Semantics

The CA may include the CPS and User Notice attributes in the Certificate Policy extension of CA, individual, and organizational certificates to notify Relying Parties about terms and conditions

7.1.9. Processing Semantics For The Critical Certificate Policies Extension

No stipulation.

7.2. CRL Profile

7.2.1. Version Number(s)

The CA shall configure the CA system to issue CRLs based on CRL Version 2 in the RFC 5280 standard.

7.2.2. CRL And CRL Entry Extensions

The CA shall include the Authority Key Identifier (AKI), CRL Number, and AIA extensions in the CRLs. Also, the CA shall add Reason Code as the CRL entry extension. Further, the CA shall populate the Reason Code extension as specified in CP Section 4.9.1.

7.3. OCSP Profile

7.3.1. Version Number(s)

The CA shall configure the VA system to accept OCSP requests and returns OCSP responses based on Version 1 of the RFC 6960 standard.

7.3.2. OCSP Extensions

The CA shall not populate the Single Extension of the OCSP responses with the reason code values in the CRLs.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1. Frequency Or Circumstances Of Assessment

The CA shall engage Qualified Auditors to assess the compliance of the Proof PKI system with this CP and associated CPS at least every 12 months.

In addition, the CA shall require Delegated Third Parties to undergo assessments by Qualified Auditors to ensure compliance with applicable requirements, agreements, and PKI related documents at least every 12 months.

8.2. Identity And Qualifications Of Assessor

The CA shall engage Qualified Auditors with the following characteristics to assess the Proof PKI system:

- Is independent from the subject of the external assessment
- Has ability to conduct an external assessment that addresses criteria specified in CP Section 8.4
- Employs individuals proficient in the examination of PKI infrastructure technology; information security tools and techniques; information technology and security auditing; and third-party attestation function
- Adhere to applicable laws, government regulations, and professional code of ethics
- Maintains a Professional Liability / Errors and Omissions insurance policy with a minimum of one million US dollars ($1,000,000) in coverage

8.3. Assessor's Relationship To Assessed Entity

The CA shall use Qualified Auditors that are independent from any relationships that may constitute a conflict of interest or may impair the auditor’s objective assessment in any way.

8.4. Topics Covered By Assessment

The CA shall engage Qualified Auditors to perform assessments of the Proof PKI system in accordance with the latest versions of the following documents:

- CA/B Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates
- CA/Browser Forum Network and Certificate System Security Requirements
- WebTrust Principles and Criteria for Certification Authorities – Network Security
- WebTrust Principles and Criteria for Certification Authorities – Network Security
- Adobe Approved Trust List 2.0 Technical Specification

In addition, the CA shall require Delegated Third Parties to undergo assessments by Qualified Auditors to ensure compliance with applicable requirements, agreements, and PKI related documents.

8.5. Actions Taken As A Result Of Deficiency

The Qualified Auditors shall provide assessment reports with their opinions and findings for any security control deficiencies. The CA shall develop corrective action plans to remediate the deficiencies. Further, the CA shall monitor the progress against corrective action plans. If the corrective actions are not being resolved, the CA shall report the issue to the PMA. If required, the CA may perform internal assessments to ensure the effectiveness of security controls.

The CA shall require Delegated Third Parties to share assessment reports. If the assessment reports have security control deficiencies, the CA shall obtain and track the corrective action plans from the Delegated Third Parties.

8.6. Communication Of Results

The CA shall provide the assessment reports and summarize the audit results for the PMA. Further, the CA shall share assessment reports with third party entities as contractually required. Additionally, the CA shall publish the assessment reports in the legal repository.

8.7. Self Audits

The CA shall conduct internal audits to evaluate the design and effectiveness of security controls for the Proof PKI system at least every 12 months. Additionally, the CA shall audit a three percent (3%) random sample of individual and organizational certificates to verify ID verification of Subscribers and Sponsors at least quarterly.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1. Fees

9.1.1. Certificate Issuance Or Renewal Fees

The CA may charge fees to issue and renew certificates.

9.1.2. Certificate Access Fees
The CA may charge fees to provide access to databases containing certificates.

9.1.3. Revocation Or Status Information Access Fees
The CA shall not charge fees to check revocation information via standard CRLs or OCSP. However, the CA may charge for value-added services (*e.g.*, customized CRLs, alternative authentication methods, etc.).

9.1.4. Fees For Other Services
The CA may charge fees for additional services (e.g., co-branded CAs, cross certification, etc.).

9.1.5. Refund Policy
The CA may offer refunds in accordance with the applicable terms and conditions.

9.2. Financial Responsibility

9.2.1. Insurance Coverage
The CA shall maintain commercial general liability insurance with policy limits of at least two million US dollars ($2,000,000) in coverage as well as Errors and Omissions/Professional Liability insurance with a policy limit of at least five million US dollars ($5,000,000) in coverage.

9.2.2. Other Assets
No stipulation.

9.2.3. Insurance Or Warranty Coverage For End Entities
The CA may offer limited warranties in accordance with the applicable terms and conditions.

9.3. Confidentiality Of Business Information

9.3.1. Scope Of Confidential Information
The CA shall specify the information to be classified as confidential in the CPS.

9.3.2. Information Not Within The Scope Of Confidential Information
The CA may treat any information not listed as confidential in the CPS as public information.

9.3.3. Responsibility To Protect Confidential Information
The CA shall contractually obligate Proof personnel to protect confidential information. Moreover, the CA shall provide security training for Proof personnel about protecting confidential information.

9.4. Privacy Of Personal Information

9.4.1. Privacy Plan
The CA shall create and follow a publicly posted privacy policy that specifies how the CA handles PII.

9.4.2. Information Treated As Private
The CA shall treat PII about Subscribers, not included in the Subject extension of individual certificates, as private.

9.4.3. Information Not Deemed Private
The CA shall not consider certificates, CRLs, or documents published in repositories to be private.

9.4.4. Responsibility To Protect Private Information
The CA shall contractually obligate Proof personnel to protect private information. Further, the CA shall provide security training for Proof personnel about protecting private information.

9.4.5. Notice And Consent To Use Private Information
The CA shall comply with the publicly posted privacy policy to store, process, and transfer PII including any notices and consents stated within this policy.

9.4.6. Disclosure Pursuant To Judicial Or Administrative Process
The CA may disclose private PII without notice to Subscribers or Sponsors as required by applicable laws, court orders, and regulations.

9.4.7. Other Information Disclosure Circumstances
The CA may use third-party vendors to perform functions in the Proof PKI system. In these cases, the CA shall contractually require third-party vendors to adhere to the CA's privacy requirements, consistent with the publicly posted privacy policy and applicable privacy laws and regulations.

9.5. Intellectual Property Rights
The CA shall own the intellectual property rights in the Proof PKI system including certificates and CRLs. Further, the CA shall grant permission to make revocation information available to Relying Parties that agree to the RPA. Moreover, the CA shall grant permission to use revocation information and distribute certificates to Application Software Suppliers in accordance with relevant agreements.

9.6. Representations And Warranties

9.6.1. CA Representations And Warranties
The CA shall represent compliance to this CP and associated CPS in all material aspects to Subscribers, Relying Parties, and Application Software Suppliers.

9.6.2. RA Representations And Warranties
The CA shall require RA or Delegated Third Parties to follow this CP and associated CPS for certificate issuance and management.

9.6.3. Subscriber Representations And Warranties
The CA shall require Subscribers and Sponsors to agree with the applicable terms and conditions and make the following representations:

- Sponsors received appropriate security training about certificates
- Subscribers and Sponsors provided accurate and complete information at all times in connection with the issuance of certificates including certificate, renewal, and rekey requests as well as any additional information requested by RA, Delegated Third Parties, or CA
- Subscribers and Sponsors took all reasonable measures to protect and control the private keys for the certificates including credentials used to access private keys
- Subscribers and Sponsors verified the accuracy of information in certificates
- Subscribers and Sponsors use certificates in compliance with the applicable laws
- Subscribers and Sponsors promptly request revocation due to actual or suspected compromise of private keys; misuse of certificates; and incorrect or inaccurate information in certificates
- Subscribers and Sponsors cease to use all private keys for revoked and expired certificates
- Subscribers and Sponsors acknowledge and accept the CA may revoke certificates immediately due to a violation of the terms and conditions or required by the CP and CPS

9.6.4. Relying Party Representations And Warranties

The Relying Parties shall make representations as required by this CP, associated CPS, and applicable terms and conditions prior to using or relying upon certificates issued by the CA.

9.6.5. Representations And Warranties Of Other Participants

No stipulation.

9.7. Disclaimers Of Warranties

ALL CERTIFICATES AND ANY RELATED SERVICES ARE PROVIDED “AS IS” AND “AS AVAILABLE” EXCEPT AS EXPRESSLY STATED IN PROOF CP SECTION 9.6.1.

TO THE MAXIMUM EXTENT PERMITTED BY LAW, PROOF DISCLAIMS ALL EXPRESS AND IMPLIED WARRANTIES, INCLUDING ALL WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT.

PROOF DOES NOT WARRANT THAT ANY SERVICE OR PRODUCT WILL MEET ANY EXPECTATIONS OR THAT ACCESS TO CERTIFICATES WILL BE TIMELY OR ERROR-FREE. FURTHER, PROOF DOES NOT GUARANTEE THE AVAILABILITY OF A PRODUCT OR SERVICE AND MAY MODIFY OR DISCONTINUE ANY PRODUCT OR SERVICE AT ANY TIME.

NO FIDUCIARY DUTY IS CREATED OR IMPLIED THROUGH THE USE OF A PROOF PRODUCT OR SERVICE BY ANY ENTITY.

9.8. Limitations Of Liability

The CA may disclaim liability in the applicable terms and conditions.

9.9. Indemnities

9.9.1. Indemnifications by CA

The CA shall represent compliance to this CP and associated CPS in all material aspects to Subscribers, Relying Parties, and Application Software Suppliers

9.9.2. Indemnification by Subscribers and Sponsors

The Subscribers and Sponsor shall indemnify the CA, to the extent permitted by applicable law, for:

- Falsehood or misrepresentation of fact by the Subscriber or Sponsor on the Certificate Application
- Failure by the Subscriber to disclose a material fact on the Certificate Application, if the misrepresentation or omission was made negligently or with intent to deceive any party
- Failure to protect the private key for the certificate, to use a trustworthy system, or to otherwise take the precautions necessary to prevent the compromise, loss, disclosure, modification, or unauthorized use of the private key for the certificate
- Use of a name (including without limitation within a common name or email address) that infringes upon the intellectual property rights of a third party.

9.9.3. Indemnification by Relying Parties

The CA shall include any indemnification requirements for Relying Parties in the associated CPS for this CP.

9.10. Term And Termination

9.10.1. Term

The CA shall consider this version of the CP to be effective until otherwise communicated through the legal repository as specified in CP Section 2.1

9.10.2. Termination

The CA shall terminate older versions of the CP effective immediately as soon as the latest version has been published in the legal repository.

Note: Some CP Sections may include future dates for certain policies or practices to become effective.

9.10.3. Effect Of Termination And Survival

The CA shall communicate the conditions and effect of terminating this CP along with which provisions will survive termination in the legal repository. At a minimum, the CA shall survive provisions related to protection of confidential information.

9.11. Individual Notices And Communications With Participants

The CA shall accept any formal notices related to this CP which either have digital signatures or have been delivered by physical mail to the address specified in CP Section 1.5.2. Also, the CA shall review and reply to valid notices in a timely manner.

9.12. Amendments

9.12.1. Procedure For Amendment

The PMA may enact amendments to this CP as required. Further, the PMA shall note significant changes, may include minor changes (*e.g.*, grammar corrections, formatting updates, etc.), in CP Appendix C. Also, the CA shall review this CA at least every 12 months. If there are no changes, the CA shall add an entry in CP Appendix C stating no changes required.

9.12.2. Notification Mechanism And Period

The PMA shall upload the latest CP version to the legal repository within seven (7) days after approval. In addition, the PMA shall notify Subscribers and Sponsor within reasonable timeframes about any major changes and effective dates to the CP.

9.12.3. Circumstances Under Which OID Must Be Changed

The PMA shall reserve the right to amend this CP. If this CP necessitates a new OID, the PMA shall include the new OID in the updated CP version. Otherwise, the CA may not have to change the OID for this CP.

9.13. Dispute Resolution Provisions

The Subscribers, Sponsors, Relying Parties, Application Software Suppliers, and any other entities shall be required to notify Proof and attempt to resolve any disputes before resorting to any dispute resolution including adjudication or any other alternative dispute resolution.

9.14. Governing Law

The CA shall abide by the laws of the State of Delaware to govern the interpretation, construction, and enforcement of this CP and all proceedings related to the Proof PKI system including tort claims without regard to any conflicts of law principles. Also, the CA shall use the State of Delaware as the non-exclusive venue and jurisdiction over any proceedings related to this CP.

9.15. Compliance With Applicable Law

The CA shall issue certificates and operate the Proof PKI in accordance with all laws applicable to its business and the certificates it issues in every jurisdiction in which it operates.

9.16. Miscellaneous Provisions

9.16.1. Entire Agreement

The CA shall enter into legally enforceable contracts that delineate terms associated with the Proof PKI system and related services.

9.16.2. Assignment

The Subscribers, Sponsors, Relying Parties, Application Software Suppliers, any other legal entities may not assign their rights or obligations without prior written consent of the CA.

9.16.3. Severability

The CA may modify the CP to address any conflicting requirements with a law, regulation, or government order in an applicable jurisdiction.

If the law, regulation, or government order no longer applies, the CA shall revert the modifications in the CP.

9.16.4. Enforcement (Attorney's Fees and Waiver of Rights)

The CA may seek indemnification and attorney's fees for damages, losses, and expenses incurred from Subscribers, Sponsors, Relying Parties, Application Software Supplier, or other legal entities due to their conduct. If the CA fails to enforce a CP provision, the CA shall not waive its rights to enforce the same CP provision or any other CP provisions in the future. Additionally, the CA shall require any waivers to be in writing and signed by the CA to be effective.

9.16.5. Force Majeure

The CA shall not be liable for any delays or failure to perform an obligation under this CP to the extent of the delay or failure is caused by an occurrence beyond the reasonable control of the CA that includes the operation of the Internet.

9.17. Other Provisions

No stipulation.

APPENDIX A | DEFINITIONS

Applicant: Is a natural person or legal entity that applies for (or seeks renewal of) a certificate. Once the certificate has been issued, the Applicant is referred to as the Subscriber.

Audit Period: Is the period between the first day (start) and the last day of operations (end) covered by the auditors in their engagement which is not the same as the time period if auditors are onsite. The coverage rules and maximum length of audit periods are defined in CP Section 8.1.

Audit Report: Is a report from the Qualified Auditor stating their opinion on whether processes and controls by CA, RA, or Delegated Third Party comply with requirements and industry standards.

Baseline Requirements: Refer to standards published by CA/B Forum including “Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates” and “Network and Certificate System Security Requirements” which form the basis for the requirements and WebTrust audits.

CA System: Is a collection of infrastructure, databases, and software to issue and manage certificates.

CAB Forum: Means the Certification Authority/Browser Forum which is a voluntary group of CAs, web browsers, and Application Software Suppliers that use X.509 V.3 digital certificates. The CAB Forum sets the guidelines and requirements to establish public trust in web browsers and other software for digital certificates.

Certificate: Is a X.509 based file that uses a digital signature to bind a public key and an identity.

Certificate Management Process: Refers to processes, practices, and procedures associated with the use of keys, software, and infrastructure by which a CA verifies PII, issues certificates, maintains repositories, and revokes certificates.

Certificate Policy: Is a set of rules that indicate the applicability of a certificate to a particular community and/or PKI implementation with common security requirements.

Certificate Problem Report: Is a complaint of suspected key compromise, certificate misuse, or other types of fraud, compromise, misuse, or inappropriate conduct related to certificates.

Certificate Profile: Means a set of requirements for certificate content and certificate extensions.

Certificate Revocation List: Refers to a regularly updated, time-stamped list of revoked certificates that is created and digitally signed by the CA that issued the certificates.

Certificate Systems: Means systems used by the CA or Delegated Third Party to verify identity; register, enroll, approve, and issue certificates; check status of certificates; provide support functions; and other PKI-related services.

Certification Authority: Is an organization that is responsible for the creation, issuance, revocation, and management of certificates. The term applies equally to Roots CAs, Intermediate CAs and Issuing CAs.

Certification Practice Statement: Is one of several documents that form the governance framework in which certificates are created, issued, managed, and used.

Country: Is either a member of the United Nations (UN) or a geographic region recognized as a Sovereign State by at least two UN member nations.

High Risk Certificate Request: Is a certificate request by an Applicant that has been flagged by the CA for additional scrutiny based on internal criteria.

Individual: Is a natural person (*a.k.a.*, human being).

Intermediate CA Certificate: Is a CA certificate issued by a Root CA certificate that is capable of issuing new certificates containing the Certificate Authority (cA) attribute in the Basic Constraints extension.

Issuing CA: Is a CA certificate issued by a Root or Intermediate CA certificate that issues certificates to Subscribers or Sponsors.

Key Compromise: Means unauthorized access or use of the private key. The unauthorized access or use may be suspected or confirmed.

Key Pair: Refers to the public and private keys for certificates. The public key appears in the Subject Public Key attribute of the certificates.

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

Online Certificate Status Protocol: Is an online certificate-checking protocol that enables Relying Parties to determine the status of a certificate.

OCSP Responder: Refers to a certificate that digitally signs OCSP responses with status of certificates.

Personally Identifiable Information: Means any information about an individual maintained, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information which is linked or linkable to an individual.

Policy Management Authority: Is an administrative body appointed by CA management to create and maintain policies described in this CP and related procedural or security policy documents.

Private Key: Is kept secret by the Subscriber or Sponsor to create digital signatures and/or decrypt data encrypted with the corresponding public key.

Public Key: Is publicly disclosed by the Subscriber or Sponsor to Relying Parties which use public keys to verify digital signatures or encrypt data.

Public Key Infrastructure: Refers to a set of infrastructure, databases, software, system, people, policies, procedures, rules, and obligations to facilitate trustworthy creation, issuance, management, and use of certificates and keys based on public key cryptography.

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

Qualified Auditor: Is a natural person or legal entity that meets the requirements of CP Section 8.2.

RA System: Refers to a collection of infrastructure, databases, and software to verify PII and legal entity information as well as create and submit certificate, renewal, rekey, and revocation requests.

Registration Authority: Refers to any legal entity that is responsible for identification and authentication of subjects of certificates. While the RA is not a CA and does not issue certificates, the RA may assist in the certificate application and/or revocation processes. RA is also used as an adjective to describe a role or function and does not necessarily imply a separate legal entity, but may be part of the CA.

Rekeying: Means the creation of a new certificate, using some or all of the information submitted from an existing certificate, and generating a new key pair.

Reliable Data Source: Refers to a data source to verify PII and legal entity information that is generally recognized among commercial entities as reliable.

Relying Party: Is any natural person or legal entity that relies on a valid certificate.

Repository: Means publicly-available web sites containing Proof policies, agreements, CA certificates, and certificate status information. Proof manages a legal repository for policies and agreements as well as a security repository for certificate status information.

Root CA: Is a top-level, self-signed CA certificate that issues other CA certificates. The Root CA certificate may be distributed by Application Software Suppliers.

Root CA System: A system used to create a Root Certificate or to generate, store, or sign with the Private Key associated with a Root Certificate.

Sponsor: Is a natural person that enrolls for a certificate on behalf of a legal entity and is legally bound by the applicable terms and conditions.

Subject: Is a natural person or legal entity identified as the Subject in a certificate.

Subscriber: Is a natural person that enrolls for a certificate and is legally bound by the applicable terms and conditions.

Validity Period: Is defined in RFC 5280 Section 4.1.2.5 as the period of time calculated based on values in notBefore through notAfter attributes, inclusive.

APPENDIX B | ACRONYMS AND ABBREVIATIONS

The following acronyms and abbreviations are used in this CP:

Acronym	Description
AIA	Authority Information Access
ANSI	American National Standards Institute
ASN.1	Abstract Syntax Notation One Encoder / Decoder
C	Country
CA	Certification Authority
CDP	CRL Distribution Point
CN	Common Name
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSR	Certificate Signing Request
DN	Distinguished Name
DSS	Digital Signature Standard
E	Email
EC	Elliptical Curve
ECDSA	Elliptic Curve Digital Signature Algorithm
FIPS	(US) Federal Information Processing Standard
HSM	Hardware Security Module
ID	Identity

IETF	Internet Engineering Task Force
NIST	National Institute of Standards and Technology
NTP	Network Time Protocol
O	Organization
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PKCS	Public Key Certificate Standard
PKI	Public Key Infrastructure
PMA	Policy Management Authority
RA	Registration Authority
RFC	Request For Comments
RP	Relying Party
RPS	Registration Practice Statement
RSA	Rivest-Shamir-Adleman (encryption algorithm)
SHA	Secure Hash Algorithm
SP	Special Publication
TLS	Transport Layer Security
URL	Uniform Resource Locator
US	United States

APPENDIX C | CHANGE HISTORY

Version	Date	Change Description	Author
1.0	25-May-2025	Released Initial version based on RFC 3647.	Michael Yatsko
1.1	30-June-2025	Changed validity periods for Issuing CAs, individual certificates, and organizational certificates; Added OIDs in Section 1.2.3; Updated Section 6.1.3 to clarify public key delivery; Removed last two sentences in Section 6.1.7. Deleted last sentence in Section 6.2.8 for redundancy; Changed two person references to mult-person; Made minor grammar updates.	Michael Yatsko
1.2	14-July-2025	Include Section 1.1.4 for service availability; Added Baseline Requirements statement in Section 1; Modified Certificate Problem Report details in Section 4.9.3.4; Updated Certificate Modification in Section 4.8.3.	Michael Yatsko