ARRIS Technology, Inc.
Certificate Policy and
Certification Practice Statement

Document Number: PR5031
Revision 2.13
Revision Date: 2026-05-21

Table of Contents

1 INTRODUCTION

This Certificate Policy and Certification Practice Statement (CP/CPS) document is published by ARRIS Technology, Inc., a wholly owned subsidiary of Vistance Networks, Inc. ("Vistance") and part of Vistance's Aurora Networks business. In this document, the words "we" and "us", and their related forms (e.g. "our", "ours") refer to ARRIS Technology, Inc., the entity that provides the PKI services to which this CP/CPS document applies.

As of December 9, 2025, we have ended operation of our public Certification Authorities (CAs). As a result, policies and practices that apply specifically to public CAs are no longer applicable. It is intended that text related to such policies and practices will be removed from this CP/CPS in future revisions.

In the meantime, despite any language to the contrary, we do not assert conformance with requirements or policies that apply specifically to public CAs, including but not limited to those from the following sources:

- *the "Baseline Requirements" document [11] of the CA/Browser Forum (CAB Forum)*
- *the Trusted Root CA Programs ("root programs") of Mozilla, Apple, Google (Chrome), and Microsoft*
- *the Common CA Database (CCADB)*

Accordingly, provisions in this CP/CPS that relate specifically to Publicly-Trusted Certificates or to participation in such public trust ecosystems shall be interpreted as inapplicable. This includes, without limitation:

- *provisions that reference the CAB Forum, root programs, the CCADB, or Certificate Transparency*
- *provisions that reference documents [11], [13]–[16] and [19], which correspond to publicly trusted certificate ecosystem requirements; such references are a strong indicator that the associated provisions are specific to public CA operations*
- *requirements specific to publicly trusted certificate issuance (e.g., domain validation methods, certificate profiles, or issuance restrictions)*
- *operational, audit, reporting, or revocation obligations derived from such programs and their associated policies and requirements*
- *interactions with root programs or Application Software Suppliers in connection with publicly trusted certificate ecosystems*

Readers should interpret as inapplicable statements regarding policies, practices, or technical specifications related to:

- *Publicly-Trusted Certificates and the CAs involved in their issuance;*
- *CAs described as participating in, or otherwise subject to the requirements and policies of, the CA/Browser Forum, the root programs of Mozilla, Apple, Google (Chrome), and Microsoft, or the CCADB; and*
- *Our CAs whose names begin with "CommScope Public Trust".*

For clarity, the exclusions in this disclaimer do not apply to the CA/Browser Forum Network and Certificate System Security Requirements [12].

The procedures described in this document are limited to certificate issuance, delivery and revocation, as applicable to our external PKI services that are hosted on the system known as PKIWorks. Revocation services include publicly accessible CRL Distribution Points and a OCSP Responder we host.

This CP/CPS encompasses PKI for multiple ecosystems, including CA/Browser Forum-compliant public CAs, WInnForum Root of Trust, DOCSIS 3.1, DOCSIS 4.0, OpenCable host, and CableCARD. As a result, there are a number of ecosystem-specific parameters included in this policy that may point to other documents, including:

- Definition of a Policy Authority (PA) for such ecosystem and PA member contact information. See Section 1.5 on the definition of a PA.
- Certificate profile
- Whether or not validity period nesting is required for a specific ecosystem
- CRL and OCSP profiles
- Retention period for private keys generated by a CA, after they had been delivered to a Subscriber.
- Audit frequency and qualifications of the auditing firm. We expect to hold audits at the frequency that will satisfy all the current PKI ecosystems using a firm that complies with all the ecosystem-specific requirements.
- Additional ecosystem-specific PKI requirements

1.1 Overview

The policies described in this document are compliant with RFC 3647.

Some of the CAs covered by this CP/CPS conform to the current version of guidelines adopted by the Certification Authority/Browser Forum ("CAB Forum") and published to their site (https://www.cabforum.org). Publicly trusted Certificates are issued and managed according to the CAB Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Certificates ("Baseline Requirements"). In the event of any inconsistency between this CP/CPS and the CAB Forum's latest published version of Baseline Requirements, the latter

shall take precedence over this document. For a full list of our Publicly-Trusted CAs under the CAB Forum ecosystem please refer to Section 7.1.

For CAs capable of issuing publicly trusted certificates, this CP/CPS further includes requirements and recommendations from:

- CAB Forum's Network and Certificate System Requirements
- Microsoft, Mozilla, Apple and Chrome Root CA programs

As of this revision, Extended Validation Certificates as well as publicly trusted certificates for email signing and secure time servers are out of scope of this CP/CPS.

This CP/CPS applies to all entities and individuals utilizing our certification services listed in this document. Other important documents that also apply to our certification services include:

- Subscriber Agreements
- Private documents governing internal procedures and operations

1.2 Document Name and Identification

This CP/CPS is known as the "ARRIS Technology, Inc. CP/CPS".

Version Control

Rev	Description	Revision Date
2.0	Add requirements for a public CA and merge with the CPS. This is the first version supporting CAs for publicly trusted certificates. Version control for prior versions of the CP/CPS was private.	4-26-2021
2.1	Added text to sec. 4.9.12 about third-party reports of private key compromise. Synced with CableLabs CP for DOCSIS 3.1 CA Updated definition of Critical Vulnerability to match the changes in the latest Browser Forum network security requirements. Updated ECDSA subscriber certificate signing algorithm in section 7.1.10.4.	8-16-2021

Rev	Description	Revision Date
2.2	Removed internal CommScope NextGen CAs from WebTrust audits. Updated reference to CableLabs Certificate Policy.	3-2-2022
2.3	Cleanup and requirements clarifications. Updates to sections: - 4.3.1 - added requirement to use current time-of-date for certificate notBefore time (no backdating) - 4.9.3.1 – clarified that revocation of precertificates is supported, even if the corresponding subscriber certificate has not been issued - 4.9.7 – added requirement (previously implicit from Baseline Requirements) on CRL's nextUpdate field - 6.1.7 – made explicit that publicly-trusted root CA can issue OCSP responder certificates	
2.4	Added copy right notice on front page. Fixed error in section 7.3 – OCSP responses for Sub-CA certificates are not directly signed by the issuing (root) CA.	
2.5	Editorial changes to section titles to fully comply with RFC 3647.	
2.6	Updates for CableLabs Certificate Policy 6.3 and addition of DOCSIS 4.0.	2-10-2023
2.7	Updated § 2.3 to limit the scope of the requirement to publish precertificates to transparency logs prior to certificate issuance. Introduced a new defined term (Trusted Root CA Program).	9-8-2023

2.8	§§ 1.1, 4.9.5, 4.9.7, 7.1.10.3, 7.1.10.4: Made minor wording changes. § 1.6: (1) Updated a number of definitions to match those in the current version of reference [11] ("CABF BR"); (2) modified definitions of "Certificate", "Subscriber", and "Root CA" by combining the existing ones with those from CABF BR; (3) added definitions of "Control" and "Technically Constrained Subordinate CA Certificate" based on those in CABF BR. § 3.2.2.8: Updated wording to explicitly relate CAA record checking to the issuance of a Publicly-Trusted Certificate. §§ 3.2.5, 4.9.10, 8.1: Added text copied/adapted from corresponding sections of CABF BR. §§ 4.9.10, 6.3.2, 7.3: Added statements that effectively incorporate by reference specific prescriptions in CABF BR. § 5.2.2: Added language to parallel language in CABF BR § 5.2.2. §§ 5.4.8, 6.5.1: Updated text to parallel language in CABF BR §§ 5 & 6.5.1 respectively. § 6.1.1.1: Added the words "physically secured environment" to align with the wording in CABF BR § 6.1.1.1. § 7.1: Updated the entry for "CA/Browser Forum" in the table of certificate profiles; under the "Timeout Period for Private Key Deletion" column, the entry now reads "N/A". § 7.1.10.4: Removed requirement that one of the CT logs precertificates are published to must be operated by Google. § 7.3: Changed occurrences of "validity period" to "validity interval", to align with the language of CABF BR § 7.3. § 8.4: Updated references to "WebTrust Principles and Criteria" documents.	2-14-2024

Rev	Description	Revision Date
	§ 8.6: Add language that audit report shall have the contents prescribed by CABF BR. § 9.3: Added language about review of Subscriber Agreement. § 7.1.10.3: Corrected misspelling in the name of the extKeyUsage extension.	
2.9	§ 1.1, 1.2: Updated the formal title of the CA/B Forum TLS Baseline Requirements document. § 1.5.2: Clarified how Certificate Problem Reports or revocation requests may be submitted using the URL in the text. § 4.3.1.1.3: Clarified that "two" in the context means "two or more". § 5.4.1: Under "Subscriber Certificate lifecycle events", added "Details of CAA record checking" to the list. Under "Trusted employee events", added the verb "access" which was previously missing from a list item. § 6.1.5: Added text to state that, for Publicly Trusted Certificates, CommScope performs recommended key quality checks. § 8.2: Reworded the reference to WebTrust principles and criteria. Added the requirement that a Qualified Auditor must be a licensed WebTrust practitioner. § 8.6: Added statement that Audit reports will be publicly available no later than 3 months after the end of the audit period. Other minor linguistic/stylistic edits.	9-27-2024

Rev	Description	Revision Date
2.10	Made changes to permit sunsetting of OCSP support for subscriber certificates issued by CommScope public CAs. Modified subscriber certificate profile for CommScope public CAs to make inclusion of OCSP URL in AIA extension optional. Discontinued the use of the "email to domain contact" method (§ 3.2.2.4.2). Updated text in § 3.2.2.4.15 to state that the "phone contact with domain contact" method shall not be used, instead of not supported. Added new section (3.2.2.4.21) on the "DNS Labeled with Account ID – ACME" method. Qualified the requirements related to tokens to avoid implying that they are always used.	07-10-2025
2.11	§ 1.6: Incorporated definitions from [11] related to linting & MPIC § 3.2.2.4.7: Added statement that validation using the method is done with MPIC § 4.2: Added list of issuer domain names CommScope CA recognizes as permitting to issue § 4.9.7: Added text on CRL publication to align with [11]; added statement of compliance with technical requirements of [11] § 4.9.9 § 5.4.1: Added MPIC events to list of events recorded § 6.1.1.2: Added statement that CommScope CA checks for weak keys as prescribed by [11] § 6.3.2: Added statement of conformance to validity period limits specified in [11] § 8.4: Updated references to WebTrust principles & criteria documents Other minor edits	9-26-2025

Rev	Description	Revision Date
2.12	§ 1: Added a notice about the ending of public CA operations and disclaiming conformance with requirements applicable to public CAs. § 1.5: Mailing address for communicating with CommScope PA removed § 2.1.1: Section content deleted; section heading changed to "(Deleted)". §§ 7.1–7.3: Entries related to public CAs removed from certificate/CRL/OCSP profiles	1/13/2026
2.13	Elaborated the notice/disclaimer added in Rev. 2.12, to clarify the scope of inapplicable provisions. Revised instances of text containing the "CommScope" name to remove or avoid use of the name. Updated PA contact email address and URL for Vistance's privacy policy. Revised or removed statements invalidated by a corporate transaction involving the CA's ultimate parent (f.k.a. CommScope) and its renaming to Vistance Network. Removed references to Relying Party Agreement (applicable to Publicly Trusted Certificates). Removed an outdated forward-looking statement about a planned phase-out of OCSP support. Removed statement about the public availability of Subscriber Agreement for public CAs and Relying Party Agreement. Other minor edits.	05/21/2026

1.2.1 References

[1] RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework http://www.ietf.org/rfc/rfc3647.txt

[2] FIPS 140-2 Security Requirements for Cryptographic Modules, http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

[3] Data-Over-Cable Service Interface Specifications, DOCSIS 3.1 Security Specification, CM-SP-SECv3.1-I07-170111.

[4] OpenCable System Security Specification, OC-SP-SEC-I08-110512, CableLabs, May 12, 2011.

[5] RFC 5280, Internet X.509 Public Key Infrastructure Certificate and CRL Profile, IETF, May 2008.

[6] RFC 6960, Online Certificate Status Protocol – OCSP, IETF, June 2013.

[7] RFC 6532, Internationalized Email Headers, IETF, February 2012.

[8] RFC 3966, The tel URI for Telephone Numbers, IETF, December 2004.

[9] RFC 3912, WHOIS Protocol Specification, IETF, September 2004.

[10] RFC 7482, Registration Data Access Protocol (RDAP) Query Format, IETF, March 2015.

[11] Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Certificates, https://cabforum.org/working-groups/server/baseline-requirements/documents/, CAB Forum.

[12] Network and Certificate System Security Requirements, https://cabforum.org/working-groups/netsec/documents/, CAB Forum.

[13] Microsoft Trusted Root Program, https://docs.microsoft.com/en-us/security/trusted-root/program-requirements, Microsoft.

[14] Mozilla Root Store Policy, https://www.mozilla.org/en-US/about/governance/policies/security-group/certs/policy/, Mozilla.

[15] Apple Root Certificate Program, https://www.apple.com/certificateauthority/ca_program.html, Apple.

[16] Chrome Root Program Policy, https://g.co/chrome/root-policy, Chromium Projects.

[17] RFC 8659, DNS Certification Authority Authorization (CAA) Resource Record, IETF, November 2019.

[18] RFC 6962, Certificate Transparency, IETF, June 2013.

[19] Common CA Database (CCADB) Policy, https://www.ccadb.org/policy.

[20] CableLabs New PKI Certificate Policy, Version 5.1, CableLabs, September 28, 2021.

[21] DPoE Security and Certificate Specification, DPoE-SP-SECv2.0-I06-180228, CableLabs, Feb 28, 2018.

[22] WInnForum CBRS Certificate Policy Specification, WINNF-17-TS-0022, Version V1.5, November 17, 2020.

[23] Apple's Certificate Transparency Policy, https://support.apple.com/en-us/HT205280, Apple.

[24] Certificate Transparency in Chrome, https://github.com/GoogleChrome/CertificateTransparency/blob/main/ct_policy.md.

[25] Data-Over-Cable Service Interface Specifications, DOCSIS 4.0 Security Specification, CM-SP-SECv4.0-I08-250903 .

[26] CableLabs 2nd GEN DOCSIS PKI Certificate Policy, Version 8.0, 10/28/2025.

[27] CableLabs PKI, Trust Infrastructure Document (Certificate Templates), C-PKI-TI-V1.6, 10/28/2025.

1.3 PKI Participants

The following are relevant to the administration and operation of the PKI covered by this CP/CPS.

1.3.1 Certification Authorities

The CA is the collection of technology and procedures that issues PKCs (Public Key Certificates or "Certificates") under this CP/CPS. ARRIS Technology, Inc. is the CA operator which performs the actual CA operations (such as creation of all the Certificates) on behalf of Subscribers.

Subscriber is an entity that receives end-entity certificates from one of the Certificate Authorities we operate.

The CA Operator is the legal entity responsible for all aspects of the issuance and management of a PKC including:

- Developing and maintaining its Certification Practice Statements (CPSs)
- Issuing compliant Certificates
- Securing delivery of Certificates to its Subscribers
- Revoking Certificates
- Generating, protecting, operating, and destroying CA private keys
- Managing all aspects of the CA services, operations, and infrastructure related to Certificates issued under this CP/CPS and ensuring that they are performed in accordance with the requirements, representations, and warranties of this CP/CPS
- Acting as a trusted party to facilitate the confirmation of the binding between a public key and the identity, and/or other attributes, of the Subject of the Certificate.

This CP/CPS is intended to be common to a number of different PKI ecosystems in which we are providing a managed PKI service. Each ecosystem has its own certificate profiles specified and typically for each ecosystem there are:

- One or more Root CAs
- A chain of one or more Sub-CAs that are under each Root CA.

1.3.2 Registration Authorities

Registration Authorities (RAs) are entities that enter into an agreement with a Certification Authority to collect and verify each Subscriber's identity and information to be entered into the Subscriber's certificates. The RA performs its function in accordance with this CP/CPS and will perform front-end functions of confirming the identity of the certificate applicant, approving or denying Certificate Applications, requesting revocation of certificates, and managing account renewals.

For some ecosystems (including the Publicly-Trusted CAs under the CAB Forum ecosystem), RA function is performed by CA Officers (defined in Section 5.2.1) and in that case it is part of the our PA. For other ecosystems, RA function may be performed by a separate company or organization.

1.3.3 Subscribers

Subscriber is the organization named in Digital Certificate Authorization Agreement (DCAA) or in a Subscriber Agreement. An authorized representative of the Subscriber, acting as a certificate applicant, shall complete the certificate application process established by the PA ("Certificate Applicant"). In response, the CA relies on the PA to confirm the identity of the Certificate Applicant and either approves or denies the application. If approved, the PA communicates to the CA, and the Subscriber may then request certificates.

Subscribers shall adopt the appropriate certificate policy requirements and any additional certificate management practices to govern the Subscriber's practice for requesting certificates and handling the corresponding private keys. The Subscriber agrees to be bound by its obligations through execution of the DCAA between the Subscriber and the CA, and any other applicable agreements. This includes the case where the Subscriber has implemented an automated manufacturing process for requesting and issuing end-entity certificates for installation into devices.

Specific agreement and certificate policy requirements for Subscribers may vary per ecosystem and are out of scope of this document.

1.3.4 Relying Parties

"Relying Party" and "Application Software Supplier" are defined in Section 1.6.

1.3.5 Other Participants

No stipulation.

1.4 Certificate Usage

This CP/CPS applies to all PKI Participants for a particular ecosystem, including Subscribers and Relying Parties. This CP/CPS sets forth policies governing the use of Certificates issued by us. Each Certificate is generally appropriate for use as set forth in the applicable specifications and agreements for a specific ecosystem.

1.4.1 Appropriate Certificate Uses

Usage of each digital certificate is restricted based on certificate extensions as specified in RFC 5280.

Basic Constraints extension specifies which certificates belong to a Certificate Authority that is permitted to issue subordinate certificates.

Key Usage and Extended Key Usage extension further limit the use of the private key as specified in the corresponding certificate profile specified in the CPS.

1.4.2 Prohibited Certificate Uses

The same digital certificate is prohibited from being utilized as both a CA Certificate and Subscriber Certificate. Only the key usages that are explicitly specified within the Basic Constraints, Key Usage and Extended Key Usage certificate extensions are permitted.

1.5 Policy Administration

Our PA is responsible for all aspects of this CP/CPS and approval of all related PKI agreements. Our PA is responsible for coordination with the Superior Entity and other external organizations for policy changes that require review or approvals of these organizations.

The Policy Authority (PA) is the entity that approves this certificate policy. The PA approves all additional documents such as customer facing agreements and forms. PA approval is also required for CA Certificate revocation approvals and large-scale device certificate revocation approvals.

All communication with the our PA, including this CP/CPS should be directed to:

#Advanced-PKI-Policy-Authority@auroranetworks.com

Contact information in Section 1.5 shall also be provided to:

- Microsoft following enrollment into Microsoft Trusted Root Program, see [13].
- CCADB, following CCADB enrollment, see [19].

1.5.1 Organization Administering the Document

Our PA is responsible for all aspects of this CP/CPS and approval of all related PKI agreements. See Section 1.5.

1.5.2 Contact Person

Communications to our PA may be submitted using the contact information in Section 1.5.

Certificate Problem Reports and revocation requests may be submitted by following the instructions at https://cert.pkiworks.com/Public/SecurityIncidentReport/ or to the PA using the contact information in Section 1.5.

1.5.3 Person Determining CPS Suitability for the Policy

See Section 1.5.

1.5.4 CPS Approval Procedures

CP/CPS document updates shall be clearly marked using Microsoft Word document revisions or equivalent.

Minor updates that include minor edits, clarifications and typo corrections shall be approved by at least one CA Officer of ours which was not the author of the CP/CPS changes. CA Officer's approval shall be indicated by filling in the approver's name and approval date in the Revision History section of the document.

Minor CP/CPS document updates shall be provided to the Superior Entity as indicated in the CP/CPS. Refer to Section 7.1 regarding Superior Entity notification requirements for each PKI ecosystem.

Major updates shall be approved by at least two CA officers of ours, none of which are the authors of the CP/CPS revision. Both CA Officers shall indicate approval by filling in their approver name and approval date in the Revision History section of the document. At least one of these two CA Officers shall be a member of the PA.

In addition, some PKI ecosystems may require the Superior Entity to approve a major CP/CPS update. Superior Entity approval will be noted in the CP/CPS Revision History. CP/CPS provides Superior Entity approval requirements of the CP/CPS for each PKI ecosystem.

1.6 Definitions and Acronyms

AICPA	American Institute of Certified Public Accountants
ADN	Authorization Domain Name
CA	Certification Authority
CAA	Certification Authority Authorization
CARL	Certification Authority Revocation List
ccTLD	Country Code Top-Level Domain
CICA	Canadian Institute of Chartered Accountants

CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CVC	Code Verification Certificate
DBA	Doing Business As
DN	Distinguished Name
DNS	Domain Name System
DTLS	Datagram Transport Layer Security
FIPS	(US Government) Federal Information Processing Standard
FQDN	Fully Qualified Domain Name
HSM	Hardware Security Module
I&A	Identification and Authentication
IETF	Internet Engineering Task Force
IM	Instant Messaging
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
ISO	International Organization for Standardization
KGF	Key Generation Facility
NIST	(US Government) National Institute of Standards and Technology
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PA	Policy Authority
PKC	Public Key Certificate
PKI	Public Key Infrastructure
RP	Relying Party
RA	Registration Authority
S/MIME	Secure MIME (Multipurpose Internet Mail Extensions)
SP	Service Party
SSL	Secure Sockets Layer

TLS	Transport Layer Security
VoIP	Voice Over Internet Protocol

Activation	The technical means to make a Certificate Authority functional, including loading or generating the CA private key in the HSM and turning on certificate and CRL signing operations.
Activation Data	Additional information (besides the CA private key) that may be required to enable certificate and CRL signing operations. User passwords, pin codes and one-time passwords are all examples of the Activation Data.
Administrator	A trusted role that installs, configures, and maintains the CA.
Affiliate	A corporation, partnership, joint venture or other entity controlling, controlled by, or under common control with another entity, or an agency, department, political subdivision, or any entity operating under the direct control of a Government Entity.
Applicant	See Certificate Applicant
Applicant Representative	natural person or human sponsor who is either the Applicant, employed by the Applicant, or an authorized agent who has express authority to represent the Applicant: (i) who signs and submits, or approves a certificate request on behalf of the Applicant, and/or (ii) who signs and submits a Subscriber Agreement on behalf of the Applicant, and/or (iii) who acknowledges the Terms of Use on behalf of the Applicant when the Applicant is an Affiliate of the CA or is the CA.
Application Software Supplier	A supplier of Internet browser software or other Relying Party application software, such as operating system software, that displays or uses Certificates and incorporates Root Certificates.
Attestation Letter	A letter attesting that Subject Information is correct written by an accountant, lawyer, government official, or other reliable third party customarily relied upon for such information.
Archive	Long-term, physically separate storage.
Audit	Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures.
Auditor	A trusted role that performs the Audit.
Audit Data	Chronological record of system activities to enable the reconstruction and examination of the sequence of events and changes in an event that are found in the computer system logs.

Audit Period	In a period-of-time audit, the period between the first day (start) and the last day of operations (end) covered by the auditors in their engagement. (This is not the same as the period of time when the auditors are on-site at the CA.) The coverage rules and maximum length of audit periods are defined in Section 8.1.
Audit Report	A report from a Qualified Auditor stating the Qualified Auditor's opinion on whether an entity's processes and controls comply with the mandatory provisions of this CP/CPS and with the requirements from each Superior Entity.
Authorization Domain Name	The FQDN used to obtain authorization for a given FQDN to be included in a Certificate. The CA may use the FQDN returned from a DNS CNAME lookup as the FQDN for the purposes of domain validation. If a Wildcard Domain Name is to be included in a Certificate, then the CA MUST remove "*." from the left-most portion of the Wildcard Domain Name to yield the corresponding FQDN. The CA may prune zero or more Domain Labels of the FQDN from left to right until encountering a Base Domain Name and may use any one of the values that were yielded by pruning (including the Base Domain Name itself) for the purpose of domain validation.
Backup	Copy of files and programs made to facilitate recovery if necessary.
Base Domain Name	The portion of an applied-for FQDN that is the first domain name node left of a registry-controlled or public suffix plus the registry-controlled or public suffix (e.g. "example.co.uk" or "example.com"). For FQDNs where the right-most domain name node is a gTLD having ICANN Specification 13 in its registry agreement, the gTLD itself may be used as the Base Domain Name.
CAA	From RFC 8659 (http://tools.ietf.org/html/rfc8659): "The Certification Authority Authorization (CAA) DNS Resource Record allows a DNS domain name holder to specify one or more Certification Authorities (CAs) authorized to issue certificates for that domain name. CAA Resource Records allow a public CA to implement additional controls to reduce the risk of unintended certificate mis-issue."
CA Certificate	A digital certificate which certifies the public key of a Certificate Authority, where this public key is utilized to validate Subscriber Certificates issued by this CA. Subscriber Certificates issued by a CA are end-entity certificates and are not considered to be CA Certificates.

CA Equipment	CA Equipment includes all the hardware elements that are necessary to operate Certificate Authorities covered by this CP/CPS, including computer systems, HSMs and HSM activation devices.
CA Key Pair	A Key Pair where the Public Key appears as the Subject Public Key Info in one or more Root CA Certificate(s) and/or Subordinate CA Certificate(s).
CA Operator	The CA Operator is the legal entity responsible for all aspects of the issuance and management of Public Key Certificates.
Certificate Applicant	The natural person or Legal Entity that applies for (or seeks renewal of) a Certificate. Once the Certificate is issued, the Applicant is referred to as the Subscriber. For Certificates issued to devices, the Applicant is the entity that controls or operates the device named in the Certificate, even if the device is sending the actual certificate request.
Certification Authority (CA)	The CA is responsible for all aspects of the issuance and management of a PKC including: registration, identification and authentication, issuance, and ensuring that all aspects of the CA services and CA operations and infrastructure related to PKCs issued under the our CP are performed in accordance with the requirements, representations, and warranties of their our CPS.
Certificate (or Public Key Certificate)	(In the issuance and management of Publicly-Trusted Certificates) An electronic document that uses a digital signature to bind a public key and an identity. (Otherwise) A digital representation of information which at least (1) identifies the certification authority issuing it, (2) names or identifies its Certificate Subject, (3) contains the Certificate Subject's public key, (4) identifies its operational period, and (5) is digitally signed by the certification authority issuing it.
Certificate Data	Certificate requests and data related thereto (whether obtained from the Applicant or otherwise) in the CA's possession or control or to which the CA has access.
Certificate Management Process	Processes, practices, and procedures associated with the use of keys, software, and hardware, by which the CA verifies Certificate Data, issues Certificates, maintains a Repository, and revokes Certificates.
Certificate Management System	A system used by a CA or Delegated Third Party to process, approve issuance of, or store certificates or certificate status information, including the database, database server, and storage.

Certificate Policy	A set of rules that indicates the applicability of a named Certificate to a particular community and/or PKI implementation with common security requirements.
Certification Practice Statement	One of several documents forming the governance framework in which Certificates are created, issued, managed, and used.
Certificate Problem Report	Complaint of suspected Key Compromise, Certificate misuse, or other types of fraud, compromise, misuse, or inappropriate conduct related to Certificates.
Certificate Profile	A set of documents or files that defines requirements for Certificate content and Certificate extensions in accordance with Section 7 of the Baseline Requirements. e.g. a Section in a CA's CPS or a certificate template file used by CA software.
Certificate Revocation List	A regularly updated time-stamped list of revoked Certificates that is created and digitally signed by the CA that issued the Certificates.
Certificate Subject	The intended user of a PKC and its corresponding private key which may be either a device, a server or one of the Certificate Authorities in a Kyrio-governed PKI ecosystem.
Certificate Systems	The system used by a CA or Delegated Third Party in providing identity verification, registration and enrollment, certificate approval, issuance, validity status, support, and other PKI-related services.
Common Vulnerability Scoring System (CVSS)	A quantitative model used to measure the base level severity of a vulnerability (see http://nvd.nist.gov/home.cfm).
Compliance Audit	A periodic audit that a CA system undergoes to determine its conformance with the relevant Certificate Policy and Certificate Practice Statement.
Compromise	A violation of a Security Policy, in which an unauthorized disclosure of, or loss of control over, sensitive information has occurred. With respect to private keys, a Compromise is a loss, theft, disclosure, modification, unauthorized use, or other Compromise of the security of such private key.

Control	In the definitions of "Affiliate", "Parent Company", and "Subsidiary Company", which are reproduced here from [11], "Control" (and its correlative meanings, "controlled by" and "under common control with") means possession, directly or indirectly, of the power to: (1) direct the management, personnel, finances, or plans of such entity; (2) control the election of a majority of the directors; or (3) vote that portion of voting shares required for "control" under the law of the entity's Jurisdiction of Incorporation or Registration but in no case less than 10%.
Country	Either a member of the United Nations OR a geographic region recognized as a Sovereign State by at least two UN member nations.
Critical Security Event	Detection of an event, a set of circumstances, or anomalous activity that could lead to a circumvention of a Zone's security controls or a compromise of a Certificate System's integrity, including excessive login attempts, attempts to access prohibited resources, DoS/DDoS attacks, attacker reconnaissance, excessive traffic at unusual hours, signs of unauthorized access, system intrusion, or an actual compromise of component integrity.
Critical Vulnerability	system vulnerability that has a CVSS v2.0 score of 7.0 or higher according to the NVD or an equivalent to such CVSS rating (see https://nvd.nist.gov/vuln-metrics/cvss), or as otherwise designated as a Critical Vulnerability by the CA or the CA/Browser Forum.
Cross-Certified Subordinate CA Certificate	A certificate that is used to establish a trust relationship between two CAs. (Also known as a Cross Certificate.)
Cryptographic Module	The set of hardware, software, firmware, or some combination thereof that implements cryptographic logic or processes, including cryptographic algorithms, and is contained within the cryptographic boundary of the module [FIPS140].
CSPRNG	A random number generator intended for use in a cryptographic system.
Deactivation	The technical means to disable a Certificate Authority, including either erasing the private key from an HSM or disabling signing permissions on the HSM with that key.
Delegated Third Party	A natural person or Legal Entity that is not the CA but is authorized by the CA, and whose activities are not within the scope of the appropriate CA audits, to assist in the Certificate Management Process by performing or fulfilling one or more of the CA requirements found herein.

Device	An entity that uses a secure connection with another device for authentication prior to gaining local network access.
Disaster Recovery	Pertaining to recovery of the Certificate Authority and its normal operations in the event of a disaster.
Disaster Recovery Plan	A documented process or set of procedures to recover and protect a business IT infrastructure in the event of a disaster.
Distribution Point	An HTTP URL where CRL files are uploaded.
DNS CAA Email Contact	The email address defined in Appendix A.1.1 of [11].
DNS CAA Phone Contact	The phone number defined in Appendix A.1.2 of [11].
Domain Authorization Document	Documentation provided by, or a CA's documentation of a communication with, a Domain Name Registrar, the Domain Name Registrant, or the person or entity listed in WHOIS as the Domain Name Registrant (including any private, anonymous, or proxy registration service) attesting to the authority of an Applicant to request a Certificate for a specific Domain Namespace.
Domain Contact	The Domain Name Registrant, technical contact, or administrative contact (or the equivalent under a ccTLD) as listed in the WHOIS record of the Base Domain Name or in a DNS SOA record, or as obtained through direct contact with the Domain Name Registrar.
Domain Name	An ordered list of one or more Domain Labels assigned to a node in the Domain Name System.
Domain Namespace	The set of all possible Domain Names that are subordinate to a single node in the Domain Name System.
Domain Name Registrant	Sometimes referred to as the "owner" of a Domain Name, but more properly the person(s) or entity(ies) registered with a Domain Name Registrar as having the right to control how a Domain Name is used, such as the natural person or Legal Entity that is listed as the "Registrant" by WHOIS or the Domain Name Registrar.
Domain Name Registrar	A person or entity that registers Domain Names under the auspices of or by agreement with: (i) the Internet Corporation for Assigned Names and Numbers (ICANN), (ii) a national Domain Name authority/registry, or (iii) a Network Information Center (including their affiliates, contractors, delegates, successors, or assignees).
Expiry Date	The "Not After" date in a Certificate that defines the end of a Certificate's validity period.

Extended Validation Certificate	A certificate that contains subject information specified in the Extended Validation Guidelines and that has been validated in accordance with these guidelines specified here: https://cabforum.org/extended-validation/.
External Compliance Auditor	A member of an external organization that performs a Compliance Audit of the CAs under the specified Certificate Policy.
Front End / Internal Support System	A system with a public IP address, including a web server, mail server, DNS server, jump host, or authentication server.
Full System Backup	A CA system backup sufficient to recover from system failure.
Fully-Qualified Domain Name:	A Domain Name that includes the labels of all superior nodes in the Internet Domain Name System.
Government Entity	A government-operated legal entity, agency, department, ministry, branch, or similar element of the government of a country, or political subdivision within such country (such as a state, province, city, county, etc.).
High Risk Certificate Request	A Request that the CA flags for additional scrutiny by reference to internal criteria and databases maintained by the CA, which may include names at higher risk for phishing or other fraudulent usage, names contained in previously rejected certificate requests or revoked Certificates, names listed on the Miller Smiles phishing list or the Google Safe Browsing list, or names that the CA identifies using its own risk-mitigation criteria.
High Security Zone	A physical location where a CA's or Delegated Third Party's Private Key or cryptographic hardware is located.
Internal Name	A string of characters (not an IP address) in a Common Name or Subject Alternative Name field of a Certificate that cannot be verified as globally unique within the public DNS at the time of certificate issuance because it does not end with a Top Level Domain registered in IANA's Root Zone Database.
IP Address	A 32-bit or 128-bit label assigned to a device that uses the Internet Protocol for communication.
IP Address Contact	The person(s) or entity(ies) registered with an IP Address Registration Authority as having the right to control how one or more IP Addresses are used.
IP Address Registration Authority	The Internet Assigned Numbers Authority (IANA) or a Regional Internet Registry (RIPE, APNIC, ARIN, AfriNIC, LACNIC).

Issuing CA	In relation to a particular Certificate, the CA that issued the Certificate. This could be either a Root CA or a Subordinate CA.
Issuing System	A system used to sign certificates or validity status information.
Key Compromise	A Private Key is said to be compromised if its value has been disclosed to an unauthorized person, or an unauthorized person has had access to it.
Key Generation Facility	Air gapped facility that includes all Certificate Authorities covered by this CPS as well as all CA Equipment utilized by these CAs. There are no network connections from outside to this facility.
Key Generation Script	A documented plan of procedures for the generation of a CA Key Pair.
Key Pair	The Private Key and its associated Public Key.
Legal Entity	An association, corporation, partnership, proprietorship, trust, government entity or other entity with legal standing in a country's legal system.
Linting	A process in which the content of digitally signed data such as a Precertificate [RFC 6962], Certificate, Certificate Revocation List, or OCSP response, or data-to-be-signed object such as a tbsCertificate (as described in RFC 5280, Section 4.1.1.1) is checked for conformance with the profiles and requirements defined in these Requirements.
Multi-Factor Authentication	An authentication mechanism consisting of two or more of the following independent categories of credentials (i.e. factors) to verify the user's identity for a login or other transaction: something you know (knowledge factor), something you have (possession factor), and something you are (inherence factor). Each factor must be independent. Certificate-based authentication can be used as part of Multifactor Authentication only if the private key is stored in a Secure Key Storage Device.
Multi-Perspective Issuance Corroboration	A process by which the determinations made during domain validation and CAA checking by the Primary Network Perspective are corroborated by other Network Perspectives before Certificate issuance.
National Vulnerability Database (NVD)	A database that includes the Common Vulnerability Scoring System (CVSS) scores of security-related software flaws, misconfigurations, and vulnerabilities associated with systems (see http://nvd.nist.gov/home.cfm).
Network Perspective	Related to Multi-Perspective Issuance Corroboration. A system (e.g., a cloud-hosted server instance) or collection of network

	components (e.g., a VPN and corresponding infrastructure) for sending outbound Internet traffic associated with a domain control validation method and/or CAA check. The location of a Network Perspective is determined by the point where unencapsulated outbound Internet traffic is typically first handed off to the network infrastructure providing Internet connectivity to that perspective.
Object Identifier	A unique alphanumeric or numeric identifier registered under the International Organization for Standardization's applicable standard for a specific object or object class.
OCSP Responder	An online server operated under the authority of the CA and connected to its Repository for processing Certificate status requests. See also, Online Certificate Status Protocol.
Online Certificate Status Protocol	An online Certificate-checking protocol that enables relying-party application software to determine the status of an identified Certificate. See also OCSP Responder.
OWASP Top Ten	A list of application vulnerabilities published by the Open Web Application Security Project (see https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project).
Parent Company	A company that Controls a Subsidiary Company.
Penetration Test	A process that identifies and attempts to exploit openings and vulnerabilities on systems through the active use of known attack techniques, including the combination of different types of exploits, with a goal of breaking through layers of defenses and reporting on unpatched vulnerabilities and system weaknesses.
PKI Participant	An individual or organization that is one or more of the following: a CA, an RA or a Subscriber.
Policy Authority	The entity that establishes certificate policies.
Precertificate	As specified in [18], a Precertificate is constructed from the Publicly-Trusted Certificate to be issued by adding a special critical poison extension to the end-entity TBSCertificate (to ensure that the Precertificate cannot be validated by a standard X.509v3 client) and then signing the resulting TBSCertificate with either a special-purpose Precertificate Signing Certificate or, the CA certificate that will sign the final certificate.
Precertificate Signing Certificate	A CA certificate utilized to sign Precertificates and which is directly certified by the (root or intermediate) CA certificate that will ultimately sign the end-entity TBSCertificate yielding the end-entity certificate.

Primary Network Perspective	The Network Perspective used by the CA to make the determination of 1) the CA's authority to issue a Certificate for the requested domain(s) or IP address(es) and 2) the Applicant's authority and/or domain authorization or control of the requested domain(s) or IP address(es).
Private Key	The key of a Key Pair that is kept secret by the holder of the Key Pair, and that is used to create Digital Signatures and/or to decrypt electronic records or files that were encrypted with the corresponding Public Key.
Public Key	The key of a Key Pair that may be publicly disclosed by the holder of the corresponding Private Key and that is used by a Relying Party to verify Digital Signatures created with the holder's corresponding Private Key and/or to encrypt messages so that they can be decrypted only with the holder's corresponding Private Key.
Public Key Infrastructure	A set of hardware, software, people, procedures, rules, policies, and obligations used to facilitate the trustworthy creation, issuance, management, and use of Certificates and keys based on Public Key Cryptography.
Publicly-Trusted Certificate	A Certificate that is trusted by virtue of the fact that its corresponding Root Certificate is distributed as a trust anchor in widely-available application software.
Qualified Auditor	A natural person or Legal Entity that meets the requirements of Section 8.2.
Random Value	A value specified by a CA to the Applicant that exhibits at least 112 bits of entropy.
Registered Domain Name	A Domain Name that has been registered with a Domain Name Registrar.
Registration Authority (RA)	Any Legal Entity that is responsible for identification and authentication of subjects of Certificates, but is not a CA, and hence does not sign or issue Certificates. An RA may assist in the certificate application process or revocation process or both. When "RA" is used as an adjective to describe a role or function, it does not necessarily imply a separate body, but can be part of the CA.
Reliable Data Source	An identification document or source of data used to verify Subject Identity Information that is generally recognized among commercial enterprises and governments as reliable, and which was created by a third party for a purpose other than the Applicant obtaining a Certificate.

Reliable Method of Communication	A method of communication, such as a postal/courier delivery address, telephone number, or email address, that was verified using a source other than the Applicant Representative.
Relying Party	Any natural person or Legal Entity that relies on a Valid Certificate. An Application Software Supplier is not considered a Relying Party when software distributed by such Supplier merely displays information relating to a Certificate.
Repository	An online database containing publicly-disclosed PKI governance documents (such as Certificate Policies and Certification Practice Statements) and Certificate status information, either in the form of a CRL or an OCSP response.
Reserved IP Address	An IPv4 or IPv6 address that is contained in the address block of any entry in either of the following IANA registries: https://www.iana.org/assignments/iana-ipv4-special-registry/iana-ipv4-special-registry.xhtml https://www.iana.org/assignments/iana-ipv6-special-registry/iana-ipv6-special-registry.xhtml
Root CA	(In the issuance and management of Publicly-Trusted Certificates) The top level Certification Authority whose Root Certificate is distributed by Application Software Suppliers and that issues Subordinate CA Certificates. (Otherwise) A Certificate Authority at the top of a certificate hierarchy that possesses a self-signed certificate. Relying parties utilize a pre-installed Root CA certificate to validate a certificate chain and establish trust with each entity participating in secure electronic communications. Within this document, unless otherwise stated a reference to a Root CA refers only to Root CAs that are managed by us and are explicitly listed in the CPS.
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.
Root Certificate	The self-signed Certificate issued by the Root CA to identify itself and to facilitate verification of Certificates issued to its Subordinate CAs.
SANS Top 25	A list created with input from the SANS Institute and the Common Weakness Enumeration (CWE) that identifies the Top 25 Most Dangerous Software Errors that lead to exploitable vulnerabilities (see http://www.sans.org/top25-software-errors/).
Secret Share	A portion of the activation data needed to operate the private key, held by individuals called “Shareholders.” A threshold

	number of Secret Shares (n) out of the total number of Secret Shares (m) must be required to operate the private key.
Secure Key Storage Device	A device certified as meeting at least FIPS 140-2 level 2 overall, level 3 physical, or Common Criteria (EAL 4+).
Secure Zone	An area (physical or logical) protected by physical and logical controls that appropriately protect the confidentiality, integrity, and availability of Certificate Systems.
Security Support System	A system used to provide security support functions, which MAY include authentication, network boundary control, audit logging, audit log reduction and analysis, vulnerability scanning, and intrusion detection (Host-based intrusion detection, Network-based intrusion detection).
Shareholders	Holders of Secret Shares needed to operate a CA private key.
Sovereign State	A state or country that administers its own government, and is not dependent upon, or subject to, another power.
Subject	The natural person, device, system, unit, or Legal Entity identified in a Certificate as the Subject. The Subject is either the Subscriber or a device under the control and operation of the Subscriber.
Subject Identity Information	Information that identifies the Certificate Subject. Subject Identity Information does not include a domain name or an IP address listed in the subjectAltName extension or the Subject commonName field.
Subordinate CA	A Certification Authority whose Certificate is signed by the Root CA, or another Subordinate CA.
Subscriber	(In the issuance and management of Publicly-Trusted Certificates) A natural person or Legal Entity to whom a Certificate is issued and who is legally bound by a Subscriber Agreement or Terms of Use. (Otherwise) The entity who requests a Certificate (e.g., a manufacturer or Cable Operator). The Subscriber is capable of using, and is authorized to use, the private key that corresponds to the public key listed in the Certificate.
Subscriber Agreement	An agreement between the CA and the Applicant/Subscriber that specifies the rights and responsibilities of the parties.
Subsidiary Company	A company that is controlled by a Parent Company.
Subscriber Certificate	A digital certificate issued by a CA to a Subscriber.

Superior Entity	An organization that is external to the CA which sets forth either some or all of the requirements that are incorporated in the Certificate Policy and to which the CA is contractually bound.
System	One or more pieces of equipment or software that stores, transforms, or communicates data.
Technically Constrained Subordinate CA Certificate	A Subordinate CA certificate which uses a combination of Extended Key Usage and/or Name Constraint extensions, as defined within the relevant Certificate Profiles of [11], to limit the scope within which the Subordinate CA Certificate may issue Subscriber or additional Subordinate CA Certificates.
Terms of Use	Provisions regarding the safekeeping and acceptable uses of a Certificate issued in accordance with this CP/CPS when the Applicant/Subscriber is an Affiliate of the CA or is the CA.
Trusted Persons	Employees that are serving in one of the Trusted Roles for managing, administering or operating a CA as specified in Section 5.2.1
Trusted Positions	A position or a role that may be assigned to each Trusted Person.
Trusted Root CA Program	A program, typically operated by an Application Software Supplier, that defines and maintains a set of root CA certificates that are treated as trusted for the purpose of validating Certificates that are intended to be Publicly-Trusted Certificates.
Trustworthy System	Computer hardware, software, and procedures that are: reasonably secure from intrusion and misuse; provide a reasonable level of availability, reliability, and correct operation; are reasonably suited to performing their intended functions; and enforce the applicable security policy.
Unregistered Domain Name	A Domain Name that is not a Registered Domain Name.
Valid Certificate	A Certificate that passes the validation procedure specified in RFC 5280.
Validation Specialist	Someone who performs the information verification duties specified by this CP/CPS.
Validity Period	The validity period as defined within RFC 5280, Section 4.1.2.5: the period of time from notBefore through notAfter, inclusive.
Vulnerability Scan	A process that uses manual or automated tools to probe internal and external systems to check and report on the status of operating systems, services, and devices exposed to the network and the presence of vulnerabilities listed in the NVD, OWASP Top Ten, or SANS Top 25.

WHOIS	Information retrieved directly from the Domain Name Registrar or registry operator via the protocol defined in RFC 3912, the Registry Data Access Protocol defined in RFC 7482, or an HTTPS website.
Wildcard Certificate	A Certificate containing at least one Wildcard Domain Name in the Subject Alternative Names in the Certificate.
Wildcard Domain Name	A string starting with "*." (U+002A ASTERISK, U+002E FULL STOP) immediately followed by a Fully-Qualified Domain Name.
Zone	A subset of Certificate Systems created by the logical or physical partitioning of systems from other Certificate Systems.

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

This chapter specifies requirements for publication of PKCs and CRLs in a repository.

2.1 Repositories

All CAs that issue Certificates under this CP/CPS shall post all CA Certificates and CRLs issued by the CA in a repository that is publicly accessible on the Internet at http://certificates.pkiworks.com/Public/CRL/.

Subscriber Certificates are not required to be published in a publicly accessible repository.

This CP/CPS and its previous versions since the last Web of Trust audit shall be publicly accessible at http://certificates.pkiworks.com/Public/Documents/. Prior to the addition of our Certificate Authorities for Publicly-Trusted Certificates, only versions of the our Certificate Policy were public.

Publicly accessible URLs for the latest version of the CP/CPS document and the last audit report shall be submitted to CCADB.

This CP/CPS shall be reviewed and updated as necessary at least once every year, as required by the Baseline Requirements [11]. CA shall indicate that this has happened by incrementing the version number and adding a dated changelog entry, even if no other changes are made to the document.

2.1.1 (Deleted)

2.2 Publication of Certification Information

This CP/CPS is publicly accessible on a 24x7 basis as specified in Section 2.1. CA Certificates, OCSP Responder and CRLs shall be publicly available on a 24x7 basis at the locations specified in corresponding CRL Distribution Point and Authority Information Access certificate extensions. The same information (except for the OCSP Responder) can also be accessed from a URL specified in Section 2.1.

The CA shall adhere to the latest published version of this CP/CPS and shall protect information not intended for public dissemination. CAB Forum's Requirements ("Requirements") are directly incorporated into this CP/CPS for applicable Certificate Authorities capable of issuing Publicly-Trusted Certificates. In the event of any inconsistency between this document and Requirements, Requirements take precedence over this document.

The CA shall host test Web pages that allow Application Software Suppliers to test their software with Subscriber Certificates that chain up to each publicly trusted Root Certificate. At a minimum, the CA shall host separate Web pages using

Subscriber Certificates that are (i) valid, (ii) revoked, and (iii) expired. These web pages are listed in Section **Error! Reference source not found.**.

2.3 Time or Frequency of Publication

Changes to this CP/CPS shall be made publicly available within thirty (30) days of approval by the PA. The CA shall increment the version number and add a dated changelog entry in each CP/CPS revision, even if no other changes are made to the document.

CAs shall promptly publish (make available in the repository) subordinate Certificate Authority (Sub-CA) certificates after they are generated. For ecosystems where Root CA is operated by us, CA Certificates shall be made publicly available within three (3) business days after issuance.

For CAs that are included in one or more Trusted Root CA Programs, prior to the issuance of a Publicly-Trusted Subscriber Certificate, a Precertificate for the to-be-issued Certificate shall be published to at least 2 separate Certificate Transparency logs, if such publication is required by the applicable programs.

Publication requirements for CRLs are provided in Section 4.9.7.

2.4 Access Controls on Repositories

The CA Certificate repositories shall be public by default, unless specified otherwise by policy for a specific ecosystem.

The OCSP and CRL repositories shall be public by default, unless specified otherwise by policy for a specific ecosystem.

The CAs shall implement controls to prevent unauthorized addition, deletion, or modification of repository entries. Authorized CA Administrator personnel are the only users that will be able to perform those actions.

3. IDENTIFICATION AND AUTHENTICATION

This chapter specifies the requirements for Identification and Authentication (I&A) of the Certificate Subject and CA.

3.1 Naming

3.1.1 Type of Names

Certificate Subject Name shall be an X.501 Distinguished Name (DN) carried in the PKC. Additionally, there may be ecosystem-specific requirement for a unique name to be included in the SubjectAlternativeName extensions. Details are specified in the ecosystem-specific certificate profiles that are identified in Section 7.1.

3.1.2 Need for Names to be Meaningful

The Certificates issued pursuant to this CP/CPS are meaningful if the names that appear in the Certificates can be understood by the Relying Parties. Names used in the Certificates shall identify the object to which they are assigned in a meaningful way.

Subscriber Certificates shall contain meaningful names that represent the Subscriber in a way that is easily understandable for humans. For devices, this may be a MAC address, model number or serial number. The Subject name in CA Certificates shall match the issuer name in Certificates issued by the CA, as required by RFC 5280 [5].

3.1.3 Anonymity or Pseudonymity of Subscribers

CAs shall not issue anonymous or pseudonymous certificates.

3.1.4 Rules for Interpreting Various Name Forms

Rules for interpreting Distinguished Name forms are specified in X.501.

3.1.5 Uniqueness of Names

Name uniqueness for certificates issued by CAs shall be enforced. Each CA shall enforce name uniqueness within the X.500 name space within its domain. Name uniqueness is not violated when multiple certificates are issued to the same Subscriber. Name uniqueness is enforced for the entire Subject Distinguished Name of the certificate rather than a particular attribute (e.g., the common name). The CA shall identify the method for checking uniqueness of Subject Distinguished Names within its domain.

3.1.6 Recognition, Authentication, and Role of Trademarks

CAs operating under this policy shall not issue a certificate knowing that it infringes a trademark, service mark, trade names, company names, DBA names or any other intellectual property right of another or that a Certificate Applicant is presenting data for any unlawful purpose whatsoever. Certificate Applicants shall not use

names in their Certificate Applications and Subscriber Certificate requests that infringe upon the Intellectual Property Rights of others.

Certificate Applicants requesting Certificates shall be responsible for the legality of the information they present for verification and/or use in Certificates for any jurisdiction in which such content may be used or viewed. Any CA of ours shall not be required to determine whether a Certificate Applicant has Intellectual Property Rights in the name appearing in a Certificate Application or to arbitrate, mediate, or otherwise resolve any dispute concerning the ownership of any intellectual property rights, including, without limitation, rights in a domain name, trade name, trademark, or service mark, and any CA of ours shall be entitled, without liability to any Certificate Applicant, to reject or suspend any Certificate Application because of such dispute. The PA shall resolve disputes involving names and trademarks.

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

If the Subscriber generates the certificate key pair, then the CA shall prove that the Subscriber possesses the private key by verifying the Subscriber's digital signature on the PKCS #10 Certificate Signing Request (CSR) with the public key in the CSR.

If the key pair is generated by the CA on behalf of a Subscriber; then in this case, proof of possession of the private key by the Subscriber is not required.

3.2.2 Authentication of Organization Identity

This section is not applicable in the case when a Superior Entity is responsible for authenticating an organization.

Requests for Certificates which include an organization identity shall be verified using the criteria described below. The CA shall inspect any document relied upon under this section for alteration or falsification.

3.2.2.1 Identity

If the Subject Identity Information is to include the name of an organization, the CA's certificate issuance process shall authenticate the identity of the organization named in the Digital Certificate Authorization Agreement by confirming that the organization:

- Exists in a business database (e.g., Dun and Bradstreet), or alternatively, has organizational documentation issued by or filed with the applicable government (e.g., government issued business credentials) that confirms the existence of the organization, such as articles of incorporation, Certificate of Formation, Charter Documents, or a business license that allow it to conduct business. For Subscribers of Publicly-Trusted Certificates, CA may instead accept an Attestation Letter for identity and address verification.
- Conducts business at the address listed in the agreement

- Is not listed on any of the following U.S. Government denied lists: US Department of Commerce' Bureau of Industry and Security Embargoed Countries List, and the US Department of Commerce' Bureau of Industry and Security Denied Entities List

In addition, CA shall perform additional organization validation steps that are required by Superior Entity for a specific ecosystem, as specified in Section 7.1.

3.2.2.2 DBA/Tradename

If the Subject Identity Information is to include a DBA or tradename, the CA shall verify the Applicant's right to use the DBA/tradename using at least one of the following:

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

3.2.2.3 Verification of Country

If the subject:countryName field is present along with subject:organizationName, then the CA shall verify the country associated with the Subject using a method identified in Section 3.2.2.1.

If the subject:countryName field is present while subject:organizationName is not, one of the following country validation methods may be utilized by the CA:

- the ccTLD of the requested Domain Name
- information provided by the Domain Name Registrar

3.2.2.4 Validation of Domain Authorization or Control

This section is applicable only to the Issuing CAs of Publicly-Trusted Certificates in order to comply with [11].

This section defines the permitted processes and procedures for validating the Applicant's ownership or control of the domain.

FQDNs containing "onion" as the rightmost label are not supported.

Completed validations of Applicant authority may be valid for the issuance of multiple Certificates over time. In all cases, the validation must have been initiated within the time period specified in Section 4.2.1 of this document) prior to Certificate issuance. For purposes of domain validation, the term Applicant includes the Applicant's Parent Company, Subsidiary Company or Affiliate.

CAs shall maintain a record of which domain validation method, including relevant BR version number, they used to validate every domain.

FQDNs may be listed in Subscriber Certificates using dNSNames in the subjectAltName extension.

3.2.2.4.1 Validating the Applicant as a Domain Contact

This domain validation method shall not be used.

3.2.2.4.2 Email to Domain Contact

This domain validation method shall not be used.

3.2.2.4.3 Phone Contact with Domain Contact

This domain validation method shall not be used.

3.2.2.4.4 Constructed Email to Domain Contact

This domain validation method is currently not supported.

3.2.2.4.5 Domain Authorization Document

This domain validation method shall not be used.

3.2.2.4.6 Agreed-Upon Change to Website

This domain validation method is currently not supported.

3.2.2.4.7 DNS Change

Confirming the Applicant's control over the FQDN by confirming the presence of a Random Value in a DNS TXT record for an Authorization Domain Name.

The CA shall provide a Random Value unique to the Certificate request and shall not use the Random Value after 30 days.

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

Validations using this method are performed with Multi-Perspective Issuance Corroboration. To count as corroborating, a Network Perspective MUST observe the same challenge information (i.e. Random Value) as the Primary Network Perspective.

3.2.2.4.8 IP Address

This domain validation method is currently not supported.

3.2.2.4.9 Test Certificate

This domain validation method shall not be used.

3.2.2.4.10 TLS Using a Random Number

This domain validation method shall not be used.

3.2.2.4.11 Any Other Method

This domain validation method shall not be used.

3.2.2.4.12 Validating Applicant as a Domain Contact

Confirming the Applicant's control over the FQDN by validating the Applicant is the Domain Contact. This method may only be used if the CA is also the Domain Name Registrar, or an Affiliate of the Registrar, of the Base Domain Name.

This domain validation method is currently not supported.

3.2.2.4.13 Email to DNS CAA Contact

This domain validation method is currently not supported.

3.2.2.4.14 Email to DNS TXT Contact

This domain validation method is currently not supported.

3.2.2.4.15 Phone Contact with Domain Contact

This domain validation method shall not be used.

3.2.2.4.16 Phone Contact with DNS TXT Record Phone Contact

This domain validation method is currently not supported.

3.2.2.4.17 Phone Contact with DNS CAA Phone Contact

This domain validation method is currently not supported.

3.2.2.4.18 Agreed-Upon Change to Website v2

This domain validation method is currently not supported.

3.2.2.4.19 Agreed-Upon Change to Website – ACME

This domain validation method is currently not supported.

3.2.2.4.20 TLS Using ALPN

This domain validation method is currently not supported.

3.2.2.4.21 DNS Labeled with Account ID – ACME

This domain validation method is currently not supported.

3.2.2.5 Authentication for an IP Address

Our CAs issuing Publicly-Trusted Certificates do not currently support an IP Address as an identity provided within SubjectAltName extension.

3.2.2.6 Wildcard Domain Validation

Our CAs issuing Publicly-Trusted Certificates do not currently support issuing certificates with wildcard domain names.

3.2.2.7 Data Source Accuracy

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

- The age of the information provided,
- The frequency of updates to the information source,
- The data provider and purpose of the data collection,
- The public accessibility of the data availability, and
- The relative difficulty in falsifying or altering the data.

Databases maintained by the CA, its owner, or its affiliated companies do not qualify as a Reliable Data Source if the primary purpose of the database is to collect information for the purpose of fulfilling the validation requirements under Section 3.2.

3.2.2.8 CAA Records

As part of the process of issuing a Publicly-Trusted Certificate, and prior to the issuance of any Precertificates, the CA shall check for CAA records and follow the processing instructions found, for each dNSName in the subjectAltName extension of the certificate to be issued, as specified in RFC 8659. If the CA issues, they shall do so within the TTL of the CAA record, or 8 hours, whichever is greater.

When processing CAA records, CAs shall process the issue, issuewild, and iodef property tags as specified in RFC 8659, although they are not required to act on the contents of the iodef property tag.

CAs shall respect the critical flag and not issue a Precertificate if they encounter an unrecognized property tag with this flag set within a CAA record applicable to this CA's domain.

CAs shall not issue a Precertificate unless the CA determines that the certificate request is consistent with the applicable CAA RRset. Following CAA record validation, our CAs shall log a Precertificate in at least two public Transparency logs. Therefore, while staying consistent with [11], no additional CAA checking is performed by our CAs for Publicly-Trusted Certificates.

The CAs shall not issue a Publicly-Trusted Certificate following a CAA record lookup failure. CAs shall document potential issuances that were prevented by a CAA record in an event log.

3.2.2.9 Multi-Perspective Issuance Corroboration

In Section 3.2.2.4, whenever a method of validating domain control is described as performed with Multi-Perspective Issuance Corroboration, the method is performed according to the requirements in Section 3.2.2.9 of [11].

3.2.3 Authentication of Individual Identity

Our CA currently does not issue Subscriber Certificates that identify a natural person.

In the case when a Superior Entity is responsible for authenticating an organization, the CA shall receive a Digital Certificate Authorization Agreement from the Superior Entity either through certified mail or electronically via an authenticated email as specified by the Superior Entity. A Digital Certificate Authorization Agreement shall include a list of administrators with their contact information, including but not limited to:

- Company affiliation
- Email address
- Phone number(s)

In other cases, when a CA is responsible for authenticating an organization according to Section 7.1, the CA's certificate issuance process shall utilize a Reliable Method of Communication to authenticate the individual identity of the:

- Representative submitting the Digital Certificate Authorization Agreement and Certificate Application, is a duly authorized representative of the organization as an employee, partner, member, agent, etc. and is authorized to act on behalf of the organization
- Corporate Contact listed in the Digital Certificate Authorization Agreement is an officer in the organization and can act on behalf of the organization
- Administrator listed in the Digital Certificate Authorization Agreement and Certificate Application, is a duly authorized representative of the organization as an employee, partner, member, agent, etc. and is authorized to act on behalf of the organization.

The CA shall verify that any company website URL which may have been provided during Applicant's signup is not flagged as a dangerous website by Google at https://transparencyreport.google.com/safe-browsing/search. If any such website is flagged as dangerous, customer's application for a Certificate Requesting Account shall be rejected outright. An exception may be made in the case that Google publicly acknowledges their mistake and updates their website with a safe status for this Applicant's URL.

The CA shall also verify that none of the names of the corporate contacts provided by an Applicant appear on the Miller Smiles list at http://www.millersmiles.co.uk/scams.php. If any such name is associated with a phishing scam, the CA shall investigate further to determine if this organization contact was actually involved in the documented phishing scam. If a link to a phishing scam is found with a high degree of confidence, customer's application for a Certificate Requesting Account shall be rejected outright.

3.2.4 Non-verified Subscriber Information

Some subject name fields do not require verification by a CA or by a PA and will be specified by ecosystem-specific requirements. Non-verified information does not include the organization name.

Verified Subscriber information inside a Certificate Signing Request (CSR) is specified in ecosystem-specific requirements and certificate profiles that are listed in Section 7. All static fields in a certificate issuer and subject name as specified in a specific certificate profile shall be validated.

3.2.5 Validation of Authority

This section is not applicable in the case when a Superior Entity is responsible for authenticating an organization.

If the Applicant for a Certificate containing Subject Identity Information is an organization, the CA shall:

- Verify the identity of the Applicant's organization as specified in Section 3.2.2.1
- Establish a process that allows an Applicant to specify the individuals who may request Certificates as specified in Section 3.2.3.
- Use a Reliable Method of Communication to verify the authenticity of the Applicant Representative's certificate request.

If an Applicant specifies, in writing, the individuals who may request a Publicly-Trusted Certificate on the Applicant's behalf, the CA SHALL NOT accept any such certificate requests that are outside the Applicant's specification. The CA SHALL provide an Applicant with a list of its authorized certificate requesters upon the Applicant's verified written request.

The Root CA shall obtain the PA's approval prior to issuing Sub-CA Certificates.

3.2.6 Criteria for Interoperation

Cross-certificates are not currently supported.

3.3 Identification and Authentication for Rekey Requests

3.3.1 Identification and Authentication for Routine ReKey

CA and Subscriber Certificate re-key shall follow the same procedures as initial certificate issuance. Identity may be established through the use of the Subscriber's current valid signature key.

3.3.2 Identification and Authentication for Rekey After Revocation

Once a certificate has been revoked issuance of a new certificate is required, and the Subscriber shall go through the initial identity validation process in Section 3.2.

3.4 Identification and Authentication for Revocation Request

After a certificate has been revoked other than during a renewal or update action, the Subscriber is required to go through the initial registration process described in Section 3.2 to obtain a new certificate.

Revocation requests shall be authenticated and may be authenticated using that certificate's public key, regardless of whether or not the associated private key has been compromised.

Prior to the revocation of a Subscriber Certificate, the CA shall authenticate the request. Acceptable procedures for authenticating revocation requests submitted by a Subscriber include:

- Communication with the Subscriber providing reasonable assurances that the person or organization requesting revocation is, in fact the Subscriber. Depending on the circumstances, such communication may include one or more of the following: telephone, facsimile, e-mail, postal mail, or courier service.
- The representative is the authenticated corporate contact, administrator, legal, or technical contact.

We may initiate the process of revoking Subscriber Certificates issued by one of the CAs it operates. We will obtain approval from the PA prior to the actual revocation. If a Subscriber Certificate is revoked, we will provide a written notice and brief explanation of the revocation to the Subscriber.

4. CERTIFICATE LIFE CYCLE OPERATIONAL REQUIREMENTS

This chapter specifies the requirements for PKC life-cycle management by all entities in the PKI.

4.1 Certificate Application

The Certificate Application is a package consisting of the following:

- The Digital Certificate Authorization Agreement or Subscriber Agreement
- The Subscriber profile containing contact information
- The Naming Document, which specifies the content to be bound in the certificate
- Any associated fees

An RA shall include the processes, procedures, and requirements of the certificate application process in the CPS.

4.1.1 Who Can Submit a Certificate Application

An application for Subscriber Certificates shall be submitted by the Subscriber or an authorized representative of the Subscriber.

We may require a Subscriber requesting a Subordinate CA certificate to undergo its own WebTrust audit and to submit its CPS for approval. As of this revision, our CAs do not issue Subordinate CA certificates to third parties capable of issuing Publicly-Trusted Certificates. All Publicly-Trusted CAs under this CPS, including Sub-CAs, are operated directly by us.

In accordance with Section 5.5.2, the CA shall maintain an internal database of all previously revoked Certificates and previously rejected certificate requests due to suspected phishing or other fraudulent usage or concerns. The CA shall use this information to identify subsequent suspicious certificate requests and disable the corresponding certificate requesting accounts at the discretion of the CA.

4.1.2 Enrollment Process and Responsibilities

The enrollment process, for a Certificate Applicant, shall include the following:

- An executed Subscriber Agreement or Terms of Use, which may be electronic. In some ecosystems this same agreement is known as DCAA or Digital Certificate Authorization Agreement. See Section 9.6.3 for more information on this agreement.
- Providing the requested information
- Responding to authentication requests in a timely manner
- Submitting required payment

Communications in the enrollment process may be electronic or non-electronic, e.g. via postal mail.

After initial enrollment and prior to the issuance of a Certificate, the CA shall obtain from the Applicant a certificate request in a form prescribed by the CA and that complies with the signed Subscriber Agreement. One batch certificate request may suffice for multiple Certificates to be issued to the same Applicant, subject to the aging and updating requirement in Section 4.2.1, provided that each Certificate is supported by a valid, current certificate request signed by the appropriate Applicant Representative on behalf of the Applicant. The certificate request shall be submitted electronically using a cryptographically secure authenticated connection.

During the Applicant's initial account enrollment process, each Applicant shall agree that all subsequently submitted certificate requests contain information that is therein correct.

All communications among CAs/RAs supporting the Certificate Application and issuance process must be authenticated and protected from modification; any electronic transmission of shared secrets must be protected. Communications may be electronic or out-of-band and must protect the confidentiality and integrity of the data.

4.2 Certificate Application Processing

When the RA function is handled by us, it is the responsibility of the PA to verify that the information in a Certificate Application is accurate.

Following successful processing of a Certificate Application, requests for Publicly-Trusted Certificates require additional processing and validation steps by the CA as specified in Section 4.3.1.1 of this document, including among other actions validation of DNS CAA records.

For the purpose of CAA record checking, a CA of ours recognizes the following issuer domain names, when specified in the issue or issuewild property tags of CAA records, as permitting it to issue:

- pkiworks.com

4.2.1 Performing Identification and Authentication Functions

The identification and authentication functions shall meet the requirements described in sections 3.2 and 3.3.

The CA shall establish and follow a documented procedure for verifying all data requested for inclusion in the Certificate by the Applicant.

The Applicant provides all the information necessary for the CA to issue a Certificate compliant with this CP/CPS during initial enrollment and creation of the Applicant's Certificate Requesting Account, as well as in each individual certificate request.

In cases where the certificate request does not contain all the necessary information to issue a Certificate, such requests shall be rejected by the CA. The CA will advise an Applicant of the missing or invalid information with an opportunity to either update the Certificate Requesting Account or certificate request.

Applicant information for Publicly-Trusted Certificates shall include, but not be limited to, at least one Fully-Qualified Domain Name to be included in the Certificate's subjectAltName extension.

Section 6.3.2 limits the validity period of Subscriber Certificates. The CA MAY use the documents and data provided in Section 3.2 to verify certificate information. The CA may reuse previous domain validations for Publicly-Trusted Subscriber Certificates, provided that the CA completed all validation (including of domain and organization attributes) itself no more than 398 days prior to issuing the Certificate.

In no case may a prior validation be reused for a Publicly-Trusted Certificate if the data used in the prior validation was obtained more than the maximum time permitted for reuse of the data prior to issuing the Certificate.

After the change to any validation method specified in the Baseline Requirements [11], a CA may continue to reuse validation data collected prior to the change, or the validation itself, for up to 398 days unless otherwise specifically stated in the latest revision of [11].

For Publicly-Trusted Certificates, we develop, maintain, and implement documented procedures that identify and require additional verification activity for High Risk Certificate Requests prior to the Certificates' approval, as reasonably necessary to ensure that such requests are properly verified under the Baseline Requirements [11]. High Risk Certificate Requests are associated with Certificate Requesting Accounts that are flagged for suspicious activity as specified in Section 4.1.1.

A Delegated Third Party is not permitted to fulfill CA's obligations.

4.2.2 Approval or Rejection of Certificate Applications

CAs shall NOT issue Publicly-Trusted Certificates containing Internal Names as specified in [11].

An RA operated by us shall obtain PA's approval of a certificate application prior to issuing a new customer any digital certificates.

A PA will approve a certificate application if all of the following criteria are met:

- A fully executed Digital Certificate Authorization Agreement
- A completed and signed Naming Document

- Successful identification and authentication of all required contact information in the Subscriber profile
- Receipt of all requested supporting documentation
- Payment (if applicable) has been arranged
- Acceptance of the certificate application would not cause a violation of the CP/CPS

4.2.3 Time to Process Certificate Applications

CAs shall begin processing certificate applications within a reasonable time of receipt. There is no time stipulation to complete the processing of an application unless otherwise indicated in the relevant Digital Certificate Authorization Agreement.

4.3 Certificate Issuance

Upon receiving a request for a Certificate, the CA/RA must verify that the information in the Certificate Application is correct and accurate.

4.3.1 CA Actions During Certificate Issuance

To issue a certificate the CA shall have received the necessary information that includes the Naming Document containing certificate profile details and a PKCS #10 certificate signing request (CSR).

Upon receiving the request, the CAs shall:

- Verify the identity of the requester
- Verify the authority of the requester and the integrity of the information in the Certificate request
- Verify all domain names inside the SubjectAltName extension for a Publicly-Trusted Certificate
- Verify that information in a certificate request is consistent with static non-changing values in the customer's Naming Document
- Verify that the Public Key complies with requirements of sections 6.1.5 and 6.1.6.
- Create and sign a Certificate if all Certificate requirements have been met
- Make the Certificate available to the Subscriber after confirming that the Subscriber has formally acknowledged its obligations

Information received from a prospective Subscriber shall be verified before inclusion in a Certificate. The CA shall not issue a Subscriber Certificate if any of the above-mentioned validation steps fail.

CA shall set the notBefore field of a Subscriber Certificate to the actual time of issuance.

All Certificate issuances by a Root CA and creations of new Root CAs shall be first authorized by a CA Officer.

4.3.1.1 Additional CA Actions Prior to Issuance of a Publicly-Trusted Certificate

CA shall perform additional actions prescribed by [11] prior to issuing a Publicly Trusted Certificate as specified in the following subsections.

Certificate requests containing an FQDN that ends on ".onion" are not supported at the present time and shall be rejected.

4.3.1.1.1 CAA Record Validation

The CA shall look for all CAA records that are associated with the FQDN in a request for a Publicly-Trusted Certificate prior to issuing such a certificate according to [11]. The CA shall look for all possible subdomains associated with the specified FQDN with the exception of a root domain.

Following the CAA record search:

- If the public DNS system is not available and the CA is not able to get a response to DNS queries after at least 3 retries, the requested Certificate shall not be issued.
- If no CAA records applicable to the specified FQDN were found, then CAA record validation passes and CA may proceed with the additional verification and processing steps that may be needed to issue a certificate as specified in [11] and Section 7.1.

  Note that multiple domain names may need to be checked. For example, for

  FQDN = myserver.bigrock.mycompany.com

  It is necessary to check for existing CAA records for both bigrock.mycompany.com and my company.com domains and in that order.
- If CAA records applicable to the specified FQDN were found but none of them authorize the issuer domain "pkiworks.com" (in the value of the "issue" tag), that implies that a CA of ours is not authorized to issue certificates for such a domain and a Certificate shall not be issued.

If at least one of the CAA records found is for "pkiworks.com" and it doesn't include any unrecognized tags, CAA record validation passed and CA may proceed with the additional verification and processing steps that may be needed to issue a certificate as specified in [11] and Section 7.1.

4.3.1.1.2 Domain Validation

Domain associated with an FQDN in the SubjectAltName extension shall be validated as specified in Section 3.2.2.4

4.3.1.1.3 Generate and Submit Precertificates

Prior to issuing a Publicly-Trusted Certificate, a CA shall first generate a Precertificate, submit it to two or more different public Certificate Transparency logs and add signed and timestamped responses from both Certificate Transparency logs into a certificate extension of the TBSCertificate as defined in [18].

4.3.1.2 Linting of To-be-signed Certificate Content

We implement a Linting process to test the technical conformity of each to-be-signed Precertificate prior to signing it.

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

CAs shall notify Subscribers that they have created the requested Certificate(s), and provide Subscribers with access to the Certificate(s) by notifying them that their Certificate(s) are available and the means for obtaining them. The CA shall notify Subscribers via email upon issuance of the requested Certificate(s) and make the Certificate(s) available to the Subscriber via Subscriber's online account. The CA archives the Certificate(s) internally.

4.4 Certificate Acceptance

Certificates will be deemed valid immediately after issuance.

4.4.1 Conduct Constituting Certificate Acceptance

Any one of the following events constitute certificate acceptance by the Subscriber:

- Failure to object in a timely manner to the certificate or its content
- Explicit confirmation of the Certificate(s) via the Subscriber's online account

4.4.2 Publication of the Certificate by the CA

CA Certificates shall be published in a publicly available repository as specified in Section 2.1.

This policy makes no stipulation regarding publication of Subscriber Certificates.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

The Root CA operating under this CPS shall notify the PA whenever the Root CA issues a Sub-CA Certificate. This does not for example apply to a Root CA which is operated by a Superior Entity which has its own separate CP and CPS.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

Subscriber private key usage shall be specified through Certificate extensions, including the key usage and extended key usage extensions, in the associated Certificate. Subscribers shall protect their private keys from unauthorized use and shall discontinue use of the private key following expiration or revocation of the

Certificate. Subscribers shall promptly request that a Certificate be revoked if the Subscriber has reason to believe that there has been a Compromise of the Certificate private key.

Certificate use shall be consistent with the keyUsage field extensions included in the Certificate.

4.5.2 Relying Party Public Key and Certificate Usage

Relying Parties should assess:

- The restrictions on key and certificate usage specified in this CP/CPS and which are specified in critical certificate extensions, including the basic constraints and key usage extensions.
- The status of the certificate and all the CA Certificates in the certificate chain. If any of the Certificates in the Certificate Chain have been revoked, the Relying Party is solely responsible to determine whether reliance on a Certificate prior to revocation of a Certificate in the Certificate chain is reasonable. Any such reliance is made solely at the risk of the Relying party.

Relying Parties acknowledge the following:

- They are solely responsible for deciding whether or not to rely on the information in a Certificate, and agree that they have sufficient information to make an informed decision.
- To the extent permitted by applicable law, we disclaim all warranties regarding the use of any Certificates, including, but not limited to any warranty of merchantability or fitness for a particular purpose. In addition, we hereby limit our liability, and exclude all liability for indirect, special, incidental, and consequential damages.
- That reliance on Certificates is restricted to the purposes for which those Certificates were issued.

4.6 Certificate Renewal

Certificate renewal is the issuance of a new certificate for an existing key pair without changing any information in the certificate except the validity period and serial number.

4.6.1 Circumstances for Certificate Renewal

CA Certificates may be renewed to maintain continuity of Certificate usage. A CA Certificate may be renewed after expiration. The original CA Certificate may or may not be revoked, but shall not be further re-keyed, renewed, or modified.

A CA Certificate may be renewed if the CA's Superior Entity reconfirms the identity of the CA.

4.6.2 Who May Request Renewal

The following may request a Certificate renewal:

- An authorized representative of the Subscriber of the Certificate
- The CA may request a renewal on behalf of a Subscriber
- The CA may request a renewal of its own Certificate
- The PA may request renewal of CA Certificate

4.6.3 Processing Certificate Renewal Requests

Certificate renewal requests shall follow the same procedures as the initial Certificate issuance.

CA Certificate renewals shall be approved by the PA.

4.6.4 Notification of New Certificate Issuance to Subscriber

CAs shall notify Subscribers that they have created the requested Certificate(s), and provide Subscribers with access to the Certificate(s) by notifying them that their Certificate(s) are available and the means for obtaining them. See Section 4.3.2 for more details.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

The following conduct constitutes Certificate acceptance by the Subscriber:

- Downloading a Certificate
- Failure to object to the Certificate or its content

4.6.6 Publication of the Renewal Certificate by the CA

CA Certificates shall be published in a publicly available repository.

This CP/CPS makes no stipulation regarding publication of Subscriber Certificates.

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

The Root CA shall notify the PA whenever the Root CA issues a Sub-CA Certificate.

4.7 Certificate Rekey

Certificate re-key consists of creating a new certificate for a different key pair (and serial number) but can retain the contents of the original certificate's subjectName. Certificate re-key does not violate the requirement for name uniqueness. The new certificate may be assigned a different validity period, key identifiers, and/or be signed with a different key.

4.7.1 Circumstance for Certificate Rekey

CA Certificates may be re-keyed:

- To maintain continuity of Certificate usage

- For loss or compromise of original certificate's private key
- By a CA during recovery from key compromise

A certificate may be re-keyed after expiration. The original certificate may or may not be revoked, but shall not be further re-keyed, renewed, or modified.

Subscriber Certificates may be rekeyed prior to their expiration. The CA is not obligated to accept rekey requests for Subscriber Certificates for any reason other than pending expiration.

4.7.2 Who May Request Certification of a New Public Key

The following may request a certificate re-key:

- The Subscriber of the certificate or an authorized representative of the Subscriber
- The CA may request a re-key of its own certificate
- The CA may re-key its issued certificates during recovery from a CA key compromise
- The PA may request a re-key of a CA Certificate or Subscriber Certificates prior to their expiration

4.7.3 Processing Certificate Rekeying Requests

For certificate re-key, the CA shall confirm the identity of the Subscriber in accordance with the requirements specified in Section 3.2 for the authentication of an original Certificate Application.

CA Certificate re-key shall be approved by the PA.

4.7.4 Notification of New Certificate Issuance to Subscriber

Notification of issuance of a re-keyed certificate to the Subscriber shall be in accordance with Section 4.3.2.

4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate

Conduct constituting Acceptance of a re-keyed certificate shall be in accordance with Section 4.4.1.

4.7.6 Publication of the Re-keyed Certificate by the CA

Publication of a re-keyed certificate shall be in accordance with Section 4.4.2.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

Notification of the issuance of certificates shall be in accordance with Section 4.4.3.

4.8 Modification

Modifying a certificate means creating a new certificate that contains a different serial number and that differs in one or more other fields from the original certificate except for the public key and validity period fields.

4.8.1 Circumstance for Certificate Modification

CA Certificates may be modified:

- For a Subscriber organization name change or other Subscriber characteristic change
- To correct subject name attributes or extension settings.

A Certificate may be modified after expiration.

The original certificate may or may not be revoked, but shall not be further re-keyed, renewed, or modified. If not revoked, the CA will flag the certificate as inactive in its database but will not publish the certificate on a CRL.

Subscriber Certificate modifications are not supported.

4.8.2 Who May Request Certificate Modification

The following may request a certificate modification:

- The CA may request a Certificate modification of its own Certificate
- The PA may request modification of CA Certificates

4.8.3 Processing Certificate Modification Requests

For certificate modification requests, the CA shall confirm the identity of the Subscriber in accordance with the requirements specified in Section 3.2 for the authentication of an initial Certificate Application.

CA Certificate modification shall be approved by the PA.

4.8.4 Notification of New Certificate Issuance to Certificate Subject

Notification of issuance of a new certificate to the Subscriber shall be in accordance with Section 4.3.2.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

Conduct constituting Acceptance of a modified certificate shall be in accordance with Section 4.4.1.

4.8.6 Publication of the Modified Certificate by the CA

Publication of a modified certificate shall be in accordance with Section 4.4.2.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

Notification of the issuance of certificates shall be in accordance with Section 4.4.3.

4.9 Certificate Revocation and Suspension

CAs operating under this CP/CPS shall make public a description of how to obtain revocation information for the Certificates they publish. This information shall be given to Subscribers during Certificate request or issuance and shall be readily available to any potential Relying Party.

The following specifies formal operational requirements of PKC revocation procedures.

4.9.1 Circumstances for Revocation

A Certificate shall be revoked when the binding between the Subject and the Subject's public key defined within the Certificate is no longer considered valid.

Whenever any of the circumstances in the following subsections occur, the associated Certificate shall be revoked and placed on the CRL. Revoked Certificates shall be included on all new publications of the Certificate status information until the Certificates expire.

In addition, if it is determined subsequent to issuance of the new Certificate that a private key used to sign requests for one or more additional Certificates may have been Compromised at the time the requests for additional Certificates were made, all Certificates authorized by directly or indirectly chaining back to that Compromised key shall be revoked.

4.9.1.1 Reasons for Revoking a Subscriber Certificate

The CA shall revoke a Certificate if one or more of the following occurs and shall do so within 24 hours for Publicly-Trusted Certificates after:

1. The Subscriber or an authorized representative of the Subscriber asks for the Certificate to be revoked for any reason whatsoever.
2. The Subscriber notifies the CA that the original certificate request was not authorized and does not retroactively grant authorization.
3. The CA obtains evidence that the Subscriber's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise.
4. The CA is made aware of a demonstrated or proven method that can easily compute the Subscriber's Private Key based on the Public Key in the Certificate.
5. The CA obtains evidence that the validation of domain authorization or control for any Fully-Qualified Domain Name or IP address in the Publicly-Trusted Certificate should not be relied upon.

Note for ecosystems outside of the CAB Forum (for certificates that are not Publicly-Trusted), revocation due to any of the above events shall take place as soon as it is reasonable but not necessarily within 24 hours.

The CA shall revoke a Certificate if one or more of the following occurs:

1. Becoming aware that Certificate no longer complies with the requirements of Sections 6.1.5 and 6.1.6.
2. Agreement with the Subscriber has been terminated.
3. The CA obtains evidence that the Certificate was misused.
4. The CA is made aware that a Subscriber has violated one or more of its material obligations under the Subscriber Agreement or Terms of Use.
5. A prerequisite to issuance of the Certificate can be shown to be incorrect if:
    - Information in the Certificate is known, or reasonably believed, to be false
    - Certificate was issued to an entity other than the one named as the Subject of the Certificate without prior authorization of the entity named as the Subject of such Certificate
    - Any other circumstance that may reasonably be expected to affect the reliability, security, integrity or trustworthiness of the Certificate or the cryptographic key pair associated with the Certificate
6. The Subscriber has not submitted payment when due
7. The CA is made aware of any circumstance indicating that use of a Fully-Qualified Domain Name or IP address in the Publicly-Trusted Certificate is no longer legally permitted (e.g. a court or arbitrator has revoked a Domain Name Registrant's right to use the Domain Name, a relevant licensing or services agreement between the Domain Name Registrant and the Applicant has terminated, or the Domain Name Registrant has failed to renew the Domain Name).
8. The CA is made aware that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate Fully-Qualified Domain Name.
9. The CA is made aware of a material change in the information contained in the Certificate.
10. The CA is made aware that the Certificate was not issued in accordance with this document.
11. The CA determines or is made aware that any of the information appearing in the Certificate that becomes invalid or is inaccurate or misleading.
12. The CA's right to issue Certificates under a particular Issuing CA expires or is revoked or terminated, unless the CA has made arrangements to continue maintaining the CRL/OCSP Repository.
13. The CA is made aware of a demonstrated or proven method that exposes the Subscriber's Private Key to compromise or if there is clear evidence that the specific method used to generate the Private Key was flawed.
14. The continued use of that Certificate is harmful to the CA, the Superior Entity, Subscribers, or any of the other organizations that are under contract with the CA.
15. The CA finds that in the ordinary course of business that the certificate should be revoked.
16. In exigent and/or emergency situation.
17. Revocation is required according to this document.

18. If the CA becomes aware that Subscriber's Private Key corresponding to Subscriber Certificate has been communicated to an unauthorized person or an organization not affiliated with the Subscriber

After any of the above revocation causing events a Publicly-Trusted certificate should be revoked within 24 hours and shall be revoked within 5 days.

Note for ecosystems outside of the CAB Forum (for certificates that are not Publicly-Trusted), revocation due to any of the above events shall take place as soon as it is reasonable but not necessarily within 5 days.

In addition:

- Microsoft may request revocation of a certificate under a CA that is participating in the Microsoft Trusted Root Program. The CA must either revoke the certificate or request an exception from Microsoft within 24 hours of receiving Microsoft's notice. Microsoft will review submitted material and inform the CA of its final decision to grant or deny the exception at its sole discretion. In the event that Microsoft does not grant the exception, the CA must revoke the certificate within 24 hours of the exception being denied.

4.9.1.2 Reasons for Revoking a Subordinate CA Certificate

The Issuing CA shall revoke a Subordinate CA Certificate if one or more of the following occurs and for Publicly-Trusted certificates shall do so within seven (7) days if one or more of the following occurs:

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

10. Microsoft requests revocation of a CA certificate that is participating in the Microsoft Trusted Root Program. The CA must either revoke the certificate or request an exception from Microsoft within 24 hours of receiving Microsoft's notice. Microsoft will review submitted material and inform the CA of its final decision to grant or deny the exception at its sole discretion. In the event that Microsoft does not grant the exception, the CA must revoke the certificate within 24 hours of the exception being denied.
11. The Issuing CA becomes aware that Subordinate CA's Private Key corresponding to the Sub-CA certificate has been communicated to an unauthorized person or an organization not affiliated with the Subordinate CA.

Note for ecosystems outside of the CAB Forum (for Subordinate CA certificates that are not Publicly-Trusted), revocation due to any of the above events shall take place as soon as it is reasonable but not necessarily within 7 days.

In addition:

- If a Subordinate CA certificate participating in CCADB program is revoked, the CCADB must be updated to mark it as revoked, giving the reason why, within 24 hours for the revocation reason #3 above, and within 7 days for any other reason.

4.9.2 Who Can Request Revocation

Revocation requests may be made by:

- The Subscriber of the certificate or any authorized representative of the Subscriber
- The CA
- The PA
- Superior Entity
- An additional organization that may be overseeing a PKI ecosystem, if specified in Section 7.2.

Additionally, for Publicly-Trusted Certificates the following may submit Certificate Problem Reports informing the Issuing CA of reasonable cause to revoke the Certificate:

- Subscribers
- Relying Parties
- Application Software Suppliers
- Other third parties

4.9.3 Procedure for Revocation Request

The CA shall maintain a continuous 24x7 ability to accept and respond to revocation requests (which may be submitted by parties specified in Section 4.9.2) and Certificate Problem Reports. Refer to Section 1.5.2 for further details.

4.9.3.1 Revocation Initiated by the CA

For PKI ecosystems where a CA is permitted to initiate revocation, A Certificate revocation request shall identify the date of the request, the Certificate to be revoked, the reason for revocation, and allow the requestor to be authenticated.

Prior to the revocation of a Subscriber Certificate, the CA shall authenticate the request. Acceptable procedures for authenticating revocation requests include:

- Email communication with the Subscriber or the PA providing reasonable assurances that the person or organization requesting revocation is, in fact who they say they are
- The representative is the authenticated corporate contact, administrator, legal, or technical contact.

CAs are entitled to request the revocation of Subscriber Certificates within the CA's subdomain. CAs shall obtain approval from the PA prior to performing the revocation functions. The CA shall send a written notice and brief explanation for the revocation to the Subscriber.

The requests from CAs to revoke a CA Certificate shall be authenticated by the PA. Reason Code must be included in revocations for intermediate certificates. When there is a Superior Entity, the requests to revoke a CA Certificate shall be approved by the Superior Entity prior to revocation taking place.

If the revocation of an intermediate certificate chaining up to a root in Mozilla's root program is due to a security concern, as well as performing the actions defined in the CCADB Policy, a security bug must be filed in Bugzilla.

Upon revocation of a Certificate, the CA that issued the Certificate shall publish notice of such revocation in the CA's repository or issue it upon request from the PA.

In the case of Publicly Trusted Subscriber Certificates, the CA shall be capable of revoking any precertificate, including precertificates for which a Subscriber Certificate was never issued. OCSP service shall be capable of providing accurate status for serial numbers of precertificates that contain an OCSP URL in an AIA extension.

4.9.3.2 Revocation Initiated by the Superior Entity

For PKI ecosystems where a Superior Entity initiates revocation, the CA shall direct any revocation requests or any security incident reports from external sources to the Superior Entity. Furthermore, the CA may determine during its internal security incident investigation that revocation may be required and will promptly notify the Superior Entity.

Superior Entity will proceed with their own investigation which will differ per ecosystem and is out of scope of this CP/CPS. Once the Superior Entity makes a decision to revoke, prior to the actual revocation it will notify the CA of the upcoming revocation and the reason for the revocation. Acceptable procedures for authenticating revocation notice from Superior Entity include:

- Email communication with the PA providing reasonable assurances that the person or organization requesting revocation is, in fact who they say they are
- The representative is the authenticated corporate contact, administrator, legal, or technical contact

Upon revocation of a Certificate, the CA that issued the Certificate shall publish notice of such revocation in the CA's repository or issue it upon request from the PA.

4.9.4 Revocation Request Grace Period

Revocation requests should be submitted as promptly as possible within a reasonable time of becoming aware of a revocation circumstance listed in Section 4.9.1.

4.9.5 Time Within Which CA Must Process the Revocation Request

For PKI ecosystems where a Superior Entity initiates revocation, the time to begin investigation is out of scope of this document.

Within ecosystem-dependent period specified in Section 7.2 of receiving a revocation request or a Certificate Problem Report, the CA shall investigate the associated facts and circumstances and shall provide a preliminary report on its findings to all parties required by applicable ecosystem-dependent agreements, Subscriber agreements and Superior Entity agreements.

In the case of Publicly-Trusted Certificates, those parties include:

- Subscriber
- Any entity reporting the Certificate Problem Report or other revocation-related notice

After reviewing the facts and circumstances, the CA shall work with the above-mentioned parties to establish whether or not the certificate will be revoked, and if so, a date on which the CA will revoke the certificate. The period from receipt of the Certificate Problem Report or revocation-related notice to published revocation shall not exceed the time frame set forth in Section 4.9.1.1.

4.9.6 Revocation Checking Requirements for Relying Parties

Relying Parties should check the status of Certificates on which they wish to rely by checking the certificate status from OCSP Responder (where available) or on the

most recent CRL from the CA that issued the Certificate, published in the web-based repository.

CAs shall provide Relying Parties with information within the certificate CRL Distribution Point extension, if present, on how to find the appropriate CRL to check the revocation status of certificates issued by the CA. When this extension is not present, CAs shall provide Relying Parties with information on how to find the appropriate CRL to check the revocation status of Certificates issued by the CA.

Old CRLs may be retained by a Relying Party for the appropriate period of time specified in the CRL profile.

4.9.7 CRL Issuance Frequency

CRLs shall be issued periodically, even if there are no changes to be made, to ensure timeliness of information.

CAs shall update and reissue CRLs at frequency dictated by an ecosystem-specific CRL profile and within an ecosystem-specific time period after revoking a Certificate, as specified in Section 7.2.

The value of the nextUpdate field in the CRL shall be determined based on a ecosystem-specific CRL profile. Unless otherwise specified in an ecosystem-specific CRL profile, in the absence of a revocation event CRLs for offline CAs shall be updated at least once every twelve (12) months and CRLs for online CAs shall be updated at least once every two (2) months.

For a CA that is subject to the requirements of [11], we will publish a complete CRL within 24 hours of the CA issuing its first Certificate.

A CA that issues Publicly-Trusted Subscriber Certificates shall: (1) update and reissue CRLs at least once every seven (7) days if all Certificates include an Authority Information Access extension with an id-ad-ocsp accessMethod ("AIA OCSP pointer"); or four (4) days in all other cases; and (2) MUST update and publish a new CRL within twenty-four (24) hours after recording a Certificate as revoked. The value of the nextUpdate field of a published CRL shall not be more than ten (10) days beyond the value of the thisUpdate field.

For CAs that issue CA Certificates and are subject to the requirements of [11], we will continue issuing CRLs until one of the following is true: (1) all Subordinate CA Certificates containing the same Subject Public Key are expired or revoked; OR (2) the corresponding Subordinate CA Private Key is destroyed.

4.9.8 Maximum Latency for CRLs

CRLs should be published promptly after generation and the exact period is configurable and dependent on specific ecosystem requirements specified in Section 7.2. For ecosystems for which this period is not specified, CRLs shall be published within 24 hours of generation.

4.9.9 Online Revocation/Status Checking Availability

CRLs shall be published by each CA in a web-based repository that permits Relying Parties to make online inquiries regarding revocation. CAs shall provide Relying Parties with information on how to find the appropriate repository to pull down the latest CRL.

OCSP responders operated by us produce responses to status requests for Subscriber Certificates that: (1) conform to RFC6960 and (2) are signed by the Issuing CA of the Certificate(s) whose revocation status is being checked.

OCSP responders operated by us for providing the revocation status of Publicly Trusted Certificates comply with the technical requirements specified in Section 4.9.9 of [11].

OCSP responders operated by us produce responses to status requests for Sub-CA Certificates that: (1) conform to RFC6960 and (2) are signed by the OCSP Responder with a certificate that chains to the CA which issued the Sub-CA certificate.

We may restrict OCSP responders we operate to accepting only OCSP requests containing exactly one queried certificate serial number.

4.9.10 Online Revocation Checking Requirements

A Relying Party should check the status of a certificate on which they wish to rely. Status check shall be performed via OCSP protocol (when the certificate contains an AIA extension with an OCSP URL) or by verifying that certificate is not found on a current non-expired CRL. Relying Party is responsible for downloading the latest CRL from an online repository.

OCSP responders operated by the CA shall support both HTTP GET and HTTP POST methods specified in RFC 6960. OCSP Responder may only be available for some of the ecosystems covered by this CP/CPS and the corresponding OCSP profiles for each supported ecosystem are specified in Section 7.3.

OCSP Responder shall obtain the latest certificate status information from each supported CA at least once every hour and shall remove any previously cached signed OCSP Responses which are determined to have an out-of-date status.

For CAs subject to the requirements of [11], we provide the status of Subordinate CA Certificates via OCSP. Certificate status information for such Subordinate CAs is updated at least every twelve months, and within 24 hours after a Subordinate CA Certificate is revoked.

OCSP responders operated by the CA shall conform to the applicable technical requirements in [11].

4.9.11 Other Forms of Revocation Advertisements Available

No stipulation.

4.9.12 Special Requirements re Key Compromise

We use commercially reasonable efforts to notify potential Relying Parties if it discovers or suspects the compromise of a Private Key. This is one of the possible events that result in certificate revocation as specified in Section 4.9.1.

A Private Key is considered to be compromised when one of the following events occurs:

- The CA obtains evidence that the Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise.
- The CA is made aware of a demonstrated or proven method that can easily compute the Private Key based on the Public Key in the Certificate.
- The CA is made aware of a demonstrated or proven method that exposes the Private Key to compromise or if there is clear evidence that the specific method used to generate the Private Key was flawed.
- If the CA becomes aware that Subscriber's Private Key corresponding to Subscriber Certificate has been communicated to an unauthorized person or an organization not affiliated with the Subscriber

Reports of private key compromise by third parties are accepted by email. A report must be accompanied by verifiable evidence that the alleged compromise has occurred. Acceptable forms of evidence include:

- a CSR (certificate signing request) with the Common Name "Proof of Key Compromise for CommScope", signed using the allegedly-compromised private key;
- a copy of the allegedly-compromised private key.

Technical and other Information related to the submission of such reports is available at https://cert.pkiworks.com/Public/SecurityIncidentReport/.

4.9.13 Circumstances for Suspension

PKC suspension is not supported under this CP/CPS.

4.9.14 Who can Request Suspension

No stipulation.

4.9.15 Procedure for Suspension Request

No stipulation.

4.9.16 Limits on Suspension Period

No stipulation.

4.10 Certificate Status Services

4.10.1 Operational Characteristics

Revocation entries on a CRL or OCSP Response shall not be removed until after the Expiry Date of the revoked Certificate.

4.10.2 Service Availability

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

The CA shall maintain an online 24x7 Repository that application software can use to automatically check the current status of all unexpired Certificates issued by the CA. The availability of the revocation status of Certificates via OCSP is applicable only when the Certificates involved contain an OCSP URL in an AIA extension.

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

4.10.3 Optional Features

No stipulation.

4.11 End of Subscription

End of subscription shall be stipulated in the Digital Certificate Authorization Agreement.

For Certificates that have expired prior to or upon end of subscription, revocation is not required. Unexpired CA Certificates shall be revoked at the end of the subscription when required by the Superior Entity.

4.12 Key Escrow and Recovery

4.12.1 Key Escrow and Recovery Policy and Practices

No stipulation.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

No stipulation.

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

All entities performing CA functions shall implement and enforce the following physical, procedural, logical, and personnel security controls for a CA.

5.1 Physical Controls

CA Equipment shall be protected from unauthorized access while the cryptographic module is installed and activated. The CA shall implement physical access controls to reduce the risk of equipment tampering even when the cryptographic module is not installed and activated. CA cryptographic tokens shall be protected against theft, loss, and unauthorized use.

All physical control requirements specified below apply equally to the CAs and any remote workstations used to administer the CAs, except where specifically noted.

5.1.1 Site Location and Construction

All CA operations shall be conducted within a physically protected environment that deters, prevents, and detects unauthorized use of, access to, or disclosure of sensitive information and systems. The location and construction of the facility housing the CA equipment, as well as sites housing remote workstations used to administer the CAs, shall be consistent with facilities used to house high value, sensitive information. The site location and construction, when combined with other physical security protection mechanisms such as security locks and intrusion sensors, shall provide robust protection against unauthorized access to the CA Equipment and records.

Root CA Systems are maintained in a High Security Zone and in an offline state or air-gapped from all other networks.

5.1.2 Physical Access

Access to each tier of physical security shall be auditable and controlled so that only authorized personnel can access each tier.

CAs shall control access to their facilities including:

- Minimizing exposure of privileged functions through definition of function-specific roles or authorization groups
- Access control enforcement of these roles or groups
- Use of proximity card identification badges
- Logging of access into and out of the CA facilities
- The use of tamper resistant locks to detect break-ins or unauthorized access to physical security tiers within the facility
- Automated notification to outside alarm monitoring agency of a potential security breach of CA facilities
- Video surveillance

At a minimum, the physical access controls for CA Equipment, as well as remote workstations used to administer the CAs, shall:

- Ensure that no unauthorized access to the hardware is permitted
- Ensure that all removable media and paper containing sensitive plaintext information is stored in secure containers
- Ensure an access log is maintained and inspected periodically
- Require two-person physical access control to the cryptographic module
- Require two-person logical access control to the computer systems or software that are connected to the cryptographic module

When not in use, removable cryptographic modules, activation information used to access or enable cryptographic modules, and CA Equipment shall be placed in secure containers. Activation data shall be either memorized or recorded and stored in a manner commensurate with the security afforded the cryptographic module, and shall not be stored with the cryptographic module or removable hardware associated with remote workstations used to administer the CA.

A security check of the CA facilities housing the CA Equipment or remote workstations used to administer the CAs shall occur if the facility is to be left unattended. At a minimum, the check shall verify the following:

- The CA Equipment is in a state appropriate to the current mode of operation (e.g., that cryptographic modules are in place when —open, and secured when —closed, and for the CA, that all equipment other than the repository is shut down)
- Any security containers are properly secured
- Physical security systems (e.g., door locks or vent covers) are functioning properly
- The area is secured against unauthorized access

5.1.3 Power and Air Conditioning

CA facilities shall be equipped with redundant power, backed up by uninterruptable power supply and by a generator sufficiently large to support the power load for the data center and to ensure continuous, uninterrupted access to electric power. Also, these facilities shall be equipped with primary and backup heating/ventilation/air conditioning systems to control temperature and relative humidity.

The CA shall have backup capability sufficient to lock out input, finish any pending actions, and record the state of the equipment automatically before lack of power or air conditioning causes a shutdown. The repositories (containing CA Certificates and CRLs) shall be provided with uninterrupted power sufficient for a minimum of six (6) hours of operation in the absence of commercial power, to maintain availability and avoid denial of service.

5.1.4 Water Exposures

CA facilities shall be constructed, equipped and installed, and procedures shall be implemented, to prevent floods or other damaging exposure to water. Potential water damage from fire prevention and protection measures (e.g., sprinkler systems) are excluded from this requirement.

5.1.5 Fire Prevention and Protection

CA facilities shall be constructed and equipped, and procedures shall be implemented, to prevent and extinguish fires or other damaging exposure to flame or smoke. These measures shall meet all local applicable safety regulations.

5.1.6 Media Storage

CAs shall protect the media holding back ups of critical system data or any other sensitive information from water, fire, or other environmental hazards, and shall use protective measures to deter, detect, and prevent the unauthorized use of, access to, or disclosure of such media.

CAs shall protect the media holding sensitive data according to the appropriate data classification level using the approved storage locations, access controls and security protections.

5.1.7 Waste Disposal

CAs shall implement procedures for the disposal of waste (paper, media, or any other waste) to prevent the unauthorized use of, access to, or disclosure of waste containing Confidential/Private Information.

CA media and documentation that are no longer needed for operations shall be destroyed in a secure manner. For example, paper documentation shall be shredded, burned, or otherwise rendered unrecoverable.

5.1.8 Off-Site Backup

CAs shall maintain backups of critical system data or any other sensitive information, including Audit Data, in a secure off-site facility. Full System Backups sufficient to recover from system failure shall be made on a periodic schedule. Backups are to be performed and stored off-site not less than once per week. At least one Full System Backup copy shall be stored at an off-site location (separate from CA Equipment). Only the latest Full System Backup need be retained.

The Full System Backup shall be stored at a site with physical and procedural controls commensurate to that of the operational CA. It must be stored at a site with a minimum of three (3) physical and procedural controls.

When a backup is stored in encrypted form, it is sufficient to protect the corresponding backup decryption keys and/or devices with the physical and procedural controls commensurate to that of the operational CA. The site for

storage of the corresponding decryption keys and/or devices may be at a different location from the location of the backups.

5.2 Procedural Controls

Procedural controls are requirements on roles that perform functions that can introduce security problems if not carried out properly, whether accidentally or maliciously. The people selected to fill these roles shall be extraordinarily responsible, or the integrity of the CA will be weakened. The functions performed in these roles form the basis of trust for the entire PKI. Two approaches are taken to increase the likelihood that these roles can be successfully carried out. The first ensures that the person filling the role is trustworthy and properly trained. The second distributes the functions among more than one person, so that any malicious activity would require collusion.

5.2.1 Trusted Roles

Employees that are designated to manage the CA's trustworthiness shall be considered to be "Trusted Persons" serving in "Trusted Positions." Persons seeking to become Trusted Persons shall meet the screening requirements of Section 5.3.2 prior to gaining access or performing tasks of a Trusted Person.

CAs shall consider the categories of their personnel identified in this Section as Trusted Persons having a Trusted Position. Trusted Persons include all employees, contractors, and consultants that have access to or control authentication or cryptographic operations. They are assigned to exactly one of the following Trusted Roles that include but are not limited to:

- CA Administrator – administration, maintenance, creation and destruction of hardware and software that is relevant to the operation of the CAs covered under this CP/CPS.
- CA Officer – oversees and approves the CA operation and policies, including this document
- Registration Officer – handles Subscriber Certificate requests and revocation requests for already vetted and registered Subscribers
- Auditor: maintains and reviews audit logs and performs internal Compliance Audits.

5.2.2 Number of Persons Required per Task

Multiparty control procedures are designed to ensure that at a minimum, two Trusted Persons are required to have either physical or logical access to the CA. Access to CA cryptographic hardware shall be strictly enforced by multiple Trusted Persons throughout its lifecycle, from incoming receipt and inspection to final logical and/or physical destruction. Once a CA device is activated with operational keys, further access controls shall be invoked to maintain split control over both physical and logical access to the device. Persons with physical access to CA modules do not hold "Secret Shares" to activate the CA and vice versa.

Two or more persons are required for the following tasks:

- Access to CA hardware
- Management of CA cryptographic hardware
- CA key generation and CA Certificate renewals
- CA signing key activation
- CA private key backup and access to the CA backup keys
- Certificate revocation may require two or more persons for some ecosystems

Where multiparty control is required, at least one of the participants shall be an Administrator. All participants shall serve in a trusted role as defined in Section 5.2.1. CAs shall establish, maintain, and enforce rigorous control procedures to ensure the segregation of duties based on job responsibility and to ensure that multiple Trusted Persons are required to perform sensitive tasks.

The private keys of CAs involved in the issuance of Publicly-Trusted Certificates shall be backed up, stored, and recovered only by personnel in trusted roles using multiparty control in a physically secured environment.

Other manual operations such as the validation and issuance of Certificates, not issued by an automated validation and issuance system, require the participation of at least 2 Trusted Persons, or a combination of at least one Trusted Person and an automated validation and issuance process. Manual operations for Key Recovery may optionally require the validation of two (2) authorized Administrators.

5.2.3 Identification and Authentication for Each Role

CAs shall confirm the identity and authorization of all personnel seeking to become Trusted Persons before such personnel are:

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

Authentication of identity shall include the personal (physical) presence of such personnel before Trusted Persons performing HR or security functions within an entity and a check of well-recognized forms of identification, such as passports and driver's licenses. The authentication to establish the first Trusted Person shall be performed by a representative from Human Resources. Identity shall be further confirmed through background checking procedures in Section 5.3.

5.2.4 Roles Requiring Separation of Duties

Roles requiring Separation of duties include (but are not limited to) all of the roles that are listed in Section 5.2.1 of this document.

No individual shall have more than one trusted role. CA shall have in place procedure to identify and authenticate its users and shall ensure that no user identity can assume multiple roles. No individual shall have more than one identity.

5.3 Personnel Controls

5.3.1 Qualifications, Experience, and Clearance Requirements

CAs shall require that personnel assigned to Trusted roles have the requisite background, qualifications, and experience or be provided the training needed to perform their prospective job responsibilities competently and satisfactorily. The requirements governing the qualifications, selection and oversight of individuals who operate, manage, oversee, and audit the CA shall be clearly documented, observed and made available for external audits. Their identities shall be verified according to Section 5.2.3 prior to performing any function associated with a Trusted Role.

5.3.2 Background Check Procedures

CAs shall conduct background check procedures for personnel tasked to become Trusted Persons. These procedures shall be subject to any limitations on background checks imposed by local law. To the extent one of the requirements imposed by this section cannot be met due to a prohibition or limitation in local law, the investigating entity shall utilize a substitute investigative technique permitted by law that provides substantially similar information, including but not limited to obtaining a background check performed by an applicable agency. Background investigations may include a:

- Current Address and previous addresses
- Confirmation of previous employment
- Confirmation of the highest or most relevant educational degree obtained (Education Report)
- Search of criminal records (Felony, Misdemeanor and Federal crime)
- Social Security Number trace

Factors revealed in a background check that may be considered grounds for rejecting candidates for Trusted Positions or for taking action against an existing Trusted Person (all subject to and in accordance with applicable law) may include but is not limited to the following:

- Misrepresentations made by the candidate or Trusted Person
- Certain criminal convictions

Background checks shall be repeated for personnel holding Trusted Positions at least every five (5) years.

5.3.3 Training Requirements

CAs shall provide their personnel with the requisite on-the-job training needed for their personnel to perform their job responsibilities relating to CA operations competently and satisfactorily. They shall also periodically review their training programs, and their training shall address the elements relevant to functions performed by their personnel.

Training programs shall address the elements relevant to the particular environment of the person being trained, including, without limitation:

- Security principles and mechanisms of the CA and the its environment
- Basic Public Key Infrastructure knowledge, authentication and vetting policies and procedures (including the CA's Certificate Policy and/or Certification Practice Statement)
- Common threats to the information verification process (including phishing and other social engineering tactics)
- Hardware and software versions in use
- All duties the person is expected to perform
- Incident and Compromise reporting and handling
- Disaster recovery and business continuity procedures
- The stipulations of this policy

The CA SHALL maintain records of such training and ensure that personnel entrusted with Validation Specialist duties maintain a skill level that enables them to perform such duties satisfactorily.

The CA SHALL document that each Validation Specialist possesses the skills required by a task before allowing the Validation Specialist to perform that task.

The CA SHALL require all Validation Specialists to pass an examination provided by the CA on the information verification requirements outlined in this document.

5.3.4 Retraining Frequency and Requirements

CAs shall provide refresher training and updates to their personnel to the extent and frequency required to ensure that such personnel maintain the required level of proficiency to perform their job responsibilities competently and satisfactorily.

All individuals responsible for PKI roles shall be made aware of changes in the CA operation. Any significant change to the operations shall have a training (awareness) plan, and the execution of such plan shall be documented. Examples of such changes are CA software or hardware upgrade, changes in automated security systems, and relocation of equipment.

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

5.3.5 Job Rotation Frequency and Sequence

No stipulation.

5.3.6 Sanctions for Unauthorized Actions

CAs shall establish, maintain, and enforce policies for the discipline of personnel following unauthorized actions. Disciplinary actions may include measures up to and including termination and shall be commensurate with the frequency and severity of the unauthorized actions.

5.3.7 Independent Contractor Requirements

Short-term contractors performing work inside the CA facilities shall be escorted by authorized CA Trusted Persons at all times.

From time to time, we also hire long-term contractors that may take on a CA operational role. Those types of contractors shall be subject to exact same hiring practice, background checks and training as regular employees of ours. All requirements for permanent personnel of ours that work in the CA facilities or otherwise participate in the operation and management of our CA operation equally apply to contractors that are in that same role.

5.3.8 Documentation Supplied to Personnel

CAs shall give their personnel the requisite training and documentation needed to perform their job responsibilities competently and satisfactorily.

5.4 Audit Logging Procedures

Audit log files shall be generated for all events relating to the security of the CA. Where possible, the audit logs shall be automatically collected. Where this is not possible, a logbook, paper form, or other physical mechanism shall be used. All CA audit logs, both electronic and non-electronic, shall be retained and made available during audits.

5.4.1 Types of Events Recorded

At a minimum, for each auditable event the record shall include:

- The type and description of event;
- The time the event occurred;
- A success or failure indication for signing;
- The identity of the equipment operator who initiated the action or of the person making the journal record, whichever is most applicable

All auditing capabilities of the CA operating system and applications shall be enabled during installation. All audit logs, whether recorded automatically or manually, shall contain the date and time, the type of event, and the identity of the entity that caused the event.

Both CA private keys and Subscriber private keys shall not be recorded into any log in any form.

CAs shall record in audit log files all events relating to the security of the CA system, including, without limitation:

- Physical Access / Site Security:
    - Personnel access to room housing CA

    - Successful and unsuccessful access attempts to the PKI system
    - Known or suspected violations of physical security
    - Electrical power outages
    - PKI and security system actions performed
    - Security profile changes
    - Firewall and router activities
    - Records of each Vulnerability Scan and Penetration Test performed
- CA Configuration:
    - CA hardware configuration
    - Installation of the operating system
    - Installation, update and removal of the software on a Certificate System
    - System configuration changes and maintenance
    - Installation of hardware cryptographic modules
    - Cryptographic module lifecycle management-related events (e.g., receipt, use, de-installation, and retirement)
    - Any time cryptographic keys connected to the operation of the CA are being accessed
    - Introduction of new Certificate Profiles and retirement of existing Certificate Profiles
- Account Administration:
    - System Administrator accounts
    - Roles and users added or deleted to the CA system
    - Changes of affiliation of an entity
    - Access control privileges of user accounts
    - Attempts to create, remove, set passwords or change the system privileges of the privileged users (trusted roles)
    - Attempts to delete or modify audit logs
    - Changes to the value of maximum authentication attempts
    - Resetting operating system clock
- CA Operational events:
    - CA Certificate requests,
    - Requests (including approvals and rejections) for renewal, re-key and revocation of CA Certificates
    - CA Key generation, including identity of HSM(s) where the key is stored
    - CA Certificate distribution
    - CA Key backups and archival
    - CA Key recovery
    - Generation of Certificate Revocation Lists and OCSP entries for CA Certificates
    - Start-up and shutdown of CA systems and applications
    - Changes to CA details or keys
    - Records of the destruction of media containing key material, activation data, or personal Subscriber information)

    - All records of security incidents that pertain to the CA, including compromises of a CA private key
    - Key Ceremony procedures for creation, destruction or modifications to a CA. Log identities of all Trusted Persons participating in each key ceremony, including Trusted Persons handling any keying material and custody of keys and devices or media holding keys.
    - System crashes, hardware failures and other anomalies
- Subscriber Certificate lifecycle events:
    - Receipt, approvals and rejections of certificate requests, including initial certificate requests, renewal, rekey and revocation requests as may be applicable to each ecosystem
    - All verification activities stipulated in this document
    - Details of CAA record checking
    - Issuance
    - Key distribution
    - Re-key
    - Renew
    - Generation and issuance of CRLs and OCSP entries
    - Archival and backup of private keys and certificates to store off site
    - Multi-Perspective Issuance Corroboration attempts from each Network Perspective
    - Multi-Perspective Issuance Corroboration quorum results for each attempted domain name represented in a Certificate request
- Trusted employee events:
    - Logon and logoff
    - Attempts to create, remove, set passwords or change the system privileges of the privileged users
    - Unauthorized attempts to access the CA system
    - Unauthorized attempts to access system files
    - Failed read and write operations on the Certificate(internal CA errors in attempting to generate a certificate)
    - Personnel changes (adding or removing a Trusted Person)
- Token events:
    - Serial number of tokens shipped to Subscriber (if applicable)
    - Account Administrator Certificates (if applicable)
    - Shipment of tokens (if applicable)
    - Tokens driver versions (if applicable)

5.4.2 Frequency of Processing Log

CAs shall review their Audit logs in response to alerts based on irregularities and incidents within their systems. CAs shall review the Audit logs periodically and shall compare their Audit logs with supporting manual and electronic logs when any action is deemed suspicious. The log review period shall be at least once every three (3) months.

Audit log processing shall consist of a review of the Audit logs and documenting the reason for all significant events in an Audit log summary. Audit log reviews shall include a verification that the log has not been tampered with, a brief inspection of all log entries, and a more thorough investigation of any alerts or irregularities in the logs. Actions taken based on Audit log reviews shall be documented.

5.4.3 Retention Period for Audit Log

Audit logs shall be retained onsite at least two (2) months after processing and thereafter may be archived. Archive records shall be retained for ten (10) years. The individual who removes Audit logs from the CA system shall be different from the individuals who, in combination, command the CA signature key.

5.4.4 Protection of Audit Log

Audit logs shall be protected from unauthorized viewing, modification, deletion, or other tampering. CA system configuration and procedures shall be implemented together to ensure that only authorized people archive or delete security Audit data. Procedures shall be implemented to protect archived data from deletion or destruction before the end of the security Audit data retention period.

Electronic audit logs shall be restricted to specific computer system users and/or groups of users such that unauthorized applications or users cannot insert events into this log.

5.4.5 Audit Log Backup Procedures

Incremental backups of Audit logs shall be created frequently, at least monthly.

5.4.6 Audit Collection System (Internal vs. External)

The audit log collection system may or may not be external to the CA system. Automated audit processes shall be invoked at system or application startup and cease only at system or application shutdown. Audit collection systems shall be configured such that security audit data is protected against loss (e.g., overwriting or overflow of automated log files). Should it become apparent that an automated audit system has failed, and the integrity of the system or confidentiality of the information protected by the system is at risk, operations shall be suspended until the problem has been remedied.

5.4.7 Notification to Event-Causing Subject

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

5.4.8 Vulnerability Assessments

The CA shall perform routine self-assessments of security controls for vulnerabilities. Events in the audit process are logged, in part, to monitor system vulnerabilities. An assessment of the vulnerabilities should be performed and documented.

The assessments shall be performed following an examination of these monitored events. The assessments shall be based on real-time automated logging data and shall be performed at least on an annual basis as input into an entity's annual Compliance Audit.

The audit data should be reviewed by an Auditor for events such as repeated failed actions, requests for privileged information, attempted access of system files, and unauthenticated responses. Auditors should check for continuity of the audit data.

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

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

Based on the Risk Assessment, the CA shall develop, implement, and maintain a security plan consisting of security procedures, measures, and products, including updates to this CP/CPS document and any additional private procedures documents as may be necessary, to manage and control the risks identified during the Risk Assessment, commensurate with the sensitivity of the Certificate Data and Certificate Management Processes. The security plan will include administrative, organizational, technical, and physical safeguards as necessary and as appropriate to the sensitivity of the Certificate Data and Certificate Management Processes. The security plan will take into account then-available technology and the cost of implementing the specific measures, and will implement a reasonable level of security appropriate to the harm that might result from a breach of security and the nature of the data to be protected.

5.5 Records Archival

CA archive records shall be sufficiently detailed to determine the proper operation of the PKI and the validity of any Certificate (including those revoked or expired) issued by the CA. Records may be kept in the form of either computer-based messages or paper-based documents, provided their indexing, storage, preservation, and reproduction are accurate, reliable, and complete.

5.5.1 Types of Records Archived

The CA records shall include all relevant evidence in the recording entity's possession, including, without limitation:

- Time stamps
- CP/CPS
- Contractual obligations and other agreements concerning operations of the CA/RA system and equipment configuration
- Modifications and updates to system or configuration
- Certificate request documentation (requests for new subscriber accounts as well as ongoing certificate requests submitted electronically)
- Records of all actions taken on Certificates issued and/or published (certificate delivery for CA and Subscriber certificates)
- Record of re-key
- Revocation request information
- Records of all CRLs issued and/or published
- Records of OCSP entries
- Audit reports
- Appointment of an individual to a Trusted Position
- Destruction of cryptographic modules
- All Certificate Compromise notifications
- Token lifetime (issuance, recovery, destruction, etc.) documentation

5.5.2 Retention Period for Archive

Archive records shall be kept for a minimum of ten (10) years without any loss of data.

The CA SHALL retain all documentation relating to Publicly-Trusted Certificate requests and the verification thereof, and all Publicly-Trusted Certificates and revocation thereof, for at least seven years after any Publicly-Trusted Certificate based on that documentation ceases to be valid.

5.5.3 Protection of Archive

An entity maintaining an archive of records shall protect the archive so that only the entity's authorized Trusted Persons are able to obtain access to the archive. The archive shall be protected against unauthorized viewing, modification, deletion, or other tampering. The archive media and the applications required to process the archive data shall be maintained to ensure that the archive data can be accessed for the retention time period.

5.5.4 Archive Backup Procedures

Entities compiling electronic information shall incrementally back up system archives of such information at least on a weekly basis and perform full backups at least on a monthly basis.

Electronic documents such as legal contracts which change very infrequently may be omitted from the routine backups and may be backed up separately in the rare event of an update.

5.5.5 Requirements for Time-Stamping of Records

CA archive records shall be automatically time-stamped as they are created. System clocks used for time-stamping shall be maintained in synchrony with an authoritative time standard.

5.5.6 Archive Collection System (Internal or External)

Archive data may be collected in any expedient manner.

5.5.7 Procedures to Obtain and Verify Archive Information

Only authorized Trusted Persons are able to obtain access to the archive. The integrity of the information is verified as usable when it is restored.

5.6 Key Changeover

When a CA Certificate is rekeyed only the new key is used to sign certificates from that time on. If the old private key is used to sign CRLs that cover certificates signed with that key, the old key shall be retained and protected.

When a CA updates its private signature key and thus generates a new public key, the CA shall notify all CAs and Subscribers that rely on the CA's certificate that it has been changed.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

In the event of suspected compromise of a CA, the CA Operator shall investigate in order to determine the nature and the degree of damage.

The PA shall be notified if any CAs operating under this policy experience the following:

- Suspected or detected compromise of the CA systems
- Physical penetration of the site housing the CA systems
- Successful denial of service attacks on CA components

The PA will take appropriate steps to protect the integrity of the PKI ecosystem and shall define a time estimate for resolution.

The CA shall re-establish operational capabilities as quickly as possible. For business continuity and disaster recovery procedures refer to Section 5.7.4.

When a CA fails to comply with any requirement of the Mozilla Root Store Policy [14] - whether it be a mis-issuance, a procedural or operational issue, or any other variety of non-compliance - the event is classified as an incident. A CA that is under the governance of [14] shall promptly report all incidents to Mozilla in the form of an Incident Report, and shall regularly update the Incident Report until the corresponding bug is marked as resolved in the mozilla.org Bugzilla system by a

Mozilla representative. CAs should cease issuance until the problem has been prevented from reoccurring.

When a CA fails to meet their commitments made in their CP/CPS, Chrome expects them to file an incident report. Due to the incorporation of the Baseline Requirements [11] into the CP/CPS, incidents may include a prescribed follow-up action, such as revoking impacted certificates within a certain timeframe. If the CA doesn't perform the required follow-up actions, or doesn't perform them in the expected time, the CA should file a secondary incident report describing any certificates involved, the CA's expected timeline to complete any follow-up actions, and what changes the CA is making to ensure they can meet these requirements consistently in the future.

When a CA participating in the Chrome Root Program [16] becomes aware of or suspects an incident, they should notify chrome-root-authority-program@google.com with a description of the incident. If the CA has publicly disclosed this incident, this notification should include a link to the disclosure. If the CA has not yet disclosed this incident, this notification should include an initial timeline for public disclosure. Chrome uses the information on the public disclosure as the basis for evaluating incidents.

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

When computing resources, software, and/or data are corrupted, CAs operating under this policy shall respond as follows:

- Before returning to operation, ensure that the system's integrity has been restored.
- If the CA signature keys are not destroyed, CA operations shall be reestablished, giving priority to the ability to generate Certificate status information within the CRL issuance schedule specified in Section 5.9.7
- If the CA signature keys are destroyed, CA operations shall be reestablished as quickly as possible, giving priority to the generation of a new CA key pair.
- The PA and Superior Entity shall be notified as soon as possible.
- A report of the incident and a response to the event, shall be promptly made by the affected CA in accordance with the documented incident and Compromise reporting and handling procedures in the applicable CPS.

5.7.3 Entity Private Key Compromise Procedures

In the event of a CA private key Compromise, the following operations shall be performed:

- The PA and the Superior Entity shall be immediately informed, as well as any entities known to be distributing the CA Certificate
- If the CA signature keys are not destroyed, CA operation shall be reestablished, giving priority to the ability to generate CRLs.
- The CA shall generate new keys

- The CA shall initiate procedures to notify Subscribers of the Compromise
- When the superior CA (e.g., Root CA) which signed the compromised CA Certificate is also operated by us, we shall revoke the certificate of the compromised CA and make the new CRL available per revocation requirements in Section 4.9.
- Subscribers will repeat the initial Certificate Application process

If the CA distributed the public key in a Certificate, the CA shall perform the following operations:

- Generate a new Certificate
- Securely distribute the new Certificate
- Initiate procedures to notify Subscribers of the Compromise

5.7.4 Business Continuity Capabilities After a Disaster

Entities operating CAs shall develop, test, document, and maintain a Disaster Recovery Plan designed to mitigate the effects of any kind of natural or man-made disaster, security compromise or business failure and to reasonably protect and notify each party relevant to CA's ecosystem. For Publicly-Trusted Certificates those parties include Application Software Suppliers, Subscribers and Relying Parties.

The Plan shall identify conditions for activating the recovery and what constitutes an acceptable system outage and recovery time for the restoration of information systems services and key business functions within a defined recovery time.

Business continuity plans shall be available to the CA's auditors upon request. The CA shall annually test, review, and update these procedures.

Additionally, the Plan shall include:

- Emergency, fallback and resumption procedures,
- Frequency for taking backup copies of essential business information and software,
- Requirement to store critical cryptographic materials (i.e., secure cryptographic device and activation materials) at an alternate location,
- Separation distance of the Disaster recovery site to the CA's main site,
- Procedures for securing the Disaster facility during the period of time following a disaster and prior to restoring a secure environment either at the original or a remote site.

The DRP shall include administrative requirements including:

- Maintenance schedule for the plan
- Awareness and education requirements
- Responsibilities of the individuals

- Regular testing of contingency plans
- The distance of recovery facilities to the CA's main site

The disaster recovery equipment shall have physical security protections comparable to the production CA system, which includes the enforcement of physical security tiers.

CAs shall have the capability of restoring or recovering essential operations within twenty-four (24) hours following a disaster with, at a minimum, support for the following functions: Certificate issuance, Certificate revocation, and publication of revocation information.

A CA's DRP shall make provisions for full recovery within one (1) week following a disaster at the primary site.

5.8 CA or RA Termination

When a CA operating under this policy terminates operations before all certificates have expired, and whenever required by a contract between the terminating CA and its Superior Entity, the CA signing keys shall be surrendered to the PA. Prior to CA termination, the CA shall provide archived data to an archive facility as specified in the CPS. As soon as possible, the CA will advise all other organizations to which it has issued certificates of its termination, using an agreed-upon method of communication.

CAs that have ceased issuing new certificates but are continuing to issue CRLs until all certificates have expired are required to continue to conform with all relevant aspects of this policy (e.g., audit logging and archives).

The termination of a CA shall be subject to the contract between the terminating CA and its Superior Entity. A terminating CA and its Superior Entity shall, in good faith, use commercially reasonable effort to agree on a termination plan that minimizes disruption to Subscribers and Relying Parties. The termination plan may cover issues such as:

- Providing notice to parties affected by the termination, such as Subscribers and Relying Parties,
- Who bears the cost of such notice, the terminating CA or the Superior Entity,
- The revocation of the Certificate issued to the CA by the Superior Entity,
- The preservation of the CA's archives and records for the time periods required in Section 5.4.6,
- The continuation of Subscriber and customer support services,
- The continuation of revocation services, such as the issuance of CRLs or the maintenance of online status checking services,
- The revocation of unexpired unrevoked Certificates of Subscribers and subordinate CAs, if necessary,

- The payment of compensation (if specified in relevant PKI agreements) to Subscribers whose unexpired unrevoked Certificates are revoked under the termination plan or provision, for the issuance of substitute Certificates by a successor CA,
- Disposition of the CA's private key and under some circumstances, when the CA private key is stored on a separate hardware token, the hardware token containing such private key, and
- Provisions needed for the transition of the CA's services to a successor CA.

For PKI hierarchies where there is no Superior Entity, we may choose to terminate the CA services, as long as termination is in compliance with all of the applicable customer agreements. Termination plan shall be approved by the PA and may include:

- Providing notice to parties affected by the termination, such as Subscribers and Relying Parties,
- The preservation of the CA's archives and records for the time periods required in Section 5.4.6,
- The continuation of Subscriber and customer support services,
- The continuation of revocation services, such as the issuance of CRLs or the maintenance of online status checking services,
- The revocation of unexpired unrevoked Subscriber Certificates and subordinate CAs, if necessary,
- Disposition of the CA's private key and under some circumstances, when the CA private key is stored on a separate hardware token, the hardware token containing such private key

For any CA under the Microsoft Trusted Root Program, CA shall inform Microsoft via email at least 120 days before transferring ownership of enrolled root or subordinate CA that chains to an enrolled root to another entity or person.

Microsoft may contact customers that Microsoft believes may be substantially impacted by the pending removal of a root CA from the Microsoft Trusted Root Program.

CA which is included in the CCADB program shall create an Audit Case to update CCADB information with the pending CA termination or ownership transfer at least 120 days in advance of that event.

6. TECHNICAL SECURITY CONTROLS

This chapter specifies the requirements for technical security controls to securely perform the functions of key generation, subject authentication, PKC issuance, and PKC revocation.

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

6.1.1.1 CA Key Pair Generation

Key pair generation shall be performed in a physically secured environment using FIPS 140 validated cryptographic modules and processes that provide the required cryptographic strength of the generated keys and prevent the loss, disclosure, modification, or unauthorized use of private keys. Any pseudo-random numbers use and parameters for key generation material shall be generated by a FIPS-approved method. CA private key protection in an HSM is specified in Section 6.2.1.

CA keys shall be generated in a Key Generation Ceremony following a prepared Key Generation Script using multi-person control for CA key pair generation, as specified in Section 6.2.2.

Each Key Generation Ceremony where a Publicly-Trusted Root CA Key Pair is generated shall be witnessed by a Qualified Auditor directly or through a review of a video of the entire CA Key Pair generation process. Qualified Auditor shall issue a report opining that the CA followed its key ceremony during its Key and Certificate generation process and the controls used to ensure the integrity and confidentiality of the Key Pair.

CA key pair generation shall create a verifiable audit trail that the security requirements for procedures were followed. The documentation of the procedure shall be detailed enough to show that appropriate role separation was used. An independent third party shall validate the execution of the key generation procedures either by witnessing the key generation or by examining the signed and documented record of the key generation.

The integrity of the hardware/software used for key generation and the interfaces to the hardware/software shall be tested prior to the start of a Key Generation Ceremony.

CA private key shall only be allowed to be extracted from an HSM for the purpose of a backup using an approved hardware backup device supplied by an HSM manufacturer.

6.1.1.2 Subscriber Key Pair Generation

The CA shall reject a certificate request if the Key Pair does not meet the requirements set forth in sections 6.1.5 and/or 6.1.6.

In addition, under the following conditions the CA shall reject any certificate requests submitted and Subscriber's Certificate Requesting Account will be suspended until the issue has been corrected to the satisfaction of the CA for all future certificate requests:

1. The CA is made aware that the specific method used to generate the Private Key was flawed
2. The CA is aware of a demonstrated or proven method that exposes the Applicant's Private Key to compromise
3. The CA has previously been made aware that the Applicant's Private Key has suffered a Key Compromise, such as through the provisions of Section 4.9.1.1
4. The CA is aware of a demonstrated or proven method to easily compute the Applicant's Private Key based on the Public Key

For requests for Publicly-Trusted Subscriber Certificates, the CA checks for Debian weak keys, ROCA vulnerability, and Close Primes vulnerability as prescribed by [11].

If a Publicly-Trusted Subscriber Certificate will contain an extKeyUsage extension containing either the values id-kp-serverAuth or anyExtendedKeyUsage, the CA shall not generate a Key Pair on behalf of a Subscriber, and shall not accept a certificate request using a Key Pair previously generated by the CA.

Subscriber key pair generation may be performed by the Subscriber or CA. If the Subscribers themselves generate private keys, then private key delivery to a Subscriber is unnecessary.

Subscriber private keys shall be generated by the CA inside a software-based or hardware-based cryptographic module that is FIPS 140-2 Level 1 or higher.

When CAs generate key pairs on behalf of the Subscriber, then the private key shall be delivered securely to the Subscriber. Private keys may be delivered electronically or on a hardware cryptographic module. In all cases, the following requirements shall be met:

- Encrypted copies of private keys may be kept by the CA prior to Subscriber acknowledging receipt and verification of the private key(s).
- CAs shall use Trustworthy Systems to deliver private keys to Subscribers and shall secure such delivery through the use of a PKCS #8 package or, at the CAs' sole discretion, any other comparably equivalent means (e.g., PKCS #12 package) in order to prevent the loss, disclosure, modification, or unauthorized use of such private keys.
- Where key pairs are pre-generated on hardware tokens, the entities distributing such tokens shall use best efforts to provide physical security of the tokens to prevent the loss, disclosure, modification, or unauthorized use of the private keys on the token. The CA shall maintain a record of the Subscriber acknowledgement of receipt of the token, if applicable.

- The Subscriber shall acknowledge receipt and verification of the private key(s). After Subscriber acknowledgement, the CA shall erase the private key(s).
- Delivery shall be accomplished in a way that ensures that the correct tokens and activation data are provided to the correct Subscribers, if applicable.
- For electronic delivery of private keys, the key material shall be encrypted using a cryptographic algorithm and key size at least as strong as the private key. Activation data shall be delivered using a separate secure channel.
- The CA shall maintain a record of the Subscriber's acknowledgement of receipt of the token, if applicable.

6.1.2 Private Key Delivery to Subscriber

Private keys generated by the CA for the Subscriber shall be delivered to Subscribers only when:

- Their Certificate Applications are approved by the PKI-PA, and
- Their key pairs are generated and are distributed to Certificate Applicants who previously completed the enrollment process.

CAs shall use Trustworthy Systems to deliver private keys to Subscribers and shall secure such delivery through the use of an encrypted PKCS #8 package or, any other comparably equivalent means in order to prevent the loss, disclosure, modification, or unauthorized use of such private keys.

6.1.3 Public Key Delivery to Certificate Issuer

The Certificate Applicant shall deliver the public key in a PKCS#10 CSR or an equivalent method ensuring that the public key has not been altered during transit, and that the Certificate Applicant possesses the private key corresponding to the transferred public key. The Certificate Applicant may submit the CSR via their online Certificate Requesting Account, which employs two-factor authentication, e.g., a USB token with the account administrator's certificate and a PIN. (This procedure is not applicable to certificate request and issuance processes conducted through interfaces intended for automated clients.).

6.1.4 CA Public Key Delivery to Relying Parties

The Root CA public key certificate shall be delivered to Relying Parties in a secure fashion to preclude substitution attacks. Acceptable methods for certificate delivery are:

- A full certificate chain that includes the Root CA Certificate and issuing CA certificate are delivered as part of Subscriber's certificate request.
- Distribution of Root CA Certificates through secure out-of-band mechanisms.
- Downloading the Root CA Certificates from trusted web sites (e.g., CA web site). The Root CA shall calculate the hash of the certificate before posting it

on a website so that it can be made available via out-of-band to Relying Parties to validate the posted Root CA Certificate.

6.1.5 Key Sizes

Public/private key sizes for both CA and Subscriber Certificates are specified in the individual ecosystem's certificate profile listed in Section 7.1.

6.1.6 Public Key Parameters Generation and Quality Checking

Public Key parameters such an Elliptic Curve group or RSA key size shall comply with the certificate profile for a specific ecosystem. In addition:

RSA: The CA shall confirm that:

- The value of the public exponent is in the range between $2^{16}+1$ and $2^{256}-1$
- The modulus size complies with the certificate profile for a specific ecosystem

ECDSA:

- Verify that the public key is a valid point on the curve specified for a particular certificate profile

For Publicly Trusted Certificates, our CAs performs the recommended public key quality checks described in [11] § 6.1.6.

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

Private Keys corresponding to Root Certificates shall not be used to sign Certificates except in the following cases:

1. Self-signed Certificates to represent the Root CA itself
2. Certificates for Subordinate CAs and Cross Certificates
3. Certificates for OCSP Responders utilized to provide the status of Subordinate CA certificates

Key Usage and Extended Key Usage extensions shall be specified per certificate profile for a specific ecosystem.

Each CA shall cease to use a key pair at the end of the key pair's defined operational lifetime or when the compromise of the private key is known or suspected.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

The CA SHALL implement physical and logical safeguards to prevent unauthorized certificate issuance. Protection of the CA Private Key outside the validated system or device specified above shall consist of physical security, encryption, or a combination of both, implemented in a manner that prevents disclosure of the Private Key.

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

6.2.1 Cryptographic Module Standards and Controls

CA Private keys shall be protected using FIPS 140-2 Level 3 systems. Private key holders shall take necessary precautions to prevent the loss, disclosure, modification, or unauthorized use of such Private Keys in accordance with this CP/CPS and contractual obligations specified in the appropriate PA Agreement.

The relevant standard for cryptographic modules is Security Requirements for Cryptographic Modules [FIPS 140-2].

- Root CAs shall perform all CA cryptographic operations on cryptographic modules rated at a minimum of FIPS 140-2 level 3 or higher.
- Sub-CAs shall use a hardware cryptographic module that is rated, configured and operated at FIPS 140-2 Level 3 or higher.

Subscribers protect private keys as specified in the appropriate Subscriber agreements.

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

Multi-person control is enforced to protect the activation data needed to activate CA private keys so that a single person shall not be permitted to activate or access any cryptographic module that contains the complete CA private signing key.

CA signature keys may be backed up only under multi-person control. Access to CA signing keys backed up for disaster recovery shall be under multi-person control. The names of the parties used for multi-person control shall be maintained on a list that shall be made available for inspection during compliance audits.

CAs may use “Secret Sharing” to split the private key or activation data needed to operate the private key into separate parts called “Secret Shares” held by individuals called “Shareholders.” Some threshold number of Secret Shares (m) out of the total number of Secret Shares (n) shall be required to operate the private key. The minimum threshold number of shares (m) needed to sign a CA Certificate shall be 3. The total number of shares (n) used shall be greater than the minimum threshold number of shares (m).

CAs may also use Secret Sharing to protect the activation data needed to activate private keys located at their respective disaster recovery sites. The minimum threshold number of shares (m) needed to sign a CA Certificate at a disaster recovery site shall be 3. The total number of shares (n) used shall be greater than the minimum threshold number of shares (m).

6.2.3 Private Key Escrow

CA private keys and Subscriber private keys shall not be escrowed.

6.2.4 Private Key Backup

CAs shall back up their private keys under the same multi-person control as the original signature key. Additional copies may exist to support a secure high-availability high-throughput system and/or for storage off-site, provided that accountability for them is maintained. The backups allow the CA to be able to recover from disasters and equipment malfunction. At least one copy of the private signature key shall be stored off-site. Private keys that are backed up shall be protected from unauthorized modification or disclosure through physical or cryptographic means. Backups, including all activation data needed to activate the cryptographic token containing the private key, shall be protected with a level of physical and cryptographic protection equal to or exceeding that for cryptographic modules within the CA site, such as at a disaster recovery site or at another secure off-site facility, such as a bank safe. All copies of the CA private signature key shall be accounted for and protected in the same manner as the original.

Device private keys may be backed up or copied, but shall be held under the control of the Subscriber or other authorized administrator. Private keys that are backed up, shall not be stored in plaintext form and storage shall ensure security controls consistent with the ecosystem-specific security specifications referenced in the CPS with which the device is compliant. Subscribers may have the option of using enhanced private key protection mechanisms available today including the use of smart cards, biometric access devices, and other hardware tokens to store private keys.

6.2.5 Private Key Archival

CA private signature keys shall not be archived. Archival of the Subscriber private keys is ecosystem-dependent and is specified for each ecosystem in the CPS. If the CA retains Subscriber private keys for business continuity purposes as permitted by a specific ecosystem, the CA shall archive such Subscriber private keys, in accordance with CP/CPS Section 5.5.

In the case of Publicly-Trusted Certificates, the CA does not generate Subscriber key pairs and does not have access to Subscriber Private Keys.

Upon expiration of a CA Certificate, the key pair associated with the Certificate will be securely retained for a period of at least five (5) years using hardware cryptographic modules that meet the requirements of this CP. These CA key pairs shall not be used for any signing events after the expiration date of the corresponding CA Certificate, unless the CA Certificate has been renewed.

6.2.6 Private Key Transfer Into or From a Cryptographic Module

The Issuing CA shall not generate the Private Key on behalf of a Subordinate CA.

CA private keys may be exported from the cryptographic module only to perform CA key backup procedures, as described in Section 6.2.4. At no time shall the private key exist in plaintext outside the cryptographic module.

All other keys shall be generated by and in a cryptographic module. In the event that a private key is to be transported from one cryptographic module to another, the private key shall be encrypted during transport; private keys shall never exist in plaintext form outside the cryptographic module boundary.

Private or symmetric keys used to encrypt other private keys for transport shall be protected from disclosure.

Entry of a private key into a cryptographic module shall use mechanisms to prevent loss, theft, modification, unauthorized disclosure, or unauthorized use of such private key.

Processing Centers generating CA private keys on one hardware cryptographic module and transferring them into another, shall securely transfer such private keys into the second cryptographic module to the extent necessary to prevent loss, theft, modification, unauthorized disclosure, or unauthorized use of such private keys. Such transfers shall be limited to making backup copies of the private keys on tokens.

CAs pre-generating private keys and transferring them into a hardware token, for example transferring generated end-user Subscriber private keys into a smart card, shall securely transfer such private keys into the token to the extent necessary to prevent loss, theft, modification, unauthorized disclosure, or unauthorized use of such private keys.

Software and hardware utilized during the key migration shall comply with Section 6.6.2.

6.2.7 Private Key Storage on Cryptographic Module

The CA SHALL protect its Private Key in a system or device that has been validated as meeting at least FIPS 140 level 3, which includes requirements to protect the Private Key and other assets against known threats.

6.2.8 Method of Activating Private Key

All CAs shall protect the activation data for their private keys against loss, theft, modification, disclosure, or unauthorized use.

CA administrators shall be authenticated to the cryptographic token before the activation of the associated private key(s). Acceptable means of authentication include but are not limited to passphrases, PINs or biometrics. Entry of activation data shall be protected from disclosure (i.e., the data should not be displayed while it is entered).

6.2.8.1 CA Administrator Activation

Method of activating the CA system by a CA Administrator shall require:

- Use a smart card, biometric access device, password in accordance with CP/CPS § 6.4.1, or security of equivalent strength to authenticate the Administrator before the activation of the private key, which includes, for instance, a password to operate the private key, a Windows logon or screen saver password, or a network logon password; and
- Take commercially reasonable measures for the physical protection of the Administrator's workstation to prevent use of the workstation and its associated private key without the Administrator's authorization.

6.2.8.2 Offline CA Private Keys

Once the CA system has been activated, a threshold number of Shareholders shall be required to supply their activation data in order to activate an offline CA's private key, as defined in Section 6.2.2. Once the private key is activated, it shall be active until termination of the session.

An offline CA under this CP/CPS may be connected to an isolated network restricted to physical tiers 4 and above and is not online in a sense of being connected to the Internet or a company Intranet.

6.2.8.3 Online Subordinate CA Private Keys

An online CA's private key shall be activated by a threshold number of Shareholders, as defined in Section 6.2.2, supplying their activation data (stored on secure media). Once the private key is activated, the private key may be active until termination of the session.

6.2.8.4 Method of Activating Subscriber Private Keys

Subscriber Private Keys are delivered to Subscriber with protection specified in Section 6.1.1.2.

6.2.9 Method of Deactivating Private Key

Cryptographic modules that have been activated shall not be available to unauthorized access. After use, the cryptographic module shall be deactivated via a manual logout procedure. CA cryptographic modules shall be stored securely when not in use.

With respect to the private keys of Root CAs, after the completion of a Key Generation Ceremony, in which such private keys are used for private key operations, the CA shall remove the token containing the private keys from the reader in order to deactivate them, or take similar action based upon the type of hardware used to store the private key. Once removed from the reader, tokens shall be securely stored.

When an online CA or an offline issuing CA on an isolated network is deactivated, the CA shall remove the token containing such CA's private key from the reader in order to deactivate it, or take similar action based upon the type of hardware used

to store the private key. Once removed from the reader, tokens shall be securely stored.

When deactivated, private keys shall be kept in encrypted form or inside an HSM only.

6.2.10 Method of Destroying Private Key

Private keys shall be destroyed in a way that prevents their theft, disclosure, or unauthorized use.

Upon termination of the operations of a CA, individuals in trusted roles shall decommission the CA private signature keys by deleting it using functionality of the token containing such CA's private key so as to prevent its recovery following deletion, or the loss, theft, modification, disclosure, or unauthorized use of such private key. CA private keys shall be destroyed in a manner that reasonably ensures that there is no residual information that could lead to the reconstruction of the key.

6.2.11 Cryptographic Module Rating

See Section 6.2.1.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

CAs may archive their public keys in accordance with Section 5.5.1.

6.3.2 Certificate Operational Periods and Key Usage Periods

The certificate validity period (i.e., certificate operational period and key pair usage period) shall be set to the time limits specified in the certificate profiles for a specific ecosystem.

Whenever required by certificate profiles for a specific ecosystem, validity periods shall be nested such that the validity periods of issued certificates shall be contained within the validity period of the issuing CA.

For Publicly-Trusted Subscriber Certificates, the Validity Period shall conform to the limits specified in [11]. The interpretation of Validity Period values shall conform to [11].

All PKI Participants shall cease all use of their key pairs after their usage periods have expired.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

The activation data (e.g., PINs, passwords, or manually-held key shares) used to unlock private keys, in conjunction with any other access control procedure, shall

have an appropriate level of strength for the keys or data to be protected and shall meet the applicable Security Policy requirements of the cryptographic module used to store the keys. CAs shall generate and install activation data for their private keys and shall use methods that protect the activation data to the extent necessary to prevent the loss, theft, modification, disclosure, or unauthorized use of such activation data.

When a CA uses passwords as activation data for the CA signing key, at a minimum the activation data shall be changed upon CA re-key and the CAs activation participants shall generate passwords that cannot easily be guessed or cracked by dictionary attacks. Participants may not need to generate activation data, for example if they use biometric access devices.

There is no stipulation for Device private keys.

6.4.2 Activation Data Protection

Data used to unlock private keys shall be protected from disclosure by a combination of cryptographic and physical access control mechanisms. Activation data should be either biometric in nature or memorized. If written down, it shall be secured at the level of the data that the associated cryptographic module is used to protect, and shall not be stored with the cryptographic module. In all cases, the protection mechanism shall include a facility to temporarily lock the account, or terminate the application, after a predetermined number of failed login attempts.

CAs shall protect the activation data for their private keys using methods that protect against the loss, theft, modification, unauthorized disclosure, or unauthorized use of such private keys.

CAs shall use multi-party control and provide the procedures and means to enable Shareholders to take the precautions necessary to prevent the loss, theft, modification, disclosure, or unauthorized use of the Secret Shares that they possess.

Shareholders shall not:

- Copy, disclose, or make the Secret Share available to a third party, or make any unauthorized use of it whatsoever
- Disclose their or any other person's status as a Shareholder to any third party

The Secret Shares and any information disclosed to the Shareholder in connection with their duties as a Shareholder shall constitute Confidential/Private Information.

CAs shall include in their DRPs provisions for making Secret Shares available at a disaster recovery site after a disaster (Note: The important aspect of disaster recovery vis-à-vis shares is that a process exists for making the necessary number of shares available, even if the requisite Shareholders are not available.)

CAs shall maintain an Audit trail of Secret Shares, and Shareholders shall participate in the maintenance of an Audit trail. The audit trail consists of manually recorded events when the Secret Shares are created. This log is protected with the rest of the log data according to Section 5.4.

6.4.3 Other Aspects of Activation Data

6.4.3.1 Activation Data Transmission

To the extent activation data for their private keys are transmitted, Activation Data Participants shall protect the transmission using methods that protect against the loss, theft, modification, unauthorized disclosure, or unauthorized use of such private keys. To the extent desktop computer or network logon user name/password combination is used as activation data for an end-user Subscriber, the passwords transferred across a network shall be protected against access by unauthorized users.

6.4.3.2 Activation Data Destruction

Activation data for CA private keys shall be decommissioned using methods that protect against the loss, theft, modification, unauthorized disclosure, or unauthorized use of the private keys protected by such activation data. After the record retention periods in Section 5.5.2 lapses, CAs shall decommission activation data by overwriting and/or physical destruction.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

CAs shall ensure that the systems maintaining CA software and data files are Trustworthy Systems secure from unauthorized access, which can be demonstrated by compliance with audit criteria applicable under Section 6.5.1. In addition, CAs shall limit access to production servers to those individuals with a valid business reason for access. General application users shall not have accounts on the production servers.

To the extent that passwords are used, CAs shall require the use of passwords with a minimum character length and a combination of alphanumeric and special characters, and shall require that passwords be changed on a periodic basis compliant with [12] and whenever necessary. Direct access to a CA's database maintaining the CA's repository shall be limited to Trusted Persons having a valid business reason for such access.

Authentication keys and passwords for any privileged account or service account on a Certificate System are changed whenever a person's authorization to administratively access that account on the Certificate System is changed or revoked.

Computer security controls are required to ensure CA operations are performed as specified in this policy. The following computer security functions may be provided by the operating system, or through a combination of operating system, software, and physical safeguards using industry best practices:

- Require authenticated logins with enforcement of multi-factor authentication for all Trusted Persons
- Verify the trustworthiness of all software required for CA operations; ensure that it is regularly scanned for malicious code, protected against spyware and viruses
- Apply recommended security patches to Certificate Systems within six (6) months of the security patch's availability, unless the CA documents that the security patch would introduce additional vulnerabilities or instabilities that outweigh the benefits of applying the security patch
- Provide discretionary access control
- Provide a security audit capability
- Enforce access control for CA services and PKI roles
- Enforce separation of duties for PKI roles
- Require identification and authentication of PKI roles and associated identities
- Prohibit object reuse or require separation for CA random access memory
- Require use of cryptography for session communication and database security
- Archive CA history and audit data
- Require self-test security-related CA services
- Require a trusted path for identification of PKI roles and associated identities
- Require a recovery mechanism for keys and the CA system
- Enforce domain integrity boundaries for security-critical processes
- Configure Issuing Systems, Certificate Management Systems, Security Support Systems, and Front-End / Internal-Support Systems by removing or disabling all accounts, applications, services, protocols, and ports that are not used in the CA's operations and allowing only those that are approved by the CA
- Grant administration access to Certificate Systems only to persons acting in Trusted Roles and require their accountability for the Certificate System's security.

For remote workstations used to administer the CAs, the computer security functions listed below are required:

- Authenticate the identity of users before permitting access to the system or applications;
- Manage privileges of users to limit users to their assigned roles;

- Generate and archive audit records for all transactions; (see Section 5.4)
- Enforce domain integrity boundaries for security critical processes; and
- Support recovery from key or system failure.

All communications between any PKI trusted role and the CA shall be authenticated and protected from modification.

For CAs subject to the requirements in [11], multi-factor authentication shall be enforced for all accounts capable of directly causing certificate issuance.

6.5.2 Computer Security Rating

No stipulation.

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

The system development controls for the CA are as follows:

- The CA shall use software that has been designed and developed under a formal, documented development methodology.
- Hardware and software procured to operate the CA shall be purchased in a fashion to reduce the likelihood that any particular component was tampered with (e.g., by ensuring the vendor cannot identify the PKI component that will be installed on a particular device).
- Hardware and software developed specifically for the CA shall be developed in a controlled environment, and the development process shall be defined and documented. This requirement does not apply to commercial off-the-shelf hardware or software.
- The CA hardware and software shall be dedicated to performing one task: the CA. There shall be no other applications, hardware devices, network connections, or component software installed that are not parts of the CA operation. Where the CA operation supports multiple CAs, the hardware platform may support multiple CAs.
- Proper care shall be taken to prevent malicious software from being loaded onto the CA Equipment. All applications required to perform the operation of the CA shall be obtained from documented sources.
- Hardware and software updates shall be purchased or developed in the same manner as the corresponding original equipment, and shall be installed by trusted and trained personnel in a defined manner.
- Establish a change management process, following the principles of documentation, approval and review, applicable to all changes to Certificate Systems, Issuing Systems, Certificate Management Systems, Security Support Systems, and Front-End / Internal-Support Systems.

6.6.2 Security Management Controls

The configuration of the CA system, in addition to any modifications and upgrades, shall be documented and controlled. There shall be a mechanism for detecting unauthorized modification to the software or configuration. The CA software, when first loaded, shall be verified as being that supplied from the vendor or as an in-house software release, with no modifications, and be the version intended for use.

6.6.3 Life Cycle Security Controls

No stipulation.

6.7 Network Security Controls

These controls comply with the most recent version of the CAB Forum Network and Certificate System Security Requirements [12].

CAs shall have production networks logically separated from other components. This separation prevents network access except through defined application processes. CAs shall use firewalls to protect the production network from internal and external intrusion and limit the nature and source of network activities that may access production systems. Equivalent security controls apply to all systems co-located in the same network with a Certificate System.

CAs and RAs must employ appropriate security measures to ensure they are guarded against denial of service and intrusion attacks. Such measures must include the use of network guards, firewalls, or filtering routers. The network guard, firewall, or filtering router must limit services allowed to and from the PKI equipment to those required to perform PKI functions. Each network boundary control is configured with rules that support only the services, protocols, ports, and communications that the CA has identified as necessary to its operations.

Protection of PKI equipment must be provided against known network attacks. All unused network ports and services must be turned off. Any network software present on the PKI equipment must be necessary to the functioning of the PKI application.

Any boundary control devices used to protect the network on which PKI equipment is hosted must deny all but the necessary services to the PKI equipment.

Repositories and remote workstations used to administer the CAs must employ appropriate network security controls. Networking equipment must turn off unused network ports and services. Any network software present must be necessary to the functioning of the equipment.

The CA must establish connection with a remote workstation used to administer the CA only after successful authentication of the remote workstation at a level of assurance commensurate with that of the CA.

6.8 Time-Stamping

Certificates, CRLs and signed OCSP Responses shall contain time and date information. Such time information need not be cryptography-based. Asserted times shall be accurate to within three minutes. Electronic or manual procedures may be used to maintain system time. Clock adjustments are auditable events (see Section 5.4.1).

7. CERTIFICATE, CRL, AND OCSP PROFILES

All CAs shall follow certificate and CRL profiles that are specified for a particular ecosystem.

7.1 Certificate Profile

All CAs shall follow certificate and CRL profiles that are specified for a particular ecosystem.

For each CA under the Microsoft Trusted Root Program, the CA shall disclose its full PKI hierarchy (all root CAs and subordinate CAs, EKUs, certificate constraints) to Microsoft on an annual basis. The CA shall keep this information accurate in the CCADB when changes occur. At the present time, we does not issue cross-certificates or Sub-CA certificates to 3rd parties and does not operate Technically Constrained Sub-CAs.

At this time, supported certificate profiles consist of:

Ecosystem	Reference for cert profiles	List of CAs	Superior Entity	Validity Period Nesting Required?	Subscriber Private Keys Archival and backups allowed?	Frequency of External Audit	Timeout Period for Private Key Deletion*	Superior Entity Review and approval of CPS required?**
DOCSIS 3.1	[3], [20]	CableLabs Device CA	CableLabs	YES	YES	Once per year	2 weeks	NO
DOCSIS 4.0	[25], [26], [27]	CableLabs Device CA RSA	CableLabs	YES	YES	Once per year	2 weeks	NO
OpenCable	[4]	CableLabs Device CAs for both Hosts and CableCARDs	CableLabs	NO	YES	Once per year	90 days	NO
CBRS/ WInnForum	[22]	WInnForum RSA CBSD Mfr CA	Insta	YES	NO	Once per year	2 weeks	YES
	[22]	WInnForum ECC Root CA0004, WInnForum RSA Root CA0004, WInnForum RSA SAS Provider CA0001, WInnForum RSA Professional Installer CA0001,	WInnForum	YES	NO	Once per year	2 weeks	NO

		WInnForum RSA CBSD Mfr CA0001 WInnForum RSA Domain Proxy CA0001						
DPoE	[21]	DPoE Manufacturer CA	CableLabs	NO	YES	Once per year	90 days	NO

* A timer is initiated after an initial download of Subscriber private keys. After the timer expires, the CA deletes its copy of the Subscriber private keys even if Subscriber did not acknowledge the download and validation of the Subscriber private keys and certificates. The corresponding timeout value varies per ecosystem as defined in this table.

** In all cases where Superior Entity approval of this CPS is required, it applies to the initial CPS review by the Superior Entity and subsequent major revisions of the CPS. Minor CPS revisions containing editorial changes and clarifications do not require Superior Entity approval but will be supplied to the Superior Entity when indicated in the above table.

In addition, the following table lists ecosystems that have additional organization validation rules that are not covered by Section 3.2.2:

Ecosystem	**Reference for organization validation rules**	**Superior Entity**	**Description of additional validation**
CBRS/ WInnForum	[22]	Insta	Lookup each requested FCC ID here: https://apps.fcc.gov/oetcf/eas/reports/GenericSearch.cfm. The first 3 or 5 characters of the FCC ID are entered into the web form as a "Grantee Code" and the rest is entered as "Product Code". Equipment Class field must also be filled in with the selection "CBD-Citizens Band Category A and B Devices" Make sure that there is at least one search result with the organization name to which we have legal rights. If the listed organization name is not known to the PA, the PA must get a confirmation from a legal officer of ours. Also, double-check that the same entry with confirmed organization name has the correct FCC ID and equipment class that were specified in the search. (Do not rely on the correctness of the FCC search.)
	[22]	WInnForum	Lookup each requested FCC ID: https://apps.fcc.gov/oetcf/eas/reports/GenericSearch

			.cfm. The first 3 or 5 characters of the FCC ID are entered into the web form as a "Grantee Code" and the rest is entered as "Product Code". Equipment Class field must also be filled in with the selection "CBD-Citizens Band Category A and B Devices". Make sure that there is at least one search result with an organization name that matches the organization in the subscriber agreement and the certificate attributes reflect this identity. For each requested FRN, use the FRN to look up the Grantee Code here: https://apps.fcc.gov/oetcf/eas/reports/GranteeSearch.cfm. Then use the Grantee Code to search for more details here: https://apps.fcc.gov/oetcf/eas/reports/GenericSearch.cfm. Equipment Class field must also be filled in with the selection "CBD-Citizens Band Category A and B Devices". Click on "View Form" on each of the entries found during this lookup to find at least one entry with the specified FRN. Make sure that the corresponding organization name matches the organization in the subscriber agreement and the certificate attributes reflect this identity. Also, double-check that the same entry with confirmed organization name has the correct FCC ID or FRN and equipment class that were specified in the search. (Do not rely on the correctness of the FCC search.) In the case that the organization name registered with the FCC ID or FRN and organization name in the subscriber agreement differ, the link between the two may be validated by: a) Public announcements of a merger or a partnership that establishes the link. b) A signed letter from the legal officer of the Subscriber's company.

Furthermore, CPS revisions that are specific to only some of the PKI ecosystems in the above table will require approvals only from the corresponding Superior Entities as indicated in the above table. After all the necessary approvals, the updated CPS will be shared with every Superior Entity that has a "YES" in the last column of the above table.

7.1.1 Version Number(s)

Only X.509 version 3 certificates are supported.

7.1.2 Certificate Extensions

Specified within ecosystem-specific certificate profiles are listed by reference in the CPS.

7.1.3 Algorithm Object Identifiers

Specified within ecosystem-specific certificate profiles are listed by reference in the Section 7.1.

7.1.4 Name Forms

Specified within ecosystem-specific certificate profiles are listed by reference in the Section 7.1.

7.1.5 Name Constraints

Specified within ecosystem-specific certificate profiles are listed by reference in the Section 7.1.

7.1.6 Certificate Policy Object Identifier

Specified within ecosystem-specific certificate profiles are listed by reference in the Section 7.1.

7.1.7 Usage of Policy Constraints Extension

Specified within ecosystem-specific certificate profiles are listed by reference in the Section 7.1.

7.1.8 Policy Qualifiers Syntax and Semantics

Specified within ecosystem-specific certificate profiles are listed by reference in the Section 7.1.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

Specified within ecosystem-specific certificate profiles are listed by reference in the Section 7.1.

7.1.10 Certificate Profile for Publicly-Trusted Certificates

Certificate profiles for Publicly-Trusted Certificates comply with [11], [13] and [14]. Additional certificate profile details that are in addition to [11], [13] and [14] are provided in the following subsections.

7.1.10.1 Publicly-Trusted Root CA

- Validity period: 25 years
- certificatePolicies extension shall not be present
- subjectName fields:
    - organizationName = CommScope

- Public key algorithms and key sizes shall be one of the following:

- RSA
  - Key size = 4096 bits
  - Signature algorithm: RSASSA-PKCS1-v1_5 with SHA-256
- ECDSA
  - NIST P-384 curve
  - Signature algorithm: ECDSA with SHA-384

7.1.10.2 Publicly-Trusted Issuing CA

- Validity period: 25 years
- certificatePolicies extension shall be present and:
  - marked as non-critical
  - shall include the following OIDs:
    - 1.3.6.1.4.1.57050.1.1.1 (corresponds to the policy set in this CP/CPS)
      - policyQualiferInfo of type CPS, include HTTP URL where the CPS of the certificate's issuer is published
    - And only one of the following (without policyQualifierInfo):
      - 2.23.140.1.2.1 (issues domain-validated certificates compliant with [11])
      - 2.23.140.1.2.2 (issues organization-validated certificates compliant with [11])

- authorityInformationAccess extension shall be present and:
  - marked as non-critical
  - include HTTP URL of the Issuing CA's certificate
  - include HTTP URL of the Issuing CA's OCSP responder

- keyUsage extension shall be critical and include the following flags:
  - keyCertSign, cRLSign, digitalSignature (for signing OCSP Responses)

- Public key algorithms and key sizes shall be one of the following:
  - RSA
    - Key size = 4096 bits
    - Signature algorithm: RSASSA-PKCS1-v1_5 with SHA-256
  - ECDSA
    - NIST P-384 curve
    - Signature algorithm: ECDSA with SHA-384

7.1.10.3 Publicly-Trusted OCSP Responder Certificates

- Validity period: 25 years
- id-pkix-ocsp-nocheck extension shall be present
- extKeyUsage extension shall be present and contain the following OID
  id-kp-OCSPSigning

- Public key algorithms and key sizes shall be one of the following:
    - RSA
        - Key size = 4096 bits
        - Signature algorithm: RSASSA-PKCS1-v1_5 with SHA-256
    - ECDSA
        - NIST P-384 curve
        - Signature algorithm: ECDSA with SHA-384

7.1.10.4 Publicly-Trusted Subscriber Certificates

- Maximum Validity Period:
    - 180 days when precertificates are published to 2 certificate transparency logs
    - 397 days when precertificates are published to 3 certificate transparency logs

- certificatePolicies extension shall be present:
    - marked as non-critical
    - shall include the following OIDs:
        - 1.3.6.1.4.1.57050.1.1.1 (corresponds to the policy set in this CP/CPS)
            - policyQualiferInfo of type CPS, include HTTP URL where the CPS of the certificate's issuer is published
        - And only one of the following (without policyQualifierInfo):
            - 2.23.140.1.2.1 (domain-validated certificates compliant with [11])
            - 2.23.140.1.2.2 (organization-validated certificates compliant with [11])

- authorityInformationAccess extension shall be present and:
    - marked as non-critical
    - include HTTP URL of the Issuing CA's certificate
    - optionally include HTTP URL of the Issuing CA's OCSP responder

- cRLDistributionPoints extension shall be present and:
    - marked as non-critical
    - include HTTP URL of the Issuing CA's CRL service

- subjectAltName extension shall be present and:
    - marked as non-critical
    - contain at least one dNSName that has been validated according to 3.2.2.4

- Public key algorithms and key sizes shall be one of the following:
    - RSA
        - Key size = 2048 bits

        - Signature algorithm: RSASSA-PKCS1-v1_5 with SHA-256
    - ECDSA
        - NIST P-256 curve
        - Signature algorithm: ECDSA with SHA-384

7.2 CRL Profile

At this time, supported CRL profiles consist of:

Ecosystem	Reference for CRL profiles	List of CAs	Superior Entity	CRL Latency	Max Time to Begin Investigation *	Additional organizations that can request revocation **	Superior Entity or CA initiates revocation?	2 Persons required for Revocation?
DOCSIS 3.1	[3], [20]	CableLabs Device CA	CableLabs	24 hours	2 business days	N/A	Superior Entity	Yes
DOCSIS 4.0	[25], [26], [27]	CableLabs Device CA RSA	CableLabs	24 hours	2 business days	N/A	Superior Entity	Yes
OpenCable	[4]	CableLabs Device CAs for both Hosts and CableCARDs	CableLabs	N/A – Revocation handled by Superior Entity	2 business days	N/A	Superior Entity	No
CBRS/WInn Forum	[22]	WInnForum RSA CBSD Mfr CA	Insta	24 hours	2 business days	WInnForum	CA	No
	[22]	WInnForum ECC Root CA0004, WInnForum RSA Root CA0004, WInnForum RSA SAS Provider CA0001, WInnForum RSA Professional Installer CA0001, WInnForum RSA CBSD Mfr CA0001 WInnForum RSA Domain Proxy CA0001	WInnForum	24 hours	2 business days	WInnForum	CA	No
DPoE	[21]	DPoE Manufacturer CA	CableLabs	N/A – Revocation not specified	2 business days	N/A	Superior Entity	No

* This is the maximum time allowed prior to commencing investigation after receiving a revocation request or a Certificate Problem Report.

** Organizations that can request revocation are listed in Section 4.9.2. These are additional organizations specific to an ecosystem that are also allowed to request revocation.

7.2.1 Version Number(s)

Only X.509 version 2 CRLs are supported.

7.2.2 CRL and CRL Entry Extensions

Specified within ecosystem-specific CRL profiles are listed by reference in Section 7.2.

7.3 OCSP Profile

Supported OCSP profiles are listed in the table below. Currently, there are no supported OCSP profiles, so the table contains no entries.

Ecosystem	Reference for OCSP profile	List of CAs	Superior Entity	Validity Interval of OCSP Response	OCSP Response Caching Strategy	Who signs OCSP Responses?

* Support for OCSP is limited to Certificates issued by the CA that contain an OCSP URL in an AIA extension. The same is true for other Subordinate CAs on the same list.

The interpretation of validity interval values shall be as defined in [11].

7.3.1 Version Number(s)

No stipulation.

7.3.2 OCSP Extensions

No stipulation.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

This chapter specifies the requirements for audits.

The CA SHALL at all times:

1. Issue Certificates and operate its PKI in accordance with all laws applicable to its business and the Certificates it issues in every jurisdiction in which it operates
2. Comply with this CP/CPS
3. Comply with the audit requirements set forth in this section

8.1 Frequency and Circumstances of Assessment

CAs operating under this policy shall be subject to a compliance audit under the following circumstances:

- If mutually agreed upon between the Superior Entity and the CA Operator.
- Or when specified by a standard for a particular PKI ecosystem.

Frequencies of compliance audits for each ecosystem are specified in Section 7.1.

For CAs that are subject to the requirements in [11], the period during which a CA issues Certificates SHALL be divided into an unbroken sequence of audit periods.

The PA may require a periodic compliance audit report of CAs operating under this policy as stated in Section 8.4.

The CA shall publicly disclose its CA business practices to the extent required by the WebTrust Principles and Criteria for Certification Authorities 2.2.1 as well as additional ecosystem-dependent requirements and agreements.

8.2 Identity/Qualifications of Assessor

The CA's audit SHALL be performed by an External Compliance Auditor which is a Qualified Auditor. A Qualified Auditor means a natural person, Legal Entity, or group of natural persons or Legal Entities that collectively possess the following qualifications and skills:

1. Independence from the subject of the audit
2. The ability to conduct an audit according to applicable WebTrust principles and criteria as detailed in [11] § 8.4
3. Employs individuals who have proficiency in examining Public Key Infrastructure technology, information security tools and techniques, information technology and security auditing, and the third-party attestation function
4. Be a licensed WebTrust practitioner
5. Bound by law, government regulation, or professional code of ethics

6. Maintains Professional Liability/Errors & Omissions insurance with policy limits of at least one million US dollars in coverage
7. Approved by the CAB Forum and Mozilla, according to the Mozilla Root Store Policy [14].

8.3 Assessor's Relationship to Assessed Entity

The External Compliance Auditor either shall be a private firm that is independent from the entity being audited, or it shall be sufficiently organizationally separated from those entities to provide an unbiased, independent evaluation. External Compliance Auditors shall not have a conflict of interest that hinders their ability to perform auditing services.

To ensure independence and objectivity, the External Compliance Auditor may not have served the entity in developing or maintaining the entity's CA facilities or CPS. Each PA shall determine whether an External Compliance Auditor meets this requirement.

8.4 Topics Covered By Assessment

CA shall undergo an annual compliance audit in accordance with

(1) "WebTrust Principles and Criteria for Certification Authorities", version 2.2 or newer; and
(2) either
    a. "WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security", version 2.7 or newer; or
    b. "WebTrust Principles and Criteria for Certification Authorities – SSL Baseline", version 2.8 or newer; and "WebTrust Principles and Criteria for Certification Authorities – Network Security", version 1.0 or newer.

Additionally, the CA will be audited for compliance with the requirements relevant to each ecosystem as indicated in Section 7.1, table column titled "Reference for Cert Profiles".

The purpose of the compliance audit shall be to verify that a CA complies with all the mandatory requirements of the current versions of this CP/CPS.

All aspects of the CA operation shall be subject to the compliance audit and should address the items listed below. A WebTrust for Certification Authorities or equivalent will satisfy this requirement.

- Identify foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of any Certificate Data or Certificate Management Processes;

- Assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of the Certificate Data and Certificate Management Processes; and
- Assess the sufficiency of the policies, procedures, information systems, technology, and other arrangements that the CA has in place to counter such threats.

8.5 Actions Taken as a Result of Deficiency

When the External Compliance Auditor finds a discrepancy between the requirements and stipulations of this CP/CPS and the design, operation, or maintenance of the PKI Authorities, the following actions shall be performed:

- The External Compliance Auditor shall note the discrepancy
- The External Compliance Auditor shall notify the parties identified in Section 8.6 of the discrepancy
- The party responsible for correcting the discrepancy will propose a remedy, including expected time for completion, to the parties identified in Section 8.6

In the event the audited entity fails to develop a corrective action plan to be implemented in a timely manner, or if the report reveals exceptions or deficiencies that the PA reasonably believes poses an immediate threat to the security or integrity of the PKI ecosystem, the PA will take actions that are appropriate to an agreement that is in place between the CA Operator and the PA.

8.6 Communications of Results

Audit results shall be communicated to the PA and may be communicated to others as deemed appropriate, including third parties entitled or required to be notified of audit results by law, regulation or agreement. Audit compliance will be communicated to other interested parties that may be ecosystem-dependent (such as Application Service Suppliers and browser vendors for Publicly-Trusted Certificates).

For CAs subject to the requirements of [11], audit reports shall contain the applicable required information detailed in [11]. Audit reports shall be made publicly available through the document repository in Section 2.1 no later than three months after the end of the audit period.

Audit reports which are being supplied to maintain a certificate within the Mozilla root program shall be provided to Mozilla via the CCADB within three months of the point-in-time date or the end date of the period.

8.7 Self-Audits

During the period in which the CA issues Certificates, the CA shall monitor adherence to this document and strictly control its service quality by performing self-audits.

For CAs capable of issuing Publicly-Trusted certificates, CA shall perform a self-audit on at least a quarterly basis against a randomly selected sample of the greater of one certificate or at least three percent of the Certificates issued by it during the period commencing immediately after the previous self-audit sample was taken. The CA shall validate the quality of the public key in each such sample certificate against industry best practice.

9. Other Business and Legal Matters

This chapter specifies requirements on general business and legal matters.

9.1 Fees

The CA Operator shall establish fees that are in agreement with a particular PKI ecosystem and policies of the PA.

9.1.1 Certificate Issuance or Renewal Fees

Subscribers may be charged a fee for the issuance, management, and renewal of certificates.

9.1.2 Certificate Access Fees

CAs shall not charge a fee as a condition of making a Certificate available in a repository or otherwise making Certificates available to Relying Parties.

9.1.3 Revocation or Status Information Access Fees

CAs shall not charge a fee as a condition of making CRLs or OCSP Responders available in a repository or otherwise available to Relying Parties.

9.1.4 Fees for Other Services

No stipulation.

9.1.5 Refund Policy

Refund policies should be stipulated in the appropriate agreement (e.g., Digital Certificate Authorization Agreement).

9.2 Financial Responsibility

9.2.1 Insurance Coverage

PKI Participants should maintain a commercially reasonable level of insurance coverage for errors and omissions, either through an errors and omissions insurance program with an insurance carrier or a self-insured retention.

9.2.2 Other Assets

CAs shall have sufficient financial resources to maintain their operations and perform their duties, and they shall be reasonably able to bear the risk of liability to Subscribers and Relying Parties.

9.2.3 Insurance or Warranty Coverage for End-Entities

No stipulation.

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

The following Subscriber information shall be kept confidential and private:

- CA application records
- Certificate Application records
- Personal or non-public information about Subscribers
- Transactional records (both full records and the Audit trail of transactions)
- Audit trail records
- Audit reports
- Contingency planning and disaster recovery plans
- Security measures controlling the operations of CA hardware and software

9.3.2 Information Not Within the Scope of Confidential Information

Certificates, Certificate revocation, and other status information, certificate and CRL repositories, and information contained within them, shall not be considered Confidential/Private Information.

9.3.3 Responsibility to Protect Confidential Information

All PKI Participants under this CP/CPS receiving private information shall secure it from compromise and disclosure to third parties.

9.4 Privacy of Personal Information

It is the responsibility of all parties to ensure privacy of personal information under their control. No personal information is registered or certified. If a party collects, transmits or stores personal information, its practices will comply with all applicable laws.

9.4.1 Privacy Plan

All customer information and all customer-specific reports regarding certificate issuance, revocations and usage shall be restricted to only the specified CA Operator personnel on a need-to-know basis. None of this information may be released to the rest of Vistance Networks or outside of Vistance Networks at any time, with the following notable exceptions:

a) When required by law within the applicable jurisdiction
b) When explicitly authorized by the affected Subscriber
c) When explicitly authorized by the PA for a specific ecosystem and when in-line with the PA agreements such as a DCAA (Digital Certificate Authorization Agreement) or a Subscriber Agreement.

Aggregate information on CA statistics which does not reveal specific customer information may be shared internally with Vistance Networks' management if explicitly permitted by the PA.

Vistance Networks' privacy policy is published at https://www.vistancenetworks.com/about-us/privacy-statement/.

9.4.2 Information Treated as Private

CAs acquiring services under this policy shall protect all Subscriber personally identifying information from unauthorized disclosure. Records of individual transactions may be released upon request of any Subscribers involved in the transaction or their legally recognized agents. The contents of the archives maintained by CAs operating under this policy shall not be released except as required by law.

9.4.3 Information Not Deemed Private

Information included in certificates and CRLs is deemed public information and is not subject to protections outlined in Section 9.4.2.

9.4.4 Responsibility to Protect Private Information

Sensitive information shall be stored securely, and may be released only in accordance with other stipulations in Section 9.4.

9.4.5 Notice and Consent to use Private Information

CAs are not required to provide any notice or obtain the consent of the Subscriber in order to release private information in accordance with other stipulations in Section 9.4.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

Except as required for operation of the PKI system, as expressly permitted or required under the CP/CPS, or as required by applicable law, no private information will be disclosed without the express written consent of the party to which that private information pertains.

9.4.7 Other Information Disclosure Circumstances

No stipulation.

9.5 Intellectual Property Rights

CAs retain all Intellectual Property Rights in and to the Certificates and revocation information that they issue.

A Certificate Applicant retains all rights it has (if any) in any trademark, service mark, or trade name contained in any Certificate Application and DN within any Certificate issued to such Certificate Applicant.

Private keys corresponding to Certificates of CAs and Subscribers are the property of the CAs and Subscribers that are the respective Subjects of these Certificates. Secret Shares of a CA's private key are the property of the CA, and the CA retains all Intellectual Property Rights in and to such Secret Shares.

9.6 Representations and Warranties

The PA shall:

- Review periodic compliance audits to ensure that CAs are operating in compliance with this CP/CPS
- Review name space control procedures to ensure that distinguished names are uniquely assigned for all certificates issued under this CP/CPS
- Revise this CP/CPS to maintain the level of assurance and operational practicality
- Publicly distribute this CP/CPS

9.6.1 CA Representations and Warranties

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

- A Subscriber that is a party to the Subscriber Agreement or Terms of Use for the Certificate

In the case of Publicly-Trusted Certificates, additional Certificate Beneficiaries include:

- All Application Software Suppliers with whom the Root CA has entered into a contract for inclusion of its Root Certificate in software distributed by such Application Software Supplier
- All Relying Parties who reasonably rely on a Valid Certificate.

The CA represents and warrants to the Certificate Beneficiaries that, during the period when the Certificate is valid, the CA has complied with this CP/CPS in issuing and managing the Certificate.

CAs operating under this CP/CPS shall warrant that:

1. The CA procedures are implemented in accordance with this CP/CPS
2. The CA operations are maintained in conformance to the stipulations of the approved CP/CPS
3. Any certificate issued is in accordance with the stipulations of this CP/CPS
4. There are no material misrepresentations of fact in the Certificate known to or originating from the entities approving the Certificate Application or issuing the Certificate
5. There are no errors in the information in the Certificate that were introduced by the entities approving the Certificate Application as a result of a failure to exercise reasonable care in managing the Certificate Application
6. Their Certificates meet all material requirements of this CP/CPS

7. The revocation of certificates in accordance with the stipulations in this CP/CPS. The CA will revoke the Certificate for any of the reasons specified in this CP/CPS.
8. Revocation services' (when applicable) use of a repository conforms to all material requirements of this CP/CPS in all material aspects.
9. Authorization for Certificate: That, at the time of issuance, the CA (i) implemented a procedure for verifying that the Subject authorized the issuance of the Certificate and that the Applicant Representative is authorized to request the Certificate on behalf of the Subject; (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in this CP/CPS.

In addition, for CAs that issue Publicly-Trusted Certificates, the CA warrants that:

10. Right to use domain name or IP Address: at the time of issuance, the CA (i) implemented a procedure for verifying that the Applicant either had the right to use, or had control of, the Domain Name(s) and IP address(es) listed in the Certificate's subject field and subjectAltName extension; (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in this CP/CPS.
11. Accuracy of information: That, at the time of issuance, the CA (i) implemented a procedure for verifying the accuracy of all of the information contained in the Certificate (with the exception of the subject:organizationalUnitName attribute); (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in this CP/CPS.
12. No misleading information: That, at the time of issuance, the CA (i) implemented a procedure for reducing the likelihood that the information contained in the Certificate's subject:organizationalUnitName attribute would be misleading; (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in this CP/CPS.
13. Identity of Applicant: That, if the Certificate contains Subject Identity Information, the CA (i) implemented a procedure to verify the identity of the Applicant in accordance with Section 3.2; (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in this CP/CPS.
14. Subscriber Agreement: That, if the CA and Subscriber are not Affiliated, the Subscriber and CA are parties to a legally valid and enforceable Subscriber Agreement that satisfies this CP/CPS, or, if the CA and Subscriber are the same entity or are Affiliated, the Applicant Representative acknowledged the Terms of Use.

Subscriber Agreements may include additional representations and warranties. If the Relying Party does not check the status of the certificates as described in this

document, the CA warranties to Relying Parties as described in Section 9.6.1 do not apply.

9.6.2 RA Representations and Warranties

RAs that perform registration functions under this CP/CPS shall warrant that:

- The RA complies with the stipulations of this CP/CPS
- The RA complies with and maintains its operations in conformance to the stipulations of the approved CPS
- There are no material misrepresentations of fact in the Certificate known to or originating from the entities approving the Certificate Application or issuing the Certificate
- There are no errors in the information in the Certificate that were introduced by the entities approving the Certificate Application as a result of a failure to exercise reasonable care in managing the Certificate Application
- Their Certificates meet all material requirements of this CP/CPS
- Revocation services (when applicable) and use of a repository conform to all material requirements of this CP/CPS in all material aspects

Subscriber Agreements may include additional representations and warranties.

9.6.3 Subscriber Representations and Warranties

Subscribers shall sign an agreement containing the requirements the Subscriber shall meet, including protection of their private keys and use of the Certificates before being issued the Certificates. In addition, Subscribers shall warrant that:

- The Subscriber shall abide by all the terms, conditions, and restrictions levied on the use of their private keys and Certificates.
- Each digital signature created using the private key corresponding to the public key listed in the Certificate is the digital signature of the Subscriber and the Certificate has been accepted and is operational (not expired or revoked) at the time the digital signature is created.
- Subscriber's private keys are protected from unauthorized use or disclosure. Subscriber will take all reasonable measures to assure control of, keep confidential, and properly protect at all times the Private Key that corresponds to the Public Key to be included in the requested Certificate(s) (and any associated activation data or device, e.g. password or token).
- All representations made by the Subscriber in the Certificate Application the Subscriber submitted are true.
- All information supplied by the Subscriber and contained in the Certificate is true.

- The Certificate is being used exclusively for authorized and legal purposes, consistent with all material requirements of this CP/CPS.
- The Subscriber will promptly notify the appropriate CA upon suspicion of misuse, loss or Compromise of the Subscriber's Private Key associated with the Public Key included in the Certificate.
- The Subscriber is an end-user Subscriber and not a CA, and is not using the private key corresponding to any public key listed in the Certificate for purposes of digitally signing any Certificate (or any other format of certified public key) or CRL, as a CA or otherwise.

Subscriber of Publicly-Trusted Certificates shall additionally warrant that:

- Subscriber will review and verify the Certificate contents for accuracy.
- Certificate is installed only on servers that are accessible at the subjectAltName(s) listed in the Certificate.
- Promptly request revocation of the Certificate, and cease using it, if any information in the Certificate is or becomes incorrect or inaccurate.
- Subscriber will promptly cease all use of the Private Key corresponding to the Public Key included in the Certificate upon revocation of that Certificate for reasons of Key Compromise.
- The Subscriber will notify the CA of any material changes to their organization name, company's legal status, address or contact information within 3 business days of any such occurrence.
- Subscriber will respond to the CA's instructions concerning Key Compromise or Certificate misuse within a specified time period.
- Subscriber acknowledges and accepts that the CA is entitled to revoke the certificate immediately if the Applicant were to violate the terms of the Subscriber Agreement or Terms of Use or if revocation is required by this CP/CPS.

Subscriber Agreements may include additional representations and warranties. Subscriber Agreements shall be reviewed for enforceability.

9.6.4 Relying Party Representations and Warranties

This CP/CPS does not specify the steps a Relying Party should take to determine whether to rely upon a certificate. The Relying Party decides, pursuant to its own policies, what steps to take. The CA merely provides the tools (i.e., certificates and CRLs) needed to perform the trust path creation, validation, and CP/CPS mappings that the Relying Party may wish to employ in its determination. Relying Parties acknowledge that they have sufficient information to make an informed decision as to the extent to which they choose to rely on the information in a Certificate, that they are solely responsible for deciding whether or not to rely on such information,

and that they shall bear the legal consequences of their failure to perform the Relying Party obligations in terms of this CP/CPS.

9.6.5 Representations and Warranties of Other Participants

No stipulation.

9.7 Disclaimers of Warranties

Determined by project-specific agreements and PA.

9.8 Limitations of Liability

In this section (i.e., Section 9.8), as well as Section 9.9 and its subsections, "the CA" means ARRIS Technology, Inc. and its Affiliates.

The liability (and/or limitation thereof) between the CA and a Subscriber shall be as set forth in the applicable DCAAs, Subscriber Agreements or Terms of Use. If the CA has issued and managed the Certificate in compliance with this CP/CPS, the CA may disclaim liability to the Certificate Beneficiaries or any other third parties for any losses suffered as a result of the use or reliance on such Certificate beyond those specified in this CP/CPS.

If the CA has not issued or managed the Certificate in compliance with its CP/CPS, the CA may seek to limit its liability to the Subscriber and to Relying Parties, regardless of the cause of action or legal theory involved, for any and all claims, losses or damages suffered as a result of the use or reliance on such Certificate by any appropriate means that the CA desires.

9.9 Indemnities

9.9.1 Indemnification by CAs

Within the scope of CAs that issue Publicly-Trusted Certificates, the CA understands and acknowledges that the Application Software Suppliers who have a Root Certificate distribution agreement in place with the Root CA do not assume any obligation or potential liability of the CA under this CP/CPS or that otherwise might exist because of the issuance or maintenance of Certificates or reliance thereon by Relying Parties or others. The CA shall defend, indemnify, and hold harmless each Application Software Supplier for any and all claims, damages, and losses suffered by such Application Software Supplier related to a Certificate issued by the CA, regardless of the cause of action or legal theory involved. This does not apply, however, to any claim, damages, or loss suffered by such Application Software Supplier related to a Certificate issued by the CA where such claim, damage, or loss was directly caused by such Application Software Supplier's software displaying as not trustworthy a Certificate that is still valid, or displaying as trustworthy: (1) a Certificate that has expired, or (2) a Certificate that has been revoked (but only in

cases where the revocation status is currently available from the CA online, and the application software either failed to check such status or ignored an indication of revoked status).

9.9.2 Indemnification by the Subscribers

To the extent permitted by applicable law, Subscribers are required to indemnify the CA for:

- Any falsehood or misrepresentation of fact by the Subscriber on its 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
- The Subscriber's failure to take the precautions necessary to prevent the compromise, loss, disclosure, modification, or unauthorized use of the Subscriber's private key(s)
- The Subscriber's use of a name (including one that infringes upon the Intellectual Property Rights of a third party)

9.9.3 Indemnification by Relying Parties

To the extent permitted by law, each Relying Party shall indemnify the CA and their respective directors, officers, employees, agents and contractors against any loss, damage, or expense, including reasonable attorney's fees, related to the Relying Party's

- Breach of applicable law
- Unreasonable reliance on a certificate
- Failure to check the certificate's status prior to use

9.10 Term and Termination

9.10.1 Term

No stipulation.

9.10.2 Termination

This CP/CPS as amended from time to time shall remain in force until it is replaced by a new version.

9.10.3 Effect of Termination and Survival

Upon termination of this CP/CPS, PKI Participants are nevertheless bound by its terms for all certificates issued for the remainder of the validity periods of such certificates.

9.11 Individual Notices and Communications with Participants

Unless otherwise specified by agreement between the parties, PKI participants shall use commercially reasonable methods to communicate with each other, taking into account the criticality and subject matter of the communication.

9.12 Amendments

9.12.1 Procedure for Amendment

We shall review this CP/CPS at least once every year. Corrections, updates, or changes to this CP/CPS shall be made available as per Section 9.12.2 and may be subject for approval by one or more PAs for different ecosystems. Suggested changes to this CP/CPS shall be communicated to the contact in Section 1.5.2; such communication shall include a description of the change, a change justification, and contact information for the person requesting the change.

Certificate Application and request validation methods are occasionally found to contain security flaws. When this happens as applicable to Certificate Authorities governed by the CAB Forum ecosystem, we shall evaluate existing practices and respond appropriately to mitigate the risk. We shall make a disclosure and/or modification to address such security flaws if requested by Mozilla, including immediately discontinuing the use of a method with the newly discovered security flaw.

9.12.2 Notification Mechanism and Period

We reserves the right to amend the CP/CPS without notification for amendments that are not material, including without limitation corrections of typographical errors, changes to URLs, and changes to contact information. The decision to designate amendments as material or non-material shall be within our sole discretion.

Change notices to this CP/CPS shall be distributed electronically to PKI Participants and observers in accordance with the document change procedures for each ecosystem.

9.12.3 Circumstances Under Which OID Must be Changed

Object Identifiers (OIDs) are specified in ecosystem-specific certificate and CRL profiles. If the corresponding industry forum decides to amend certificate or CRL profiles, including a change in the OIDs, CA Operator will make the necessary changes to comply.

Furthermore, any change to this CP/CPS which substantially affects the operation of CAs issuing Publicly-Trusted Certificates will also alter the OID of the new version of this CP/CPS.

9.13 Dispute Resolution Provisions

Dispute resolution will differ on a per-ecosystem basis and depends on the applicable business agreements between the PKI participants.

9.14 Governing Law

Governing law will differ on a per-ecosystem basis and depends on the applicable business agreements between the PKI participants as well as on the jurisdiction.

9.15 Compliance with Applicable Law

This CP/CPS is subject to applicable national, state, local, and foreign laws, rules, regulations, ordinances, decrees, and orders including, but not limited to, restrictions on exporting or importing software, hardware, or technical information. All CAs operating under this policy are required to comply with applicable law.

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

No stipulation.

9.16.2 Assignment

No stipulation.

9.16.3 Severability

Should it be determined that one section of this CP/CPS is incorrect or invalid, the other sections of this CP/CPS shall remain in effect until the CP/CPS is updated. The process for updating this CP/CPS is described in section 9.12.

In the event that a clause or provision of this CP/CPS is held to be unenforceable by a court of law or other tribunal having authority, the remainder of the CP/CPS shall remain valid.

Additionally, for CAs that issue Publicly-Trusted Certificates under the CA/Browser Forum ecosystem:

- In the event of a conflict between this CP/CPS and a law, regulation or government order (hereinafter 'Law') of any jurisdiction in which a CA operates or issues certificates, a CA may modify any conflicting requirement to the minimum extent necessary to make the requirement valid and legal in the jurisdiction. This applies only to operations or certificate issuances that are subject to that Law. In such event, the CA shall immediately (and prior to issuing a certificate under the modified requirement) include in Section 9.16.3 of the CA's CP/CPS a detailed reference to the Law requiring a

modification of the Baseline Requirements under this section, and the specific modification to this CP/CPS implemented by the CA.

- The CA shall also (prior to issuing a certificate under the modified requirement) notify the CA/Browser Forum of the relevant information newly added to its CP/CPS by sending a message to questions@cabforum.org and receiving confirmation that it has been posted to the Public Mailing List and is indexed in the Public Mail Archives available at https://cabforum.org/pipermail/public/ (or such other email addresses and links as the Forum may designate), so that the CA/Browser Forum may consider possible revisions to [11] accordingly.
- Any modification to CA practice enabled under this section shall be discontinued if and when the Law no longer applies, or [11] is modified to make it possible to comply with the CA/Browser Forum requirements and the Law simultaneously. An appropriate change in practice, modification to the CA's CP/CPS and a notice to the CA/Browser Forum, as outlined above, shall be made within 90 days.

9.16.4 Enforcement (Attorney's fees and waiver of rights)

No stipulation.

9.16.5 Force Majeure

To the extent permitted by applicable law, Subscriber Agreements and DCAAs shall include a force majeure clause protecting PA and the applicable Subscriber.

9.17 Other Provisions

No stipulation.