ARRIS Certificate Policy
Version 1.4.2

Doc# PR5031

8/15/2019

Table of Contents

1. INTRODUCTION

The procedures described in this document are limited to certificate issuance, delivery and revocation – as applicable to ARRIS's external PKI services that are hosted on the system called PKIWorks where all key and certificate generation is done in an offline air-gapped facility called ARRIS KGF (Key Generation Facility).

This CP encompasses PKI for many ecosystems, including DOCSIS 3.0 and 3.1, OpenCable host and CableCARD, PacketCable, etc. Because of that, there are a number of ecosystem-specific parameters to this policy that may point to other documents, including:

- Definition of a Policy Authority (PA) for that ecosystem and PA member contact information. See section 1.5 on the definition of a PA.
- Certificate profile
- Validity period nesting is required or not for a specific ecosystem?
- CRL profile
- 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. ARRIS expects to hold audits at the frequency that will satisfy all the current PKI ecosystems and using a firm that complies with all the ecosystem-specific requirements.
- Additional ecosystem-specific PKI requirements not covered by this CP

1.1 Overview

The policies, described in this document are compliant with RFC 3647. CommScope has purchased ARRIS and is now the parent company of ARRIS. This business transaction does not affect any of the business or technical terms outlined in this document.

1.2 Document Name and Identification

This CP is known as the "ARRIS CP".

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, Inrternet X.509 Public Key Infrastructure Certificate and CRL Profile, IETF, May 2008.

1.3 PKI Participants

The following are relevant to the administration and operation of the ARRIS PKI.

1.3.1 Certification Authorities

The CA is the collection of technology and procedures that issues PKCs (Public Key Certificates) under this ARRIS CP. ARRIS is the CA operator which performs the actual CA operations (such as creation of all the CA Certificates) on behalf of customers.

Subscriber is an entity that receives device PKCs from one of the Device Certificate Authorities operated by ARRIS.

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 and ensuring that they are performed in accordance with the requirements, representations, and warranties of this CP
- 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 is intended to be common to a number of different ecosystems and PKI echo systems in which ARRIS is providing a managed PKI service. Each ecosystem has its own certificate profiles specified and typically for each ecosystem there are:

- A single Root CA
- A chain of one or more Sub-CAs that are under the Root CA.

All security policies in this document are common to these ecosystems. The CPS has a separate section outlining a list of ecosystem-specific certificate and CRL profiles and parameters.

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 the CP and this 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, RA function is performed by CA Officers and in that case it is part of the ARRIS 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). An authorized representative of the Subscriber, acting as a Certificate Applicant, shall complete the certificate application process established by the PA. 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 can 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 PA, 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 DCAA agreement and certificate policy requirements for Subscribers may vary per ecosystem and are out of scope of this document.

1.3.4 Relying Parties

The Relying Party is any entity that validates the binding of a public key to the Subscriber's name in a device certificate. The Relying Party is responsible for deciding whether or how to check the validity of the certificate by checking the appropriate certificate status information. The Relying Party can use the certificate to verify the integrity of a digitally signed message, to identify the initiator of a communication, or to establish confidential communications with the holder of the certificate.

1.3.5 Other Participants

No stipulation.

1.4 Certificate Usage

This CP applies to all PKI Participants for a particular ecosystem, including Subscribers and Relying Parties. This CP sets forth policies governing the use of ARRIS-issued Certificates. 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 specified which certificates belong to a Certificate Authority which 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

The ARRIS PA is responsible for all aspects of this CP and approval of all related PKI agreements. ARRIS 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 Certificate Practice Statement (CPS), customer facing agreements and forms. PA approval is also required for CA Certificate revocation approvals and large-scale device certificate revocation approvals.

All communications with the ARRIS PA, including this CP should be directed to:

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

or

ARRIS

ATTN: ARRIS Advanced PKI Policy Authority

6450 Sequence Dr.

San Diego, CA 92121, USA

1.5.1 Organization Administering the Document

The ARRIS PA is responsible for all aspects of this CPS and approval of all related PKI agreements. See section 1.5.

1.5.2 Contact Person

See section 1.5.

1.5.3 Person Determining CPS Suitability for the Policy

See section 1.5.

1.5.4 CPS Approval Procedures

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 ARRIS CA Officer which was not the author of the 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 CPS document updates shall be provided to the Superior Entity as indicated in the CPS.

Major updates shall be approved by at least two ARRIS CA officers, none of which are the authors of the 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 CPS update. Superior Entity approval will be noted in the CPS Revision History. CPS provides Superior Entity approval requirements of the CPS for each PKI ecosystem.

1.6 Definitions and Acronyms

CA	Certification Authority
CARL	Certification Authority Revocation List
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CVC	Code Verification Certificate
DN	Distinguished Name
DTLS	Datagram Transport Layer Security
HSM	Hardware Security Module

I&A	Identification and Authentication
IETF	Internet Engineering Task Force
KGF	Key Generation Facility
OID	Object Identifier
PA	Policy Authority
PKC	Public Key Certificate
PKI	Public Key Infrastructure
RP	Relying Party
RA	Registration Authority
SP	Service Party
TLS	Transport Layer Security

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, pincodes and one-time passwords are all examples of the Activation Data.
Administrator	A trusted role that installs, configures, and maintains the CA.
Applicant	Entity which is requesting a PKC, limited to an end-entity (device or server) PKC.
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.
Backup	Copy of files and programs made to facilitate recovery if necessary.
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, including computer systems, HSMs and HSM activation devices.
CA Operator	The CA Operator is the legal entity responsible for all aspects of the issuance and management of Public Key Certificates.
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 ARRIS CP are performed in accordance with the requirements, representations, and warranties of their ARRIS CPS.

Certificate (or Public Key Certificate)	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 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 the ARRIS-Kyrio PKI ecosystem.
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.
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].
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.
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.
External Compliance Auditor	A member of an external organization that performs a Compliance Audit of the CAs under the specified Certificate Policy.
Full System Backup	A CA system backup sufficient to recover from system failure.
Key Generation Facility	Air gapped facility that includes all ARRIS operated 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.
Policy Authority	The entity that establishes certificate policies.
PKI Participant	An individual or organization that is one or more of the following: a CA, an RA or a Subscriber.

Relying Party	The entity which is in communication with an end-entity (device or server) and is responsible for validating the corresponding PKC.
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.
Shareholders	Holders of Secret Shares needed to operate a CA private key.
Subscriber	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 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.
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.

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 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 and its previous versions since the last Web of Trust audit shall be publicly accessible at http://certificates.pkiworks.com/Public/Documents/.

2.2 Publication of Certification Information

This CP, CA Certificates, and CRLs shall be publicly available. There is no requirement for the publication of CPSs of the Root CAs or Sub-CAs that issue Certificates under this CP. The CA shall protect information not intended for public dissemination.

2.3 Time or Frequency of Publication

Changes to this CP shall be made publicly available within thirty (30) days of approval by the PA.

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 ARRIS, CA Certificates shall be made publicly available within three (3) business days after issuance.

No stipulation for Device PKCs.

Publication requirements for CRLs are provided in CP § 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 CRL repository 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.

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 Types 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 out of scope of this general CP and are specified in the ecosystem-specific certificate profiles.

3.1.2 Need for Names to Be Meaningful

The Certificates issued pursuant to this CP 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 the trademark of another. Certificate Applicants shall not use names in their Certificate Applications that infringe upon the Intellectual Property Rights of others.

Any ARRIS CA 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 ARRIS CA 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

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
- 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

3.2.3 Authentication of Individual Identity

The CA's certificate issuance process shall 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.

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.

3.2.5 Validation of Authority

The CA's certificate issuance process shall confirm that the:

- Corporate Contact listed in the Digital Certificate Authorization Agreement is an officer in the organization who can sign on behalf of the organization and bind the organization to the terms and conditions of the agreement
- Representative submitting the Digital Certificate Authorization Agreement and certificate application is authorized to act on behalf of the organization
- Administrators listed on the Digital Certificate Authorization Agreement and certificate application are authorized to act on behalf of the organization
- Contacts listed on the Digital Certificate Authorization Agreement are authorized to act on behalf of the organization

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

3.2.6 Criteria for Interoperation

No stipulation.

3.3 Identification and Authentication for Re-key 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 device's current valid signature key.

3.3.2 Identification and Authentication of Re-Key and Renewal 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 per CP § 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 per CP § 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.

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
- 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 their 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.

An application for CA Certificates is not supported by the current version of the CPS. The intent is to provide managed CA services such that all CAs in an ecosystem are managed by ARRIS.

4.1.2 Enrollment Process and Responsibilities

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

- Completing the Certificate Application package
- Providing the requested information
- Responding to authentication requests in a timely manner
- Submitting required payment

Communication of information may be electronic or out-of-band.

4.2 Certificate Application Processing

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

4.2.1 Performing Identification and Authentication Functions

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

4.2.2 Approval or Rejection of Certificate Applications

ARRIS-operated RA 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 CPS or the CP

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 or CPS.

4.3 Certificate Issuance

4.3.1 CA Actions during Certificate Issuance

To issue a certificate the CA shall receive 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
- 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

4.3.2 Notification to Certificate Subject of Certificate Issuance

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. Certificates shall be made available to Subscribers, either via download from a website or via a message sent to the Subscriber containing the Certificates.

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 CP § 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 Certificate Subject 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 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, ARRIS disclaims 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, ARRIS hereby limits its liability, and excludes 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 Circumstance 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 Certificate Subject

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.

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 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 Re-Key

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 Re-key

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.

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 that prior to their expiration

4.7.3 Processing Certificate Re-keying Requests

For certificate re-key, the CA shall confirm the identity of the Subscriber in accordance with the requirements specified in this CP § 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 Certificate Subject

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

4.8.5 Conduct Constituting Acceptance of Modified Certificate

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

4.8.6 Publication of the Modified Certificate by the CA

Publication of a modified certificate shall be in accordance with CP § 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 CP § 4.4.3.

4.9 Certificate Revocation and Suspension

CAs operating under this CP 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. Examples of circumstances that invalidate the binding are:

- The Subscriber or an authorized representative of the Subscriber asks for the Certificate to be revoked for any reason whatsoever
- The Subscriber's private key corresponding to the public key in the Certificate has been lost or Compromised:
    - Disclosed without authorization
    - Stolen
- The Subscriber can be shown to have violated the stipulations of its DCAA
- The DCAA with the Subscriber has been terminated
- There is an improper or faulty issuance of a Certificate
- A prerequisite to the issuance of the Certificate can be shown to be incorrect if:
    - Information in the Certificate is known, or reasonably believed, to be false
    - 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
    - The Subscriber has not submitted payment when due

- Identifying information of the Subscriber in the Certificate becomes invalid
- Attributes asserted in the Subscriber's Certificate are incorrect
- The Certificate was issued:
    - In a manner not in accordance with the procedures required by the applicable CPS
    - To an entity other than the one named as the Subject of the Certificate. Unless the entity is authorized to use that name.
    - Without the authorization of the entity named as the Subject of such Certificate
- The Subscriber's organization name changed
- The CA determines that any of the information appearing in the Certificate is inaccurate or misleading
- 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
- The CA finds that in the ordinary course of business that the certificate should be revoked
- In exigent and/or emergency situation

Whenever any of the above circumstances 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.

4.9.2 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 the CPS.

4.9.3 Procedure for Revocation Request

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. The CA shall specify the steps involved in the process of requesting a Certificate revocation in its CPS.

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.

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.

4.9.3.2 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. 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 CP § 4.9.1.

4.9.5 Time within which CA Must Process the Revocation Request

For PKI ecosystems where a CA is permitted to initiate revocation, CAs shall begin investigation of a Certificate revocation request within two (2) business days of receipt to decide whether revocation or other appropriate action is warranted based upon the circumstances of the request in CP § 4.9.1.

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

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 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 the CPS.

The value of the nextUpdate field in the CRL shall be determined based on a ecosystem-specific CRL profile. Unless otherwise specified in a ecosystem-specific CRL profile, in the absence of a revocation event CRLs shall be updated once every twelve (12) months.

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.

4.9.9 On-line 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.

4.9.10 On-line Revocation Checking Requirements

A Relying Party should check the status of a certificate on which they wish to rely. If the Relying Party does not check the status of the certificates as described in this paragraph or the CPS, the Relying Party shall not assert any claim against the CA related to or arising out of the Relying Party's reliance on the certificate.

4.9.11 Other Forms of Revocation Advertisements Available

No stipulation.

4.9.12 Special Requirements Regarding Key Compromise

When a CA Certificate is revoked a CRL shall be issued within 24 hours of notification.

4.9.13 Circumstances for Suspension

PKC suspension is not supported under this CP.

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

Certificate status shall be available via CRL through a URL specified in a CA's CPS.

4.10.2 Service Availability

Certificate Status Services shall be available 24 x 7. CRL capability should provide a response time of ten (10) seconds or less under normal operating conditions.

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. MANAGEMENT, OPERATIONAL, AND PHYSICAL 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.

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 KGF
- 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 to the KGF
- 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 KGF 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 primary and backup power systems 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.

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.

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 CP § 5.3.2.

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 that materially affect:

- CA Administrator – administration, maintenance, creation and destruction of hardware and software that is relevant to the operation of the CAs covered under this CP.
- 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
- CA signing key activation
- CA private key backup and access to the CA backup keys

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 CP § 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.

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 CP § 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 set forth in the CPS.

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
- 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

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 KGF shall be escorted by authorized CA Trusted Persons at all times.

From time to time, PKI Center also hires 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 ARRIS employees. All requirements for permanent ARRIS personnel that work in the KGF or otherwise participate in the operation and management of the ARRIS CA 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.

shall

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 of event;
- The time the event occurred;
- A success or failure indication for signing;
- The identity of the equipment operator who initiated the action; and,

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.

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
  - Access to the CA server
  - Known or suspected violations of physical security
  - Electrical power outages
- CA Configuration:
  - CA hardware configuration
  - Installation of the operating system
  - Installation of the CA software
  - System configuration changes and maintenance
  - Installation of hardware cryptographic modules
  - Cryptographic module lifecycle management-related events (e.g., receipt, use, de-installation, and retirement)
- Account Administration:
  - System Administrator accounts
  - Roles and users added or deleted to the CA system
  - 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:
  - Key generation
  - 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)
- Certificate lifecycle events:
  - Issuance

    - Re-key
    - Renew
    - Revocation
- Trusted employee events:
    - Logon and logoff
    - Attempts to create, remove, set passwords or change the system privileges of the privileged users
    - Unauthorized attempts to the CA system,
    - Unauthorized attempts to access system files,
    - Failed read and write operations on the Certificate
    - Personnel changes
- Token events:
    - Serial number of tokens shipped to Subscriber
    - Account Administrator Certificates
    - Shipment of tokens
    - Tokens driver versions

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.

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.

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

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. 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.

5.5 Records Archive

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 Events 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
- Records of all actions taken on Certificates issued and/or published
- Record of re-key
- Revocation request information
- Records of all CRLs issued and/or published
- 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.

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.

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 Recovery Procedures for Key Compromise

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 ARRIS, ARRIS 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, and maintain a Disaster Recovery Plan designed to mitigate the effects of any kind of natural or man-made disaster. 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.

Additionally, the Plan shall include:

- 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 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 CP § 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, ARRIS 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 CPS § 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

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

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.

6.1.1.2 Subscriber Key Pair Generation

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 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.
- 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.
- 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.

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 a PKCS #8 package or, in CableLabs' sole discretion, any other comparably equivalent means (e.g., encryption) 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 the Certificate Applicant possesses the private key corresponding to the transferred public key. The Certificate Applicant will 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.

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 aredelivered 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 the CPS.

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.

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

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

6.2 Private Key Protection and Cryptographic Module Engineering Controls

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 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 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 section 5.5.

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

CA private keys may be exported from the cryptographic module only to perform CA key backup procedures, as described in CP 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.

6.2.7 Private Key Storage on Cryptographic Module

No stipulation beyond that specified in FIPS 140-2 for CA private keys.

6.2.8 Method of Activating Private Keys

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 § 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 CP § 6.2.2. Once the private key is activated, it shall be active until termination of the session.

6.2.8.3 Online Subordinate CA Private Keys

All online CAs under this CP are online on an isolated network and are not online in a sense of being connected to the Internet or a company Intranet.

An online CA's private key shall be activated by a threshold number of Shareholders, as defined in CP § 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 Methods of Deactivating Private Keys

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 offline 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 is taken offline, 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.

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 CP § 6.2.1.

6.3 Other Aspects of Key Management

6.3.1 Public Key Archival

CAs may archive their public keys in accordance with CP § 5.5.1.

6.3.2 Certificate Operational Periods/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.

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 as set forth in the respective CPS.

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.

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 CP § 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 CP § 5.4.1. 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.

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.

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 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.

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:

- Require authenticated logins
- 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.

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 CP § 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.

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.

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

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.

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 and CRLs shall contain time and date information. Such time information need not be cryptographic-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 CP § 5.4.1).

7. CERTIFICATE AND CRL PROFILES

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

7.1 Certificate Profile

Ecosystem specific certificate profiles shall be specified in the CPS.

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 CPS.

7.1.4 Name Forms

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

7.1.5 Name Constraints

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

7.1.6 Certificate Policy Object Identifier

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

7.1.7 Usage of Policy Constraints Extension

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

7.1.8 Policy Qualifiers Syntax and Semantics

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

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

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

7.2 CRL Profile

Ecosystem specific CRL profiles shall be specified in the CPS.

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 the CPS.

7.3 OCSP Profile

No stipulation.

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.

8.1 Frequency of Audit or Assessments

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 the CPS.

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

8.2 Identity & Qualifications of Assessor

External Compliance Auditors performing the Audit shall be either 1) from an independent Audit firm that is approved to Audit according to AICPA/CICA WebTrust for Certification Authorities principles and criteria, or 2) an IT security specialist and PKI subject matter expert who can offer input regarding acceptable risks, mitigation strategies, and industry best practices.

The qualified audit firm shall be bound by law, government regulation, or professional code of ethics and shall maintain Professional Liability/Errors & Omissions insurance with policy limits of at least one million US dollars in coverage.

8.3 Assessor's Relationship to Assessed Entity

The 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 insure independence and objectivity, the External Compliance Auditor may not have served the entity in developing or maintaining the entity's Key Generation Facility or CPS. Each PA shall determine whether an External Compliance Auditor meets this requirement.

8.4 Topics Covered By Assessment

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. The Audit must be a WebTrust for Certification Authorities or an equivalent Audit standard approved by PA.

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 of this CP or the stipulations in the 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 CP § 8.6 of the discrepancy; and
- The party responsible for correcting the discrepancy will propose a remedy, including expected time for completion, to the parties identified in CP § 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 Communication of Results

Audit results shall be communicated to the PA and may be communicated to others as deemed appropriate.

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 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 Private Information

All PKI Participants under this CP 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 ARRIS or outside of ARRIS 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 the DCAA (Digital Certificate Authorization Agreement).

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

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 pubic 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/Administrative Process

Except as required for operation of the PKI system, as expressly permitted or required under the CP, 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:

- Approve the CPS for each CA that issues certificates under this policy
- Review periodic compliance audits to ensure that CAs are operating in compliance with their approved CPSs
- Review name space control procedures to ensure that distinguished names are uniquely assigned for all certificates issued under this CP
- Revise this CP to maintain the level of assurance and operational practicality
- Publicly distribute this CP
- Coordinate modifications to this CP to ensure continued compliance by CAs operating under approved CPSs

9.6.1 CA Representations and Warranties

CAs operating under this CP shall warrant that:

- The CA procedures are implemented in accordance with this CP
- The CA will provide their CPS to the PA, as well as any subsequent changes, for conformance assessment
- The CA operations are maintained in conformance to the stipulations of the approved CPS
- Any certificate issued is in accordance with the stipulations of this CP
- 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 and the applicable CPS, and
- The revocation of certificates in accordance with the stipulations in this CP
- Revocation services (when applicable) and use of a repository conform to all material requirements of this CP and the applicable CPS in all material aspects.

Subscriber Agreements may include additional representations and warranties.

9.6.2 RA Representations and Warranties

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

- The RA complies with the stipulations of this CP
- 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 and the applicable CPS
- Revocation services (when applicable) and use of a repository conform to all material requirements of this CP and the applicable 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.
- 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.
- The Subscriber will promptly notify the appropriate CA upon suspicion of loss or Compromise of their private key(s).
- 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.

DCAAs may include additional representations and warranties

9.6.4 Relying Party Representations and Warranties

This CP 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 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.

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

The liability (and/or limitation thereof) of Subscribers shall be as set forth in the applicable DCAAs.

9.9 Indemnities

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

- Falsehood or misrepresentation of fact by the Subscriber on the 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 that infringes upon the Intellectual Property Rights of a third party)

9.10 Term and Termination

9.10.1 Term

No stipulation.

9.10.2 Termination

This CP 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, 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

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

9.12.2 Notification Mechanism and Period

ARRIS reserves the right to amend the CP 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 ARRIS's sole discretion.

Change notices to this CP 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 shall 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.

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 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 is incorrect or invalid, the other sections of this CP shall remain in effect until the CP is updated. The process for updating this CP is described in CP § 9.12.

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

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 (DCAAs) shall include a force majeure clause protecting PA and the applicable Subscriber.

9.17 Other Provisions

No stipulation.