Cisco RXC Certificate Policy

Cisco Systems Cryptographic Services (ciscopki-public@external.cisco.com)

Version 1.10, 2022-Jan-19

Table of Contents

Cisco Systems has implemented Certificate Authorities (CAs) to provide a source of publicly trusted *identities for clients and servers using Secure Sockets Layer (SSL) and Transport Layer Security (TLS) communications. These Certificate Authorities consist of systems, products, and services that both protect the CA's private key and manage the X.509 certificates (SSL certificates) issued from the Certificate Authority. To meet new standards for public trust, Cisco is instantiating a new root CA and subordinate CA chain, subject from initialization to the guidelines established by the Certificate Authority and Browser Forum ("CAB Forum"). The purpose of this document is to establish the frameworks for the lifecycle (issuance, renewal, revocation, etc.) of these certificates and the policies and practices that shall be applicable to them within Cisco Systems.*

Document Metadata

Version History

Version	Date	Changes
1.0	2014-Jun-30	First version of document, current through CABF Guidelines v1.1.8
1.1	2016-Nov-01	Incorporates intermediate versions and updates through CABF Guidelines v1.4.1
1.2	2017-Apr-06	Incorporates CABF Guidelines v1.4.2 and 1.4.3
1.3	2017-May-08	Clarifies IDN handling in certificates, certificate removal from CRLs, adjustments to notBefore, and use of Delegated Third Parties in CA operation; incorporates CABF Guidelines v1.4.4 through 1.4.7
1.4	2017-Aug-16	Adds Creative Commons license for distribution
1.5	2017-Sep-07	Update to CAA-specific language in section 4.2.1
1.6	2018-Feb-01	Removes redundant 'Approvals' section Incorporates Baseline Requirements updates through v1.5.4 ANNUAL REVIEWS: Merged in records of new issuances, to make the timeline clearer 1.5.3.3: Removal of exception in numbering for reviews, thus requiring version number updates always; update to language requiring version differentiation declarations. 4.9.5: Conforming revocation request periods more tightly to the BRs
1.7	2019-Feb-06	Added language to 3.1.1 about certificates containing underscore characters Changed 4.9.1.1 name to Reasons for Revoking a Subscriber and added lanuage to the section Changed 4.9.1.2 name to Reasons for Revoking a Subordinate CA Certificate and added lanuage to the section Added language to 4.9.3 and 4.9.4 Added definitions for Key Compromise and Whois
1.8	2019-April-10	Added lanuage to 3.1.1 about IP address validation. Added definitions for IP Address, IP Address Contact, and IP Address Registration Authority
1.9	2020-May-20	No changes; annual review complete
1.10	2022-Jan-19	Update OID policies table in section 1.2

Annual Reviews

Version	Date	Name	Title
1.0	2014-Jul-10	*First version issued*	
1.0	2015-Sep-25	Jos Purvis	PKI Compliance
1.1	2016-Nov-01	*New version issued*	
1.2	2017-Apr-06	*New version issued*	
1.3	2017-May-08	*New version issued*	

Version	Date	Name	Title
1.4	2017-Aug-16	*New version issued*	
1.5	2017-Sep-07	*New version issued*	
1.6	2018-Feb-01	*New version issued*	
1.7	2019-Feb-06	*New version issued*	
1.8	2019-April-10	*New version issued*	
1.9	2020-May-20	*New version issued*	
1.10	2022-Jan-19	*New version issued*	

Chapter 1. Introduction

1.1. Overview

Cisco Systems has implemented Certificate Authorities (CAs) to provide a source of publicly trusted identities for clients and servers using Secure Sockets Layer (SSL) and Transport Layer Security (TLS) communications. These Certificate Authorities consist of systems, products, and services that both protect the CA's private key and manage the X.509 certificates (SSL certificates) issued from the Certificate Authority. To meet new standards for public trust, Cisco is instantiating a new root CA and subordinate CA chain, subject from initialization to the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates established by the Certificate Authority and Browser Forum ("CAB Forum").

The purpose of this document is to establish the frameworks for the lifecycle (issuance, renewal, revocation, etc.) of these certificates and the policies and practices that shall be applicable to them within Cisco Systems.

1.1.1. Compliance

All certificate authorities subscribing to this Policy shall conform to the current version of the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, published at www.cabforum.org. In the event of any inconsistency between this document and those Requirements, those Requirements take precedence over this document.

1.2. Certificate Policy Identification

The IANA-assigned Object Identifier (OID) for the Cisco private enterprise is

`cisco OID :: = {iso(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) cisco(9)}`	`(1.3.6.1.4.1.9)`

Under this OID arc, Cisco has defined the following PKI-specific OIDs:

`cisco-pki OID ::= { cisco 21 }`	`(1.3.6.1.4.1.9.21)`
`cisco-pki-policies OID ::= { cisco-pki 1 }`	`(…9.21.1)`
`cisco-pki-policies-ssl OID ::= { cisco-pki-policies 22 }`	`(…9.21.1.22)`
`cisco-pki-policies-ssl-version OID ::= { cisco-pki-policies-ssl 0 }`	`(…9.21.1.22.0)`

This document is associated with the Cisco-assigned OID `1.3.6.1.4.1.9.21.1.22`. CAs subordinated to a subscribing root shall be assigned an OID derived from `1.3.6.1.4.1.9.21.1.22` in order of creation (for instance, the first created subordinated CA will be assigned `…21.1.22.0`), and SHALL list this OID in their Certification Practice Statement. In compliance with the CAB Forum Baseline Requirement 9.3.1, all subordinate certificate authorities subscribing to this Policy MUST contain and assert their assigned certificate policy identifier, and MUST also include `organizationName`, `localityName`, `stateOrProvinceName` (if applicable), and `countryName` in the Subject field of issued certificates. Root certificate authorities subscribing to this document MUST NOT include the `certificatePolicies` extension in their own certificates.

1.3. PKI Participants

1.3.1. Certification Authorities

The Cisco CA/B-F Root CA (known here as "RXC-R2") and its designated and approved subordinate CAs, owned by Cisco Systems Inc. and operated by Cisco Systems Corporate Information Security group, are the only CAs authorized to issue certificates under this Certificate Policy. This Policy is binding on every Authorized CA that issues certificates that identify this Policy, and governs the CA's performance with respect to all certificates it issues that reference this Policy. Specific practices and procedures by which the CA implements the requirements of this Policy are set forth by the CA in its Certification Practice Statement ("CPS").

1.3.2. Delegated Third Parties

Cisco Systems does not traditionally employ the use of Registration Authorities or other Delegated Third Parties in conjunction with certificate issuance practices. If an Issuing CA utilizes a Registration Authority to broker the application for and issuance of certificates, said third party must be declared in the Issuing CA's Certification Practice Statement. If Cisco Systems opts to employ a Delegated Third Party to operate a Certificate Authority on behalf of Cisco that is subordinated to a CA subscribed to this policy, the subordinating CA must declare this in its Certification Practice Statement.

Regardless of function, all delegated parties shall be subject to all of the requirements established in this Certificate Policy, as well as the Certification Practice Statement of the Issuing CA. In addition, Cisco Systems shall be responsible for conducting an annual review of each such third party against applicable CP and CPS documents as well as the standard WebTrust audit criteria as specified in section 8.4, or shall ensure that an Independent Auditor has completed a successful audit of the third party's relevant systems against the same set of standards.

1.3.3. Subscribers

For the purposes of this document, Subscribers are natural persons that have ultimate authority over a private key corresponding to a public key that is submitted to the certificate authority. Subscribers who have submitted a public key to an Issuing CA but have not yet received an issued certificate from the CA are known as Applicants; those who have received an issued certificate are Subscribers. Subscribers shall hold specific identifying information in the form of documentation or electronic identification that authorizes them to receive certificates from the Issuing CA; this information is explained in section 3. A Subscriber may be the Subject referred to in the Subject naming field of an issued certificate, or the Subject field may refer to an entity under the control of the Subscriber (such as a server or client device).

1.3.4. Relying Parties

Relying Parties are natural or legal persons that rely upon the digital certificate or signature verifiable with reference to a public key listed in a subscriber's certificate. For example, partners of Cisco Systems who access an HTTP resource encrypted with TLS using a server certificate issued by an Issuing CA under this policy would be considered Relying Parties.

Relying Parties may also include the following:

- Cisco agencies and businesses that contractually agree to this Policy with the Corporate Information Security Department and/or with the CA;
- Individuals that contractually agree to this Policy with the Corporate Information Security Department and/or with the CA;
- Entities that have entered into a Certificate Trust Agreement with Cisco Systems wherein this Certificate Policy is specifically referenced.

1.3.5. Other Participants

No stipulation.

1.4. Certificate Usage

1.4.1. Appropriate Certificate Uses

Certificates issued under this Certificate Policy by an Issuing CA shall be used only for the purposes identified specifically by the Issuing CA in its Certification Practice Statement, and shall include certificates issued for the purposes of secure Authentication, Identity Assurance, or Encryption and Integrity Protection of data.

1.4.2. Prohibited Certificate Uses

Certificate uses are restricted using certificate extensions on key usage and extended key usage. Usage of certificates in violation of key usage constraints is unauthorized and may invalidate warranties made under this Policy.

1.4.3. Certificate Extensions

Certificates issued under this Policy that contain Certificate Extensions shall utilize Extensions defined by the X.509 v.3 standard as a minimum. Issuing CAs may include Certificate Extensions that constrain the usage, role, or capabilities of the issued certificate.

1.4.4. Critical Extensions

Certificates issued under this Policy shall, at a minimum, include the following Critical Certificate Extensions:

- A basic constraint indicating whether the certificate subject is a Certificate Authority or not;
- A constraint indicating the acceptable usage of the key;
- A constraint indicating the number of levels in the CA hierarchy of the certificate.

1.5. Policy Administration

1.5.1. Organization Administering the Document

This Policy is administered by the Corporate Information Security group of Cisco Systems, Inc.:

Corporate Headquarters
Cisco Systems Inc.
170 West Tasman
San Jose, CA 95134

1.5.2. Contact Person

Please send PKI-based correspondence to:

Cisco Systems Inc.
7025 Kit Creek Road
P.O. Box 14987
Research Triangle Park, NC
27709-4987
Attn: J.P. Hamilton
Phone number: 919.392.1481
E-mail address: ciscopki-public@external.cisco.com

CA Policy Authority:

Cisco Systems Inc.
7025 Kit Creek Road
P.O. Box 14987
Research Triangle Park, NC
27709-4987
Attn: J.P. Hamilton
Phone number: 919.392.1481
E-mail address: ciscopki-public@external.cisco.com

1.5.3. Certificate Policy Approval Procedures

Changes to this CP are made by the Cisco Systems Information Security Policy Management Authority ("Cisco PMA"), which includes members of Cisco's Corporate Information Security Group. Changes are proposed by members of the Cisco PMA, reviewed by the entire group, formally approved individually, and then incorporated into an updated document that is assigned a subsequent version number. Approved versions of this document shall be published to the main Cisco PKI Policies page located at www.cisco.com/security/pki/policies/index.html.

The updated version of this document shall be considered binding on all Issuing CAs and relevant subscribers within 30 days of issuance.

1.5.3.1. Certification Practice Statement Approvals

The Cisco PMA shall be responsible for reviewing the compliance of relevant CPS documents for Issuing CAs and ensuring their compliance with this document and the guidelines of the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates.

1.5.3.2. Notifications of Changes

The Cisco PMA shall be responsible for providing notifications of changes to this document to the administrative teams of affected Issuing CAs.

1.5.3.3. Version Management and Changes

CP and CPS documents shall contain a version history table or notation indicating a history of changes to the document, the appropriate versions, and the approvals obtained thereunto. Version numbers shall be assigned as follows:

- Minor version numbers shall be incremented when the document contains only minor corrective updates, such as editorial corrections or contact information updates;
- Major version numbers shall be assigned for all changes considered more significant than minor updates.

CAs shall declare an effective date in their CPS for any changes, and shall indicate how a Relying Party may differentiate certificates issued under differing versions of the CPS (e.g. by comparing the notBefore data of the certificate to the effective date of the CPS).

1.6. Definitions and Acronyms

See Appendix A: Definitions and Acronyms

Chapter 2. Publication and Repository Responsibilities

2.1. Repositories

Cisco Systems maintains a public repository of CA information and policy documents, available at www.cisco.com/security/pki/policies/index.html. A copy of the latest version of this document shall be made publicly available at that URL. Issuing CAs shall, at a minimum, contribute their relevant documentation as specified in section 2.2 to this repository, in addition to or in lieu of any other repository specific to the Issuing CA.

2.2. Publication of Certification Information

The Issuing CA shall operate or contribute to a secure on-line repository and/or other certificate validation service that is available to Benefiting Parties and that contains:

- Issued certificates that reference this Policy, when publication is authorized by the subscriber;
- A Certificate Revocation List ("CRL") or online certificate status database;
- The CA's certificate for its signing key;
- Past and current versions of the CA's public CPS;
- A copy of this Policy; and
- Other relevant information relating to certificates that reference this Policy.

2.3. Time or Frequency of Publication

All information authorized to be published in a repository shall be published promptly after such information is authorized and available to the Issuing CA. Certificates issued by the CA that reference this Policy will be published promptly upon acceptance of such certificate by the subscriber, and when publication is authorized by the subscriber. Information relating to the revocation of a certificate will be published in accordance with section 2.2.

2.4. Access Controls on Repositories

The Issuing CA shall make its repository available to Benefiting Parties and subscribers 24 hours per day, 7 days per week, subject to reasonable scheduled maintenance and the CA's specific terms of access. The CA shall not impose any access controls on this Policy, the CA's certificate for its signing key, and past and current versions of the CA's public CP. The Issuing CA may impose access controls on certificates, certificate status information, or CRLs at its discretion, subject to agreement between the CA and subscriber and/or the CA and Benefiting Parties, in accordance with provisions published in its CP, CPS or otherwise.

Chapter 3. Identification and Authentication

Issuing CAs shall maintain appropriate procedures to address the recognition of trademark rights with regards to certificate naming practices, as applicable. Issuing CAs shall authenticate the requests of parties wishing to be issued or to revoke certificates under this Policy.

3.1. Naming

Subject to the requirements noted below, certificate applications may be communicated from the applicant to the CA or an RA, (and authorizations to issue certificates may be communicated from an RA to the CA) (1) electronically via E-mail or a web site, provided that all communication is secure, such as by using a suitable cryptographic protocol for electronic communications, (2) by registered first class U.S. mail, or (3) in person.

3.1.1. Types of Names

The subject name used for certificate applicants shall be the X.500 Distinguished Name consisting of an authenticated, fully qualified domain name (FQDN) placed in the common name (CN) field and the subject alternative name (SAN) field as a DNS-type name.

Certificates containing underscore characters ("_") in domain labels in dNSName entries MAY be issued as follows: * dNSName entries MAY include underscore characters such that replacing all underscore characters with hyphen characters ("-") would result in a valid domain label, and; * Underscore characters MUST NOT be placed in the left most domain label, and; * Such certificates MUST NOT be valid for longer than 30 days.

CAs under this policy shall specify in their Certification Practice Statements whether they permit the use of Internationalized Domain Names (IDNs) in their certificates, and how these domain names are translated or represented if permitted. CAs under this policy must not issue certificates containing private/reserved IP addresses or bare hostnames (i.e. 'hostname' instead of 'hostname.domain.tld') in the common name or subject alternative name fields. CAs may permit the use of non-private/reserved IP addresses in certificates; if permitted, CAs must specify the validation processes they employ for validating control over IP addresses in certificate signing requests.

The RXC CA does not issue certificates to non-IANA-controlled top-level domains (e.g. ".local"), but may issue certificates to entities whose FQDN is legitimate but not resolvable to an IP address through publicly available DNS servers, in conformance to the strictures identified in the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates. Determination of IANA-controlled top-level domains is achieved by consulting the Root Zone Database (iana.org) maintained by the Internet Assigned Numbers Authority (IANA). In conformance to the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, the RXC CA does not issue certificates with `commonName` or `subjectAltName` entries that are bare hostnames (e.g. 'hostname' instead of 'hostname.domain.tld') or that are private/reserved IP addresses (those marked by IANA as reserved). The RXC CA does not permit the use of Internationalized Domain Names (IDNs) in the `commonName` or `subjectAltName` fields of any certificate it issues. Certificate requests containing IDNs will be rejected.

3.1.2. Need for Names to Be Meaningful

The Issuing CA shall ensure that the subject name listed in all certificates has a reasonable association with the authenticated information of the subscriber.

3.1.3. Anonymity or Pseudonymity of Subscribers

The Issuing CA shall not permit anonymous or pseudonymous certificate requests and shall ensure that any requests originate from the subscriber or a properly identified proxy.

3.1.4. Rules for Interpreting Various Name Forms

Distinguished Names in certificates shall be interpreted using X.500 standards and ASN.1 syntax.

3.1.5. Uniqueness of Names

The subject name or a combination of the subject name and other data fields listed in a certificate shall be unambiguous for all certificates issued by the Issuing CA.

3.1.6. Role of Trademarks in Certificate Content

Issuing CAs shall not knowingly issue certificates with content that infringes upon the intellectual property rights of another entity. Issuing CAs are not required, under this Policy, to validate an Applicant's right to use a trademark beyond validating the association between the Applicant and the information presented; Issuing CAs may reject applications or revoke certificates that are found to be part of a trademark dispute or violation.

3.2. Initial Identity Validation

Issuing CAs shall validate the identity of Applicants requesting certificates and the content of requested certificates using a procedure documented and established in the Issuing CA's Certification Practice Statement (CPS). Said Procedure may incorporate any legal means permitted by the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates to validate the information supplied.

An applicant for a certificate shall complete a certificate application in a form prescribed by the CA and enter into a subscriber agreement with the Issuing CA. All applications are subject to review, approval and acceptance by the Issuing CA.

3.2.1. Identification and Authentication

CAs must define procedures for validating the origin and identity of certificate requests, as well as the set of identities for which requests are considered valid. This definition must be included in the CA's CPS.

3.2.2. Method to Prove Possession of the Private Key

The CA shall establish that the applicant is in possession of the private key corresponding to the public key submitted with the application in accordance with an appropriate secure protocol, such as that described in the IETF PKIX Certificate Management Protocol or through other verifiable means.

3.2.3. Authentication of Organization Identity

For Certificates specifying an Organization Identity, Applicants must supply sufficient information about the organization to validate the organization's existence and function as a legal entity (e.g. organization name, registered address, etc.) and the certificate Applicant's association with the Organization in question and authorization to request a certificate. The set of this information that must be supplied, and the procedures for authenticating it, shall be enumerated by the Issuing CA in its Certification Practice Statement. In addition to any requirements established by the Issuing CA, the applicant's ownership or control of all requested Domain(s) must be verified by a suitable method such as the inspection of WHOIS records, contact with the Domain Registrar, email challenge/responses in line with the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates or an alternative practical demonstration of control of the Domain(s).

Further information may be requested from the Applicant and other information and or methods may be utilized in order to achieve an appropriate level of confidence.

3.2.4. Authentication of Individual Identity

Where Individual Identity elements such as an email address or personal name would be incorporated into the contents of the issued certificate, the Issuing CA shall enumerate specific requirements for the authentication of Individual Identity information and shall identify procedures for said authentication within its Certification Practice Statement. At this time, this Policy does not authorize the issuance of certificates whose Subject is a natural person, so there are no further stipulations around the verification of individual identity.

3.2.5. Non-Verified Subscriber Information

Issuing CAs must maintain a documented process to ensure that Applicants cannot add self-reported, unverified information to the contents of the `Subject:organizationalUnitName` field.

3.2.6. Validation of Authority

The Issuing CA shall ensure that the Applicant is in possession of the private key associated with the certificate request per section 3.2.1. In addition, the Issuing CA shall verify that the Applicant has ownership or control of the domain name in the certificate through a reliable means of communication with the organization or individual Applicant, together with verification by either a challenge-response mechanism or direct confirmation with the contact listed with the Domain Name Registrar or WHOIS. The Issuing CA shall finally verify that the Applicant is authorized to request and receive a certificate on behalf of the Organization in question. The process for these validation steps shall be enumerated in the Issuing CA's CPS.

3.2.7. Criteria for Interoperation

No stipulation.

3.3. Certificate Re-Key

Issuing CAs shall treat certificate re-key requests identically to applications for new certificates for the purposes of Identification, Authorization, and Publication.

3.3.1. Identification and Authentication for Re-Key Requests

No further stipulation beyond section 3.3.

3.3.2. Identification and Authentication for Routine Re-Key

No further stipulation beyond section 3.3.

3.3.3. Identification and Authentication for Re-Key after Revocation

Revoked or expired certificates shall never be renewed. Applicants that reference this Policy shall be re-authenticated by the CA or RA during the certificate application process, just as with a first-time application.

3.4. Certificate Revocation

A revocation request that is submitted electronically may be authenticated on the basis of a digital signature using the private key associated with the certificate whose revocation is requested. The identity of a person submitting a revocation request in any other manner shall be authenticated as per section 3.2 above. Other revocation request authentication mechanisms may be used as well so long as these authentication mechanisms viably detect unauthorized revocation requests. Revocation requests shall be handled and processed according to the requirements specified in section 4.9.

Chapter 4. Certificate Life-Cycle Operational Requirements

4.1. Certificate Application

An applicant for a certificate shall complete a certificate application in a form prescribed by the Issuing CA and enter into a subscriber agreement with the Issuing CA. All applications are subject to review, approval and acceptance by the Issuing CA.

4.1.1. Who Can Submit a Certificate Application

Issuing CAs shall define specifically the set of applicants approved to submit a certificate application, and shall list this set explicitly in the Issuing CA's Certification Practice Statement (CPS).

4.1.2. Enrollment Process and Responsibilities

Issuing CAs shall maintain documented processes that validate the certificate's identifying information that will be presented to relying parties. Applicants shall ensure they submit sufficient information to permit Issuing CAs to successfully perform this validation. Issuing CAs and their designated RA proxies shall protect all communications with Applicants and Subscribers and shall securely store all information presented or collected as part of the application and validation process.

4.2. Certificate Application Processing

4.2.1. Performing Identification and Authentication Functions

Issuing CAs shall maintain controls that ensure the sufficient authentication of certificate applicants in line with the Issuing CA's CPS. Initial validation of identification information may be automated or manual, but shall be performed by the Issuing CA or a known, documented Registration Authority (RA) or proxy on behalf of the Issuing CA. All communications as well as all information presented or collected during the application process shall be protected by the Issuing CA and its designated RA proxies. Future authentication of repeat applicants and subsequent authentication checks may be authenticated using single or multiple factors of authentication.

CAs under this policy shall maintain separately or subscribe to a centrally managed list of DNS domains ("Cisco Whitelist") verified as owned by Cisco Systems. The contents of this list shall be verified annually by members of the Cisco Systems Policy Management Authority or Cisco CA administrators under their direction.

For each dNSName in the subjectAltName or Common Name of a presented certificate request, CAs under this policy must follow this process for domain validation in addition to any other validation requirements:

- If the domain in question appears on the Cisco Whitelist, the CA does not need to check for CAA records in DNS prior to issuing a certificate. In this case, the CA MUST record that CAA was not checked for that domain due to presence on the whitelist.
- Otherwise, the CA MUST check for CAA records in the DNS record of the domain in question, following all of the requirements laid out in section 3.2.2.8 of the CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates. The CA MUST NOT issue if the CAA records dictate otherwise, and MUST indicate in its Certification Practice Statement whether it will treat record lookup failures that meet the strictures of the CA/Browser Forum Guidelines section 3.2.2.8 as permission to issue or will refuse to issue without an authoritative response, and MUST list in its Certification Practice Statement the Issuer Domain Name or Names that it recognizes as granting permission to issue if present in the 'issue' or 'issuewild' CAA record fields.

If CAA records are checked–whether successful or not–the CA MUST record CAA checking information and results in sufficient detail to reconstruct the chain of events leading to issuance or issuance failure. CAs may provide this feedback to contacts specified in the CAA iodef records at their discretion.

CAs that have previously obtained validation and authorization information for a certificate application may store this information for future applications by the same identified party. In no case may a CA re-use validation or authorization information obtained more than 825 days prior to the application being considered.

4.2.2. Approval or Rejection of Certificate Applications

Issuing CAs shall issue a positive, unambiguous notification to the subscriber indicating the approval or rejection of a certificate application.

4.2.3. Time to Process Certificate Applications

Issuing CAs shall ensure that certificate applications are processed in a timely fashion.

4.3. Certificate Issuance

4.3.1. CA Actions during Certificate Issuance

Issuing CAs shall communicate with Registration Authorities (RAs) or relevant proxy services using authenticated, encrypted communications channels.

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

Upon successful completion of the subscriber I&A process in accordance with this Policy and CPS, the Issuing CA shall issue the requested certificate, notify the applicant thereof, and make the certificate available to the applicant pursuant to a procedure whereby the certificate is initially delivered to, or available for pickup by, the subscriber only.

4.4. Certificate Acceptance

4.4.1. Conduct Constituting Certificate Acceptance

Following issuance of a certificate, the CA shall contractually require the subscriber to indicate either acceptance or rejection of the certificate to the Issuing CA, in accordance with procedures established by the Issuing CA and specified in the Issuing CA's Certification Practice Statement (CPS). CAs may regard a lack of explicit rejection as acceptance of the certificate.

4.4.2. Publication of the Certificate by the CA

No stipulation beyond section 2.2.

4.4.3. Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

4.5. Key Pair and Certificate Usage

4.5.1. Subscriber Private Key and Certificate Usage

Issuing CAs shall establish a set of security control obligations for subscribers and shall document these in a Subscriber Agreement to which Applicants must agree prior to being issued a certificate from the Issuing CA. At a minimum, the following obligations shall apply to all subscribers:

i. All subscribers shall ensure the protection of the private key associated with certificates.

ii. Subscribers shall either ensure that a private key is not replicable, or shall ensure that any copies or backups meet the same security standard as the protections around the private key.

iii. Subscribers shall not use a Private Key in violation of the appropriate key usage and extended key usage fields as indicated in the corresponding digital certificate.

4.5.2. Relying Party Public Key and Certificate Usage

Issuing CAs must describe in their CPS documents the conditions under which issued certificates may be relied upon and the mechanisms available for verifying the public key of the CA and the validity of issued certificates (e.g. CRL, OCSP).

4.6. Certificate Renewal

Certificate Renewal is defined as the issuance of a new certificate with the same details as a previously issued certificate, as well as the same public key. Certificates created successfully by an Issuing CA under this Policy may not be renewed; if the Issuing CA opts to support renewal requests, it shall specify this in its Certification Practice Statement (CPS), and must do so only by treating renewal requests identically to new certificate requests for the purposes of Identification, Authorization, and Publication.

4.6.1. Circumstance for Certificate Renewal

Not applicable

4.6.2. Who May Request Renewal

Not applicable

4.6.3. Processing Certificate Renewal Requests

Renewals shall be performed under this Policy by treating all renewal requests as if they were first-time certificate application requests. All Subscriber and Issuing CA obligations stated in this Policy apply to the renewal request. A subscriber will submit the new certificate request to the Issuing CA. The Issuing CA shall issue a new certificate using the newly submitted information and adhering to the I&A policies set forth herein and in the associated CPS. The CA shall not be required to take action to inform subscribers of the need for a renewal.

4.6.4. Notification of New Certificate Issuance to Subscriber

See section 4.3.2.

4.6.5. Conduct Constituting Acceptance of a Renewal Certificate

See section 4.4.1.

4.6.6. Publication of the Renewal Certificate by the CA

See section 4.4.2.

4.6.7. Notification of Certificate Issuance by the CA to Other Entities

See section 4.4.3.

4.7. Certificate Re-Key

Certificate Re-Key is defined as the issuance of a new certificate with the same details as a previously issued certificate, but a different public key. Certificates created successfully by the Issuing CA under this Policy may not be re-keyed; they may only be revoked and new certificates issued instead.

4.7.1. Circumstance for Certificate Re-Key

Not applicable

4.7.2. Who May Request Certification of a New Public Key

Not applicable

4.7.3. Processing Certificate Re-Keying Requests

Not applicable

4.7.4. Notification of New Certificate Issuance to Subscriber

Not applicable

4.7.5. Conduct Constituting Acceptance of a Re-Keyed Certificate

Not applicable

4.7.6. Publication of the Re-Keyed Certificate by the CA

Not applicable

4.7.7. Notification of Certificate Issuance by the CA to Other Entities

Not applicable

4.8. Certificate Modification

Certificate Modification is defined as the issuance of a new certificate with different details from a previously issued certificate but the same public key. Certificates created successfully by the Issuing CA under this Policy may not be modified, they may only be revoked and new certificates issued instead.

4.8.1. Circumstance for Certificate Modification

Not applicable

4.8.2. Who May Request Certificate Modification

Not applicable

4.8.3. Processing Certificate Modification Requests

Not applicable

4.8.4. Notification of New Certificate Issuance to Subscriber

Not applicable

4.8.5. Conduct Constituting Acceptance of Modified Certificate

Not applicable

4.8.6. Publication of the Modified Certificate by the CA

Not applicable

4.8.7. Notification of Certificate Issuance by the CA to Other Entities

Not applicable

4.9. Certificate Revocation and Suspension

Certificate Revocation is defined as blacklisting a previously issued certificate by having the Issuing CA add the certificate's serial number and the date of revocation to a Certificate Revocation List (CRL), and then signing the CRL using the Issuing CA's private key. Certificate Suspension is defined as the temporary blacklisting of a certificate with an option to "undo" the blacklisting at a future date.

4.9.1. Circumstances for Revocation

The Issuing CA shall revoke a certificate:

- Upon request of the subscriber;
- Upon failure of the subscriber to meet its material obligations under this Certificate Policy, any applicable CPS, or any other agreement, regulation, or law applicable to the certificate that may be in force;
- If knowledge or reasonable suspicion of compromise is obtained;
- If the CA determines that the certificate was not properly issued in accordance with this Policy and/or any applicable CPS.

In the event that the Issuing CA ceases operations, all certificates issued by the CA shall be revoked prior to the date that the CA ceases operations. The Issuing CA is required to provide subscribers adequate notice to provide them the opportunity to address any business impacting issues stemming from this revocation.

4.9.2. Reasons for Revoking a Subscriber Certificate

A subscriber may request revocation of its certificate at any time for any reason. The Issuing CA may also revoke a certificate upon failure of the subscriber to meet its obligations under this Certificate Policy, the applicable CPS, or any other agreement, regulation, or law applicable to the certificate that may be in force.

The CA SHALL revoke a Certificate within 24 hours if one or more of the following occurs: 1. The Subscriber requests in writing that the CA revoke the Certificate; 2. The Subscriber notifies the CA that the original certificate request was not authorized and does not retroactively grant authorization; 3. The CA obtains evidence that the Subscriber's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise; or 4. The CA obtains evidence that the validation of domain authorization or control for any Fully-Qualified Domain Name or IP address in the Certificate should not be relied upon.

The CA SHOULD revoke a certificate within 24 hours and MUST revoke a Certificate within 5 days if one or more of the following occurs: 1. The Certificate no longer complies with the requirements of Sections 6.1.5 and 6.1.6; 2. The CA obtains

evidence that the Certificate was misused; 3. The CA is made aware that a Subscriber has violated one or more of its material obligations under the Subscriber Agreement or Terms of Use; 4. The CA is made aware of any circumstance indicating that use of a Fully-Qualified Domain Name or IP address in the Certificate is no longer legally permitted (e.g. a court or arbitrator has revoked a Domain Name Registrant's right to use the Domain Name, a relevant licensing or services agreement between the Domain Name Registrant and the Applicant has terminated, or the Domain Name Registrant has failed to renew the Domain Name); 5. The CA is made aware that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate Fully-Qualified Domain Name; 6. The CA is made aware of a material change in the information contained in the Certificate; 7. The CA is made aware that the Certificate was not issued in accordance with these Requirements or the CA's Certificate Policy or Certification Practice Statement; 8. The CA determines or is made aware that any of the information appearing in the Certificate is inaccurate; 9. The CA's right to issue Certificates under these Requirements expires or is revoked or terminated, unless the CA has made arrangements to continue maintaining the CRL/OCSP Repository; 10. Revocation is required by the CA's Certificate Policy and/or Certification Practice Statement; or 11. The CA is made aware of a demonstrated or proven method that exposes the Subscriber's Private Key to compromise, methods have been developed that can easily calculate it based on the Public Key (such as a Debian weak key, see wiki.debian.org/SSLkeys), or if there is clear evidence that the specific method used to generate the Private Key was flawed.

4.9.2.1. Reasons for Revoking a Subordinate CA Certificate

A subscriber shall promptly request revocation of a certificate whenever any of the information on the certificate changes or becomes obsolete, or whenever the private key associated with the certificate, or the media holding the private key associated with the certificate is compromised or is suspected of having been compromised.

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

4.9.3. Who Can Request Revocation

Only the subscriber and the Issuing CA are permitted to request revocation of a certificate issued pursuant to this Policy. Outside entities such as Relying Parties and partners may submit problem reports to Cisco to inform Cisco of reasonable cause to initiate revocation, using the contact information defined by the CA in section 1.5.2.

4.9.4. Identification and Authentication for Revocation Request

CAs shall provide Subscribers, Relying Parties, Application Software Suppliers, and other third parties with clear instructions for reporting suspected Private Key Compromise, Certificate misuse, or other types of fraud, compromise, misuse, inappropriate conduct, or any other matter related to Certificates. These instructions must be provided in section 1.5.2 of their published CPS, which must be made readily available online. CAs must maintain a 24x7 ability to accept and respond to revocation requests and problem reports through this reporting system.

The Issuing CA shall authenticate a request for revocation using the same controls used to identify and authenticate the original certificate request. Should automated request, submission, and validation of the subscriber information not be available for any reason, manual validation of that information shall be performed by a member of the Issuing CA administrative team operating in a Trusted Role, per section 5.2.1.

4.9.5. Procedure for Revocation Request

A certificate revocation request should be promptly communicated to the Issuing CA, either directly or through a Registration Authority (RA). A certificate revocation request may be communicated electronically if it is digitally signed with the private key corresponding to the certificate to be revoked. Alternatively, the subscriber may request revocation by contacting the CA or an authorized RA in person and providing adequate proof of identification in accordance with this Policy.

Once revoked, the certificate serial number and the date and time of the revocation shall be added to the appropriate certificate status verification system (e.g. CRL, OCSP), along with any other information such as revocation reason codes that are defined by the Issuing CA in its Certification Practice Statement (CPS). The certificate status verification system shall then be updated in a timeframe defined by the Issuing CA's CPS. All revocation requests and the resulting actions taken by the CA shall be archived in accordance with the CPS for that CA. Whenever an on-line certificate status database is used as an alternative to a CRL, such database shall be updated within two hours of the completion of revocation.

4.9.6. Revocation Request Grace Period

Issuing CAs may establish a grace period in their Certification Practice Statements (CPSs) within which a subscriber may take action itself to request revocation of a certificate due to suspected key compromise, use of a weak key, or similar Subscriber-related issues. Under no circumstances shall this grace period exceed the limits established by the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates.

Within 24 hours after receiving a Certificate Problem Report, the CA SHALL investigate the facts and circumstances related to a Certificate Problem Report and provide a preliminary report on its findings to both the Subscriber and t he entity who filed the Certificate Problem Report.

After reviewing the facts and circumstances, the CA SHALL work with the Subscriber and any entity reporting the Certificate Problem Report or other revocation-related notice to establish whether or not the certificate will be revoked, and if so, a date which the CA will revoke the certificate. The period from receipt of the Certificate Problem Report or revocation-related notice to published revocation MUST NOT exceed the time frame set forth in Section 4.9.1.1. The date selected by the CA SHOULD consider the following criteria: 1. The nature of the alleged problem (scope, context, severity, magnitude, risk of harm); 2. The consequences of revocation (direct and collateral impacts to Subscribers and Relying Parties); 3. The number of Certificate Problem Reports received about a particular Certificate or Subscriber; 4. The entity making the complaint (for example, a complaint from a law enforcement official that a Web site is engaged in illegal activities should carry more weight than a complaint from a consumer alleging that she didn't receive the goods she ordered); and 5. Relevant legislation.

4.9.7. Revocation Request Processing Requirement

Issuing CAs shall begin investigation into suspected key compromise or certificate misuse within 24 hours of receipt of the report of the issue.

4.9.8. Revocation Checking Requirement for Relying Parties

Relying Parties should validate the suitability of a presented certificate for its intended use, and should authenticate the information presented with regards to the validity of the certificate and its trust chain. Issuing CAs shall ensure all appropriate information is included in issued certificates that would assist with this validity verification process, such as URLs to policies and certificate validity status services.

4.9.9. CRL Issuance Frequency

Subscribing CAs must provide a service that reports on the validity of issued certificates, but CAs may choose to use Certificate Revocation Lists (CRLs), contribute information to an Online Certificate Status Protocol (OCSP) service, or some combination of these. CAs issuing CRLs that report on the status of end-entity or Subscriber certificates must issue CRLs at least every seven days, and must set the nextUpdate field in the CRL to no greater than ten days past the value of the thisUpdate field. CAs issuing CRLs that report on the status of Subordinate CA certificates must issue CRLs at least annually,

and must set the value of the nextUpdate field in the CRL to no more than twelve months beyond the value of the thisUpdate field. In all cases, upon a new revocation event, a new CRL will be issued and published within twenty-four hours of the completion of the revocation process. The Issuing CA will ensure that superseded CRLs are removed from the CRL Distribution Point location upon posting of the latest CRL.

4.9.10. Online Certificate Status Protocol Update Frequency

Subscribing CAs have the option of contributing revocation data to an Online Certificate Status Protocol (OCSP) service. In the event that an OCSP service is used, OCSP data must be updated every four days whether any new information has been published or not, and OCSP responses must be configured with a maximum expiration time of ten days. Certificate revocations must be updated in the OCSP service within twenty-four hours of the relevant certificate revocation event.

4.9.11. Maximum Latency for CRLs and Online Status Checking Mechanisms

Issuing CAs shall ensure that the network latency for responding to requests for CRLs or online certificate status checks via OCSP does not exceed ten seconds under normal network operating conditions.

4.9.12. Notification with Regards to Possible Key Compromise

Issuing CAs shall make reasonable efforts to contact Subscribers regarding the detection of a possible key compromise or other revocation-requiring event.

4.9.13. Circumstances for Certificate Suspension

Issuing CAs under this Policy shall not support Certificate Suspension.

4.9.14. Who Can Request Suspension

Not applicable

4.9.15. Procedure for Certificate Suspension

Not applicable

4.9.16. Limits on Suspension Period

Not applicable

4.10. Certificate Status Services

See section 2.

4.11. Removal of Certificates from Revocation Status Services

CAs must continue reporting the revocation status of a certificate until one full revocation issuance has occurred past the expiration date of the certificate. CAs may cease reporting on the revocation status of the certificate at any time after that, as CA staff deem appropriate.

4.12. End of Subscription

No stipulation.

4.13. Key Escrow and Recovery

CAs under this policy should not escrow private keys of subscribers. CAs must detail in their Certification Practice Statements (CPSs) whether key escrow is performed; if escrow is performed, CAs must protect escrowed keys using hardware holding a FIPS140-2 Level 3 security certification at all times, and must document the process for escrowing keys and recovering escrowed keys.

Chapter 5. Facility, Management, and Operational Controls

5.1. Physical Controls

5.1.1. Site Location and Construction

Issuing CA infrastructure, including all hosts and cryptographic devices directly involved in the Issuing CA system, shall be housed in a secure datacenter that restricts physical access to the CA infrastructure from unauthorized personnel at all times.

5.1.2. Physical Access

The facility housing the Issuing CA infrastructure shall restrict access to the CA to only the members of the Issuing CA's administrative team that serve in a Trusted Role, per section 5.2.1. The Issuing CA's administrative team shall be responsible for identifying the members who shall have physical access, and for reviewing that list on a regular basis to ensure it remains up to date. Physical access to the CA infrastructure shall require identifying tokens that strongly authenticate and authorize members of the Issuing CA administrative team. All physical access to the Issuing CA infrastructure shall be logged and recorded.

5.1.3. Power and Air Conditioning

The Issuing CA physical infrastructure shall be supplied with power and air conditioning commensurate with its operating requirements. The Issuing CA administrative team shall ensure that such power and air conditioning supplies are sufficiently redundant to ensure the continued operation of the Issuing CA under adverse conditions for a long enough period to either gracefully shut down the CA or to transition its functions securely and safely to another location.

5.1.4. Water Exposures

The facility housing the Issuing CA's infrastructure shall be supplied with sufficient protections to guard against water exposure as much as reasonably possible, such as flood and leak detection mechanisms, elevated equipment racks, and safeguards on fire sprinkler systems.

5.1.5. Fire Prevention and Protection

The facility housing the Issuing CA's infrastructure shall be outfitted with fire detection mechanisms sufficient to reasonable business practices, along with such fire suppression systems as are deemed reasonable and safe. In the event that the facility uses a water-based fire suppression system, appropriate detection and correction mechanisms must be in place to safeguard against leaks. The fire detection mechanisms must be tested at least annually; all detection and suppression mechanisms shall be maintained according to the manufacturer's recommendations.

5.1.6. Media Storage

The Issuing CA shall store all sensitive media, including CA archival backups, escrowed subscriber keys, subscriber information, and CA backups, on physical media that are protected against accidental damage (electrical, fire, water, magnetic). Media containing backup or archival information shall be duplicated and stored in a separate location from the original media.

5.1.7. Waste Disposal

All sensitive documents generated as a result of the functions of the Issuing CA shall be shredded securely once no longer required for operation. Sensitive equipment or media that are no longer needed for operation shall be securely wiped in a sufficient manner to ensure data are destroyed and non-recoverable, in a process witnessed by at least two individuals acting in a Trusted Role (per section 5.2.1).

5.1.8. Off-Site Backup

Backups of CA systems sufficient to enable restoring the Issuing CA to full functionality shall be created and stored in a separate physical location from the primary operating location of the Issuing CA.

5.2. Procedural Controls

5.2.1. Trusted Roles

All employees, contractors, and consultants of the Issuing CA (collectively "personnel") that have access to or control over cryptographic operations that may materially affect the CA's issuance, use, suspension, or revocation of certificates, including access to restricted operations of the CA's repository, shall, for purposes of this Policy, be considered as serving in a trusted role. Such personnel include, but are not limited to, system administration personnel, operators, engineering personnel, and executives who are designated to oversee the CA's operations.

5.2.2. Number of Persons Required per Task

To ensure that one person acting alone cannot circumvent safeguards, responsibilities at a CA server must be shared by multiple roles and individuals. Each account on the CA server shall have limited capabilities commensurate with the role of the account holder.

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

5.2.3. Identification and Authentication for Each Role

All Issuing CA personnel shall have their identity and authorization verified before they are:

i. Included in the access list for the Issuing CA site;

ii. Included in the access list for physical access to the system;

iii. Given a Certificate or other cryptographic token for the performance of their CA role; or

iv. Given an account on the PKI system.

Each of these Certificates and/or accounts (with the exception of CA signing Certificates) shall be directly attributable to an individual and shall be restricted to actions authorized for that role through the use of CA software, operating system and procedural controls. When accessed across shared networks, CA operations shall be secured, using mechanisms such as token-based strong authentication and encryption.

5.2.4. Roles Requiring Separation of Duties

To best ensure the integrity of the Issuing CA equipment and operation, it is recommended that wherever possible a separate individual be identified for each Trusted Role. The separation provides a set of checks and balances over the Issuing CA operation. Under no circumstances will the incumbent of a CA role perform his or her own auditor function.

5.3. Personnel Controls

5.3.1. Background and Qualifications

Issuing CAs, RAs, and VSPs shall formulate and follow personnel and management policies sufficient to provide reasonable assurance of the trustworthiness and competence of their employees and of the satisfactory performance of their duties in manner consistent with this Policy.

5.3.2. Background Investigation

All CAs shall conduct an appropriate investigation of all personnel who serve in trusted roles (prior to their employment and periodically thereafter as necessary), to verify their trustworthiness and competence in accordance with the requirements of this Policy and the CA's personnel practices or equivalent. All personnel who fail an initial or periodic investigation shall not serve or continue to serve in a trusted role.

5.3.3. Training Requirements

All CA, RA, and VSP personnel shall receive proper training in order to perform their duties, and update briefings thereafter as necessary to remain current.

5.3.4. Documentation Supplied to Personnel

All CA, RA, and VSP personnel shall be provided with comprehensive user manuals detailing the procedures for certificate creation, update, renewal, suspension, and revocation, and software functionality.

5.4. Audit Logging Procedures

Issuing CAs subscribing to this Policy shall generate audit log files for all events relating to the ongoing operation of the CA, as well as specific relevant security events. Where possible, audit logs shall be automatically created and monitored; where this is not possible, a paper logbook or other physical mechanism shall be used. At a minimum, each log entry (whether electronic or physical) shall include the following information:

- The date and time of the event;
- The type of event;
- The success or failure of the action (as appropriate);
- The identity of the entity and/or operator that caused the event;
- The identity of the subject or target of the event;
- The cause of the event (insofar as this may be determined).

5.4.1. Types of Events Recorded

Issuing CAs shall establish the set of events and records archived, and shall document this in the Issuing CA's Certification Practice Statement (CPS). At a minimum, the following information must be archived by, or on behalf of, the Issuing CA:

- All computer security audit data;
- All certificate application data provided or collected;
- All certificates and all CRLs or other certificate status records generated;
- Key histories;
- All correspondence between the CA and designated RAs or VSPs, and/or subscribers.

5.4.2. Frequency of Processing Log

Where possible, security event logs shall be created at the time of the event. Where this is not possible, the logs shall be created and must be verified by at least two members of the Issuing CA administrative team, operating in a Trusted Role per section 5.2.1.

5.4.3. Retention Period for Audit Log

All security audit logs shall be retained for a period of seven years past the dissolution of the CA and shall be made available during compliance audits.

5.4.4. Protection of Audit Log

Electronic security audit logs shall be protected from tampering using logical means such as cryptographic signatures or automated replication to a protected archive. Physical security audit logs shall be created using tamper-resistant methods and shall be routinely inspected and reconciled to detect tampering.

5.4.5. Audit Log Backup Procedures

Issuing CAs shall make regular backups of electronic security audit logs. No stipulations are made regarding backups of physical security audit logs.

5.4.6. Vulnerability Assessments

Issuing CAs shall conduct regular vulnerability assessments of the Issuing CA infrastructure and assets that ensure the logical and physical security of the assets against unauthorized access, modification, tampering, or denial of the certificate issuance process.

5.5. Records Archival

CAs conforming to this policy shall retain documentation, including audit logs, issuance and validation records, and other operational documentation for a period of seven years past the dissolution of the CA or to the extent permitted and required by applicable local law. Documentation so retained shall be made available during public trust audits; CAs may make this information available through other means at the discretion of the CA operator. Where a CA opts to make such documentation available, it shall detail in its Certification Practice Statement what is made available and the means for requesting it.

5.6. Business Continuity and Disaster Recovery

5.6.1. Incident and Compromise Handling Procedures

Issuing CAs must have in place an appropriate disaster recovery/business resumption plan and must set up and render operational a facility located in an area that is geographically remote from the primary operational site, capable of providing CA Services in accordance with this Policy within seventy-two (72) hours of an unanticipated emergency. Such plan shall include a complete and periodic test of readiness for such facility. Such plan shall be referenced within the Issuing CA's CPS or other appropriate documentation available to Qualified Relying Parties.

5.6.2. Business Continuity Requirements

Issuing CAs shall ensure that their continuity plans are sufficient to provide operations 24 hours per day, 7 days per week, 365 days per year, with at least a 99% availability excluding planned maintenance activities.

5.6.3. Key Compromise Plan

The Issuing CA must have in place an appropriate key compromise plan that addresses the procedures that will be followed in the event of a compromise of the private signing key used by the CA to issue certificates. Such plan shall include procedures for revoking all affected certificates and promptly notifying all subscribers and all Qualified Relying Parties. The key compromise plan shall be documented in, or referenced from, the Issuing CA's Certification Practice Statement (CPS).

5.7. CA Termination

In the event that the CA ceases operation, all subscribers, RAs, VSPs, and Qualified Relying Parties must be promptly notified of the termination. In addition, all CAs with which cross-certification agreements are current at the time of cessation must be promptly informed of the termination. All certificates issued by the CA that reference this Policy must be revoked no later than the time of termination.

5.8. CA or RA Termination

In the event that the CA ceases operation, the Subscribers, RAs, VSPs, and Benefiting Parties will be promptly notified of the termination. In addition, all CAs with which cross-certification agreements are current at the time of cessation will be promptly informed of the termination. All certificates issued by the CA that reference this Policy will be revoked no later than the time of termination.

Chapter 6. Technical Security Controls

6.1. Key Pair Generation and Installation

6.1.1. Key Pair Generation

Key pairs for the Issuing CA, RAs, VSPs, and subscribers shall be generated in such a way that the private key is not known by anyone other than the authorized user of the key pair. Acceptable ways of accomplishing this include:

- Having all users (CAs, RAs, VSPs, and subscribers) generate their own keys on a trustworthy system, and not reveal the private keys to anyone else;
- Having keys generated in hardware tokens from which the private key cannot be extracted.

Key pairs for VSPs and subscribers may be generated and stored in either hardware or software. Key pairs for CAs must be generated in hardware.

6.1.1.1. CA and RA Key Pair Generation

CA and RA keys shall be generated and stored in hardware tokens holding a FIPS 140-2 Level 3 certification. The generation of a CA key pair shall take place using a pre-established key generation script that is performed by at least two CA operators (a minimum of one performing, one witnessing) acting in a Trusted Role per section 5.2.1. CA key generation ceremonies shall be videotaped/recorded as they are performed. A copy of the video recording and the signed script for the key generation ceremony shall be retained as part of the standard records for the Issuing CA, per section 5.4.1.

6.1.2. Private Key Delivery to Subscriber

When private keys are generated by the CA and delivered to the subscriber, the private key must be cryptographically wrapped using a NIST-approved private- key-wrapping algorithm with appropriate symmetric key length.

6.1.3. Public Key Delivery to Certificate Issuer

The subscriber's public key shall be transferred to the RA or CA in a way that ensures that (1) it has not been changed during transit; (2) the sender possesses the private key that corresponds to the transferred public key; and (3) the sender of the public key is the legitimate user claimed in the certificate application.

6.1.4. CA Public Key Delivery to Relying Parties

The public key of the CA signing key pair may be delivered to subscribers in an on-line transaction in accordance with IETF PKIX Part 3, or via another appropriate mechanism.

6.1.5. Key Sizes

Issuing CA key pairs and Subscriber certificate key pairs shall be RSA 2048-bit or larger, ECC secp256r1 or larger, or algorithms with equivalent cryptographic strength. Hashing of information shall be performed using at least Secure Hash Algorithm 2 (SHA-2) with a 256-bit hash length (SHA-256) or better.

6.1.6. Public Key Parameters Generation and Quality Checking

Public key parameters shall be generated and checked in accordance with the standard that defines the cryptographic algorithm in which the parameters are to be used. Issuing CAs shall take appropriate measures to validate the suitability of keys presented by Applicants, such as testing for known weak keys or weak encryption parameters, and shall reject unsuitable keys during the application process.

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

Issuing CAs shall set the Key Usage field of issued certificates in accordance with the proposed field of application, following the protocols established in version 3 of the X.509 standard.

6.2. Private Key Protection and Cryptographic Module Engineering Controls

The Issuing CA shall protect its private key(s) using a hardware based cryptographic device holding a FIPS 140-2 level 3 or higher certification, in accordance with the provisions of this Policy. The CA, RAs, and VSPs shall each protect their private key(s) in accordance with the provisions of this Policy.

6.2.1. Cryptographic Module Standards and Controls

The Issuing CAs' signing key generation, storage and signing operations shall be performed using a hardware-based cryptographic module holding a FIPS 140-2 Level 3 or higher certification.

6.2.2. Private Key (N out of M) Multi-Person Control

Multi-person control is a security mechanism that requires multiple authorizations for access to the CA Private Signing Key. Access to (including activation of) the Issuing CA Private Signing Key shall require authorization and validation by multiple parties, including CA personnel and security officers. This mechanism prevents a single party (CA or otherwise) from gaining access to the CA Private Signing Key. Issuing CA Private Signing Keys shall be backed up only under two-person control by administrators acting in a Trusted Role, as defined in Section 5.2.1.

6.2.3. Private Key Escrow

Subscriber private keys must never be revealed to the Issuing CA and are therefore never escrowed.

6.2.4. Private Key Backup, Archival, and Restoration

The private keys for the Issuing CAs shall be backed up, archived and restored using either a NIST-approved key wrapping algorithm or the FIPS 140-2 Level 3 method provided by the HSM vendor.

6.2.5. Private Key Transfer into or from a Cryptographic Module

Private keys for Issuing CAs shall not be generated outside of a cryptographic module holding a FIPS 140-2 Level 3 or higher certification. Should there be a need to migrate keys from one module to another (such as for backup or hardware replacement), the keys shall be archived from the initial module and restored on the new module using either a NIST-approved key wrapping algorithm or the method provided by the HSM vendor.

6.2.6. Private Key Storage on Cryptographic Module

Issuing CAs and RAs shall ensure that private keys are always stored on a cryptographic module holding a FIPS 140-2 Level 3 or higher certification. VSPs and Subscribers may opt to store private keys in a cryptographic module or in software.

6.2.7. Method of Activating a Private Key

When being readied for use, CA Private Key material shall be activated under two-person control, using the method provided by the manufacturer of the hardware security module in use.

6.2.8. Method of Deactivating a Private Key

When no longer in use, CA Private Key material shall be de-activated using the method provided by the manufacturer of the hardware security module in use.

6.2.9. Method of Destroying a Private Key

Upon expiration or revocation of a certificate, or other termination of use of a private key for creating signatures, all copies of the private key shall be securely destroyed in such a manner as to ensure no copy of the private key can be resurrected or restored for use.

6.2.10. Cryptographic Module Rating

All hardware security modules (HSMs) used by Issuing CAs or subscribers shall hold a FIPS 140-2 hardware standard certification at Level 3 or higher.

6.3. Other Aspects of Key Pair Management

6.3.1. Public Key Archival

The public keys of the Issuing CAs and Subscriber public keys shall be archived in the regular backups of the Repository where the digital certificates are published.

6.3.2. Certificate Operational Periods and Key Pair Usage Periods

Issuing CAs shall establish the standard validity period for certificates issued under this Policy, and shall document those validity periods in their Certification Practice Statements (CPSs). At a minimum, the validity period for certificates issued under this Policy shall not exceed the recommended length for the encryption algorithm used in the certificate, as established in NIST publication SP800-131A ("Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths"). In addition, Issuing CAs must comply with the CAB Forum Minimum Guidelines for Publicly Trusted SSL Certificates with respect to the maximum validity, which may reduce the effective available certificate term.

6.4. Activation Data

Information used to wrap or activate Issuing CA key pairs shall be of a strength commensurate with the data protected. If such data must be transmitted from one computer to another (such as for remote administration purposes), the channel used to transmit the data shall be encrypted and strongly authenticated sufficient to securely identify the participants in the communication.

Issuing CAs shall store activation materials separate from the Issuing CA physical hardware, when the activation materials are not actively in use, and shall protect activation materials with a combination of logical and physical protections sufficient to require multi-person access per section 6.2.2.

6.5. Computer Security Controls

The Issuing CA shall institute documented security hardening procedures based on a combination of vendor recommendations and industry best practices, to improve the security of the operating environment on all Issuing CA systems. These procedures shall specify the hardening steps to take and the basis for the hardening steps. In particular, CAs shall require that access to the certificate authority issuance functions requires multiple factors of authentication such as a password plus a physical access token, biometric authenticator, or one-time password generator.

6.6. Life-Cycle Technical Controls

6.6.1. System Development Controls

Issuing CAs shall instantiate documented software testing and change control procedures for the implementation of software on operational CA systems. Such controls shall, at a minimum, specify procedures for software testing and release to production, modifications to code, and shall include provisions for emergency software fixes if these are permitted.

6.6.2. Security Management Controls

Issuing CAs shall ensure that software elements considered in production are protected from unauthorized modification, and periodically verified to ensure their integrity.

6.6.3. Life-Cycle Security Controls

The Issuing CA shall instantiate documented procedures for the lifecycle management of hardware and software components of the CA.

6.7. Network Security Controls

The CA server and any repositories shall be protected through network firewalls configured only to allow the protocols required for the secure operation of the CA's services. Where employed, application proxies shall be configured to permit only the commands required for the secure operation of the CA's services.

6.7.1. Change Management Process

All CA components shall follow the principles of documentation, approval, and testing to ensure that all changes to Certificate Systems, Issuing Systems, Certificate Management Systems, Security Support Systems, and Front-End / Internal-Support Systems followa defined Change Management Process.

6.7.2. Monitoring and Alerting

All CA components shall continuously monitor, detect, and alert personnel to any configuration change to Certificate Systems, Issuing Systems, Certificate Management Systems, Security Support Systems, and Front-End / Internal-Support Systems unless the change has been authorized through a change management process. All CA components shall respond to the alert and initiate a plan of action within at most twenty-four (24) hours.

6.8. Time-stamping

All Issuing CA components shall be regularly synchronized with a reliable time service such as an Atomic Clock or Network Time Protocol (NTP) server. A dedicated authority (Time Stamping Server) may be used to provide this time stamp. Time derived from this service shall be used for the following purposes:

- Validity Time for a CA Certificate;
- Revocation Time for a CA Certificate;
- Determining Validity or Post Time for CRL updates;
- Issuance of Subscriber/End Entity certificates.

Time may be automatically or manually synchronized; clock adjustments shall be regarded as auditable events.

6.8.1. Time and Issuance Dates

The issuance time and date for certificates issued under this policy, as recorded by the CA in the `notBefore` field of the issued certificate, must be a reasonable reflection of the time and date the certificate was actually generated. CA staff or the CA software may adjust the `notBefore` time-stamp in order to meet technical compatibility requirements, but in no cases shall the `notBefore` contents be adjusted to avoid policy date cutoffs or deadlines. If time-stamps are or may be automatically adjusted by software (e.g. to allow for immediate use of certificates), CAs must disclose this in their Certification Practice Statements. If time-stamps are manually adjusted by CA staff prior to issuance, this must be recorded as part of the issuance documentation for that certificate and retained.

Chapter 7. Certificate, CRL, and OCSP Profiles

7.1. Certificate Profiles

Issuing CAs shall establish a standard certificate profile for each certificate issued, and shall document or reference that profile from the Issuing CA's Certification Practice Statement (CPS). All such certificate profiles shall be verified to conform to version 3 of the X.509 standard, RFC 5280, the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, and any other applicable best practices. In compliance with RFC 5280, Root CAs subscribing to this policy MUST ensure the Certificate Issuer Distinguished Name field matches the Subject Distinguished Name field, to support Name chaining.

7.2. Certificate Revocation List (CRL) Profiles

Certificate Revocation Lists (CRLs) issued by Issuing CAs under this Policy shall be issued in the X.509 version 2 format. Supported CRL extensions and the level of support for them shall be identified by the Issuing CA's Certification Practice Statement (CPS) or by specific contract with a Qualified Relying Party.

7.3. Online Certificate Status Profile (OCSP) Profiles

Where CAs use or contribute information to an Online Certificate Status Profile (OCSP) responder service, the OCSP service shall be configured to deliver responses in the OCSP v1 format, in conformance with RFC 2560 and/or RFC 5019. CAs contributing information to an OCSP responder service shall establish a profile indicating supported fields and extensions for responses.

Chapter 8. Compliance Audit and Other Assessments

The Issuing CA will ensure that: (i) it only accepts information from entities that understand and are obligated to comply with this Policy; (ii) it complies with the provisions of this Policy in its certification and Repository services, issuance and revocation of Certificates and issuance of CRLs; (iii) it makes reasonable efforts to ensure adherence to this Policy with regard to any Certificates issued under it; and (iv) any identification and authentication procedures are implemented as set forth in the relevant CP and CPS documents.

8.1. Assessment of Compliance

Issuing CAs shall maintain and certify compliance by means of a review from an independent auditor on at least an annual basis. The audit must cover the Issuing CA's infrastructure, policies, and practices in line with its published CPS document, and must be recursive through the hierarchy of Registration Authorities and Subordinate CAs chained from the Issuing CA.

8.2. Qualifications of Auditor

Reviews and certifications of compliance under this document must be performed by a Qualified Auditor. A person or organization shall be considered a Qualified Auditor if the person or organization collectively meet the following standards:

- Independence from the subject of the audit;
- Certification as an auditor by the AICPA or CICA to perform reviews against the WebTrust for Certification Authorities; and
- Possession of the technical skills and knowledge in Public Key Infrastructure (PKI) technologies and related information security policies, practices, and standards.

8.3. Auditor's Relationship to Audited Entity

Issuing CAs must choose a Qualified Auditor who is completely independent of the Issuing CA. Reviews of the Issuing CA by a subsidiary or parent organization shall not be considered fully independent.

8.4. Content of Audit

Issuing CAs shall ensure and certify that they meet the guidelines contained in the current applicable versions of the AICPA/CICA Trust Service Principles and Criteria for Certification Authorities (WebTrust for CA) and the guidelines contained in the AICPA/CICA WebTrust for Certification Authorities SSL Baseline Requirements Audit Criteria.

8.5. Actions Taken as a Result of Deficiency

Should a compliance review identify material discrepancies between the Issuing CA's controls and the qualifying audit guidelines, the Issuing CA shall be responsible for creating a suitable corrective action plan to eliminate the deficiency.

8.6. Communication of Audit Results

The results of each annual compliance audit must be communicated to the Issuing CA's administrative team by any subordinate CAs, and to the Issuing CA's Root CA by the Issuing CA's administrative team, in the event that those teams differ.

Chapter 9. Other Business and Legal Matters

9.1. Fees

No stipulation.

9.2. Financial Responsibility

The financial responsibility of managing and maintaining the certificate authority and relevant Issuing CAs shall be the sole responsibility of Cisco Systems, Inc.

9.3. Confidentiality of Business Information

Issuing CAs must ensure that they comply with any applicable company policies and standards regarding protection of the business information they collect in the course of issuing certificates, provided that said compliance does not conflict with applicable regulatory requirements that may supersede them.

9.4. Privacy of Personal Information

Issuing CAs must disclose if they collect information for certificates that is considered Personally Identifiable Information (PII) for any natural person or organization; this information should not be collected as part of the certificate issuance process. Issuing CAs that do collect this information must disclose what information is collected and the reasons for the collection, and must have controls in place to ensure the privacy of that information to a standard commensurate with any applicable federal, state, local, or international privacy regulations that may apply to it.

9.5. Intellectual Property Rights

Issuing CAs must disclose the disposition of intellectual property rights for the information they collect and process as part of the certificate issuance process.

9.6. Representations and Warranties

9.6.1. Certificate Authority (CA) Obligations

The Issuing CAs are responsible for all aspects of the issuance and management of their issued certificates, including control over the application/enrollment process, the identification and authentication process, the certificate manufacturing process, publication of the certificate (if required), suspension and/or revocation of the certificate, renewal of the certificate, validation services, and for ensuring that all aspects of the CA Services and CA operations and infrastructure related to certificates issued under this Policy are performed in accordance with the requirements and representations of this Policy.

9.6.2. Certificate Status Validation Obligations

The CA shall be responsible for providing a means by which certificate status (valid, suspended, or revoked) can be determined by a Benefiting party. However, the CA may [delegate/subcontract] performance of this obligation to an identified validation services provider ("VSP"), provided the CA remains primarily responsible for performance of those services by such third party in a manner consistent with the requirements of this Policy.

9.6.3. Subscriber Obligations

In all cases, the subscriber is obligated to:

- Generate a key pair using a trustworthy system, and take reasonable precautions to prevent any loss, disclosure, or unauthorized use of the private key;
- Warrant that all information and representations made by the subscriber that are included in the certificate are true;
- Use the certificate exclusively for authorized and legal purposes, consistent with this Policy;
- Cease using the certificate and request the CA revoke the certificate promptly if any information in the certificate becomes incorrect or inaccurate;
- Cease using the certificate and associated private key and instruct the CA to revoke the certificate promptly upon any actual or suspected loss, disclosure, or other compromise of the subscriber's private key.

A Certificate Holder who is found to have acted in a manner counter to these obligations will have his, her, or its Certificate revoked, and will forfeit all claims he, she, or it may have against the Issuing CA.

9.6.4. Benefiting Party Obligations

A Benefiting party has a right to rely on a certificate that references this Policy only if the certificate was used and relied upon for lawful purposes and under circumstances where:

- The Benefiting Party entered into a Benefiting Party Agreement which incorporates by reference the provisions of this Policy regarding the Issuing CA's and the Benefiting Party's rights and obligations;
- The reliance was reasonable and in good faith in light of all the circumstances known to the benefiting party at the time of reliance;
- The purpose for which the certificate was used was appropriate under this Policy;
- The benefiting party checked the status of the certificate prior to reliance.

A Benefiting party found to have acted in a manner counter to these obligations would forfeit all claims he, she, or it may have against the Issuing CA.

9.6.5. Registration Authority (RA) Obligations

In general, the CA shall be responsible for performing all identification and authentication functions and all certificate manufacturing and issuing functions. The CA may delegate performance of these obligations to an identified registration authority ("RA"), provided the CA remains primarily responsible for the performance of those services by such third parties in a manner consistent with the requirements of this Policy. The ability to delegate or subcontract these obligations requires the approval of Cisco Systems Corporate Information Security group.

9.6.6. CA Representations

By issuing a certificate that references this Policy, the Issuing CA certifies to Benefiting Parties who reasonably and in good faith rely on the information contained in the certificate during its operational period and in accordance with this Policy, that:

- The CA has issued, and will manage, the certificate in accordance with this Policy;
- The CA has complied with the requirements of this Policy and its applicable CPS when authenticating the subscriber and issuing the certificate;
- There are no misrepresentations of fact in the certificate known to the CA, and the CA has taken reasonable steps to verify additional information in the certificate unless otherwise noted in its CPS;
- Information provided by the subscriber in the certificate application for inclusion in the certificate has been accurately transcribed to the certificate;
- The certificate meets all material requirements of this Policy and was processed according to the CA's CPS.

9.6.7. Benefiting Party Warranties

Unless an explicit contractual agreement exists between Cisco Systems and a Benefiting Party, Cisco Systems is not representing any warranty to a Benefiting Party that exercises reliance on certificates issued under this Policy. In such instances where an explicit and separate Certificate Warranty agreement exists between the Benefiting Party and Cisco Systems, Cisco Systems may warrant that:

- The Issuing CA has issued and managed the Certificate in accordance with this Policy;
- The Issuing CA complied with the requirements of this Policy and any applicable CPS when authenticating requests for subordinate CA certificates;
- There are no material misrepresentations of fact in the Certificate known to the Issuing CA, and the Issuing CA has taken steps as required under this Policy to verify the information contained in the Certificate;
- The Issuing CA has taken the steps required by this Policy to ensure that the Certificate Holder's submitted information has been accurately transcribed to the Certificate;
- Information provided by the Issuing CA concerning the current validity of the Certificate is accurate and that validity has not been diminished by the Issuing CA's failure to promptly revoke the Certificate in accordance with this Certificate Policy; and
- The issued Certificate meets all material requirements of this Policy and any applicable CPS.

These warranties may be applied to any Benefiting Party who: (i) enters into a separately executed warranty agreement with Cisco Systems; (ii) relies on the issued Certificate in an electronic transaction in which the issued Certificate played a material role in verifying the identity of one or more persons or devices; (iii) exercises Reasonable Reliance on that Certificate; and (iv) follows all procedures required by this Policy and by the applicable Benefiting Party Agreement for verifying the status of the issued Certificate. These warranties are made to the Benefiting Party as of the time the CA's certificate validation mechanism is utilized to determine Certificate validity, and only if the Certificate relied upon is valid and not revoked at that time.

9.6.8. End Entity Agreements

The Issuing CA may enter into agreements with End Entities governing the provision of Certificate and Repository services and delineating the parties' respective rights and obligations.

The Issuing CA will ensure that any Certificate Agreements incorporate by reference the provisions of this Policy regarding the Issuing CA's and the Certificate Holder's rights and obligations. In the alternative, the Issuing CA may ensure that any Certificate Agreements, by their terms, provide the respective rights and obligations of the Issuing CA and the Certificate Holders as set forth in this Policy, including without limitation the parties' rights and responsibilities concerning the following:

- Procedures, rights and responsibilities governing (i) application for an issued Certificate, (ii) the enrollment process, (iii) Certificate issuance, and (iv) Certificate Acceptance;
- The Certificate Holder's duties to provide accurate information during the application process;
- The Certificate Holder's duties with respect to generating and protecting its Keys;
- Procedures, rights and responsibilities with respect to Identification and Authentication (I&A);
- Any restrictions on the use of issued Certificates and the corresponding Keys;
- Procedures, rights and responsibilities governing (a) notification of changes in Certificate information, and (b) revocation of issued Certificates;
- Procedures, rights and responsibilities governing renewal of issued Certificates;
- Any obligation of the Certificate Holder to indemnify any other Participant;
- Provisions regarding fees;
- The rights and responsibilities of any RA that is party to the agreement;

- Any warranties made by the Issuing CA and any limitations on warranties or liability of the Issuing CA and/or an RA;
- Provisions regarding the protection of privacy and confidential information; and
- Provisions regarding Alternative Dispute Resolution.

Nothing in any Certificate Agreement may waive or otherwise lessen the obligations of the Certificate Holder as provided in section 9.6.3 of this Policy.

The Issuing CA will ensure that any Benefiting Party Agreement incorporate by reference the provisions of this Policy regarding the Issuing CA's and the Benefiting Party's rights and obligations. Nothing in a Benefiting Party Agreement may waive or otherwise lessen the obligations of the Benefiting Party as provided in this Policy.

9.7. Warranty Limitations

The warranties offered to both Certificate Holders and Benefiting Parties will be subject to the limitations set forth in this Policy. Cisco Systems may provide further limitations and exclusions on these warranties as deemed appropriate, relating to: (i) failure to comply with the provisions of this Policy or of any agreement with the Issuing CA; (ii) other actions giving rise to any loss; (iii) events beyond the reasonable control of the CA; and (iv) time limitations for the filing of claims. However, such limitations and exclusions may not, in any event, be less than those provided for in Section 9.6.7.

9.8. Liability

The Issuing CA assumes limited liability only to Benefiting Parties who have entered into a Benefiting Party Agreement. The Issuing CA may be responsible for direct damages suffered by benefiting parties who have executed a Benefiting Party Agreement that are caused by the failure of the Issuing CA to comply with the terms of this Policy (except when waived by contract), and sustained by such benefiting parties as a result of reliance on a certificate in accordance with this Policy. The liability of the Issuing CA is limited to these conditions and to conditions set forth in the terms of specific Benefiting Party Agreements.

Except as expressly provided in this Policy and in its CPS, the Issuing CA disclaims all other warranties and obligations of any type, including any warranty of merchantability, any warranty of fitness for a particular purpose, and any warranty of accuracy of information provided.

The liability of the Issuing CA under this Policy to Benefiting Parties who have executed a Benefiting Party agreement shall be limited to direct damages, and shall not exceed $1000.00, except when waived by contract. The Issuing CA shall have no liability for consequential damages. Under no circumstances will the Issuing CA be responsible for direct or consequential damages to benefiting parties who have not entered into a Benefiting Party Agreement with Cisco Systems, Inc.

9.9. Indemnities

No further stipulation.

9.10. Term and Termination

No further stipulation.

9.11. Individual Notices and Communications with Participants

No further stipulation.

9.12. Amendments

9.12.1. Procedure for Amendment

This document shall be amended in accordance with practices detailed in section 1.5.3.

9.12.2. Notification Mechanism and Period

Changes to this document will be in the form of an updated document file with changes reflected in the version section. The updated version of the document will be linked to from the main Cisco PKI Policies page located at www.cisco.com/security/pki/policies/index.html.

9.12.3. Circumstances Under Which OID Must Be Changed

The Object Identifier for this document must be updated in accordance with the change management and version number assignment practices identified in section 1.5.3.3.

9.13. Dispute Resolution Procedures

Disputes among Cisco Systems and a Benefiting Party will be resolved pursuant to provisions in the applicable Certificate Trust Agreements between Cisco and the Benefiting Party. Disputes between entities who are not Benefiting Parties and Cisco Systems carry no stipulation.

9.14. Governing Law

This Policy shall be construed, and any legal relations between the parties hereto shall be determined, in accordance with the laws of the United States and the State of California, without regard to any conflict of law provisions thereof.

9.14.1. Interpretation & Enforcement

Each provision of this Policy has been subject to mutual consultation, negotiation, and agreement, and shall not be construed for or against any party.

9.14.2. Severability

If any portion or term of this Policy is held unenforceable by a court of competent jurisdiction, the remainder of this Policy shall not be affected and shall remain fully in force and enforceable.

9.14.3. Survival

No stipulation unless parties have entered into a Benefiting Party Agreement with Cisco Systems.

9.14.4. Merger/Integration

No stipulation unless parties have entered into a Benefiting Party Agreement with Cisco Systems.

9.15. Compliance with Applicable Law

No stipulation except as specified in section 9.14.

9.16. Miscellaneous Provisions

9.16.1. Notice

All notices and other communications hereunder shall be in writing and shall be deemed given (a) on the same day if delivered personally, (b) three business days after being mailed by registered or certified mail (return receipt requested), or (c) on the same day if sent by telecopy, confirmed by telephone, to each of the contacts listed in section 1.5.2 above.

Chapter 10. References

10.1. Normative References

This document attempts to address control elements enumerated in RFC 3647, RFC 2527, the guidelines contained in version 2.0 of the AICPA/CICA Trust Service Principles and Criteria for Certification Authorities (WebTrust for CA), and the guidelines contained in the amended version 1.4.3 of the AICPA/CICA WebTrust for Certification Authorities SSL Baseline Requirements Audit Criteria.

10.2. Informative References

Controls detailed in this document were informed by perusal of publicly available PKI policies and standards. Any similarity to other documents is attributed where appropriate and otherwise entirely unintentional.

Appendix A: Definitions and Acronyms

Affiliated Individual

An affiliated individual is the subject of a certificate that is affiliated with a sponsor approved by the CA (such as an employee affiliated with an employer). Certificates issued to affiliated individuals are intended to be associated with the sponsor and the responsibility for authentication lies with the sponsor.

Authorized CA

A certification authority that has been authorized by the Certificate Policy Management Authority to issue certificates that reference this policy.

Benefiting Party

A recipient of a digitally signed message who relies on a certificate to verify the integrity of a digital signature on the message (through the use of the public key contained in the certificate), and the identity of the individual that created said digital signature.

CA

Certification Authority

Certificate

A record that, at a minimum: (a) identifies the certification authority issuing it; (b) names or otherwise identifies its subscriber; (c) contains a public key that corresponds to a private key under the sole control of the subscriber; (d) identifies its operational period; and (e) contains a certificate serial number and is digitally signed by the certification authority issuing it. As used in this Policy, the term of “Certificate” refers to certificates that expressly reference this Policy in the "Certificate Policies" field of an X.509 v.3 certificate.

Certificate Revocation List (CRL)

A time-stamped list of revoked certificates that has been digitally signed by a certification authority.

Certification Authority

A certification authority is an entity that is responsible for authorizing and causing the issuance of a certificate. A certification authority can perform the functions of a registration authority (RA) and a certificate manufacturing authority (CMA), or it can delegate either of these functions to separate entities.

A certification authority performs two essential functions. First, it is responsible for identifying and authenticating the intended subscriber to be named in a certificate, and verifying that such subscriber possesses the private key that corresponds to the public key that will be listed in the certificate. Second, the certification authority actually creates (or manufactures) and digitally signs the certificate. The certificate issued by the certification authority then represents that certification authority’s statement as to the identity of the device named in the certificate and the binding of that device to a particular public-private key pair.

Certification Practice Statement (CPS)

A statement of the practices that a certification authority employs in issuing, suspending, and revoking certificates and providing access to same. It is recognized that some certification practice details constitute business sensitive information that may not be publicly available, but which can be provided to certificate management authorities under non-disclosure agreement.

CPS

See Certification Practice Statement.

CRL

See Certificate Revocation List.

FIPS (Federal Information Processing Standards)

These are Federal standards that prescribe specific performance requirements, practices, formats, communications protocols, etc. for hardware, software, data, telecommunications operation, etc. Federal agencies are expected to apply these standards as specified unless a waiver has been granted in accordance with FIPS waiver procedures.

IETF (Internet Engineering Task Force)

The Internet Engineering Task Force is a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of Internet architecture and the efficient and robust operation of the Internet.

IP Address

A 32-bit or 128-bit label assigned to a device that uses the Internet Protocol for communication.

IP Address Contact

The person(s) or entity(ies) registered with an IP Address Registration Authority as having the right to control how one or more IP Addresses are used.

IP Address Registration Authority

The Internet Assigned Numbers Authority (IANA) or a Regional Internet Registry (RIPE, APNIC, ARIN, AfriNIC, LACNIC).

Key Compromise

A Private Key is said to be compromised if its value has been disclosed to an unauthorized person or an unauthorized person has had access to it.

Key Pair

Two mathematically related keys, having the properties that (a) one key can be used to encrypt a message that can only be decrypted using the other key, and (b) even knowing one key, it is computationally infeasible to discover the other key.

Object Identifier

An object identifier is a specially formatted number that is registered with an internationally recognized standards organization.

OID

See Object Identifier.

Operational Period of a Certificate

The operational period of a certificate is the period of its validity. It would typically begin on the date the certificate is issued (or such later date as specified in the certificate), and end on the date and time it expires (as noted in the certificate) unless previously revoked or suspended.

PIN

Personal Identification Number

PKI

Public Key Infrastructure

PKIX

An IETF Working Group developing technical specifications for a PKI components based on X.509 Version 3 certificates.

Policy

This Certificate Policy document.

Policy Administering Organization

The entity specified in section 1.4.

Private Key

The key of a key pair used to create a digital signature. This key must be kept secret, and under the sole control of the individual or entity whose identity is associated with that digital signature.

Public Key

The key of a key pair used to verify a digital signature. The public key is made freely available to anyone who will receive digitally signed messages from the holder of the key pair. The public key is usually provided via delivery of a certificate issued by a certification authority and might also be obtained by accessing a repository. A public key is used to verify the digital signature of a message purportedly sent by the holder of the corresponding private key.

RA

See Registration Authority.

Registration Authority

An entity that is responsible for identification and authentication of certificate subjects, but that does not sign or issue certificates (i.e., a RA is delegated certain tasks on behalf of a CA).

Repository

A trustworthy system for storing validity and other information relating to certificates.

Responsible Individual

A person designated by a sponsor to authenticate individual applicants seeking certificates on the basis of their affiliation with the sponsor.

Revocation (Revoke)

To prematurely end the operational period of a certificate from a specified time forward.

Sponsor

An organization with which a subscriber is affiliated (e.g., as an employee, user of a service, business partner, customer, etc.).

Subject

A person or device whose public key is certified in a certificate. Also referred to as a "subscriber."

Subscriber

A subscriber is an entity who: (a) is the subject named or identified in a certificate issued to such person or device; (b) holds a private key that corresponds to a public key listed in that certificate; and (c) the entity to whom digitally signed messages verified by reference to such certificates are to be attributed. See "subject."

Suspension (suspend)

To temporarily halt the operational validity of a certificate for a specified time period or from a specified time forward.

Trustworthy System

Computer hardware, software, and procedures that: (a) are reasonably secure from intrusion and misuse; (b) provide a reasonable level of availability, reliability, and correct operation; (c) are reasonably suited to performing their intended functions; and (d) adhere to generally accepted security procedures.

Valid Certificate / Validity

A certificate is only valid when (a) a certification authority has signed/issued it; (b) the subscriber listed in it has accepted it; (c) it has not yet expired; and (d) has not been revoked.

Validation Services Provider (VSP)

An entity that maintains a repository accessible to the public (or at least to benefiting parties) for purposes of obtaining copies of certificates or an entity that provides an alternative method for verifying the status of such certificates.

VSP

See Validation Services Provider.

Whois

Information retrieved directly from the Domain Name Registrar or registry operator via the protocol defined in RFC 3912, the Registry Data Access Protocol defined in RFC 7482, or an HTTPS websiteinformation retrieved directly from the Domain Name Registrar or registry operator via the protocol defined in RFC 3912, the Registry Data Access Protocol defined in RFC 7482, or an HTTPS website.