



Cisco RXC Certification Practice Statement

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

Version 2.9, 2022-Jan-19

Table of Contents

| | |
|---|----|
| Document Metadata | 2 |
| Version History | 2 |
| Annual Reviews | 2 |
| 1. Introduction | 4 |
| 1.1. Overview | 4 |
| 1.2. Certificate Policy and Identification | 4 |
| 1.3. PKI Participants | 4 |
| 1.4. Certificate Usage | 5 |
| 1.5. Policy Administration | 6 |
| 1.6. Definitions and Acronyms | 7 |
| 2. Publication and Repository Responsibilities | 8 |
| 2.1. Repositories | 8 |
| 2.2. Publication of Certification Information | 8 |
| 2.3. Time or Frequency of Publication | 8 |
| 2.4. Access Controls on Repositories | 8 |
| 3. Identification and Authentication | 9 |
| 3.1. Naming | 9 |
| 3.2. Initial Identity Validation | 9 |
| 3.3. Certificate Re-Key | 10 |
| 3.4. Certificate Revocation | 11 |
| 4. Certificate Life-Cycle Operational Requirements | 12 |
| 4.1. Certificate Application | 12 |
| 4.2. Certificate Application Processing | 12 |
| 4.3. Certificate Issuance | 12 |
| 4.4. Certificate Acceptance | 13 |
| 4.5. Key Pair and Certificate Usage | 13 |
| 4.6. Certificate Renewal | 14 |
| 4.7. Certificate Re-Key | 14 |
| 4.8. Certificate Modification | 15 |
| 4.9. Certificate Revocation and Suspension | 15 |
| 4.10. Certificate Status Services | 18 |
| 4.11. Removal of Certificates from Revocation Status Services | 18 |
| 4.12. End of Subscription | 18 |
| 4.13. Key Escrow and Recovery | 18 |
| 5. Facility, Management, and Operational Controls | 19 |
| 5.1. Physical Controls | 19 |
| 5.2. Procedural Controls | 20 |
| 5.3. Personnel Controls | 20 |
| 5.4. Audit Logging Procedures | 21 |
| 5.5. Records Archival | 22 |
| 5.6. Business Continuity and Disaster Recovery | 22 |
| 5.7. CA Termination | 23 |
| 5.8. CA or RA Termination | 23 |

| | |
|---|----|
| 6. Technical Security Controls | 24 |
| 6.1. Key Pair Generation and Installation | 24 |
| 6.2. Private Key Protection and Cryptographic Module Engineering Controls | 25 |
| 6.3. Other Aspects of Key Pair Management | 26 |
| 6.4. Activation Data | 26 |
| 6.5. Computer Security Controls | 26 |
| 6.6. Life-Cycle Technical Controls | 26 |
| 6.7. Network Security Controls | 27 |
| 6.8. Time-stamping | 27 |
| 7. Certificate, CRL, and OCSP Profiles | 28 |
| 7.1. Certificate Profiles | 28 |
| 7.2. Certificate Revocation List (CRL) Profiles | 28 |
| 7.3. Online Certificate Status Profile (OCSP) Profiles | 29 |
| 8. Compliance Audit and Other Assessments | 30 |
| 8.1. Assessment of Compliance | 30 |
| 8.2. Qualifications of Auditor | 30 |
| 8.3. Auditor's Relationship to Audited Entity | 30 |
| 8.4. Content of Audit | 30 |
| 8.5. Actions Taken as a Result of Deficiency | 30 |
| 8.6. Communication of Audit Results | 30 |
| 9. Other Business and Legal Matters | 31 |
| 9.1. Fees | 31 |
| 9.2. Financial Responsibility | 31 |
| 9.3. Confidentiality of Business Information | 31 |
| 9.4. Privacy of Personal Information | 31 |
| 9.5. Intellectual Property Rights | 31 |
| 9.6. Representations and Warranties | 31 |
| 9.7. Warranty Limitations | 33 |
| 9.8. Liability | 34 |
| 9.9. Indemnities | 34 |
| 9.10. Term and Termination | 34 |
| 9.11. Individual Notices and Communications with Participants | 34 |
| 9.12. Amendments | 34 |
| 9.13. Dispute Resolution Procedures | 34 |
| 9.14. Governing Law | 35 |
| 9.15. Compliance with Applicable Law | 35 |
| 9.16. Miscellaneous Provisions | 35 |
| 10. References | 36 |
| 10.1. Normative References | 36 |
| 10.2. Informative References | 36 |
| Appendix A: Definitions and Acronyms | 37 |

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 describe the practices that Cisco Systems ("Cisco") follows for the operation and management of the CA/B-F External Root CA ("RXC-R2 CA") within Cisco Systems Inc., and the practices governing the issuance and life cycle of certificates issued from the RXC-R2 CA, for the benefit of relying users.

Document Metadata

Version History

| Version | Date | Changes |
|---------|----------------|---|
| 1.0 | 2014-Jun-30 | First version of document, current through CABF Guidelines v1.1.8 |
| 2.0 | 2016-Nov-01 | Updates to explicitly incorporate changes from the CA/Browser Forum Requirements through version 1.4.1 |
| 2.1 | 2017-Apr-06 | Incorporates CABF Guidelines v1.4.2 and 1.4.3 |
| 2.2 | 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 |
| 2.3 | 2017-Aug-16 | Adds Creative Commons license for distribution |
| 2.4 | 2018-Feb-01 | Removes redundant 'Approvals' section Incorporates Baseline Requirements updates through v1.5.4 TITLE: Fixed document title to accurately reflect CPS vs. CP 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; notBefore date update 3.2.1: Clarified language around validation of certificate requests 3.2.6: Removed duplicate sentence about cross-certification 5.5: Fixed titles of WebTrust and BR documents |
| 2.5 | 2019-Feb-06 | Updated language in 6.5 from multiple factor authentication to Multi-Factor Authentication Added definitions for Key Compromise, Multi-Factor Authentication, Secure Key Storage, and Whois |
| 2.6 | 2019-April-10 | Added definitions for IP Address, IP Address Contact, and IP Address Registration Authority. Added section 7.1.4.1 about subject information. |
| 2.7 | 2020-August-24 | Review update only (no content changes) |
| 2.8 | 2022-Jan-19 | Update OID policies table in section 1.2 |

Annual Reviews

| Version | Date | Name | Title |
|---------|-------------|------------|-----------------------------|
| 1.0 | 2014-Jul-10 | | <i>First version issued</i> |
| 1.0 | 2015-Sep-25 | Jos Purvis | PKI Compliance |
| 2.0 | 2016-Nov-01 | | <i>New version issued</i> |
| 2.1 | 2017-Apr-06 | | <i>New version issued</i> |
| 2.2 | 2017-May-08 | | <i>New version issued</i> |
| 2.3 | 2017-Aug-16 | | <i>New version issued</i> |

| Version | Date | Name | Title |
|----------------|----------------|-------------|---------------------------|
| 2.4 | 2018-Feb-01 | | <i>New version issued</i> |
| 2.5 | 2019-Feb-06 | | <i>New version issued</i> |
| 2.6 | 2019-April-10 | | <i>New version issued</i> |
| 2.7 | 2020-August-24 | | <i>New version issued</i> |
| 2.8 | 2022-Jan-19 | | <i>New version issued</i> |

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 guidelines established by the Certificate Authority and Browser Forum ("CAB Forum").

The purpose of this document is to describe the practices that Cisco Systems ("Cisco") follows for the operation and management of the CA/B-F External Root CA ("RXC-R2 CA") within Cisco Systems Inc., and the practices governing the issuance and life cycle of certificates issued from the RXC-R2 CA, for the benefit of relying users.

This document is licensed under a Creative Commons Attribution-NoDerivatives 4.0 International License. For more information about this license, visit creativecommons.org/licenses/by-nd/4.0/ or contact the Creative Commons Foundation at PO Box 1866, Mountain View, CA 94042 USA.

1.2. Certificate Policy and Identification

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

| | |
|---|------------------------------|
| <code>cisco OID ::= { iso(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) cisco(9) }</code> | <code>(1.3.6.1.4.1.9)</code> |
|---|------------------------------|

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

| | |
|---|---------------------------------|
| <code>cisco-pki OID ::= { cisco 21 }</code> | <code>(1.3.6.1.4.1.9.21)</code> |
| <code>cisco-pki-policies OID ::= { cisco-pki 1 }</code> | <code>(...9.21.1)</code> |
| <code>cisco-pki-policies-ssl OID ::= { cisco-pki-policies 22 }</code> | <code>(...9.21.1.22)</code> |
| <code>cisco-pki-policies-ssl-version OID ::= { cisco-pki-policies- ssl 0 }</code> | <code>(...9.21.1.22.0)</code> |

In compliance with the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, the RXC-R2, as a root certificate authority, does not include the `certificatePolicies` extension on its own certificate. All subordinate CA certificates issued from the RXC-R2 CA include the `certificatePolicies` extension, and assert a policy identifier assigned to them at creation derived from the `1.3.6.1.4.1.9.21.1.22` tree and documented in their Certification Practice Statements.

1.3. PKI Participants

1.3.1. Certification Authorities

This Certification Practice Statement ("CPS") describes and governs the practices of certificate issuance for the Cisco CA/B-F Root CA ("RXC-R2 CA") under the requirements set forth in the Cisco RXC Certificate Policy. Issuing CAs subordinated to the RXC-R2 CA must define a separate CPS governing their issuance and management of certificates.

All certificate authorities maintaining adherence to this CPS 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.

1.3.2. Registration Authorities

Cisco Systems does not traditionally employ the use of Registration Authorities in conjunction with certificate issuance practices. The RXC-R2 CA does not employ a registration authority, nor does it include Delegated Third Parties in the operation of any of its functions.

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 SSL using a server certificate issued by the RXC-R2 CA 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

RXC-R2 CA issues certificates only for subordinated certificate authorities and online certificate status protocol signing. The management team of the RXC-R2 CA employs policy and technical constraints to define the appropriate use of each issued certificate, and shall ensure that certificate holders use their issued certificates only for the purposes so identified, including secure Authentication, Identity Assurance, or Encryption and Integrity Protection of data.

1.4.2. Prohibited Certificate Uses

The RXC-R2 CA restricts the use of issued certificates 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. The RXC-R2 CA reserves the right to revoke certificates used in violation of their permitted usage.

1.4.3. Certificate Extensions

The RXC-R2 CA uses software and policy constraints to ensure it issues all certificates using Extensions defined by the X.509 v.3 standard. Issued certificates may include Certificate Extensions that constrain the usage, role, or capabilities of the issued certificate, as appropriate for the certificate.

1.4.4. Critical Extensions

All certificates issued by the RXC-R2 CA, 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.

The inclusion of these extensions is ensured through the use of software and policy constraints.

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 CPS are made by Cisco's Policy Management Authority (PMA), which includes members of Cisco's Corporate Information Security Group. Changes are proposed by members of the Policy Management Authority, 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 the document shall be considered binding on the RXC-R2 CA and relevant subscribers within 30 days of issuance.

1.5.3.1. Certification Practice Statement Approvals

All certificate authorities subordinated to the RXC-R2 CA shall define a specific CPS governing their issuance and maintenance of certificates, and their conformance to the Cisco RXC Certificate Policy and to the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates managed by the CA/Browser Forum. The Cisco Systems Information Security Policy Management Authority reviews the CPS of all subordinated CAs at least annually to ensure documents are properly structured and conform to these Policies. Changes to this CPS are made using the procedure and practice outlined in section 1.5.3.

1.5.3.2. Notifications of Changes

The Cisco Systems PMA is responsible for providing notifications of changes to this document to any Relying Parties that have entered into an agreement requiring notification, and to the management team of any subordinated CA.

1.5.3.3. Version Management and Changes

This CPS document contains a version history table recording the history of changes to this document, the appropriate versions, and the approvals obtained thereunto. Version numbers are 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.

This version of the document is effective as of 10 April 2019; certificates issued from the RXC-R2 CA with a notBefore date of 10 April 2019 may be relied on as validated under the standards and practices detailed in this version 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. The RXC-R2 CA contributes relevant documentation as specified in section 2.2 to this repository.

2.2. Publication of Certification Information

The RXC-R2 CA contributes to Cisco's secure on-line repository and certificate validation service that is available to Benefiting Parties as required by the Cisco RXC Certificate Policy, section 2.2. The RXC-R2 CA's contribution includes: (1) issued certificates that reference this Policy, when publication is authorized by the subscriber; (2) a Certificate Revocation List ("CRL") and information updated into Cisco's online certificate status database (located at pkivcs.cisco.com/pki/ocsp); (3) the RXC-R2 CA's certificate for its signing key; and (4) past and current versions of this CPS document.

2.3. Time or Frequency of Publication

All information authorized to be published in Cisco's repository shall be published promptly after such information is authorized and available to the RXC-R2 CA. Certificates issued by the RXC-R2 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

Cisco makes its CA information repository available to Benefiting Parties and subscribers 24 hours per day, 7 days per week, subject to reasonable scheduled maintenance. The RXC-R2 CA does not impose any access controls on this Policy, the CA's certificate for its signing key, and past and current versions of the relevant CP and CPS documents. The RXC-R2 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 the Cisco RXC Certificate Policy and in this document.

Chapter 3. Identification and Authentication

The management team of the RXC-R2 CA reviews applicant certificate information in order to address the recognition of trademark rights with regards to certificate naming practices, as applicable. The RXC-R2 CA authenticates the requests of parties wishing to be issued or to revoke certificates under this Policy using either technical authentication methods such as electronic authentication, or using specifically issued identification documents, as appropriate.

3.1. Naming

The RXC-R2 CA is maintained in a secure data center without any connection to outside networks. Certificate applications must therefore, after vetting, be transported in person to the certificate authority infrastructure and transferred directly to the CA for processing. Presentation of applicant materials is limited to the employees of Cisco Systems.

3.1.1. Types of Names

The RXC-R2 CA employs technical and policy constraints on its issuance software to ensure that the subject name used for certificate applicants is an X.509 Subject Distinguished Name (subjectDN).

The RXC-R2 CA does not permit the use of Internationalized Domain Names (IDNs), IP addresses, or bare hostnames (i.e. 'hostname' instead of 'hostname.domain.tld') in the **commonName** or **subjectAltName** fields of any certificate it issues. The RXC-R2 CA does not permit the use of IP addresses of any kind in issued certificates. Certificate requests containing any of the above values will be rejected.

3.1.2. Need for Names to Be Meaningful

The RXC-R2 CA and its administrative team reviews all applicant materials either electronically or manually to 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 administrative team of the RXC-R2 CA does not permit anonymous or pseudonymous certificate requests: all requests must originate from a properly identified and authenticated certificate authority owned and operated by Cisco Systems.

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 RXC-R2 CA utilizes an electronic record of issued certificates to ensure that the subject name or the combination of the subject name and other data fields listed in a certificate are unambiguous for all certificates issued.

3.1.6. Role of Trademarks in Certificate Content

The RXC-R2 CA does not, by practice, issue certificates with content that infringes upon the intellectual property rights of another entity. The RXC-R2 CA does not specifically review certificates for intellectual property infringement, but reserves the right to revoke any issued certificates that are found to violate intellectual property rights.

3.2. Initial Identity Validation

The management team of the RXC-R2 CA individually validates any certificate applicant to ensure that it is an authorized subordinated certificate authority or Online Certificate Status Protocol (OCSP) signer, fully owned and operated by Cisco

Systems. For each authorized CA, the management team of the RXC-R2 CA completes a CA Description Form, describing the purpose and technical constraints of the CA; this document is reviewed and approved by the Cisco Systems Information Security Policy Management Authority and serves as a subscriber agreement for the subordinated CA, since both the subordinated CA and the RXC-R2 CA are under the control of the Cisco Systems Information Security group. For OCSP signers, the RXC-R2 CA management team maintains documentation of the systems authorized to operate the OCSP service, and ensures that OCSP certificates are only granted to those systems, which are fully under the control and ownership of Cisco Systems.

3.2.1. Identification and Authentication

The RXC-R2 CA employs technical and procedural constraints to validate that all requests for certificates originate from an authenticated and verified member of the Cryptographic Services team of Cisco Systems and are approved by the Policy Management Authority prior to issuance.

3.2.2. Method to Prove Possession of the Private Key

The management team of the RXC-R2 CA establishes that the applicant is in possession of the private key corresponding to the public key submitted with the application by manually ensuring that the private key is fully under the control of Cisco Systems.

3.2.3. Authentication of Organization Identity

For Certificates specifying an Organization Identity, the management team of the RXC-R2 CA reviews the certificate application materials to ensure supplied materials conform to standard Cisco Systems organizational information.

3.2.4. Authentication of Individual Identity

Not applicable. The RXC-R2 CA does not issue certificates whose Subject is a natural person.

3.2.5. Non-Verified Subscriber Information

The administrators of the RXC-R2 CA manually structure the supplied certificate signing request information for all applicants to ensure no unverified information is placed in the contents of certificate fields.

3.2.6. Validation of Authority

The management team of the RXC-R2 CA ensure that all private keys associated with presented certificate requests are fully under the control of Cisco Systems and that any subordinated certificate authorities, OCSP signers, and their associated domain names are fully under the ownership and control of Cisco Systems.

The RXC-R2 CA has not issued any Cross Certificates, nor has it been the Subject of a Cross Certificate by another Certificate Authority.

3.2.7. Criteria for Interoperation

No stipulation.

3.3. Certificate Re-Key

The RXC-R2 CA treats 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

The RXC-R2 CA does not renew revoked or expired certificates. Applicants to the RXC-R2 CA that reference this Policy are re-authenticated during the certificate application process, just as with a first-time application.

3.4. Certificate Revocation

A revocation request that is submitted electronically to the RXC-R2 CA is authenticated on the basis of a digital signature using the private key associated with the certificate whose revocation is requested and manually verified by the administration team of the RXC-R2 CA prior to revocation. All revocation requests are processed manually and requested specifically by the administration team of the RXC-R2 CA, and are processed according to the requirements in section 4.9.

Chapter 4. Certificate Life-Cycle Operational Requirements

4.1. Certificate Application

For each subordinated CA, the management team of the RXC-R2 CA completes a CA Description Form, describing the purpose and technical constraints of the CA; this document is reviewed and approved by the Cisco Systems Information Security Policy Management Authority and serves as a subscriber agreement for the subordinated CA, since both the subordinated CA and the RXC-R2 CA must be under the control of the Cisco Systems Information Security group. For OCSP signers, the RXC-R2 CA management team maintains documentation of the systems authorized to operate the OCSP service, and ensures that OCSP certificates are only granted to those systems, which are fully under the control and ownership of Cisco Systems.

4.1.1. Who Can Submit a Certificate Application

The RXC-R2 CA only issues certificates to subordinated CAs and Online Certificate Status Protocol (OCSP) response signing systems fully under the control of the Cisco Systems Information Security group.

4.1.2. Enrollment Process and Responsibilities

All identifying information in an applicant entity shall be verified manually by the administrative team of the RXC-R2 CA to ensure it is valid. Information communicated or collected as part of this validation process is contained in a document management system operated by the administrative team of the RXC-R2 CA.

4.2. Certificate Application Processing

4.2.1. Performing Identification and Authentication Functions

All validation of identifying information for certificate applicants is manually verified by the administrative team of the RXC-R2 CA prior to certificate issuance. All certificates issued by the RXC-R2 CA are to subordinated CAs wholly owned and controlled by Cisco Systems and within domains controlled by Cisco Systems. CA staff manually review each certificate to ensure all domains present are owned by Cisco by checking them against the Cisco-managed whitelist of Cisco-owned domains: provided all domain names are present on the whitelist, no CAA checking is performed for the domains prior to issuance. Should any domain in the presented signing request not be present on the whitelist, the RXC-R2 CA will refuse to issue a certificate.

4.2.2. Approval or Rejection of Certificate Applications

The RXC-R2 CA software is configured to return a positive, unambiguous notification indicating the approval or rejection of a certificate application.

4.2.3. Time to Process Certificate Applications

The administrative team of the RXC-R2 CA ensures that all certificate applications are completed in a timely fashion, as defined by the business needs governing the creation of the applicant.

4.3. Certificate Issuance

4.3.1. CA Actions during Certificate Issuance

The RXC-R2 CA is maintained in a fully offline system with network communications physically limited to the CA system and the Hardware Security Module (HSM) associated with it. All communications between the CA and the HSM are protected

using Transport Layer Security with mutual cryptographic authentication of the entities involved. Any information transmitted into or out of the RXC-R2 CA must be stored on physical media and manually copied into and out of the RXC-R2 CA systems.

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 the Cisco RXC Certificate Policy and this CPS, the RXC-R2 CA issues the requested certificate and returns a positive notification to the CA administrator of issuance. The CA administrator is then responsible for notifying the subscriber entity manually and delivering the certificate only to the subscriber entity using a secure transport method such as encrypted storage media or an encrypted network transmission.

4.4. Certificate Acceptance

4.4.1. Conduct Constituting Certificate Acceptance

Following the issuance of a subordinated CA certificate, the administrative team of the RXC-R2 CA record the issuance event on the CA Description Form maintained for the subscriber, which record positively indicates acceptance of the issued certificate. Following the issuance of an OCSP response signing certificate, the CA administrator will install the certificate on the OCSP signing system, indicating 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

Subscribers, who are all Issuing CAs and OCSP response signing systems, maintain their private keys and any backup copies of those keys in a Hardware Security Module (HSM) that holds a FIPS 140-2 Level 3 certification. The administrative team of the RXC-R2 CA ensure the subscriber entity meets this standard prior to the issuance of a certificate.

4.5.2. Relying Party Public Key and Certificate Usage

The RXC-R2 CA issues certificates to CAs that are subordinated to it and whose Certification Practice Statements (CPSs) have been reviewed and validated as conforming to the Cisco RXC Certificate Policy and to the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, published at www.cabforum.org. The issuance of a certificate for a subscriber CA from the RXC-R2 CA attests that:

- The subscriber entity is fully owned and operated by Cisco Systems Information Security group;
- The subscriber CA's CPS (as applicable) has been validated to conform to the Cisco RXC Certificate Policy and to the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates;
- The security of the subscriber entity meets Cisco corporate policies and standards for the operation of a certificate authority or OCSP response signing system in addition to the above-named standards; and
- The identity of the subscriber entity has been validated and may be relied on as associated with the public key contained in the certificate issued.

Relying parties should use the means listed in section 2 to verify the public key of the CA and the validity of issued certificates.

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. The RXC-R2 CA supports renewal, but treats all 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 are performed by the RXC-R2 CA by treating all renewal requests as if they were first-time certificate application requests.

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. The RXC-R2 CA does not support certificate re-key operations.

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. The RXC-R2 CA does not support certificate modification operations.

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 RXC-R2 CA revokes a certificate:

- Upon request of the administrative team of the RXC-R2 CA;
- If knowledge or reasonable suspicion of compromise is obtained;
- If the administrative team of the RXC-R2 CA determines that the certificate was not properly issued in accordance with the Cisco RXC Certificate Policy, the Baseline Requirements for the Issuance and Management of Publicly- Trusted Certificates, or this CPS.

In the event that the RXC-R2 CA ceases operations, all certificates issued by the RXC-R2 CA will be revoked prior to the date that the CA ceases operations. The RXC-R2 CA will provide subscribers adequate notice wherever possible to provide them the opportunity to address any business impacting issues.

4.9.1.1. Permissive Revocation

The administrative team of the RXC-R2 CA may initiate revocation of issued certificates at any time for any reason, and may also revoke a certificate upon failure of the subordinated CA 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.

4.9.1.2. Required Revocation

The administrative team of the RXC-R2 CA shall promptly initiate 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.

4.9.2. Who Can Request Revocation

Only the administrative team of the RXC-R2 CA are permitted to request revocation of a certificate issued by the RXC-R2 CA. 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 in section 1.5.2.

4.9.3. Identification and Authentication for Revocation Request

Requests for revocation shall be reviewed and manually authenticated and approved by at least two members of the administrative team of the RXC-R2 CA operating in a Trusted Role per section 5.2.1, to ensure they originate from a member of the administrative team and are valid.

4.9.4. Procedure for Revocation Request

All certificate revocation requests must be manually communicated to the RXC-R2 CA using physical media. Revocation requests should be electronically signed by the private key associated with the certificate to be revoked, but may be manually revoked by members of the administrative team acting in a Trusted Role per section 5.2.1.

Once revoked, the certificate serial number, the date and time of the revocation, and the revocation reason code (where applicable) are added to the certificate status verification systems defined in section 2 (e.g. CRL, OCSP). The certificate status verification system and OCSP database are then updated to current status within twenty-four hours of the completion of revocation. All revocation requests and the resulting actions taken by the CA shall be archived as CA security events in accordance with the guidelines defined in section 5.4.

4.9.5. Revocation Request Grace Period

In the event that business constraints restrict the immediate revocation of a subscriber CA, the administrative team of the RXC-R2 CA may, at its discretion, provide a grace period of up to twenty-four hours prior to revocation. This grace period may not be extended, must be openly declared and documented when granted, and may only be granted when the impact created by immediate revocation is determined by the Cisco Systems Information Security Policy Management Authority to significantly exceed the impact of delaying revocation.

4.9.6. Revocation Request Processing Requirement

No further stipulation.

4.9.7. 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. The RXC-R2 CA uses a combination of policy and technical constraints to ensure that all relevant information useful for this validity verification process is included in every certificate issued. This information includes, but is not limited to, the URLs to policies and to certificate validity status services as defined in section 2.

4.9.8. Certificate Revocation List Issuance Frequency

The RXC-R2 CA meets the requirements around revocation issuance defined in the CAB Forum Base Requirements for Publicly Trusted Certificates, as appropriate. CRLs created by the RXC-R2 CA are issued at least annually whether any new information has been published or not. Upon a new revocation, a new CRL will be issued and published within twenty-four hours of the completion of the revocation process. The management team of the RXC-R2 CA ensures that superseded CRLs are removed from the CRL Distribution Point location upon posting of the latest CRL.

4.9.9. Online Certificate Status Protocol Update Frequency

In addition to providing CRLs, the RXC-R2 CA contributes revocation information to a centralized Online Certificate Status Protocol (OCSP) service run by Cisco, as described in section 2. The OCSP service meets the requirements established by the CAB Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates. Information in the OCSP service is updated every four days, and revocation data are supplied to the OCSP service within twenty-four hours of the relevant revocation event.

4.9.10. Maximum Latency for CRLs and Online Status Checking Mechanisms

The RXC-R2 CA uses software monitoring systems to 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.

4.9.11. Notification with Regards to Possible Key Compromise

No further stipulation.

4.9.12. Circumstances for Certificate Suspension

The RXC-R2 CA does not support Certificate Suspension.

4.9.13. Who Can Request Suspension

Not applicable

4.9.14. Procedure for Certificate Suspension

Not applicable

4.9.15. Limits on Suspension Period

Not applicable

4.10. Certificate Status Services

See section 2.

4.11. Removal of Certificates from Revocation Status Services

No further stipulation.

4.12. End of Subscription

No stipulation.

4.13. Key Escrow and Recovery

See section 6.1.2.

Chapter 5. Facility, Management, and Operational Controls

5.1. Physical Controls

5.1.1. Site Location and Construction

The RXC-R2 CA infrastructure, including all hosts and cryptographic devices directly involved in the CA, are 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 RXC-R2 CA infrastructure restricts access to the CA to only the members of the RXC-R2 CA's administrative team that serve in a Trusted Role, per section 5.2.1. The RXC-R2 CA's administrative team are responsible for identifying the members who shall have physical access, and for reviewing that list at least annually to ensure it remains up to date. Physical access to the CA infrastructure requires at least two separate authentication factors (e.g. a badge and a biometric identification such as fingerprint) that strongly authenticate and authorize members of the RXC-R2 CA administrative team. All physical access to the RXC-R2 CA infrastructure is logged and recorded using video and electronic records.

5.1.3. Power and Air Conditioning

The RXC-R2 CA physical infrastructure is supplied with power and air conditioning commensurate with its operating requirements. The RXC-R2 CA administrative team ensure that such power and air conditioning supplies are sufficiently redundant to ensure the continued operation of the 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 RXC-R2 CA's infrastructure is supplied with sufficient protections to guard against water exposure as much as reasonably possible, including 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 RXC-R2 CA's infrastructure is outfitted with fire detection mechanisms sufficient to reasonable business practices, along with such fire suppression systems as are deemed reasonable and safe. Since the data center facility uses a water-based fire suppression system, appropriate detection and correction mechanisms have been established to safeguard against leaks. The fire detection mechanisms are tested at least annually; all detection and suppression mechanisms are maintained according to the manufacturer's recommendations.

5.1.6. Media Storage

The administrative team of the RXC-R2 CA stores 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 are 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 RXC-R2 CA are shredded securely once no longer required for operation. Sensitive equipment or media that are no longer needed for operation are 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 RXC-R2 CA to full functionality are created and stored in a separate physical location (Cisco's Mountain View and San Jose campuses) away from the primary operating location of the RXC-R2 CA.

5.2. Procedural Controls

5.2.1. Trusted Roles

All employees, contractors, and consultants of the RXC-R2 CA (collectively "personnel" or "the administrative team") 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, are 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 are shared by multiple roles and individuals. Each account on the CA server is established with limited capabilities commensurate with the role of the account holder.

The RXC-R2 CA uses multi-user controls around key materials and physical access systems, as well as policies and procedures, to ensure that no single individual may gain access to End Entity Private Keys associated with the RXC-R2 CA. Multi-user control is required through technical and procedural controls for CA Key generation, revocation updates, and certificate issuance, as outlined in Section 6.2.2. All other duties associated with CA roles may be performed by an individual operating alone. The RXC-R2 CA uses a strict employee verification process as well as technical and procedural controls and periodic reviews of activities to provide oversight of all activities performed by privileged CA role holders.

5.2.3. Identification and Authentication for Each Role

All RXC-R2 CA personnel have their identity and authorization verified before they are: (i) included in the access list for the RXC-R2 CA site; (ii) included in the access list for physical access to the system; (iii) given a Certificate or access token for the performance of their CA role; or (iv) given an account on the PKI system. The use of each of these access tokens and/or accounts (with the exception of CA certificates) is (i) directly attributable to an individual; and (ii) is restricted to actions authorized for that role through the use of CA software, operating system and procedural controls. CA operations are never accessed across a network.

5.2.4. Roles Requiring Separation of Duties

To best ensure the integrity of the RXC-R2 CA equipment and operation, a separate individual is identified for each Trusted Role when performing CA operations such as key generation, revocation updates, or certificate issuance. Under no circumstances does the incumbent of a CA role perform his or her own auditor function.

5.3. Personnel Controls

5.3.1. Background and Qualifications

Cisco Systems and the Cisco Systems Information Security group utilizes personnel and management policies and practices sufficient to provide reasonable assurance of the trustworthiness and competence of their employees and of the satisfactory performance of their duties. These policies and practices are defined by the corporate policies and practices of Cisco Systems, as well as by specific internal practice documents maintained by the Cisco Systems Information Security group that specify requirements for the operation of the CA.

5.3.2. Background Investigation

Cisco Systems conducts a thorough investigation of all personnel who serve in trusted roles (prior to their employment and periodically thereafter as necessary) to verify their trustworthiness and competence. All personnel who fail an initial or periodic investigation do not serve or continue to serve in a trusted role.

5.3.3. Training Requirements

All CA, RA, and VSP personnel receive thorough and documented training in order to perform their duties, and receive additional training and update briefings thereafter as necessary to remain current in their knowledge of CA operations and of PKI and security domains in general.

5.3.4. Documentation Supplied to Personnel

All CA personnel are provided with comprehensive electronic user manuals detailing the procedures for certificate creation, update, renewal, suspension, and revocation, and the details of software functionality.

5.4. Audit Logging Procedures

The RXC-R2 CA generates 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 are automatically created and monitored; where this is not possible, a paper logbook or other physical mechanism is used. At a minimum, each log entry (whether electronic or physical) includes 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

The RXC-R2 CA records and archives the following types of security event data:

- 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 subscribing parties.

5.4.2. Frequency of Processing Log

Where possible, security event logs are created at the time of the event. Where this is not possible, the logs are created and then verified by at least two members of the RXC-R2 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 will be retained for a period of seven years past the dissolution of the CA and are made available during compliance audits.

5.4.4. Protection of Audit Log

Electronic security audit logs are protected from tampering using periodic manual replication to a protected archive. Physical security audit logs are created using tamper-resistant methods and are routinely inspected and reconciled to detect tampering and anomalous behavior.

5.4.5. Audit Log Backup Procedures

The RXC-R2 CA's infrastructure systems make regular backups of electronic security audit logs.

5.4.6. Vulnerability Assessments

The RXC-R2 CA administrative team conducts vulnerability assessments of the RXC-R2 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. Since the RXC-R2 CA infrastructure is maintained fully offline (not connected to any outside network), these assessments are conducted annually.

5.5. Records Archival

Cisco maintains all documentation pertaining to the operation of the RXC-R2 CA that is required to support audits under the WebTrust for CA guidelines and CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates. This includes but is not limited to the following:

- Certificate signing requests;
- Certificate signing request information validation checks and results;
- Any additional information collected in support of a certificate signing request;
- Audit logs from CA systems as specified in section 5.4;
- Software and system backups from CA systems.

This information is subject to the retention requirements laid out in the RXC Certificate Policy, section 5.5. Cisco does not ordinarily make this data available to outside parties except as required by applicable law or to auditors as part of a requested audit of the RXC-R2 CA. Those wishing copies of this data may submit a request to the contacts specified in section 1.5 and the request will be reviewed by the Cisco Policy Management Authority.

5.6. Business Continuity and Disaster Recovery

5.6.1. Incident and Compromise Handling Procedures

The Cisco Systems Information Security group has in place a disaster recovery/business resumption plan, and has set up and made operational a facility located in an area that is geographically remote from the primary operational site, capable of providing CA Services within seventy-two (72) hours of an unanticipated emergency. The plan includes a complete and periodic test of readiness for the facility. A copy of the disaster recovery/business continuity plans and reviews are made available to auditors and to qualified Relying Parties upon request.

5.6.2. Business Continuity Requirements

The Cisco Systems Information Security group ensures that 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 Cisco Systems Information Security group has defined a 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. The plan includes procedures for revoking all affected certificates and promptly notifying all subscribers and all Qualified Relying Parties. The key compromise plan is maintained as part of the disaster recovery plans established by the Cisco Systems Information Security group and is available upon request to auditors or to qualified Relying Parties.

5.7. CA Termination

No further stipulation.

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 RXC-R2 CA and for any subscriber CAs are generated in such a way that the private key is not known by anyone other than the authorized user of the key pair, by hardware tokens that hold the FIPS 140-2 Level 3 certification to generate and store the private key material, configured to prevent extraction of the key material in an unencrypted form.

6.1.1.1. CA and RA Key Pair Generation

All RXC-R2 CA private keys are generated and stored hardware tokens that hold the FIPS 140-2 Level 3 certification. The generation of the RXC-R2 CA key pair took place using a pre-established key generation script performed by at least two CA operators (a minimum of one performing, one witnessing) acting in a Trusted Role per section 5.2.1. All subscriber CA keys associated with certificates issued by the RXC-R2 CA must have been generated using a key generation process that meets the same controls as the RXC-R2 CA key generation ceremony. The RXC-R2 CA key generation ceremony was videotaped/recorded as it was performed. A copy of the video recording and the signed script for the key generation ceremony is retained as part of the standard records for the RXC-R2 CA, per section 5.4.1.

6.1.2. Private Key Delivery to Subscriber

Not applicable. The RXC-R2 CA does not generate private keys on behalf of subscribers, nor does it store private keys not directly associated with RXC-R2 CA.

6.1.3. Public Key Delivery to Certificate Issuer

A subscribing CA's public key is transferred to the RA or CA using physical media that remains under the control of at least two CA operators (a minimum of one performing, one witnessing) acting in a Trusted Role per section 5.2.1, from the time of subscriber generation (as witnessed or performed by the same CA operators) to the time of certificate issuance by the CA (as witnessed or performed by the same CA operators).

6.1.4. CA Public Key Delivery to Relying Parties

The public key of the CA signing key pair is delivered to subscribers in an on-line transaction in accordance with IETF PKIX Part 3, using the certificate repositories defined in section 2.

6.1.5. Key Sizes

The RXC-R2 CA keys use the RSA encryption algorithm at a 2048-bit key length. Hashing of information is performed using the Secure Hash Algorithm 2 (SHA-2) with a 256-bit hash length (SHA-256).

6.1.6. Public Key Parameters Generation and Quality Checking

Public key parameters are generated and checked in accordance with the standard that defines the cryptographic algorithm in which the parameters are to be used. The administrative team of the RXC-R2 CA shall review manually the keys generated by subscriber CAs to ensure they do not meet the definition of weak keys or encryption parameters.

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

The RXC-R2 CA automatically sets 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.

The RXC-R2 CA only issues certificates to properly authenticated subordinated certificate authorities and OCSP responders.

6.2. Private Key Protection and Cryptographic Module Engineering Controls

The RXC-R2 CA protects its private key(s) using a hardware-based cryptographic device holding a FIPS 140-2 Level 3 certification, in accordance with the provisions of the RXC CP. All subscribing CAs subordinated to the RXC-R2 CA protect their keys similarly.

6.2.1. Cryptographic Module Standards and Controls

The signing key generation, storage and signing operations for the RXC-R2 CA are performed using a hardware-based cryptographic module that holds a FIPS 140-2 Level 3 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 RXC-R2 CA Private Signing Key requires 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. RXC-R2 CA Private Signing Keys are 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 are never be revealed to the RXC-R2 CA and are therefore never escrowed.

6.2.4. Private Key Backup, Archival, and Restoration

The private keys for the RXC-R2 CA are backed up, archived and restored using either a NIST-approved key wrapping algorithm or the method provided by the HSM vendor.

6.2.5. Private Key Transfer into or from a Cryptographic Module

Private keys for RXC-R2 CA were generated inside a cryptographic module holding a FIPS-140-2 Level 3 certification. Should there be a need to migrate keys from one module to another (such as for backup or hardware replacement), the keys are 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

All RXC-R2 CA private keys are always stored on a cryptographic module holding a FIPS 140-2 Level 3 certification.

6.2.7. Method of Activating a Private Key

When being readied for use, RXC-R2 CA Private Key material is 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, RXC-R2 CA Private Key material is 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 are 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 the RXC-R2 CA hold a FIPS 140-2 certification at Level 3.

6.3. Other Aspects of Key Pair Management

6.3.1. Public Key Archival

The public keys of the RXC-R2 CA are archived in the regular backups of the Repository where the digital certificates are published (defined in section 2).

6.3.2. Certificate Operational Periods and Key Pair Usage Periods

The standard validity period for subordinate CA certificates issued by the RXC-R2 CA is twenty years.

6.4. Activation Data

Information used to wrap or activate RXC-R2 CA key pairs uses, at a minimum, symmetric encryption equal to or greater than AES-256 and asymmetric encryption equal to or greater than RSA-2048. Information transmitted between the CA and its associated Hardware Security Module meets or exceeds this standard of protection.

The RXC-R2 CA stores activation materials separate from the CA physical hardware when the activation materials are not actively in use, using a physical safe kept under guard at all times with access that requires two administrators with separate access codes to open.

6.5. Computer Security Controls

The RXC-R2 CA has instituted documented security hardening procedures based on a combination of vendor recommendations and industry best practices, to improve the security of the operating environment on the RXC-R2 CA system. The RXC-R2 infrastructure is maintained in a fully offline secure environment with no outside connectivity. Access to the CA by administrators requires Multi-Factor Authentication from each administrator and multiple administrators acting in concert.

6.6. Life-Cycle Technical Controls

6.6.1. System Development Controls

The RXC-R2 CA administrative team has instantiated documented software testing and change control procedures for the implementation of software on operational CA systems. The controls specify procedures for software testing and release to production and for modifications to code, and include provisions for emergency software fixes.

6.6.2. Security Management Controls

The RXC-R2 CA has physical and logical security measures in place to ensure that software elements considered in production are protected from unauthorized modification, and periodically verified to ensure their integrity. Such measures include the manual verification of code prior to use, as well as physical protections and a lack of outside connectivity that

prevent unauthorized modification.

6.6.3. Life-Cycle Security Controls

The RXC-R2 CA maintains documented procedures for the lifecycle management of hardware and software components of the CA.

6.7. Network Security Controls

Not applicable. The RXC-R2 CA does not communicate with any outside network entity, existing on a closed network that consists only of the RXC-R2 CA and its associated Hardware Security Module (HSM).

6.8. Time-stamping

All RXC-R2 CA components are manually synchronized with a Network Time Protocol (NTP) server. Time derived from this service is 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.

6.8.1. Time and Issuance Dates

The RXC-R2 CA software does not automatically adjust notBefore time-stamps for any reason.

Chapter 7. Certificate, CRL, and OCSP Profiles

7.1. Certificate Profiles

The RXC-R2 CA has established a standard certificate profile for each certificate issued; a copy of the profile used is maintained in a separate document that is available upon request to the parties identified in section 1.5. All certificate profiles have been verified to conform to version 3 of the X.509 standard and to RFC 5280.

7.1.1. Version Number

Certificates issued by the RXC-R2 CA are created in compliance with version 3 of the X.509 standard, and contain a version number indicating this compliance.

7.1.2. Certificate Extensions

The RXC-R2 CA issues certificates in compliance with version 3 of the X.509 standard and with RFC 5280. A combination of policies and software controls are used to ensure that issued certificates meet these strictures, including the use and formatting of any certificate extensions included with issued certificates.

7.1.3. Certificate Signature Algorithms

Certificates issued by RXC-R2 CA contain signature algorithm identifiers containing the OID corresponding to the cryptographic algorithms in use. The OIDs currently in use are:

- sha256WithRSAEncryption (OID [1.2.840.113549.1.1.11](#)).

7.1.4. Name Forms

All certificates issued from the RXC-R2 CA contain Name Forms that conform to RFC 5280, and a Serial Number field guaranteed to be unique that contains at least 64 bits of entropy drawn from a cryptographically secure pseudo-random number generator (CSPRNG). Within issued certificates, the Issuer Distinguished Name field is automatically set by the CA at issuance to "CN=Cisco RXC-R2, O=Cisco, C=US".

7.1.5. Subject Information

Subject attributes will not contain blank metadata such as '.', '-', and ' ' (i.e. space) characters.

7.1.6. Certificate Policy OID

Certificates issued from the RXC-R2 CA contain a Certificate Policy OID field set to conform to the OIDs documented in section 1.2.

7.1.7. Validity Period

Certificates issued from the RXC-R2 CA are set to a validity period not to exceed twenty years from the date of issuance.

7.2. Certificate Revocation List (CRL) Profiles

Certificate Revocation Lists (CRLs) issued by the RXC-R2 CA are issued in the X.509 version 2 format. The RXC-R2 CA has established a standard CRL profile; a copy of the profile used is maintained in a separate document that is available upon request to the parties identified in section 1.5.

7.3. Online Certificate Status Profile (OCSP) Profiles

The RXC-R2 CA contributes information to Cisco's Online Certificate Status Profile (OCSP) responder, as detailed in section 2. OCSP services are configured to conform to RFC 6960; the URL for Cisco's OCSP service is included in issued certificates via the Authority Information Access (AIA) extension. The RXC-R2 CA has established a standard OCSP response profile; a copy of the profile used is maintained in a separate document that is available upon request to the parties identified in section 1.5.

Chapter 8. Compliance Audit and Other Assessments

The administrative team of the RXC-R2 CA is responsible for ensuring that: (i) the CA only accepts information from entities that understand and are obligated to comply with this Policy; (ii) the CA complies with the provisions of this Policy in its certification and Repository services, issuance and revocation of Certificates and issuance of CRLs; (iii) the CA personnel make reasonable efforts to ensure adherence to this Policy with regard to any Certificates issued under it; and (iv) that any identification and authentication procedures are implemented as set forth in the relevant CP and CPS documents.

8.1. Assessment of Compliance

The Cisco Systems Information Security group maintains and certifies compliance with relevant CP and standards documents by means of a review from an independent auditor on at least an annual basis. The audit covers the RXC-R2 CA's infrastructure, policies, and practices in line with its published CPS document, and is recursive through the hierarchy of Subordinate CAs chained from the RXC-R2 CA.

8.2. Qualifications of Auditor

Reviews and certifications of compliance under this document are performed by a Qualified Auditor. A person or organization is 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

The RXC-R2 CA administrative team selects a Qualified Auditor who is completely independent of the CA by using auditors whose companies are not owned, operated by, subordinated to, or otherwise obligated to Cisco Systems and its subsidiary corporate holdings.

8.4. Content of Audit

The Cisco Systems Information Security group ensures and certifies that they meet 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. An attestation to this effect is presented as part of the routine compliance audit, and signed by the Director responsible for the operation of the Certificate Authority.

8.5. Actions Taken as a Result of Deficiency

Should a compliance review identify material discrepancies between the RXC-R2 CA's controls and the qualifying audit guidelines, the RXC-R2 CA administrative team shall collectively be responsible for creating a suitable corrective action plan to eliminate the deficiency.

8.6. Communication of Audit Results

No further stipulation.

Chapter 9. Other Business and Legal Matters

9.1. Fees

No stipulation.

9.2. Financial Responsibility

The financial responsibility of managing and maintaining the RXC-R2 CA is the sole responsibility of Cisco Systems, Inc.

9.3. Confidentiality of Business Information

The administrative team of the RXC-R2 CA 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

The RXC-R2 CA does not collect information for certificates that is considered Personally Identifiable Information (PII) for any natural person or organization.

9.5. Intellectual Property Rights

Intellectual property rights for the information collected and processed as part of the certificate issuance process are assigned to Cisco Systems, unless specifically and legally assigned otherwise beforehand.

9.6. Representations and Warranties

9.6.1. Certificate Authority (CA) Obligations

The management team of the RXC-R2 CA 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

Certificate status (valid, suspended, or revoked) for certificates issued by the RXC-R2 CA may be determined according to the methods and repositories defined in section 2 of this document.

9.6.3. Subscriber Obligations

In all cases, subscribing CAs are 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;
- 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 RXC-R2 CA.

9.6.4. Benefiting Party Obligations

No further stipulations.

9.6.5. Registration Authority (RA) Obligations

Not applicable. The RXC-R2 CA does not employ Registration Authorities of any kind.

9.6.6. CA Representations

By issuing a certificate that references this Policy, the RXC-R2 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 RXC-R2 CA has issued and managed the Certificate in accordance with this Policy;
- The RXC-R2 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 RXC-R2 CA, and the RXC-R2 CA has taken steps as required under this Policy to verify the information contained in the Certificate;
- The RXC-R2 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 RXC-R2 CA concerning the current validity of the Certificate is accurate and that validity has not been diminished by the RXC-R2 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 RXC-R2 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 RXC-R2 CA will ensure that any Certificate Agreements incorporate by reference the provisions of this Policy regarding the RXC-R2 CA's and the Certificate Holder's rights and obligations. In the alternative, the RXC-R2 CA may ensure that any Certificate Agreements, by their terms, provide the respective rights and obligations of the RXC-R2 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 RXC-R2 CA and any limitations on warranties or liability of the RXC-R2 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 RXC-R2 CA will ensure that any Benefiting Party Agreement incorporate by reference the provisions of this Policy regarding the RXC-R2 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 RXC-R2 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 RXC-R2 CA assumes limited liability only to Benefiting Parties who have entered into a Benefiting Party Agreement. The RXC-R2 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 RXC-R2 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 RXC-R2 CA is limited to these conditions and to conditions set forth in the terms of specific Benefiting Party Agreements.

Except as expressly provided in the Cisco RXC Certificate Policy and in this document, the RXC-R2 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 RXC-R2 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 RXC-R2 CA shall have no liability for consequential damages. Under no circumstances will the RXC-R2 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 stipulations except as otherwise specified in section 9.

9.10. Term and Termination

No further stipulation except as otherwise specified in section 9.

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.

Cross Certificate

A certificate that establishes trust between two certificate authorities.

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.

Multi-Factor Authentication

An authentication mechanism consisting of two or more of the following independent categories of credentials (i.e. factors) to verify the user's identity for a login or other transaction: something you know (knowledge factor), something you have (possession factor), and something you are (inherence factor). Each factor must be independent. Certificate-based authentication can be used as part of Multifactor Authentication only if the private key is stored in a Secure Key Storage Device.

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.

Secure Key Storage

A device certified as meeting at least FIPS 140-2 level 2 overall, level 3 physical, or Common Criteria (EAL 4+).

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