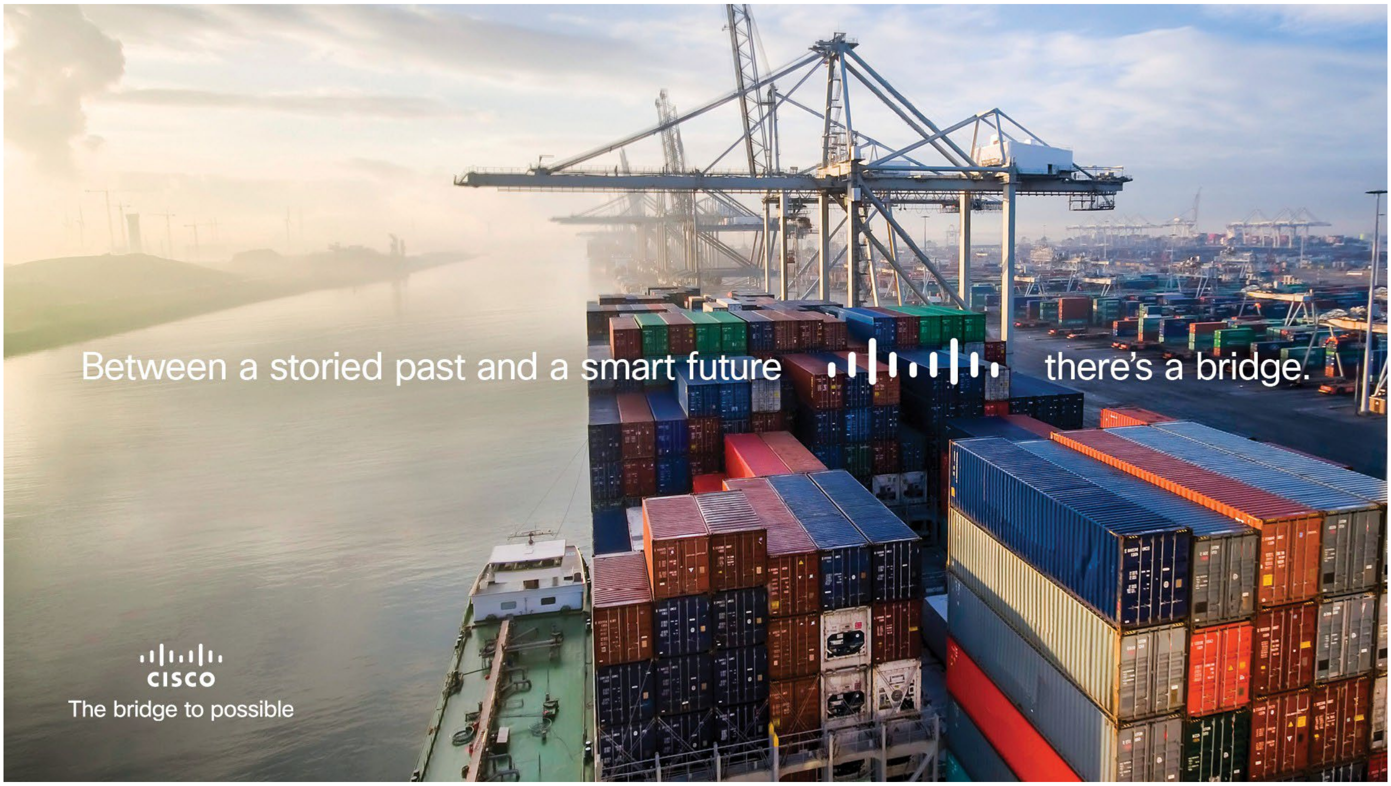

Cisco's Internal Root CA Certificate Policy

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

Version 1.0, July-10-2024

Table of Contents

1. Introduction 4
1.1. Overview 4
1.2. Document name and identification 4
1.3. PKI participants 4
1.4. Certificate usage 5
1.5. Policy administration 5
1.6. Definitions and acronyms 6
2. PUBLICATION AND REPOSITORY RESPONSIBILITIES 6
2.1. Repositories 6
2.2. Publication of certification information 6
2.3. Time or frequency of publication 6
2.4. Access controls on repositories 7
3. IDENTIFICATION AND AUTHENTICATION 7
3.1. Naming 7
3.2. Initial identity validation 7
3.3 Identification and authentication for re-key requests 8
3.4 Identification and authentication for revocation request 8
4. CERTIFICATE LIFE-CYCLE OPERATIONAL RE- QUIREMENTS 8
4.1 Certificate Application 8
4.2. Certificate application processing 8
4.3. Certificate issuance 9
4.4. Certificate acceptance 9
4.5. Key Pair and certificate usage 9
4.6. Certificate renewal 9
4.7. Certificate re-key 10
4.8. Certificate modification 11
4.9. Certificate revocation and suspension 11
4.10 Certificate status services 14
4.11 End of subscription 15
4.12 Key escrow and recovery 15
5. MANAGEMENT, OPERATIONAL AND PHYSICAL CONTROLS 15
5.1 Physical controls 16
5.2 Procedural controls 17
5.3 Personnel controls 17
5.4. Audit logging procedures 18
5.4.9 Records archival 19
5.7. Compromise and disaster recovery 19
5.8 CA or RA termination 20
6. TECHNICAL SECURITY CONTROLS 21
6.1 Key Pair generation and installation 21
6.2 Private Key Protection and Cryptographic Module Engineering Controls 22

6.3 Other aspects of Key Pair management 23
6.4 Activation data 23
6.5 Computer security controls 24
6.6 Life cycle technical controls 24
6.7 Network security controls 25
6.8 Time-stamping 25
7. CERTIFICATE, CRL, AND OCSP PROFILES 25
7.1 CERTIFICATE PROFILE 25
Table 7.1: OIDs for Signature Algorithms 26
7.2 CRL profile 27
7.3 OCSP profile 28
8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS 28
8.1 Frequency or circumstances of assessment 29
8.2 Identity/qualifications of assessor 29
8.3 Assessor’s relationship to assessed entity 29
8.4 Topics covered by assessment 29
8.5 Actions taken as a result of deficiency 29
8.6 Communication of results 29
8.7 Self-Audits 30
9. OTHER BUSINESS AND LEGAL MATTERS 30
9.1 Fees 30
9.2 Financial responsibility 30
9.3 Confidentiality of business information 30
9.4 Privacy of personal information 31
9.5 Intellectual property rights 31
9.6 Representations and warranties 31
9.7 Disclaimers of warranties 32
9.8 Limitations of liability 32
9.9 Indemnities 32
9.10 Term and termination 32
9.11 Individual notices and communications with participants 32
9.12 Amendments 32
9.13 Dispute resolution provisions 33
9.14 Governing law 33
9.15 Compliance with applicable law 33
9.16 Miscellaneous provisions 33
9.17 Other provisions 33
Appendix A: Terminology and Definitions 34
Appendix B: Document History 37

1. Introduction

1.1. Overview

The Cisco Public Key Infrastructure ("Cisco PKI"), has been established by Cisco Systems Cryptographic Services ("Cisco"), to enable reliable and secure identity authentication, and to facilitate the preservation of confidentiality and integrity of data in electronic transactions.

This certificate policy (CP) is the principal statement of policy governing the CAs within the Cisco PKI. It sets forth the business, legal, and technical requirements for approving, issuing, managing, using, revoking, and renewing, Cisco Certificates and providing associated trust services for all Participants. These requirements protect the security and integrity of the Cisco PKI and comprise a single set of rules that apply consistently to all CAs therein, so as to provide assurance of uniform trust throughout it.

1.2. Document name and identification

Cisco utilizes many Object Identifiers (OIDs) for its issuance policies. Please reach out to ciscopki-public@external.cisco.com for a current list of OIDS.

All CAs in this document will follow the following: 1.3.6.1.4.1.9.21.1 Cisco PKI Policies Arc

This CP applies to all CAs that issue certificates asserting a Cisco Cryptographic Services OID. By including a Cisco Cryptographic Services OID, the CA asserts that the certificate was issued and is managed in accordance with this CP and the relevant CPS.

1.3. PKI participants

1.3.1. Certification authorities

Cisco Cryptographic Services maintains the Certification Authorities (CA) authorized to issue public key certificates within the Cisco PKI.

This Certificate Policy document is applicable to all "Root CAs" listed under "Certificates" at https://www.cisco.com/security/pki/ with the exception of Root CAs that already have dedicated Certificate Policy documents found at https://www.cisco.com/security/pki/policies/.

1.3.2. Registration Authorities

The operators of the Cisco PKI shall be responsible for performing all identification and authentication functions and all certificate manufacturing and issuing functions. The Cisco Public Key Infrastructure may NOT delegate performance of these obligations to a registration authority (RA). The CA must remain primarily responsible for the performance of all CA services in a manner consistent with the requirements of this Policy. The ability to delegate or subcontract these obligations is not permitted.

1.3.3. Subscribers

No stipulation.

1.3.4. Relying parties

A Relying Party is any individual or entity that acts in reliance on a Cisco Certificate to verify a digital signature and/or decrypt an encrypted document or message.

1.3.5. Other participants

Not applicable.

1.4. Certificate usage

1.4.1. Appropriate certificate uses

The primary goal of this Policy is to enable efficient and secure electronic communication, while addressing Relying Parties' concerns about the trustworthiness of Certificates.

1.4.2. Prohibited certificate uses

No stipulation.

1.5. Policy administration

1.5.1. Organization administering the document

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, California 95134

1.5.2. Contact person

Cryptographic Services

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, California 95134

ciscopki-public@external.cisco.com

To notify Cisco of a CA service outage or a security issue including a suspected Private Key compromise, Certificate misuse, or other types of fraud, compromise, misuse, inappropriate conduct, or any other matter related to Certificates, please contact us using the e-mail address ciscopki-public@external.cisco.com

1.5.3. Person determining CPS suitability for the policy

Cisco Cryptographic Services determines the suitability of CPSs published in response to this CP.

1.5.4. CP approval procedures

Approvals of this CP and any amendments thereof are made by Cisco Cryptographic Services. Amendments SHALL be made by publishing a new version of this CP at https://www.cisco.com/security/pki/policies/

This CP and associated documents are available from the Repository at https://www.cisco.com/security/pki/policies/

1.6. Definitions and acronyms

See Appendix A.

1.6.4. Conventions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in these Requirements SHALL be interpreted in accordance with RFC 2119.

By convention, this document omits time and timezones when listing effective requirements such as dates. Except when explicitly specified, the associated time with a date shall be 00:00:00 UTC.

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

The CA SHALL develop, implement, enforce, and update a Certification Practice Statement as needed.

2.1. Repositories

The CA SHALL make revocation information for Subordinate Certificates and Subscriber Certificates available in accordance with this Policy.

2.2. Publication of certification information

The CA SHALL publicly disclose its Certificate Policy and/or Certification Practice Statement through an appropriate and readily accessible online means that is available on a 24x7 basis. The CA SHALL publicly disclose its CA business practices to the extent required by the CA's selected audit scheme (see Section 8.4).

Section 4.2 of a CA's Certificate Policy and/or Certification Practice Statement SHALL state the CA's policy or practice on processing CAA Records for Fully-Qualified Domain Names; that policy shall be consistent with this CP. It shall clearly specify the set of Issuer Domain Names that the CA recognizes in CAA "issue" or "issuewild" records as permitting it to issue.

2.3. Time or frequency of publication

Cisco Cryptographic Services SHALL develop, implement, enforce, and update a Certificate Policy and/or Certification Practice Statement that describes in detail how the CA implements the latest version of these Requirements. The CA SHALL indicate conformance with this requirement by incrementing the version number and adding a dated changelog entry.

2.4. Access controls on repositories

The CA shall make its Repository publicly available in a read-only manner.

3. IDENTIFICATION AND AUTHENTICATION

3.1. Naming

3.1.1. Types of names

No stipulation.

3.1.2. Need for names to be meaningful

No stipulation.

3.1.3. Anonymity or pseudonymity of Subscribers

No stipulation.

3.1.4. Rules for interpreting various name forms

No stipulation.

3.1.5. Uniqueness of names

No stipulation.

3.1.6. Recognition, authentication, and role of trademarks

No stipulation.

3.2. Initial identity validation

3.2.1. Method to prove possession of private key

No stipulation.

3.2.2. Authentication of organization identity

No stipulation.

3.2.3 Authentication of individual identity

No stipulation.

3.2.4. Non-verified Subscriber information

No stipulation.

3.2.5. Validation of authority

Requests must come internally via an MFA authenticated mechanism.

3.2.6 Criteria for interoperation

No stipulation.

3.3 Identification and authentication for re-key requests

3.3.1 Identification and authentication for routine re-key

No stipulation.

3.3.2 Identification and authentication for re-key after revocation

No stipulation.

3.4 Identification and authentication for revocation request

No stipulation.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate Application

4.1.1 Who can submit a certificate application

In accordance with Section 5.5.2, the CA SHALL maintain an internal database of all previously revoked Certificates and previously rejected certificate requests due to suspected phishing or other fraudulent usage or concerns.

4.1.2 Enrollment process and responsibilities

Prior to the issuance of a Certificate, the CA SHALL obtain the following documentation from the Applicant:

A certificate request, which may be electronic

The CA SHOULD obtain any additional documentation the CA determines necessary to meet these Requirements.

Prior to the issuance of a Certificate, the CA SHALL obtain from the Applicant a certificate request in a form prescribed by the CA and that complies with these Requirements.

4.2. Certificate application processing

4.2.1. Performing identification and authentication functions

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

Section 6.3.2 limits the validity period of Subscriber Certificates.

The CA SHALL develop, maintain, and implement documented procedures that identify and require additional verification activity for High Risk Certificate Requests prior to the Certificate's approval, as reasonably necessary to ensure that such requests are properly verified under these Requirements.

4.2.2. Approval or rejection of certificate applications

Certificate applications are reviewed by Cryptographic Service's Policy Management Authority.

4.2.3. Time to process certificate applications

No stipulation.

4.3. Certificate issuance

4.3.1. CA actions during certificate issuance

Certificate issuance by the Root CA SHALL require an individual authorized by the CA (i.e. the CA system operator, system officer, or PKI administrator) to deliberately issue a direct command in order for the Root CA to perform a certificate signing operation.

4.3.2. Notification to Subscriber by the CA of issuance of certificate

No stipulation.

4.4. Certificate acceptance

4.4.1. Conduct constituting certificate acceptance

No stipulation.

4.4.2. Publication of the certificate by the CA

No stipulation.

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

No stipulation.

4.5.2. Relying party public key and certificate usage

No stipulation.

4.6. Certificate renewal

Certificates may be Reissued. Certificate Reissuance includes issuance of a new Certificate consisting of a new Serial Number, new Validity Period, and may also include new information for other Certificate fields.

4.6.1. Circumstance for certificate renewal

No stipulation.

4.6.2. Who may request renewal

No stipulation.

4.6.3. Processing certificate renewal requests

No stipulation.

4.6.4. Notification of new certificate issuance to Subscriber

No stipulation.

4.6.5. Conduct constituting acceptance of a renewal certificate

No stipulation.

4.6.6. Publication of the renewal certificate by the CA

No stipulation.

4.6.7. Notification of certificate issuance by the CA to other entities

No stipulation.

4.7. Certificate re-key

4.7.1. Circumstance for certificate re-key

No stipulation.

4.7.2. Who may request certification of a new public key

No stipulation.

4.7.3. Processing certificate re-keying requests

No stipulation.

4.7.4. Notification of new certificate issuance to Subscriber

No stipulation.

4.7.5. Conduct constituting acceptance of a re-keyed certificate

No stipulation.

4.7.6. Publication of the re-keyed certificate by the CA

No stipulation.

4.7.7. Notification of certificate issuance by the CA to other entities

No stipulation.

4.8. Certificate modification

4.8.1. Circumstance for certificate modification

No stipulation.

4.8.2. Who may request certificate modification

No stipulation.

4.8.3. Processing certificate modification requests

No stipulation.

4.8.4. Notification of new certificate issuance to Subscriber

No stipulation.

4.8.5. Conduct constituting acceptance of modified certificate

No stipulation.

4.8.6. Publication of the modified certificate by the CA

No stipulation.

4.8.7. Notification of certificate issuance by the CA to other entities

No stipulation.

4.9. Certificate revocation and suspension

4.9.1. Circumstances for revocation

The CA SHALL revoke a Certificate within 24 hours if one or more of the following occurs:

1. The Subscriber requests in writing that the CA revoke the Certificate;
2. The Subscriber notifies the CA that the original certificate request was not authorized and does not retroactively grant authorization;
3. The CA obtains evidence that the Subscriber's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise;

The CA SHOULD revoke a certificate within 24 hours and MUST revoke a Certificate within 10 days if one or more of the following occurs:

1. The Certificate no longer complies with the requirements of Sections 6.1.5 and 6.1.6;
2. The CA obtains evidence that the Certificate was misused;
3. The CA is made aware that a Subscriber has violated one or more of its material obligations under the Subscriber Agreement or Terms of Use;
4. The CA is made aware of any circumstance indicating that use of a Fully-Qualified Domain

Name or IP address in the Certificate is no longer legally permitted (e.g. a court or arbitrator has revoked a Domain Name Registrant's right to use the Domain Name, a relevant licensing or services agreement between the Domain Name Registrant and the Applicant has terminated, or the Domain Name Registrant has failed to renew the Domain Name);

5. The CA is made aware that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate Fully-Qualified Domain Name;
6. The CA is made aware of a material change in the information contained in the Certificate;
7. The CA is made aware that the Certificate was not issued in accordance with these Requirements or the CA's Certificate Policy or Certification Practice Statement;
8. The CA determines or is made aware that any of the information appearing in the Certificate is inaccurate;
9. The CA's right to issue Certificates under these Requirements expires or is revoked or terminated, unless the CA has made arrangements to continue maintaining the CRL/OCSP Repository;
10. Revocation is required by the CA's Certificate Policy and/or Certification Practice Statement; or

11. The CA is made aware of a demonstrated or proven method that exposes the Subscriber's Private Key to compromise or if there is clear evidence that the specific method used to generate the Private Key was flawed.

4.9.1.2 Reasons for Revoking a Subordinate CA Certificate

The Issuing CA SHALL revoke a Subordinate CA Certificate within seven (7) days if one or more of the following occurs:

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

4.9.2. Who can request revocation

The Subscriber, RA, or Issuing CA can initiate revocation. Additionally, Subscribers, Relying Parties, Application Software Suppliers, and other third parties may submit Certificate Problem

Reports informing the issuing CA of reasonable cause to revoke the certificate.

4.9.3. Procedure for revocation request

The CA SHALL provide a process for Subscribers to request revocation of their own Certificates. The process MUST be described in the CA's Certificate Policy or Certification Practice Statement.

The CA SHALL maintain a continuous 24x7 ability to accept and respond to revocation requests and Certificate Problem Reports.

The CA SHALL provide Subscribers, Relying Parties, Application Software Suppliers, and other third parties with clear instructions for reporting suspected Private Key Compromise, Certificate misuse, or other types of fraud, compromise, misuse, inappropriate conduct, or any other matter related to Certificates.

4.9.4. Revocation request grace period

No stipulation.

4.9.5. Time within which CA MUST process the revocation request

The CA will take reasonable steps to process revocation requests without delay.

4.9.6. Revocation checking requirement for relying parties

Following certificate issuance, a certificate may be revoked for any reason stated in Section 4.9. Therefore, relying parties should check the revocation status of all certificates that contain a CDP or OCSP pointer.

4.9.7. CRL issuance frequency (if applicable)

The CA takes reasonable steps to publish Information relating to the status of a Certificate issued, as being Suspended or Revoked, including the CRLs created by any CA, to the Repository without delay.

4.9.8. Maximum latency for CRLs (if applicable)

CRLs shall be published no later than the time specified in the "nextUpdate" field of the previously issued CRL.

4.9.9 On-line revocation/status checking availability

OCSP responses MUST conform to RFC6960 and/or RFC5019. OCSP responses MUST either:

1. Be signed by the CA that issued the Certificates whose revocation status is being checked, or
2. Be signed by an OCSP Responder whose Certificate is signed by the CA that issued the Certificate whose revocation status is being checked.

In the latter case, the OCSP signing Certificate MUST contain an extension of type id-pkix-ocsp-nocheck, as defined by RFC6960.

4.9.10 On-line revocation checking requirements

OCSP responders operated by the CA SHALL support the HTTP GET method, as described in

RFC 6960 and/or RFC 5019.

The validity interval of an OCSP response is the difference in time between the thisUpdate and nextUpdate field, inclusive.

If the OCSP responder receives a request for the status of a certificate serial number that is "unused", then the responder SHOULD NOT respond with a "good" status.

If the OCSP responder is for a CA that is not Technically Constrained in line with Section 7.1.5, the responder MUST NOT respond with a "good" status for such requests.

4.9.11 Other forms of revocation advertisements available

No Stipulation.

4.9.12 Special requirements related to key compromise

See Section 4.9.1

4.9.13 Circumstances for suspension

No Stipulation.

4.9.14 Who can request suspension

Not applicable.

4.9.15 Procedure for suspension request

Not applicable.

4.9.16 Limits on suspension period

Not applicable.

4.10 Certificate status services

4.10.1 Operational characteristics

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

4.10.2 Service availability

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

The CA SHALL maintain an online 24x7 Repository that application software can use to automatically check the current status of all unexpired Certificates issued by the CA. The CA SHALL maintain a continuous 24x7 ability to respond internally to a high-priority certificate revocation request.

4.10.3 Optional features

No stipulation.

4.11 End of subscription

No stipulation.

4.12 Key escrow and recovery

4.12.1 Key escrow and recovery policy and practices

No stipulation.

4.12.2 Session key encapsulation and recovery policy and practices

Not applicable.

5. MANAGEMENT, OPERATIONAL AND PHYSICAL CONTROLS

The CA SHALL develop, implement, and maintain a comprehensive security program designed to:

1. Protect the confidentiality, integrity, and availability of Certificate Data and Certificate Management Processes;
2. Protect against anticipated threats or hazards to the confidentiality, integrity, and availability of the Certificate Data and Certificate Management Processes;
3. Protect against unauthorized or unlawful access, use, disclosure, alteration, or destruction of any Certificate Data or Certificate Management Processes;
4. Protect against accidental loss or destruction of, or damage to, any Certificate Data or Certificate Management Processes; and
5. Comply with all other security requirements applicable to the CA by law.

The Certificate Management Process MUST include:

1. physical security and environmental controls;
2. system integrity controls, including configuration management, integrity maintenance of trusted code, and malware detection/prevention;
3. network security and firewall management, including port restrictions and IP address filtering;
4. user management, separate trusted-role assignments, education, awareness, and training; and
5. logical access controls, activity logging, and inactivity time-outs to provide individual accountability.

The CA's security program MAY include a Risk Assessment that:

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

2. Assesses the likelihood and potential damage of these threats, taking into consideration the sensitivity of the Certificate Data and Certificate Management Processes; and

3. Assesses the sufficiency of the policies, procedures, information systems, technology, and other arrangements that the CA has in place to counter such threats.

Based on the Risk Assessment, the CA SHALL develop, implement, and maintain a security plan consisting of security procedures, measures, and products designed to achieve the objectives set forth above and to manage and control the risks identified during the Risk Assessment, commensurate with the sensitivity of the Certificate Data and Certificate Management Processes. The security plan MUST include administrative, organizational, technical, and physical safeguards appropriate to the sensitivity of the Certificate Data and Certificate Management Processes. The security plan MUST also take into account then-available technology and the cost of implementing the specific measures, and SHALL implement a reasonable level of security appropriate to the harm that might result from a breach of security and the nature of the data to be protected.

5.1 Physical controls

The CA infrastructure SHALL be located and operated from secure Cisco facilities. Detailed security procedures MUST be in place and followed that prohibit unauthorized access and entry into the areas of the facilities in which CA systems reside.

5.1.1 Site location and construction

No stipulation.

5.1.2 Physical access

The CA SHALL have in place appropriate physical security controls to restrict access to all hardware and software used for providing CA Services. Access to such hardware and software SHALL be limited to those personnel performing in a trusted role and two-person access SHALL be enforced.

5.1.3 Power and air conditioning

No stipulation.

5.1.4 Water exposures

No stipulation.

5.1.5 Fire prevention and protection

No stipulation.

5.1.6 Media storage

No stipulation.

5.1.7 Waste disposal

No stipulation.

5.1.8 Off-site backup

No stipulation.

5.2 Procedural controls

5.2.1 Trusted roles

No stipulation.

5.2.2. Number of persons required per task

The Private Key SHALL be backed up, stored, and recovered only by personnel in trusted roles using, at least, dual control in a physically secured environment.

5.2.3 Identification and authentication for each role

No stipulation.

5.2.4 Roles requiring separation of duties

No stipulation.

5.3 Personnel controls

5.3.1 Qualifications, experience, and clearance requirements

Prior to the engagement of any person in the Certificate Management Process, whether as an employee, agent, or an independent contractor of the CA, the CA SHALL verify the identity and trustworthiness of such person.

5.3.2 Background check procedures

No stipulation.

5.3.3 Training requirements

No stipulation.

5.3.4 Retraining frequency and requirements

No stipulation.

5.3.5 Job rotation frequency and sequence

No stipulation.

5.3.6 Sanctions for unauthorized actions

No stipulation.

5.3.7 Independent contractor requirements

No Stipulation.

5.3.8. Documentation supplied to personnel

No stipulation.

5.4. Audit logging procedures

5.4.1 Types of events recorded

The following data and files must be archived by, or on behalf of, the CA:

- All computer security audit data produced by the Root CA machine
- All certificate application data
- All certificates, and all CRLs or certificate status records
- Key histories Internal Customer Root CA Certificate Policy 15
- All correspondence between the CA, RAs, VSPs, and/or subscribers

5.4.2 Frequency of processing log

No stipulation.

5.4.3 Retention period for audit log

Archive of the key and certificate information must be retained for at least the lifetime of the CA. Archives of the audit trail files must be retained for at least five (5) years after the lifetime of the CA has ended.

5.4.4 Protection of audit log

No stipulation.

5.4.5 Audit log backup procedures

During the compliance audit required by this Policy, the auditor shall verify the integrity of the archives, and if either copy is found to be corrupted or damaged in any way, it shall be replaced with the other copy held in the separate location.

5.4.6 Audit collection system (internal vs. external)

No stipulation.

5.4.7 Notification to event-causing subject

No stipulation.

5.4.8 Vulnerability assessments

Additionally, the CA's security program MAY include a Risk Assessment that:

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

5.4.9 Records archival

5.4.10 Types of records archived

The following data and files must be archived by, or on behalf of, the CA:

- All computer security audit data produced by the Root CA machine
- All certificate application data
- All certificates, and all CRLs or certificate status records
- Key histories
- All correspondence between the CA, RAs, VSPs, and/or subscribers

5.4.11 Retention period for archive

Archive of the key and certificate information must be retained for at least the lifetime of the CA. Archives of the audit trail files must be retained for at least five (5) years after the lifetime of the CA has ended.

5.4.12 Protection of archive

The archive media must be protected either by physical security alone, or a combination of physical security and suitable cryptographic protection. It should also be provided adequate protection from environmental threats such as temperature, humidity and magnetism.

5.4.13 Archive backup procedures

Adequate backup procedures must be in place so that in the event of the loss or destruction of the primary archives, a complete set of backup copies will be readily available within a short period of time.

5.4.14 Requirements for time-stamping of records

No stipulation.

5.4.15 Archive collection system (internal or external)

No stipulation.

5.4.16 Procedures to obtain and verify archive information

During the compliance audit required by this Policy, the auditor shall verify the integrity of the archives, and if either copy is found to be corrupted or damaged in any way, it shall be replaced with the other copy held in the separate location5.6 Key changeover

5.7. Compromise and disaster recovery

5.7.1 Incident and compromise handling procedures

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

5.7.2 Recovery procedures if computing resources, software, and/or data are corrupted

No stipulation.

5.7.3 Recovery procedures after key compromise

The CA must have in place an appropriate key compromise plan that addresses the procedures that will be followed in the event of a compromise of the private signing key used by the CA to issue certificates. Such plan shall include procedures for revoking any affected certificates and promptly notifying subscribers and Benefiting Parties.

5.7.4 Business continuity capabilities after a disaster

No 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. The CA private key will be maintained in its Hardware Security Module (HSM) for 5 years past either termination or expiration of the CA certificate, after which it will be destroyed using the FIPS 140-1 Level 3 or higher approved mechanism supplied by the HSM.

6. TECHNICAL SECURITY CONTROLS

6.1 Key Pair generation and installation

6.1.1 Key Pair generation

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

• Having all users (CAs, RAs, VSPs, and subscribers) generate their own keys on a trustworthy system, and not reveal the private keys to anyone else

• Having keys generated in hardware tokens from which the private key cannot be extracted CA and RA keys must be generated in hardware tokens. Key pairs for VSPs and subscribers can be generated in either hardware or software

6.1.2 Private key delivery to Subscriber

See section 6.1.1

6.1.3 Public key delivery to certificate issuer

No stipulation.

6.1.4 CA public key delivery to relying parties

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

6.1.5 Key sizes

For RSA key pairs the CA SHALL:

- Ensure that the modulus size, when encoded, is at least 2048 bits, and;
- Ensure that the modulus size, in bits, is evenly divisible by 8.

For ECDSA key pairs, the CA SHALL:

- Ensure that the key represents a valid point on the NIST P-256, NIST P-384 or NIST P-521 elliptic curve.

The CPS must require a minimum of 2048-bit key sizes for all subscriber (sub-CA) certificates in order to comply with this Policy.

6.1.6 Public key parameters generation and quality checking

Public key parameters SHALL be generated in accordance with IETF specified standards such as RFC5758 and RFC8017.

6.1.7 Key usage purposes (as per X.509 v3 key usage field)

Private Keys corresponding to Root Certificates MUST NOT be used to sign Certificates except in the following cases:

1. Self-signed Certificates to represent the Root CA itself;
2. Certificates for Subordinate CAs and Cross Certificates;
3. Certificates for infrastructure purposes (administrative role certificates, internal CA opera- tional device certificates); and
4. Certificates for OCSP Response verification.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

The CA SHALL implement physical and logical safeguards to prevent unauthorized certificate issuance.

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

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

6.2.1 Cryptographic module standards and controls

The CA signing key generation, storage and signing operations shall be performed using a hardware-based cryptographic module rated at FIPS 140-2 Level 3 or higher. Subscribers (sub-CAs) shall also use FIPS 140-2 Level 3 or higher approved cryptographic modules.

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. For example, access to the CA Private Signing Key should require authorization and validation by multiple parties, including CA personnel and separate security officers. This mechanism prevents a single party (CA or otherwise) from gaining access to the CA Private Signing Key.

The Issuing CA's private key must be protected by multi person control for all functions. The parties used for two-person control will be maintained on a list that will be made available for inspection by the audit personnel identified in section 8.

6.2.3 Private key escrow

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

6.2.4 Private key backup

The private keys for both the Issuing CA and Subscribers (sub-CAs) must be backed up in accordance with Cisco Systems' "PKI Root Creation and Storage Guidelines" document.

6.2.5 Private key archival

The private keys for both the Issuing CA and Subscribers (sub-CAs) must be archived in accordance with Cisco Systems' "PKI Root Creation and Storage Guidelines" document.

6.2.6 Private key storage on cryptographic module

The private keys for both the Issuing CA and Subscribers (sub-CAs) must be generated/entered into cryptographic modules in accordance with Cisco Systems' "PKI Root Creation and Storage Guidelines" document.

6.2.7 Method of activating private key

The private key of both the Issuing CA and Subscribers (sub-CAs) must be activated by two or more personnel in accordance with the FIPS 140-2 Level 3 or higher standard.

6.2.8 Method of deactivating private key

The private key of both the Issuing CA and Subscribers (sub-CAs) must be deactivated by two or more personnel in accordance with the FIPS 140-2 Level 3 or higher standard.

6.2.9 Method of destroying private key

Upon expiration or revocation of a certificate, or other termination of use of a private key for creating signatures, all copies of the private key shall be securely destroyed.

6.2.10 Cryptographic Module Rating

No stipulation.

6.3 Other aspects of Key Pair management

6.3.1 Public key archival

The public key of the Issuing CA and Subscriber public keys are archived both in the system backups of the offline Root CA, and in the regular backups of the Repository where the digital certificates are published.

6.3.2 Certificate operational periods and Key Pair usage periods

The Issuing CA key pair may be replaced as its certificate expires.

6.4 Activation data

There is no activation data needed or required for subscribers of the Root CAs as every subscriber is a subordinate CA and the sub-CA certificates are hand-delivered back to the sub-CA and installed by agents of Cisco Systems, Inc.

6.4.1 Activation data generation and installation

No stipulation.

6.4.2 Activation data protection

No stipulation.

6.4.3 Other aspects of activation data

No stipulation.

6.5 Computer security controls

6.5.1 Specific computer security technical requirements

The Root CA servers must be offline at all times. Under no circumstances will the server be networked in any fashion. Any repositories must be protected through application-level firewalls (or separate ports of a single firewall) configured to allow only the protocols and commands required for the secure operation of the repository.

6.5.1.1. Change Management Process

The Root CAs follows the principles of documentation, approval and testing, to ensure that all changes to Certificate Systems, Issuing Systems, Certificate Management Systems, Security Support Systems, and Front-End / Internal-Support Systems follow said Change Management Process.

6.5.1.2. Monitoring and Alerting

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

6.5.2 Computer security rating

The Issuing CA must only use cryptographic modules that meet the requirements in section 6.2, 6.2.1, and 6.2.2.

6.6 Life cycle technical controls

6.6.1 System development controls

No stipulation.

6.6.2 Security management controls

No stipulation.

6.6.3 Life cycle security controls

No stipulation.

6.7 Network security controls

No stipulation.

6.8 Time-stamping

No stipulation.

7. CERTIFICATE, CRL, AND OCSP PROFILES

7.1 CERTIFICATE PROFILE

The CA SHALL meet the technical requirements set forth in Section 2.2 – Publication of Information, Section 6.1.5 – Key Sizes, and Section 6.1.6 – Public Key Parameters Generation and Quality Checking.

7.1.1 Version Number(s)

Certificates MUST be of type X.509v3.

7.1.2 Certificate Extensions

No Stipulation.

7.1.2.1 Root CA Certificate

a. basicConstraints

This extension MUST appear as a critical extension. The cA field MUST be set true. The pathLenConstraint field SHOULD NOT be present.

b. keyUsage

This extension MUST be present and MUST be marked critical.

7.1.2.2 Subordinate CA Certificate

a. certificatePolicies

This extension MUST be present and SHOULD NOT be marked critical.

certificatePolicies:policyIdentifier (Required)

The following fields MAY be present if the Subordinate CA is not an Affiliate of the entity that controls the Root CA.

certificatePolicies:policyQualifiers:policyQualifierId (Optional) id-qt 1 [RFC 5280].

certificatePolicies:policyQualifiers:qualifier:cPSuri (Optional)

HTTP URL for the Root CA's Certificate Policies, Certification Practice Statement, Relying Party Agreement, or other pointer to online policy information provided by the CA.

b. cRLDistributionPoints

This extension SHALL be present. If present, MUST NOT be marked critical. I CRLs are used then it MUST contain the HTTP URL of the CA's CRL service.

c. authorityInformationAccess

This extension SHOULD be present. It MUST NOT be marked critical.

It SHOULD contain the HTTP URL of the Issuing CA's certificate (accessMethod = 1.3.6.1.5.5.7.48.2). It MAY contain the HTTP URL of the Issuing CA's OCSP responder (accessMethod = 1.3.6.1.5.5.7.48.1).

d. basicConstraints

This extension MUST be present and MUST be marked critical. The cA field MUST be set true. The pathLenConstraint field MAY be present.

e. keyUsage

This extension MUST be present and MUST be marked critical. Bit positions for keyCertSign and cRLSign MUST be set. If the Subordinate CA Private Key is used for signing OCSP responses, then the digitalSignature bit MUST be set.

7.1.2.3 All Certificates All other fields and extensions MUST be set in accordance with RFC 5280. The CA SHALL NOT issue a Certificate that contains a keyUsage flag, extendedKeyUsage value, Certificate extension, or other data not specified in Section 7.1.2.1, Section 7.1.2.2, or Section 7.1.2.3 unless the CA is aware of a reason for including the data in the Certificate.

CAs SHALL NOT issue a Certificate with:

a) Extensions that do not apply in the context of the public Internet (such as an extendedKeyUsage value for a service that is only valid in the context of a privately managed network), unless: i. such value falls within an OID arc for which the Applicant demonstrates ownership, or ii. the Applicant can otherwise demonstrate the right to assert the data in a public context; or

b) semantics that, if included, will mislead a Relying Party about the certificate information verified by the CA (such as including extendedKeyUsage value for a smart card, where the CA is not able to verify that the corresponding Private Key is confined to such hardware due to remote issuance).

7.1.3 Algorithm Object Identifiers

Algorithm object identifier OlDs are allocated to algorithms supported and used by Cisco and are in compliance with x.509 standards.

Certificates issued by any Issuing CA that chains up to The Root CA shall identify the signature algorithm using one of the following OIDs:

Table 7.1: OIDs for Signature Algorithms

id-dsa-with-sha1	1.2.840.10040.4.3
sha-1WithRSAEncryption	1.2.840.113549.1.1.5
sha256WithRSAEncryption	1.2.840.113549.1.1.11

ecdsa-with-SHA1	1.2.840.10045.4.1
ecdsa-with-SHA224	1.2.840.10045.4.3.1
ecdsa-with-SHA256	1.2.840.10045.4.3.2
ecdsa-with-SHA384	1.2.840.10045.4.3.3
ecdsa-with-SHA512	1.2.840.10045.4.3.4

Certificates issued from an Issuing CA that chains up to The Root CA shall identify the cryptographic algorithm associated with the subject public key using one of the following OIDs:

Table 7.2: OIDs for Subject Public Key Algorithms

id-dsa	1.2.840.10040.4.1
RsaEncryption	1.2.840.113549.1.1.1
Dhpublicnumber	1.2.840.10046.2.1
id-ecPublicKey	1.2.840.10045.2.1

7.1.4 Name Forms

Names for the “Issuer” and “Subject” fields of each Certificate type are of the X.500 DN form. Distinguished names shall be composed of standard attribute types.

7.1.5. Name Constraints

No stipulation.

7.1.6 Certificate Policy Object Identifier

Each Certificate issued contains the OID in the Certificate policy extension.

7.1.7 Usage of Policy Constraints extension

No stipulation.

7.1.8 Policy qualifiers syntax and semantics

No stipulation.

7.1.9 Processing semantics for the critical Certificate Policies extension

No stipulation.

7.2 CRL profile

7.2.1 Version number(s)

No stipulation.

7.2.2 CRL and CRL entry extensions

1. reasonCode (OID 2.5.29.21)

If present, this extension MUST NOT be marked critical.

If a CRL entry is for a Root CA or Subordinate CA Certificate, including Cross Certificates, this CRL entry extension MUST be present. If a CRL entry is for a Certificate not technically capable of causing issuance, this CRL entry extension SHOULD be present, but MAY be omitted, subject to the following requirements.

The CRLReason indicated MUST NOT be unspecified (0). If the reason for revocation is unspecified, CAs MUST omit reasonCode entry extension, if allowed by the previous requirements.

If a reasonCode CRL entry extension is present, the CRLReason MUST indicate the most appropriate reason for revocation of the certificate, as defined by the CA within its CP/CPS.

7.3 OCSP profile

If an OCSP response is for a Root CA or Subordinate CA Certificate, including Cross Certificates, and that certificate has been revoked, then the revocationReason field within the RevokedInfo of the CertStatus MUST be present.

The CRLReason indicated MUST contain a value permitted for CRLs, as specified in Section 7.2.2.

7.3.1 Version number(s)

No stipulation.

7.3.2 OCSP extensions

All use of standard OCSP request and response extensions shall comply with [RFC2560].

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

The CA SHALL at all times:

1. Issue Certificates and operate its PKI in accordance with all laws applicable to its business and the Certificates it issues in every jurisdiction in which it operates;
2. Comply with these Requirements;
3. Comply with the audit requirements set forth in this section; and
4. Be licensed as a CA in each jurisdiction where it operates, if licensing is required by the laws of such jurisdiction for the issuance of Certificates.

The Issuing CA (and each RA and/or VSP, as applicable) shall submit to an annual compliance audit by an entity as directed by Cisco Systems' Corporate Information Security group. Said entity shall be approved by Cisco Systems and qualified to perform a security audit on a CA based on significant experience in the application of PKI and cryptographic technologies. The purpose of such audit shall be to verify that the CA has in place a system to assure the quality of the CA Services that it provides, and that complies with all of the requirements of this Policy and its CPS.

Issuing CA inspection results must be submitted to the Issuing CA's regulator or licensing body where applicable, and the Policy Management Authority (PMA) of this Policy. If irregularities are found, the Issuing CA must submit a report to its regulator or licensing body and the PMA as to any action the Issuing CA will take in response to the inspection report. Where the Issuing CA fails to take appropriate action in response to the inspection report, the Issuing CA's regulator, licensing body or the PMA may:

(i) indicate the irregularities, but allow the Issuing CA to continue operations until the next programmed inspection;

(ii) allow the Issuing CA to continue operations for a maximum of thirty (30) days pending correction of any problems prior to revocation;

(iii) downgrade the assurance level of any Certificates issued by the Issuing CA (including Cross Certificates); or

(iv) revoke the Issuing CA's Certificate.

Any decision regarding which of these actions to take will be based on the severity of the irregularities. Any remedy may include permanent or temporary CA cessation, but all relevant factors must be considered prior to making a decision. A special audit may be required to confirm the implementation and effectiveness of the remedy. The Issuing CA will post any appropriate results of an inspection, in whole or in part, so that it is accessible for review by Certificate Holders, Authorized Benefiting Parties and RAs. The manner and extent of the publication will be defined by the Issuing CA.

8.1 Frequency or circumstances of assessment

See section 8.

8.2 Identity/qualifications of assessor

See section 8.

8.3 Assessor's relationship to assessed entity

See section 8.

8.4 Topics covered by assessment

See section 8.

8.5 Actions taken as a result of deficiency

No stipulation.

8.6 Communication of results

See section 8.

8.7 Self-Audits

No stipulation.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

9.1.1 Certificate issuance or renewal fees

No stipulation.

9.1.2 Certificate access fees

No stipulation.

9.1.3 Revocation or status information access fees

No stipulation.

9.1.4 Fees for other services

No stipulation.

9.1.5 Refund policy

No stipulation.

9.2 Financial responsibility

9.2.1 Insurance coverage

No stipulation.

9.2.2 Other assets

No stipulation.

9.2.3 Insurance or warranty coverage for end-entities

No stipulation.

9.3 Confidentiality of business information

9.3.1 Scope of confidential information

No stipulation.

9.3.2 Information not within the scope of confidential information

No stipulation.

9.3.3 Responsibility to protect confidential information

No stipulation.

9.4 Privacy of personal information

9.4.1 Privacy plan

No stipulation.

9.4.2 Information treated as private

No stipulation.

9.4.3 Information not deemed private

No stipulation.

9.4.4 Responsibility to protect private information

No stipulation.

9.4.5 Notice and consent to use private information

No stipulation.

9.4.6 Disclosure pursuant to judicial or administrative process

No stipulation.

9.4.7 Other information disclosure circumstances

No stipulation.

9.5 Intellectual property rights

No stipulation.

9.6 Representations and warranties

9.6.1 CA representations and warranties

No stipulation.

9.6.2 RA representations and warranties

No stipulation.

9.6.3 Subscriber representations and warranties

No stipulation.

9.6.4 Relying party representations and warranties

No stipulation.

9.6.5 Representations and warranties of other participants

No stipulation.

9.7 Disclaimers of warranties

No stipulation.

9.8 Limitations of liability

No stipulation.

9.9 Indemnities

No stipulation.

9.10 Term and termination

9.10.1 Term

No stipulation.

9.10.2 Termination

No stipulation.

9.10.3 Effect of termination and survival

No stipulation.

9.11 Individual notices and communications with participants

No stipulation.

9.12 Amendments

9.12.1 Procedure for amendment

No stipulation.

9.12.2 Notification mechanism and period

No stipulation.

9.12.3 Circumstances under which OID MUST be changed

No stipulation.

9.13 Dispute resolution provisions

No stipulation.

9.14 Governing law

No stipulation.

9.15 Compliance with applicable law

No stipulation.

9.16 Miscellaneous provisions

9.16.1 Entire agreement

No stipulation.

9.16.2 Assignment

No stipulation.

9.16.3 Severability

No stipulation.

9.16.4 Enforcement (attorneys′ fees and waiver of rights)

No stipulation.

9.16.5 Force Majeure

No stipulation.

9.17 Other provisions

No stipulation.

Appendix A: Terminology and Definitions

This appendix provides definitions for specific terms used throughout this Certificate Policy document to ensure clarity and consistency. The terms defined here are derived from common standards and conventions used in policy documents including reference to IETF RFC 2119

Terminology

1. **SHALL**:
   - **Definition**: Indicates a requirement that must be strictly followed to conform to the document. Non-compliance is not permissible.
   - **Usage Example**: "The certificate authority (CA) SHALL verify the identity of the applicant before issuing a certificate."
2. **MUST**:
   - **Definition**: Synonymous with "SHALL." Indicates a mandatory requirement.
   - **Usage Example**: "All certificates MUST include the CA's digital signature."
3. **SHALL NOT**:
   - **Definition**: Indicates a prohibition. The action is explicitly forbidden and non-compliance is not permissible.
   - **Usage Example**: "The CA SHALL NOT issue a certificate without verifying the applicant's identity."
4. **MUST NOT**:
   - **Definition**: Synonymous with "SHALL NOT." Indicates a prohibited action.
   - **Usage Example**: "Certificates MUST NOT be issued with expired validation data."
5. **SHOULD**:
   - **Definition**: Indicates a recommended practice or suggestion. Compliance is encouraged but not mandatory.
   - **Usage Example**: "The CA SHOULD provide certificate status information via an online certificate status protocol (OCSP)."
6. **SHOULD NOT**:
   - **Definition**: Indicates a recommended practice or suggestion to avoid. Non-compliance is allowed but not recommended.
   - **Usage Example**: "The CA SHOULD NOT issue certificates for more than three years."
7. **MAY**:
   - **Definition**: Indicates an optional practice or action. Compliance is at the discretion of the implementer.
   - **Usage Example**: "The CA MAY provide additional services such as timestamping."

8. **CAN**:
   - **Definition**: Indicates possibility or capability, without implying a requirement or recommendation.

- **Usage Example**: "Subscribers CAN use their certificates for both email and document signing."

9. **OPTIONAL**:
   - **Definition**: Indicates that a feature or action is not mandatory and is left to the discretion of the implementer.
   - **Usage Example**: "Implementing key recovery mechanisms is OPTIONAL."

10. **Certificate Authority (CA)**:

    Definition: An organization that is responsible for the creation, issuance, revocation, and management of Certificates. The term applies equally to both Roots CAs and Subordinate CAs.

11. **Subscriber**:

    Definition: An individual or entity that has been issued a digital certificate by the CA.

12. **Digital Certificate**:

    Definition: An electronic document used to prove the ownership of a public key. It includes information about the key, the identity of the owner, and the digital signature of the CA that issued it.

13. **Public Key Infrastructure (PKI)**:

    Definition: A framework for creating, managing, distributing, using, storing, and revoking digital certificates.

14. **Certificate Revocation List (CRL)**:

    Definition: A list of certificates that have been revoked by the CA before their expiration date.

15. **Online Certificate Status Protocol (OCSP)**:

    Definition: A protocol used for obtaining the revocation status of a digital certificate.

16. **Registration Authority (RA)**:

    Definition: An entity that is responsible for accepting requests for digital certificates and authenticating the entity making the request.

17. **Repository**:

    Definition: A system for storing and making available digital certificates and other related information such as CRLs.

18. **Private Key**:

    Definition: A cryptographic key that is kept secret and is used to create digital signatures and decrypt data.

19. **Public Key**:

    Definition: A cryptographic key that is publicly available and is used to verify digital signatures and encrypt data.

20. **Key Pair**:

    Definition: A pair of cryptographic keys consisting of a public key and a private key used in public key cryptography.

21. **Trust Anchor**:

    Definition: A trusted entity, such as a root CA, whose public key is used to validate digital certificates.

22. **Key Usage**:

    Definition: The intended use of a cryptographic key, such as for digital signatures, key encipherment, or data encipherment.

23. **Certificate Policy (CP)**:

    Definition: A document that specifies the practices and standards a CA uses in issuing certificates.

24. **Certification Practice Statement (CPS)**:

    Definition: A document that describes in detail the practices a CA employs in issuing and managing certificates.

25. **Relying Party**:

    Definition: An entity that relies on the validity of the information in a digital certificate.

26. **Cross-Certification**:

    Definition: A process in which two CAs certify each other's public keys, establishing trust between their respective PKIs.

27. **Subject**:

    Definition: The entity identified by a digital certificate, typically including information such as the entity's name, organization, and public key.

28. **End-Entity (or Leaf) Certificate**:

    Definition: A certificate issued to an end-user or device, typically used for authenticating the identity of the certificate holder.

29. **Root Certificate**:

    Definition: A self-signed certificate issued by a root CA, which forms the basis of trust in a PKI.

30. **Intermediate Certificate**:

    Definition: A certificate issued by a CA that is subordinate to a root CA and can issue end-entity certificates or further intermediate certificates.

31. **Certificate Chain**:

    Definition: A sequence of certificates, starting from the end-entity certificate and ending with the root certificate, used to verify the validity of a certificate.

32. **Revocation**:

    Definition: The process of invalidating a certificate before its expiration date, typically due to compromise or other security concerns.

33. **Validity Period**:

    Definition: The time period during which a digital certificate is considered valid and can be used.

34. **Non-repudiation**:

    Definition: A property that ensures a party cannot deny the authenticity of their digital signature or the integrity of the signed data.

Appendix B: Document History

Version	Date	Change owner	Note
1.0	8-2-2024	CA Policy Authority	Initial publication