Cisco ECC Root CA Certificate Policy

Identity Assurance Services

version 1.0

2013-Sep-30

Cisco Systems • 7025 Kit Creek Road, Research Triangle Park, NC

Table of Contents

Version Information

Version 1.0 – 2013-Sep-30

First version of document

Approvals

Version	Name	Title	Date
1.0	Alex Wight	PKI Architect	2013-Sep-26
	Eric Hampshire	PKI Operations	2013-Sep-26
	Jos Purvis	PKI Compliance Program Manager	2013-Sep-20
	J.P. Hamilton	PKI Manager	2013-Sep-26
	Bill Friedman	Senior Corporate Counsel	2013-Sep-25

Annual Reviews

Version	Name	Title	Date

1 Introduction

Cisco Systems has implemented a Root Certificate Authority (CA) to provide a trust anchor for cryptographic communications using X.509 certificates. The Root CA consists of systems, products and services that both protect the Root CA's private key, and manage the subordinate CA X.509 certificates (sub-CA certificates) issued from the Root CA.

The purpose of this document is to describe the framework for the use (issuance, renewal, revocation, and policies) of the ECC Root Certificate Authority within Cisco Systems Inc., and with external entities.

1.1 Background

A public-key certificate binds a public-key value to a set of information that identifies the entity associated with use of the corresponding private key (this entity is known as the "subject" of the certificate). A certificate is used by a "certificate user" or "benefiting party" that needs to utilize the public key distributed via that certificate (a certificate user is typically an entity that is verifying a digital signature created by the certificate's subject). The degree to which a certificate user can trust the binding embodied in a certificate depends on several factors. These factors include the practices followed by the Certification Authority (CA) in authenticating the subject; the CA's operating policy, procedures, and security controls; the subject's obligations (for example, in protecting the private key); and the stated undertakings and legal obligations of the CA (for example, warranties and limitations on liability).

1.1.1 PKI Hierarchy

The Cisco ECC Root CA is a self-signed Root CA created in a secure key generation process by multiple agents of Cisco Systems, Inc.

The Cisco ECC Root CA will only issue subordinate CA certificates and delegated OCSP Response Signing certificates, according to the policies stated in this document.

The Cisco ECC Root CA is operated in an offline (non-networked) mode and is physically secured separately from the rest of the Cisco Systems' computing assets. The Cisco Corporate Information Security group is responsible for the physical access controls protecting the offline Root CA.

Being a self-signed root, the Cisco ECC Root CA hierarchy consists of only one certificate - the Cisco ECC Root CA (RX-E2), which is owned and operated by Cisco Systems, Inc.

1.2 Policy Identification

The assertion of a Certificate Policies Object Identifier (CP OID) within the CertificatePolicies X.509 v3 extension will only be carried out by subordinate CAs that issue end-entity certificates. Therefore, there is no CP extension present in the Cisco ECC Root CA certificate and the assignment of a CP OID is not within the scope of this document.

1.2.1 Certificate Types

The Cisco ECC Root CA issues only subordinate CA certificates and delegated OCSP Response Signing certificates. Other than OCSP Response Signing certificates, no end-entity certificates will be issued from the Cisco ECC Root CA. The sub-CA certificates issued by the Cisco ECC Root CA will include the CP OID(s) assigned to the Certificate Policy of the particular type of end-entity certificate issued by the sub-CA.

1.2.1.1 Certificate Profile

The Cisco ECC Root CA certificate profile is obtainable by downloading the actual Root CA certificate itself from http://www.cisco.com/security/pki/certs/eccroot.cer or through correspondence to the parties listed in section 1.4.

1.3 Community & Applicability

1.3.1 Certification Authorities (CAs)

This Policy is binding on the offline root CA “Cisco ECC Root CA”. Specific practices and procedures by which the Root CA implements the requirements of this Policy shall be set forth by the CA in a certification practice statement ("CPS") or other publicly available document, or by contract with any Benefiting Party (see 1.3.5 below).

1.3.1.1 CAs Authorized to Issue Certificates under this Policy

The offline root CA “Cisco ECC Root CA”, owned by Cisco Systems, Inc. and operated by Cisco Systems Corporate Information Security group, is the only CA authorized to issue certificates under this policy.

1.3.2 Registration Authorities

See Section 2.1.2 .

1.3.3 Validation Services

See Section 2.1.3 .

1.3.4 Subscribers

The Subscribers of the Cisco ECC Root CA are limited to subordinate CAs and holders of OCSP Response Signing certificates only.

1.3.5 Benefiting Parties

This Policy is intended for the benefit of the following persons who may rely on certificates that reference this Policy ("Benefiting Parties"):

- 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.

1.3.6 Applicability

1.3.6.1 Suitable Applications

Sub-CA certificates issued under this policy may be used in any application which requires the assembly of a cryptographic chain up to the Cisco ECC Root CA for signature verification, establishment of trust, and/or certificate validation purposes.

1.4 Contact Details

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

1.4.1 Changes to the Certificate Policy

1.4.1.1 Procedure for Changes

Changes to this CP are made by the Cisco's Policy Management Authority (PMA), which includes Cisco's Corporate Security Programs Office and Legal department. Changes will be in the form of a document update with changes reflected in the version section. Changed versions will be linked to by the main Cisco PKI Policies page located at: http://www.cisco.com/security/pki/policies/index.html.

1.4.1.2 Change Notification

Benefiting Parties are defined here as entities who have entered into a Certificate Trust Agreement with Cisco Systems wherein this Certificate Policy is specifically referenced. Cisco's PMA will notify all Benefiting Parties of any changes to the CP or CPS as defined in the specific Certificate Trust Agreement between Cisco Systems and the Benefiting Party. Entities who are not Benefiting Parties will not be notified of changes but may learn of changes by viewing the current CP or CPS published to Cisco's public repository.

1.4.2 Contact Information

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

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 No.: +1 919-392-1481
E-mail address: ciscopki-public@external.cisco.com

2 General Provisions

2.1 Obligations

2.1.1 CA Obligations

The root CA “Cisco ECC Root CA” is responsible for all aspects of the issuance and management of its 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.

2.1.1.1 Representations by the CA

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

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

2.1.1.2 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 by the Cisco ECC Root CA. In such instances where an explicit and separate Certificate Warranty agreement exists between the Benefiting Party and Cisco Systems, Cisco Systems may warrant that:

- The Issuing CA has issued and managed the Certificate in accordance with this Policy;
- The Issuing CA complied with the requirements of this Policy and any applicable CPS when authenticating requests for subordinate CA certificates;
- There are no material misrepresentations of fact in the Certificate known to the Issuing CA, and the Issuing CA has taken steps as required under this Policy to verify the information contained in the Certificate;
- The Issuing CA has taken the steps required by this Policy to ensure that the Certificate Holder's submitted information has been accurately transcribed to the Certificate;

- Information provided by the Issuing CA concerning the current validity of the Certificate is accurate and that validity has not been diminished by the Issuing CA's failure to promptly revoke the Certificate in accordance with this Certificate Policy; and
- The issued Certificate meets all material requirements of this Policy and any applicable CPS.

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

2.1.1.3 Warranty Limitations

The warranties offered to both Certificate Holders and Benefiting Parties will be subject to the limitations set forth in this Policy. Cisco Systems may provide further limitations and exclusions on these warranties as deemed appropriate, relating to: (i) failure to comply with the provisions of this Policy or of any agreement with the Issuing CA; (ii) other actions giving rise to any loss; (iii) events beyond the reasonable control of the CA; and (iv) time limitations for the filing of claims. However, such limitations and exclusions may not, in any event, be less than those provided for in 2.1.1.2.

2.1.1.4 Time between Certificate Request and Issuance

There is no stipulation for the period between the receipt of an application for a Certificate and the issuance of a Certificate, but the Issuing CA will make reasonable efforts to ensure prompt issuance.

2.1.1.5 Certificate Revocation and Renewal

The Issuing CA must ensure that any procedures for the expiration, revocation and renewal of an issued Certificate will conform to the relevant provisions of this Policy and will be expressly stated in a Certificate Agreement and any other applicable document outlining the terms and conditions of certificate use, including ensuring that: (i) Key Changeover Procedures are in accordance with this Policy; (ii) notice of revocation of a Certificate will be posted to an online certificate status database and/or a certificate revocation list (CRL), as applicable, within the time limits stated in this Policy; and (iii) the address of the online certificate status database and/or CRL is defined in the issued certificate.

2.1.1.6 End Entity Agreements

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

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

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

Nothing in any Certificate Agreement may waive or otherwise lessen the obligations of the Certificate Holder as provided in Section 2.1.4 of this Policy.

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

2.1.1.7 Ensuring Compliance

The Issuing CA must ensure that: (i) it only accepts information from entities that understand and are obligated to comply with this Policy; (ii) it complies with the provisions of this Policy in its certification and Repository services, issuance and revocation of Certificates and issuance of CRLs; (iii) it makes reasonable efforts to ensure adherence to this Policy with regard to any Certificates issued under it; and (iv) any identification and authentication procedures are implemented as set forth in Part 3.

2.1.2 Registration Authority (RA) Obligations

The operators of the Cisco ECC Root CA shall be responsible for performing all identification and authentication functions and all certificate manufacturing and issuing functions. The Cisco ECC

Root CA 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.

2.1.3 Certificate Status Validation Obligations

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

2.1.4 Subscriber Obligations

In all cases, the subscriber is obligated to:

- Generate a key pair using a trustworthy system, and take reasonable precautions to prevent any loss, disclosure, or unauthorized use of the private key;
- Warrant that all information and representations made by the subscriber that are included in the certificate are true;
- Use the certificate exclusively for authorized and legal purposes, consistent with this Policy;
- 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 Subscriber who is found to have acted in a manner counter to these obligations will have its certificate revoked, and will forfeit all claims it may have against the Issuing CA.

2.1.5 Benefiting Party Obligations

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

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

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

2.2 Liability

The Issuing CA assumes limited liability only to Benefiting Parties who have entered into a Benefiting Party Agreement. The Issuing CA may be responsible for direct damages suffered by

benefiting parties who have executed a Benefiting Party Agreement that are caused by the failure of the Issuing CA to comply with the terms of this Policy (except when waived by contract), and sustained by such benefiting parties as a result of reliance on a certificate in accordance with this Policy, but only to the extent that the damages result from the use of certificates for the suitable applications listed in Section 1.3.6. The liability of the Issuing CA is limited to these conditions and to conditions set forth in the terms of specific Benefiting Party Agreements.

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

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

2.3 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.

2.3.1 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.

2.3.2 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

2.3.5 Merger/Integration

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

2.3.6 Notice

All notices and other communications hereunder shall be in writing and shall be deemed given (a) on the same day if delivered personally, (2) 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 1.4.2 above.

2.4 Fees

The Issuing CA shall not impose any fees on the reading of this Policy or its CPS. The Issuing CA may charge access fees on certificates, certificate status information, or CRLs, subject to agreement between the CA and subscriber and/or between the CA and a Benefiting Party, and in accordance with a fee schedule published by the CA in its CPS or otherwise.

2.5 Publication & Validation Services

2.5.1 Publication of CA Information

The Issuing CA shall operate a secure on-line repository and/or other certificate validation service that is available to Benefiting Parties and that contains: (1) issued certificates that reference this Policy, when publication is authorized by the subscriber; (2) a Certificate Revocation List ("CRL") or on-line certificate status protocol (OCSP) database; (3) the CA's certificate for its signing key; (4) past and current versions of the CA's public CPS; (5) a copy of this Policy; and (6) other relevant information relating to certificates that reference this Policy.

2.5.2 Frequency of Publication

All information authorized to be published in a repository shall be published promptly after such information is authorized and available to the Issuing CA. Certificates issued by the CA that reference this Policy will be published promptly upon acceptance of such certificate by the subscriber, and when publication is authorized by the subscriber. Information relating to the revocation of a certificate will be published in accordance with section 4.4.3.

2.5.3 Access Controls

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

2.6 Compliance Audit

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.

2.7 Confidentiality Policy

Information regarding subscribers that is submitted on applications for certificates will be kept confidential by the Issuing CA and shall not be released without the prior consent of the subscriber, unless otherwise required by law. In addition, personal information submitted to the CA by subscribers must:

- Be made available to the subscriber for individual review following an authenticated request by said subscriber;
- Be subject to correction and/or update by said subscriber;
- Be protected by the CA in such a way as to insure the integrity of said personal information.

The foregoing shall not apply, however, to information appearing on certificates, or to information regarding subscribers that is obtained by CA from public sources. Under no circumstances shall the CA, any RA, or any VSP have access to the private keys of any subscriber to whom it issues a certificate that references this Policy.

2.8 Intellectual Property Rights

The Cisco ECC Root CA key pair, certificate, certification practice statement, and this certificate policy are the physical and intellectual property of Cisco Systems, Inc. Cisco retains all Intellectual Property Rights in and to these items. Intellectual Property Rights between Cisco and Benefiting Parties will be governed by this Certificate Trust Agreement.

3 Identification and Authentication

3.1 Initial Registration

Due to the offline nature of the Root CA, and subject to the requirements noted below, certificate applications may only be communicated from the applicant to the CA in person via physical media (such as a floppy disk, CD-ROM or USB storage device).

3.1.1 Types of Names

The subject name used for certificate applicants shall be the subscriber's authenticated common name in the form of an X.500 Distinguished Name.

3.1.2 Name Meanings

The subject name listed in all certificates must have a reasonable association with the authenticated information of the subscriber.

3.1.3 Rules for Interpreting Various Name Forms

No stipulation.

3.1.4 Name Uniqueness

The subject name or a combination of the subject name and other data fields listed in a certificate shall be unambiguous and unique for all certificates issued by the CA. If necessary, additional characters may be appended to the authenticated common name to ensure the name's uniqueness within the domain of certificates issued by the CA.

3.1.5 Verification of Key Pair

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

3.1.6 Subscriber Identification & Authentication (I&A)

A certificate request may only be made by an agent of Cisco Systems Inc. on behalf of current or proposed subordinate Certificate Authority or OCSP responder and for whom the certificate request is attributable for the purposes of accountability and responsibility. For I&A of the requesting agent, the Issuing CA must follow this Policy's requirements, as outlined in section

3.1.7 The applicant is required to provide authentication information and any applicable attributes, public keys and contact information.

3.1.7 Cisco Systems Agent Identification and Authentication (I&A)

The Issuing CA must establish the identity of the agent and authenticate the agent's permission to represent a current or proposed subordinate CA or OCSP responder prior to certificate issuance.

In addition, the CA may deliver certificate activation data with respect to such agent by (i) in-person delivery, based on the CA's personal knowledge of the agent or reasonable identification at the time of delivery, or (ii) use of a Shared Secret between the CA and the agent, previously established in connection with the prior identification and ongoing relationship described above.

The CA will ensure that it has collected, reviewed, and kept records of the information regarding the agent's identity that meets the minimum requirements of its Human Resource policy, or other similar procedures, which may include verification of all of the following identification information supplied by the Applicant: (i) photographic identification; (ii) first name, middle initial, and last name; (iii) street address; and (iv) home or work telephone number.

3.2 Renewal Applications

Renewals shall be performed under this Policy by treating all renewal requests as if they were first-time certificate application requests. All Subscriber and Issuing CA obligations stated in this Policy apply to the renewal request. A subscriber will submit the new certificate request to the Issuing CA. The Issuing CA shall issue a new certificate using the newly submitted information and adhering to the I&A policies set forth herein and in the associated CPS.

3.3 Re-Key after Revocation

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

3.4 Revocation Request

The Issuing CA, when faced with a revocation request, must adopt authentication mechanisms that balance the need to prevent unauthorized requests against the need to quickly revoke the Certificate.

Upon receipt of a revocation request, the identity of the requestor will be authenticated using the same mechanisms.

4 Operational Requirements

4.1 Certificate Application

An applicant for a certificate shall complete a certificate application in a format prescribed by the Issuing CA. All applications are subject to review, approval and acceptance by the Issuing CA. The subscriber certificate application process may only be initiated by agents of Cisco Systems, Inc.

4.2 Certificate Issuance

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

4.3 Certificate Acceptance

Following issuance of a certificate, the acceptance or rejection of the certificate by the subscriber, in this case the sub-CA, is solely at the discretion of the sub-CA operator, provided the acceptance or rejection is in accordance with procedures established by the Issuing Root CA and/or specified in the CPS.

4.4 Certificate Revocation

4.4.1 Circumstances for Revocation

The issuing CA shall revoke a certificate:

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

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

4.4.1.1 Permissive Revocation

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

4.4.1.2 Required Revocation

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

4.4.2 Who Can Request Revocation

The only persons permitted to request revocation of a certificate issued pursuant to this Policy are the subscriber and the Issuing CA.

4.4.3 Procedure for Revocation Request

A certificate revocation request should be promptly communicated to the Issuing CA. Due to the offline nature of the root CA, all certificate revocation requests must be communicated to the root CA in person by providing adequate proof of identification in accordance with this Policy.

4.4.3.1 Certificate Status or CRL Update

Promptly following revocation, the CRL or certificate status database, as applicable, shall be updated in accordance with the CPS for that CA. All revocation requests and the resulting actions taken by the CA shall be archived in accordance with the CPS for that CA.

4.4.4 Revocation Request Grace Period

Requests for revocation shall be processed within the timeframe delineated by the CPS for the issuing CA.

4.4.5 Certificate Suspension

The procedures and requirements stated for certificate revocation must also be followed for certificate suspension where implemented.

4.4.6 CRL Issuance Frequency

CRLs will be issued at least annually, even if there are no changes or updates to be made. Upon a new revocation, a new CRL will be issued and published within three business days. The Issuing CA will ensure that superceded CRLs are removed from the CRL Distribution Point location upon posting of the latest CRL.

4.4.7 On-Line Revocation/Status Checking Availability

Whenever an on-line certificate status database is used as an alternative to a CRL, such database shall be updated as soon as is technically possible after revocation or suspension.

4.5 Computer Security Audit Procedures

All significant security events on the Issuing CA system should be automatically recorded in audit trail files. Such files shall be retained for at least six (6) months onsite, and thereafter shall be securely archived as per Section 4.6.

4.6 Records Archival

4.6.1 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.

4.6.2 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.

4.6.3 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.

4.6.4 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.

4.6.5 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 location.

4.7 Key Changeover

Key Changeover is not supported for the Cisco ECC Root CA.

4.8 Compromise and Disaster Recovery

4.8.1 Disaster Recovery Plan

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.

4.8.2 Key Compromise Plan

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.

4.9 CA 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 7 years past either termination or expiration of the CA certificate, after which it will be destroyed using the FIPS 140-2 level 3 or higher approved mechanism supplied by the HSM.

5 Physical, Procedural, and Personnel Security Controls

5.1 Physical Security—Access Controls

The CA, all RAs, and VSPs, shall implement appropriate physical security controls to restrict access to the hardware and software (including the server, workstations, and any external cryptographic hardware modules or tokens) used in connection with providing CA Services. Access to such hardware and software shall be limited to those personnel performing in a Trusted Role as described in Section 5.2.1. Access shall be controlled through the use of; electronic access controls, mechanical combination locksets, or deadbolts. Such access controls must be manually or electronically monitored for unauthorized intrusion at all times.

5.2 Procedural Controls

5.2.1 Trusted Roles

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

5.2.2 Multiple Roles (Number of Persons Required Per Task)

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

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

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

5.2.3 Identification and Authentication for Each Role

All Issuing CA personnel must have their identity and authorization verified before they are: (i) included in the access list for the Issuing CA site; (ii) included in the access list for physical access to the system; (iii) given a Certificate for the performance of their CA role; or (iv) given an account on the PKI system. Each of these Certificates and/or accounts (with the exception of CA signing Certificates) must: (i) be directly attributable to an individual; and (ii) be restricted to actions authorized for that role through the use of CA software, operating system and procedural controls. When accessed across shared networks, CA operations must be secured, using mechanisms such as token-based strong authentication and encryption.

5.3 Personal Security Controls

5.3.1 Background and Qualifications

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

5.3.2 Background Investigation

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

5.3.3 Training Requirements

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

5.3.4 Documentation Supplied to Personnel

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

6 Technical Security Controls

6.1 Key Pair Generation and Protection

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, VSP, and RA keys must be generated in hardware tokens. Key pairs for subscribers may be generated in either hardware or software.

6.1.2 Private Key Delivery to Entity

See Section 6.1.1.

6.1.3 Subscriber Public Key Delivery to CA

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

6.1.4 CA Public Key Delivery to Users

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

The Cisco ECC Root CA Certificate Authority utilizes a secp384r1 RSA key pair. The CPS must require a minimum of 384-bit key sizes for all subscriber certificates in order to comply with this Policy.

6.2 CA Private Key Protection

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 Standards for Cryptographic Module

The "Cisco ECC Root 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 shall also use FIPS 140-2 Level 3 or higher approved cryptographic modules.

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

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 2.6 above.

6.2.3 Subscriber 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 Entry into 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 activated 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.

6.3 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 Key Replacement

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

6.3.3 Restrictions on CA's Private Key Use

The CA's signing key used for issuing certificates that conform to this Policy shall be used only for signing certificates and, optionally, CRLs or other validation service responses.

A private key used by a RA or VSP for purposes associated with its RA or VSP function shall not be used for any other purpose without the express permission of the CA.

6.4 Activation Data

There is no activation data needed or required for subscribers of the Cisco ECC Root CA because every subscriber is either a subordinate CA or an OCSP responder. In both cases, the certificates are hand-delivered and installed by agents of Cisco Systems, Inc.

6.5 Security Management Controls

6.5.1 Network Security Controls

The Issuing CA (Cisco ECC Root CA) server 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.

6.5.2 Cryptographic Module Engineering Controls

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

7 Certificates and CRL Profiles

7.1 Certificate Profile

The Cisco ECC Root CA certificate profile is obtainable by downloading the actual Root CA certificate itself from http://www.cisco.com/security/pki/certs/eccroot.cer or through correspondence to the parties listed in section 1.4.

7.2 CRL Profile

CRLs will be issued in the X.509 version 2 format. The public CPS shall identify the CRL extensions supported and the level of support for these extensions.

8 Definitions

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 person named in the certificate and the binding of that person to a particular public-private key pair.

Certification Practice Statement (CPS) - A "certification practice statement" is 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 should be provided to certificate management authorities under non-disclosure agreement.

CPS - See Certification Practice Statement.

CRL - See Certificate Revocation List.

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

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

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

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

OCSP - The Online Certificate Status Protocol (OCSP) is an Internet protocol used for obtaining the revocation status of an X.509 digital certificate.

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 and currently envisioned to be known as the Federal Policy Management Authority.

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 and retrieving certificates and other information relating to those certificates.

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

Revocation (Revoke) - To prematurely end the operational period of a certificate from a specified time forward.

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

Subject - A person 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; (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 certificate 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.