Cisco SSCA Certificate Policy and Practice Statements

Corporate Security Programs Office
Version 1.0 – October 21, 2010

Table of Contents

Version Information:
Version 1.0 – 10/21/2010:

First version of document written by Jedidiah Bowers

Approvals:

Version	Name	Title	Date
1.0	Alex Wight JP Hamilton	PKI Architect PKI Program Manager	10/22/2010 10/22/2010

1. Introduction

Cisco Systems has implemented a Certificate Authority (CA) to provide server authentication for Secure Sockets Layer (SSL) communications. The CA consists of systems, products and services that both protect the CA's private key, and manage the X.509 certificates (SSL certificates) issued from the CA. This CA, Cisco SSCA is a subordinate CA signed by IdenTrust's "DST Root CA X3" Root CA.

The purpose of this document is to describe the framework for SSL certificate use (issuance, renewal, revocation, and policies) within Cisco.

1.1 Background

A public-key certificate binds a public-key value to a set of information that identifies the entity (such as a person, organization, account, or site) 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 use, and rely upon the accuracy of, the public key distributed via that certificate (a certificate user is typically an entity that is verifying a digital signature from the certificate's subject or an entity sending encrypted data to the 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).

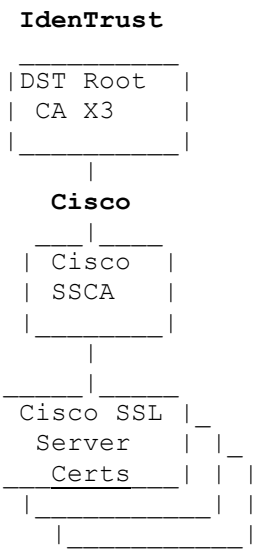
1.1.1 Cisco SSCA PKI Hierarchy

The Cisco SSCA is a subordinate CA which was signed by "DST Root CA X3", a Root CA owned and operated by IdenTrust, Inc., of San Francisco, CA (www.identrust.com).
The Cisco SSCA will only issue SSL Server certificates to hosts belonging to a Cisco-owned domain. This prevents the Cisco SSCA from

issuing an SSL Server certificate to any server whose DNS entry and IP routing is outside of Cisco's control.

The Cisco SSCA is operated in an on-line (fully networked) mode and is only accessible from the Cisco network. It is firewalled from any external network. The Cisco Information Security group is responsible for the firewall Access Control Lists, and Cisco LAN-Operations is responsible for firewall maintenance.

The current Cisco SSCA hierarchy appears below, and consists of one Root Certificate Authority (DST Root CA X3), owned and operated by IdenTrust, and the Cisco SSCA subordinate CA, owned and operated by Cisco.



1.2 Policy Identification

The IANA-assigned OID for the Cisco private enterprise is:
cisco OID :: = {iso(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) cisco(9)} **(1.3.6.1.4.1.9)**

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

cisco-pki OID ::= { cisco 21 } **(1.3.6.1.4.1.9.21)**
cisco-pki-policies OID ::= { cisco-pki 1 } **(….9.21.1)**
cisco-pki-policies-ssl OID ::= { cisco-pki-policies 1 } **(….9.21.1.1)**
cisco-pki-policies-ssl-version OID ::= { cisco-pki-policies-ssl 0 } **(….9.21.1.1.0)**

Thus, the OID representing this version of the Cisco SSCA Certificate Policy is **1.3.6.1.4.1.9.21.1.1.0**. This OID is embedded as the Policy Identifier in the X.509 v3 certificatePolicies extension of all issued SSL certificates conforming to this policy statement. Any changes in the Cisco SSCA Certificate Policy will result in an increment of the cisco-pki-policies-ssl-version OID. For example, the next version of this policy statement (v1.1) would change the CP OID to 1.3.6.1.4.1.9.21.1.1.1, and so forth.

1.2.1 Certificate Types

The Cisco SSCA issues only one type of certificates, SSL Server certificates. SSL Certificates are only issued to hosts that are part of cisco.com or a Cisco-owned domain.

1.2.1.1 Certificate Profile

The Cisco SSL Server certificate profile is specified in a separate document, obtainable through correspondence to the parties listed in section 1.4 below.

1.3 Community & Applicability

1.3.1 Certification Authorities (CAs)

This Policy is binding on each Authorized CA that issues certificates that identify this Policy, and governs its performance with respect to all certificates it issues that reference this Policy. Specific practices and procedures by which the CA implements the requirements of this Policy are set forth by the CA in this combined certificate policy ("CP") and certification practice statement ("CPS"), or by contract with a Qualified Relying Parties.

1.3.1.1 CAs Authorized to Issue Certificates under this Policy

The online subordinate CA "Cisco SSCA", owned by Cisco Systems, Inc. and operated by Cisco Systems Information Security group, is currently the only CA authorized to issue certificates under this policy.

1.3.2 Registration Authorities and Certificate Manufacturing Authorities

See Section 2.1.2.

1.3.3 Validation Services

See Section 2.1.2.

1.3.4 Subscribers

The Issuing CA may only issue certificates that reference this Policy to Employees of Cisco Systems. These individuals can include, but are not limited to, Full, Part-time, Exempt, Non-Exempt, or other employees working under the auspices of Cisco Systems, to include individual contractors.

1.3.5 Relying Parties

This Policy is intended for the benefit of the following persons who may rely on certificates that reference this Policy ("Qualified Relying 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

Certificates issued under this policy should only be used to provide server authentication to a benefiting party in the context of an SSL key exchange or "handshake".

1.4 Contact Details

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

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

Please send PKI based correspondence to
7025 Kit Creek Road
P.O. Box 14987
Research Triangle Park
Attn: J.P. Hamilton
Phone number: 919-392-1481

E-mail address: ciscopki-public@external.cisco.com

2 General Provisions

2.1 Obligations

2.1.1 CA Obligations

The Issuing 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 the subscriber, and to all Qualified Relying 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 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 this CPS.
- Information provided by the subscriber in the certificate application for inclusion in the certificate has been accurately transcribed to the certificate.
- The certificate meets all material requirements of this Policy and was processed according to this 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 Issuing 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 CPS when verifying the identity of the Certificate Holder;
- 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 all 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 CPS.

These warranties apply 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 Qualified Relying 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) the End

Entity's (a) improper use of Certificates or Key Pairs, (b) failure to safeguard Private Keys, (c) failure to comply with the provisions of this Policy or of any agreement with the Issuing CA, and/or (d) other actions giving rise to any loss; (ii) events beyond the reasonable control of the CA; and (i) 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.

2.1.1.5 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.

2.1.1.6 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 Section 5.6; (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 Section 4.9; and (iii) the address of the online certificate status database and/or CRL is defined in the issued certificate.

2.1.1.7 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 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.

2.1.1.8 Ensuring Compliance

The Issuing CA must ensure that: (i) it only accepts information from RAs 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 RA and End Entity adherence to this Policy with regard to any Certificates issued under it; and (iv) its or any RAs' authentication and validation procedures are implemented as set forth in Part 3.

2.1.2 Registration Authority (RA) Obligations

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

2.1.3 Certificate Status Validation Obligations

The CA shall be responsible for providing a means by which certificate status (valid, suspended, or revoked) can be determined by a Benefiting party. However, the CA may [delegate/subcontract] performance of this obligation to an identified validation services provider ("VSP"), provided 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 Certificate Holder who is found to have acted in a manner counter to these obligations will have his, her or its Certificate revoked, and will forfeit all claims he, she or it may have against the Issuing CA.

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 is responsible to Qualified Relying Parties for direct damages suffered by such relying parties 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 relying 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.

Except as expressly provided in this Policy and 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 shall be limited to direct damages, and shall not exceed $1000.00. The Issuing CA shall have no liability for consequential damages.

2.3 Interpretation & Enforcement

2.3.1 Governing Law

The enforceability, construction, interpretation, and validity of this Policy shall be governed by the laws of the United States and the State of California.

2.3.2 Dispute Resolution Procedures

No stipulation

2.4 Fees

The Issuing CA shall not impose any fees on the reading of this Policy and 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 this 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 Qualified Relying 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 database; (3) the CA's certificate for its signing key; (4) a copy of this Policy and CPS; and (5) 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 Qualified Relying 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 and CPS, or the CA's certificate for its signing key. 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 Qualified Relying Parties, in accordance with provisions published in this CPS or otherwise.

2.6 Compliance Audit

The Issuing CA (and each RA and 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 Infosec 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 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 Relying 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.

3. Identification and Authentication

3.1 Initial Registration

Subject to the requirements noted below, certificate applications may be communicated from the applicant to the CA or an RA, (and authorizations to issue certificates may be communicated from an RA to the CA), (1) electronically via E-mail or a web site, provided that all communication is secure, such as (1) by using a suitable cryptographic

protocol for electronic communications, (2) by first class U.S. mail, or (3) in person.

3.1.1 Types of Names

The subject name used for certificate applicants shall be the X.509 Distinguished Name consisting of an authenticated, fully qualified domain name (FQDN) placed in the common name (CN) field and the subject alternative name (SAN) field as a DNS type name. All FQDNs in the CN or SAN must be owned and controlled by Cisco.

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 numbers or letters may be appended to the real 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 SSL Server Certificate Identification and Authentication (I&A)

A SSL Server Certificate request identifying the SSL server as the subject of a Certificate may only be made by an Employee of Cisco Systems and for whom the SSL Server certificate request is attributable for the purposes of accountability and responsibility. For the I&A of the requesting Employee, the CA must follow this Policy's requirements, as outlined in section 3.1.7, for the applicable assurance level as if the Employee were applying for the certificate on his, her or its own behalf. The applicant is required to provide registration information such as SSL Server identification and any applicable attributes, public keys and contact information. The CA will also ensure the SSL Server certificate is issued only for hosts that are owned and operated by Cisco Systems or one of its subsidiaries.

3.1.7 Cisco Systems Employee I & A

If (i) the Issuing CA has previously established the identity of one of its employee, and (ii) the Issuing CA and the Employee have an ongoing, trusted business relationship sufficient to satisfy the CA of the Individual’s identity, then the CA may rely on such prior identification and ongoing relationship to satisfy the I&A requirements of this Policy and to process the request for a Certificate. In addition, the CA may deliver certificate activation data with respect to such Employee by (i) in-person delivery, based on the CA’s personal

knowledge of the Employee or reasonable identification at the time of delivery, or (ii) use of a Shared Secret between the CA and the CA's Employee, previously established in connection with the prior identification and ongoing relationship described above.

The CA will ensure that it has collected or reviewed, and kept records of the type and details of, information regarding the employee'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) first name, middle initial, and last name; (ii) street address; and (iii) home or work telephone number.

3.2 Renewal Applications

In "traditional" certificate renewal, a new Certificate is created with the same name, Public Key, and authorizations as the old one, but with a new, extended Validity Period and a new serial number. "Traditional" certificate renewals are not performed under this Policy due to the lack of support within client certificate stores and the complexity of implementing such a solution.

Renewals shall be performed under this Policy by replacing the old certificate and key pair with a new key pair and certificate. A subscriber will generate new keys and 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 this 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

A revocation request that is submitted electronically may be authenticated on the basis of a digital signature using the private key associated with the certificate whose revocation is requested. The identity of a person submitting a revocation request in any other manner shall be authenticated as per section 3.1.7 above. Other revocation request authentication mechanisms may be used as well so long as these authentication mechanisms viably detect unauthorized revocation requests.

4 Operational Requirements

4.1 Certificate Application

An applicant for a certificate shall complete a certificate application in a form prescribed by the CA and enter into a subscriber agreement with the Issuing CA. All applications are subject to review, approval and acceptance by the Issuing CA. The SSL certificate application process may only be initiated by Cisco Employees.

4.2 Certificate Issuance

Upon successful completion of the subscriber I&A process in accordance with this Policy and 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 CA shall contractually require the subscriber to indicate acceptance or rejection of the certificate to the CA, in accordance with procedures established by the CA and specified in this 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 and 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 CPS.

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

4.4.1.1 Permissive Revocation

A subscriber may request revocation of his, her, or 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 and 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, either directly or through a Registration Authority (RA). A certificate revocation request may be communicated electronically if it is digitally signed with the private key corresponding to the

certificate to be revoked. Alternatively, the subscriber may request revocation by contacting the CA or an authorized RA in person and providing adequate proof of identification in accordance with this Policy.

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 this CPS. All revocation requests and the resulting actions taken by the CA shall be archived in accordance with this CPS.

4.4.4 Revocation Request Grace Period

Requests for revocation shall be processed within the timeframe delineated in this 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 monthly, even if there are no changes or updates to be made, to ensure timeliness of information. Upon revocation, a new CRL will be issued and published within one hour. 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
- All certificate application data
- All certificates, and all CRLs or certificate status records generated
- Key histories
- All correspondence between the CA and 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

No stipulation.

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 this CPS or other appropriate documentation available to Qualified Relying 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 all affected certificates and promptly notifying all subscribers and all Qualified Relying Parties.

4.9 CA Termination

In the event that the CA ceases operation, all subscribers, RAs, VSPs, and Qualified Relying 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.

5 Physical, Procedural, and Personnel Security Controls

5.1 Physical Security -- Access Controls

The CA, and 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 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 limited capabilities commensurate with the role of the account holder.

The Issuing CA must ensure that no single individual may gain access to End Entity Private Keys stored by the Issuing CA. At a minimum, procedural or operational mechanisms 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 Issuing CA 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 accounts (with the exception of CA signing Certificates) must: (i) be directly attributable to an individual; (ii) not be shared; and (iii) 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 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 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 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 SSCA Certificate Authority utilizes a 2048-bit RSA key pair. As of December 10, 2010, all end-entity key pairs and certificates are enforced to be at least 2048-bits in length.

6.2 CA Private Key Protection
The Issuing CA shall protect its private key(s) using a FIPS 140-2 level 3 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
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 use FIPS 140-2 Level 1 or higher approved cryptographic modules.

6.2.2 Private Key Multi-Person Control (M-of-N)
No stipulation.

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.

CA Private Signing Keys may be backed up only under two-person control. The parties used for two-person control will be maintained on a list that will be made available for inspection by PKI Service Providers.

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
An entity may optionally back up its own private key.

6.2.5 Private Key Archival
An entity may optionally archive its own private key.

6.2.6 Private Key Entry into Cryptographic Module
No stipulation.

6.2.7 Method of Activating Private Key
No stipulation.

6.2.8 Method of Deactivating Private Key
No stipulation.

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
No stipulation.

6.3.2 Key Replacement
The Issuing CA key pair must be replaced as its certificate expires. RA and subscriber key pairs must be replaced not less than every two (2) years and a new certificate issued.

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
No stipulation.

6.5 Security Management Controls

6.5.1 Network Security Controls
The CA server and any repositories must be protected through application level (proxy) firewalls (or separate ports of a single firewall) configured to allow only the protocols and commands required for the secure operation of the CA's services.

6.5.2 Cryptographic Module Engineering Controls
No stipulation.

7 Certificates and CRL Profiles

7.1 Certificate Profile

The SSL certificate profile is specified in a separate document, obtainable 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. Supported CRL extensions and the level of support for them shall be identified in this combined CP and CPS document or by specific contract with a Qualified Relying Party.

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 - Means a certification authority that has been authorized by the Federal 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 Certificate Practices Statement.

CRL - See Certificate Revocation List.

EV Certificate – See Extended Validation Certificate.

Extended Validation Certificate – An SSL certificate issued under stricter guidelines and offers a greater degree of assurance that the identity being presented has been verified.

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

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

OID - See Object Identifier.

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

PIN - Personal Identification Number

PKI - Public Key Infrastructure

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

Policy - Means this Certificate Policy.

Policy Administering Organization - The entity specified in Section 1.4 and currently envisioned to be known as the Federal Policy Management Authority.

Private Key - Means 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 - Means 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.

Revoke A Certificate - Means 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 a person who (1) is the subject named or identified in a certificate issued to such person and (2) holds a private key that corresponds to a public key listed in that certificate, and (3) the person to whom digitally signed messages verified by reference to such certificate are to be attributed. See "subject."

Suspend a Certificate - Means to temporarily suspend the operational period of a certificate for a specified time period or from a specified time forward.

Trustworthy System - Means 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 - Means a certificate that: (1) a certification authority has issued; (2) the subscriber listed in it has accepted; (3) has not expired; and (4) has not been revoked. Thus, a certificate is not "valid" until it is both issued by a certification authority and has been accepted by the subscriber.

Validation Services Provider (VSP) - An entity that maintains a repository accessible to the public [or at least to relying 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.