Cisco Root CA 2048 Certification Practice Statement

Cisco Systems Certification Practice Statement

Cisco Systems has implemented Certificate Authorities (CAs) to provide a source of publicly trusted identities for clients and servers using Secure Sockets Layer (SSL) and Transport Layer Security (TLS) communications. These Certificate Authorities consist of systems, products, and services that both protect the CA's private key and manage the X.509 certificates (SSL certificates) issued from the Certificate Authority. The purpose of this document is to describe the practices that Cisco Systems follows in issuing and managing Sub-CA Certificates signed by the PKI Root Certificate Authority "Cisco Root CA 2048", and to inform potential users of Sub-CA Certificates issued by the Root CA about what they need to know prior to benefiting from the Certificates.

Cisco Root CA 2048 Certification Practice Statement

Cisco Systems Certification Practice Statement

Table of Contents

Document Metadata

Version History

Version	Date	Changes
1.1	2006-Jan-29	*First version of document*
1.2	2007-Sep-17	*Changes*
		Updated: Cover version number and date, corporate logo
		Added: "Version Information" section
		Added: "Approvals" section
		Section numbers incremented for additions of sections 1 & 2
	Section 3.3 (was 1.3)	**Deleted**: "...PKI industry practices in securing and performing its operations with regard to..." **Added**: "...the highest level of PKI industry practices in securing and performing its operations of..."
	Sections 3.4 3.4.1 3.4.1.1 3.4.1.2 3.4.2	**Added**: entire sections
	Section 4.2 (was 2.2)	**Deleted**: "...regularly archived and reviewed by security personnel..." Added: "...archived and reviewed by security personnel on an annual basis."
	Section 4.3.3 (was 2.3.3)	**Deleted**: "...periodic system backups and securely stores system recovery data offsite in order to recover from a system failure. System backups are tested for their integrity at least annually." **Added**: "...system backups, including event journal data, on at least an annual basis and securely stores this data offsite in order to recover from a system failure. System backups are tested for their integrity and event journals are reviewed at least annually." **Added**: "The geographically separate backup site is located more than 2000 miles from the primary operations center to maintain business continuity in the event of a large-scale geographic disaster."
	Section 4.3.4 (was 2.3.4)	**Deleted**: "The Root CA's Private Key is retired after 25 years from its creation date. Once a key is retired or if the key is compromised, the hardware token storing The Root CA Private Key will be re-initialized using a F IPS 140-1 approved zeroization mechanism or be physically destroyed using FIPS 140-1 methods to prevent the key from being recovered or reused." **Added**: "The Root CA's Private Key is retired seven years after its certificate expiration. Once its key is retired or if the key is compromised, the hardware token storing The Root CA Private Key will be re-initialized using the FIPS 140-1 level 3 or higher approved zeroization mechanism implemented by the hardware token manufacturer to prevent the key from being recovered or reused. Validation of the successful destruction of the private key will be performed by listing the contents of the hardware token

		using utilities provided by the hardware token manufacturer to ensure that the token ’s memory was zeroized successfully .”
	Section 4.5.1	**Added**: entire section
	Section 4	**Deleted**: entire section (moved contact info up to 3.4.2)

1.3	2016-Oct-18	*Changes*
	Section 1.1	Added "Cisco Systems has implemented Certificate Authorities (CAs) to provide a source of publicly trusted identities for clients and servers using Secure Sockets Layer (SSL) and Transport Layer Security (TLS) communications. These Certificate Authorities consist of systems, products, and services that both protect the CA's private key and manage the X.509 certificates (SSL certificates) issued from the Certificate Authority."
	Section 1.2	Deleted “or” before ‘(“CPS”)’
	Section 1.5.2	Updated contact names and email addresses.
	Section 2.2	Fixed typo "AIPCA" for "AICPA"
	Sections 2.3.1, 2.3.3, 2.3.4, 2.3.6	Updated references "FIPS 140-1" to "FIPS 140-2"
	Section 3.1	Removed "," before "take a form prescribed..."
	Section 3.5	Fixed typo "CICSO" for "CISCO"
	Appendix A	Updated terms and definitions to match current practice.

Approvals

Version	Date	Name	Title
1.2	2007-Sep-26	J.P. Hamilton	PKI Program Manager
		Alex Wight	PKI Architect
		Bill Friedman	Senior Corporate Counsel
1.3	2016-Oct-18	J.P. Hamilton	Cryptographic Services Manager
		Alex Wight	PKI Architect
		Brian Stone	Cryptographic Services Ops Manager
		Jos Purvis	Cryptographic Services Compliance

1 Introduction

1.1 Overview

Cisco Systems has implemented Certificate Authorities (CAs) to provide a source of publicly trusted identities for clients and servers using Secure Sockets Layer (SSL) and Transport Layer Security (TLS) communications. These Certificate Authorities consist of systems, products, and services that both protect the CA's private key and manage the X.509 certificates (SSL certificates) issued from the Certificate Authority. The purpose of this document is to describe the practices that Cisco Systems follows in issuing and managing Sub-CA Certificates signed by the PKI Root Certificate Authority "Cisco Root CA 2048", and to inform potential users of Sub-CA Certificates issued by the Root CA about what they need to know prior to benefiting from the Certificates.

1.2 What is a Certification Practice Statement?

A Certification Practice Statement ("CPS") explains background information for use by Benefiting Parties who utilize Certificates. A Certificate may contain a reference to a Certificate Policy ("CP") or CPS in order to enable Benefiting Parties and other interested persons to locate further information about the Certificate and the entity that issued it. This CPS is a statement of the general practices that The Root CA follows in issuing Certificates and explains what a Certificate provides and means, what a Benefiting Party and other interested persons need to do to reasonably rely on the Certificate, and how to obtain help and resolve problems regarding the Certificate. For information about particular certificates issued by The Root CA, review the applicable Certificate Policy at *http://www.cisco.com/security/pki/policies/index.html*.

1.3 Legal Obligations

The Root CA, the subscribers of the certificates it issues ("Sub-CAs", "Subscribers" or "Certificate Holders"), and those who want to utilize Certificates ("Benefiting Parties") must have a mutual understanding, usually by express agreement, concerning their rights, duties and expectations of one to another. This CPS is not a contract but rather a description and overview of what Benefiting Parties and other interested persons need to know and do to utilize Certificates issued by The Root CA. This CPS does not in and of itself specify any legally binding rights or obligations, although it may discuss contractual obligations that are set out more authoritatively in a contract or Certificate Policy. Because this document is only a simple summary of highlights from contracts and other documents regarding reliance on The Root CA Certificates, those contracts take precedence over this document.

If you do not agree to the terms and conditions of the Certificate Policy applicable to a given certificate, you may not utilize The Root CA for a determination of the certificate's validity and Cisco Systems disclaims any and all liability should you utilize the certificate.

See subsection "3.4 Enrolling as a Benefiting Party" for more information about how to enter into a contract for reliance services.

1.4 Detailed Practice Specifications

This document is a simple, user-friendly description of how to use Certificates issued from The Root CA. It is not a legal contract, nor is it a technical specification of everything The Root CA does with regard to Certificates. For most

Benefiting Parties, the technical details of how a Certificate works are not relevant or helpful. Specific contracts with Benefiting Parties usually provide the information and assurances that make it unnecessary for those parties to familiarize themselves with the details of The Root CA's certification practices, technical security measures or the operation of certification and Public Key Cryptography technology.

Cisco's certification processes are examined and approved by disinterested and widely-respected auditors and technical security experts. The findings of these experts, which are based on extensive site visits and actual observation, attest that Cisco Systems follows the highest level of PKI industry practices in securing and performing its operations of the Cisco Root CA 2048.

1.5 Certification Practice Statement Administration

This Certification Practice Statement (CPS) is administered by the Corporate Information Security group of Cisco Systems, Inc.

1.5.1 Changes to the CPS

1.5.1.1 Procedure for Changes

Changes to this CPS 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*.

1.5.1.2 Change Notification

Benefiting Parties are defined here as entities who have entered into a Certificate Trust Agreement with Cisco Systems wherein this CPS 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.

1.5.2 Contact Information

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

PKI Operations Manager:

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

Policy Management Authority:

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

1.6 Checking the Authenticity of This Document

Documents retrieved from World Wide Web sites are generally vulnerable to tampering while in transit and do not include proof of authenticity. The document you are reading now is most likely authentic and unaltered, but there is a chance that it may have been tampered with. Upon request, Cisco Systems can provide a digitally signed electronic version of this document and/or a written version.

2 Certification Practices

2.1 Trustworthiness and Operative Personnel

As a Certification Authority, Cisco's goal is to provide a trustworthy infrastructure to ensure the reliability of Digital Certificates.

In furtherance of this goal, Cisco only hires "Operative Personnel" who are trustworthy. Operative Personnel are Cisco employees who operate the systems used to issue certificates, create The Root CA's private keys and administer The Root CA's computing facilities. Cisco takes special steps to assure that these persons are qualified to act as Operative Personnel. The Root CA performs background checks on all of its Operative Personnel. The Root CA's Operative Personnel must also have sufficient knowledge of Public Key Infrastructures, asymmetric cryptosystems and the laws applicable to Certification Authorities.

2.2 Audits and Regulatory Oversight

Cisco Systems is an experienced, worldwide provider of services facilitating trustworthy electronic commerce, and is subject to regulatory oversight by federal and state authorities. The Root CA operates under the regulatory oversight and auditing of the Internal Controls Services group of Cisco Systems, reporting to the senior management of Cisco Systems, Inc. The Root CA is also audited on an annual basis by an external auditor who is certified to perform the AICPA WebTrust for CA audit on the Root CA.

The Root CA systems log security-related events in an audit log, which is archived and reviewed by security personnel on an annual basis. The Root CA is also audited annually by a well-respected accounting and information security organization. On a regular basis, Cisco examines The Root CA's computer facilities and operations for security, fault tolerance and the service commitments. These reviews, including on-site inspections, of The Root CA's operations and facilities all help to ensure high quality and reliability in certification services.

2.3 Root Key & Certificate Generation

Cisco's practices in creating The Root CA Certificate, in signing and issuing Sub-CA Certificates with The Root CA's Private Key, and in revoking invalid Certificates are crucial to the reliability and trustworthiness of Cisco's Public Key Infrastructure ("PKI"). This section explains in greater detail the technical certification practices performed by The Root CA.

2.3.1 Root Certificate and Key Pair Creation

Generation of The Root CA's Certificate and Key Pair were performed using only approved cryptographic standards published by the National Institute of Standards and Technology in Federal Information Processing Standards Publication, FIPS PUB No. 140-2, "Security Requirements for Cryptographic Modules" ("FIPS 140-2"). The protocol and procedure for Root Certificate and Key Pair generation is confidential and based on the need to ensure that Key Generation and Private Key delivery takes place in a secure and trustworthy environment. The Key Generation event is documented in writing and by other means to enable the parties to determine afterwards in a provable manner that the key generation and certificate creation occurred in a secure and trustworthy manner. All parts of the record are marked by witnesses for authentication purposes, and the record is stored in a secure location.

2.3.2 Secure Facility and System Security

All of The Root CA computer systems are located in a secure facility, are operated in an offline (non-networked) mode, and are 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.

2.3.3 Key Protection, System Backup and Business Continuity

The Root CA Private Key is heavily protected and stored in cryptographic modules that meet or exceed FIPS 140-2 Level 3 standards. The Root CA makes copies of its private Certificate-signing keys solely for backup and disaster-recovery purposes and stores all copies of The Root CA's Private Keys in a secure and trustworthy environment. Also, The Root CA makes system backups, including event journal data, on at least an annual basis and securely stores this data in order to recover from a system failure. System backups are tested for their integrity and event journals are reviewed at least annually. The Root CA also maintains a geographically separate secure site for system failover and a Business Continuity Plan ("BCP") to maintain and recover system resources and functionality in the event of a catastrophe. The geographically separate backup site is located more than 2000 miles from the primary operations center to maintain business continuity in the event of a large-scale geographic disaster.

2.3.4 Root Key Compromise

Cisco has undertaken the previously stated security measures to ensure that The Root CA's Private Key is not compromised. However, in the event that such compromise occurs, a contingency plan provides that Certificate Holders will be notified, notice will be posted on Cisco Systems' web site and in the Root CA's Certificate Revocation List ("CRL"), and contingency measures will be immediately taken to address the compromise. The Root CA's Private Key is retired seven years after its certificate expiration. Once its key is retired or if the key is compromised, the hardware token storing The Root CA Private Key will be re-initialized using the FIPS 140-2 level 3 or higher approved zeroization mechanism implemented by the hardware token manufacturer to prevent the key from being recovered or reused. Validation of the successful destruction of the private key will be performed by listing the contents of

the hardware token using utilities provided by the hardware token manufacturer to ensure that the token's memory was zeroized successfully.

2.3.5 Certificate and Validation Message Signing

The Root CA's Private Key is only used for signing Sub-CA Certificates and Certificate Revocation Lists (CRLs). The strength of The Root CA's Signing Key is equal to or greater than a 2048-bit RSA key. RSA is a public-key cryptosystem published by Ron Rivest, Adi Shamir, and Leonard Adleman.

2.3.6 Private Key Security

Cisco takes great precautions to protect The Root CA's Private Key and the Private Keys of Sub-CAs. In all cases, a Root or Sub-CA's Private Key will be generated and all copies shall remain in a hardware security module ("HSM") that meets or exceeds F IPS 140-2 Level 3 standards.

2.4 Identification and Authentication ("I&A") Practices

The Cisco Root CA 2048 issues only Subordinate CA ("Sub-CA") certificates. No end-entity certificates will be issued from the Cisco Root CA 2048.

2.4.1 Subordinate CA Certificates

The issuance process for a Sub-CA Certificate requires, at a minimum, two agents, or "Root CA Administrators" who are authorized to access the offline Root CA. These Root CA Administrators must perform a series of physical and logical I&A procedures which provide The Root CA with acceptable levels of identification and authentication. During each procedure, the respective authentication system verifies and confirms that the information provided is consistent with pre-established authentication and authorization data.

In order to become a Root CA Administrator, an employee is required to have undergone Cisco's standard Human Resources ("HR") procedures for new hires which includes verification of the following identification information: (i) government-issued photographic identification such as a driver's license, passport, or military ID; (ii) full legal name; (iii) birth date; (iv) street address; (v) home telephone number; and (vi) Social Security or other similar governmental identification number. Root CA Administrators are also put through an extensive background check for criminal history.

2.5 Certificate Revocation

Sub-CAs are required to request Revocation in the event that their Private Key has been, or is suspected to have been, compromised or if any information contained in the Certificate changes or becomes false or misleading. The Root CA revokes Sub-CA Certificates and gives notice of such Revocation within a reasonable time after receipt of a verifiable Revocation request from the Sub-CA. Revocation requests may be made directly to The Root CA for Sub-CA Certificates. Notices of Revocation are published in The Root CA's Repository. Even if there are no newly revoked Sub-CA Certificates, The Root CA publishes a Certificate Revocation List (CRL) at least on an annual basis. If a Sub-CA Certificate is revoked, The Root CA publishes a new CRL within three business days. Once published, the new CRL replaces the previous CRL . The Root CA provides CRLs solely for the convenience of Benefiting Parties who desire to use CRLs for business reasons particular to them, and does not recommend the use of a cached CRL to verify the validity of a Certificate because it does not always provide the most timely revocation information.

2.5.1 CRL Profile

All CRLs issued from The Root CA conform to the IETF / PKIX specification for x.509 version 2 CRLs. At the time of writing, this specification is located at *http://www.ietf.org/rfc/rfc3280.txt*, section 5. CRLs issued by The Root CA are valid for 1 year from the date of issuance, but will be superseded by a new CRL within 3 business days upon revocation of a subscriber.

The specific CRLv2 extensions that are populated in CRLs issued by The Root CA are as follows:

- Authority Key Identifier (non-critical) – matches the value of the Subject Key Identifier extension in the X .509v 3 certificate of The Root CA (`27f3c8151e6e9a020916ad2ba089605fda7b2faa`)
- CA Version (non-critical) – v0.0 at the time of this CPS writing.
- CRL Number (non-critical) – an incremental counter of the number of CRLs issued by The Root CA.
- Next CRL Publish (non-critical) – barring any new revocations, the date by which the next CRL will be published and available at the public repository.

3 Certificate Status Information

3.1 Determine what a Certificate Says and Means

You can use your Web Browser to view the contents of The Root CA Certificate in order to find out what the Sub-CA Certificate says and means. You can use your Web Browser to find out whether the Sub-CA Certificate has expired, and to find the location of the Repository to check for Revocation.

The Root CA Certificate and Sub-CA Certificates issued from The Root CA take a form prescribed in Internet technical standards, such as X.509 version 3 of the International Telecommunications Union. The X.509 format provides a specification for certain fields to contain human-readable information. For example, the X.509 format contains a field listing the CA's name and another field listing the CA's Public Key. Because standards such as X.509 do not define the meaning of Certificate data with sufficient clarity and precision, you cannot know exactly what the Certificate means just by looking at the Certificate. Therefore, you should also refer to *http://www.cisco.com/security/pki/policies/index.html* to review the relevant Certificate Policy applicable to The Root CA.

3.2 Checking Certificate Status

Cisco assures that the Sub-CA Certificates it issues are accurate as of the time they are issued. However, events that occur after issuance may cause some fact listed in the Certificate to be no longer true. When you receive an unexpired Sub-CA Certificate, it will not be apparent from the Certificate whether it is still valid. The Root CA revokes a Sub-CA Certificate when the Sub-CA requests Revocation or when some other worthy reason for Revocation exists, such as when the Private Key has been lost or stolen. Once revoked, a Sub-CA Certificate is permanently invalid and unreliable. To discover whether a Sub-CA Certificate has been revoked, you can check the CRL in The Root CA's Repository. It is imperative that you use, and make a record of using, a CRL to check whether a Sub-CA Certificate is still valid or has been revoked at the time of reliance on the Certificate. To make that check, you must inquire about the current validity or Revocation of the Sub-CA Certificate using the CRL distribution point identified in the Sub-CA Certificate (or as provided in your Benefiting Party Agreement).

If you choose to utilize a Sub-CA Certificate without checking the Repository for a Sub-CA Certificate's validity, you do so at your own risk.

3.3 Reasonable Reliance

Merely verifying the Digital Signature and validating a Sub-CA Certificate does not protect you from all of the risks of utilizing digitally-signed data. You are still required to use common sense in utilizing Sub-CA Certificates. This is called "Reasonable Reliance." If you have reason to doubt the authenticity of a Sub-CA, or if you suspect that anything is otherwise amiss with the Sub-CA Certificate, DO NOT utilize the Sub-CA Certificate. Instead, obtain help from The Root CA as described below. Moreover, because you must never utilize a Sub-CA Certificate that has expired or has been revoked, always check the validity of a Sub-CA Certificate. Whatever else may be required, you have an overriding obligation to act reasonably under the circumstances when you utilize a The Root CA and/or a Sub-CA Certificate from The Root CA.

3.4 Enrolling as a Benefiting Party

You may obtain information on becoming a Benefiting Party by contacting the CA Policy Authority listed in section 1.5.2 below.

3.5 DISCLAIMER OF LIABILITY

EXCEPT AS OTHERWISE SPECIFIED HEREIN, C IS C O SYSTEMS, INC. DISCLAIMS ANY AND ALL REPRESENTATIONS AND WARRANTIES OF ANY TYPE WITH RESPECT TO ANY SUB-CA CERTIFICATE ON WHICH YOU MAY RELY, WHETHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, AND NONINFRINGEMENT.

IF YOU CHOOSE TO UTILIZE A CERTIFICATE WITHOUT ACCEPTING AND HONORING THE TERMS AND CONDITIONS OF SUCH USE (AS SPECIFIED IN A CERTIFICATE, CERTIFICATE POLICY OR RELYING PARTY AGREEMENT), YOU DO SO AT YOUR OWN PERIL AND ASSUME ALL ASSOCIATED RISK, AND IN NO CIRCUMSTANCE SHALL CISCO SYSTEMS, INC. BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, SPECIAL, OR INCIDENTAL DAMAGES, WHETHER IN CONTRACT OR IN TORT, EVEN IF CISCO SYSTEMS, INC. HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Appendix A: Definitions and Acronyms

Activation Data:

Data that is required to access or operate cryptographic modules (e.g., Personal Identification Numbers or "PINs").

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.

Applicant

A Person who initiates the Registration Process in order to obtain a digital certificate.

Application

A designated software program or set of programs.

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

CA Services

Services relating to the creation, issuance, or management of certificates by CAs. These services are set forth in this CPS and in the applicable PKI documents.

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 Policy

A set of rules which indicates the applicability of a named Certificate to a particular community and/or PKI implementation.

Certificate Revocation List (CRL)

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

Certification Authority

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

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

Certification Practice Statement (CPS)

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

CPS

See Certification Practice Statement.

CRL

See Certificate Revocation List.

Digital Signature

The data produced by transforming an electronic record using Public Key Cryptography and the Private Key of the signer of the record, so that a Benefiting Party, having the original electronic record, the data produced by the transformation process, and the signer's Public Key, can accurately determine: (i) whether the data produced by the transformation process was generated using the Private Key that corresponds to the signer's Public Key; and (ii) whether the original electronic record has been altered since the transformation.

Distinguished Name (DN)

Distinguished Names (DNs) are used in Certificates and in an X.500-based Repository to uniquely represent Subjects identified in Certificates.

End-Entity

The entity that controls the private key corresponding to the public key embedded in a digital certificate that is not a CA certificate.

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.

HSM

See Hardware Security Module

Hardware Security Module (HSM)

A hardware device used to provide secure cryptographic processing capabilities and secure storage of cryptographic private keys.

I&A

See Identification and Authentication.

Identification and Authentication ("I&A")

The process set forth in an applicable Authentication Policy, CPS, and/or applicable Certificate Policy for ascertaining and confirming the identity of any Applicant requesting a certificate through appropriate inquiry and investigation.

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.

Issuing CA

The CA identified in the "Issuer Distinguished Name " field of a particular Certificate.

Key-pair

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

Object Identifier

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

OID

See Object Identifier.

Operational Period of a Certificate

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

Organization

A legal entity, a group of Persons working for a common business purpose, or a sole proprietorship.

Organizational Unit

A sub-group or unit within an Organization.

PIN
Personal Identification Number

PKI
See "Public Key Infrastructure".

PKI Implementation
An application or other system involving the use of Public Key Cryptography and X.509 digital Certificates.

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

Person
A living human being.

Policy
This Certificate Policy document.

Policy Administering Organization
The entity specified in section 1.4.

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

Program Participants
This term includes all CAs, RAs, Repositories, Sub-CAs, Benefiting Parties, and the PKI Review Board. It does not include Applicants.

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.

Public Key Cryptography
A type of cryptography, also known as asymmetric cryptography, which uses a unique Public/Private Key Pair of mathematically related numbers. The holder of the Key Pair may make the Public Key available to anyone who wishes to use it, while the holder must keep the Private Key secret. One of the keys can be used to encrypt information or generate a Digital Signature, but only the other corresponding key can decrypt that information or verify that Digital Signature.

Public Key Infrastructure (PKI)
A set of hardware, software, people, procedures, rules, policies, and obligations used to facilitate the trustworthy creation, issuance, management, and use of Certificates and keys based on Public Key Cryptography.

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).

Registration Process: The process, for obtaining a Certificate, implemented by the RA i n accordance with the obligations imposed on the RA i n this CPS and the applicable PKI documents.

Repository

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

Responsible Individual

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

Revocation (Revoke)

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

Sponsor

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

Subject

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

Subordinate Certificate Authority (Sub-CA)

A Certificate Authority whose behavior is constrained by a more authoritative CA, and whose key-pair key is certified by that more authoritative CA.

Subscriber

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

Subject

The Person, Device, System, or Application named in the Subject Distinguished Name “SubjectDN” field of a Certificate.

Suspension (suspend)

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

System

A physically distinct hardware processing platform.

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.