



FOR PUBLIC DISTRIBUTION

**AOL[®] Root Certifier
Certificate Policy
and
Certification Practice Statement**

AOL LLC
22000 AOL Way
Dulles VA 20166 USA
IT Security Department

© Copyright 2008 AOL LLC. All rights reserved.

AOL LLC hereby permits each person having a copy of a certificate issued by the AOL root certifier to copy this document in its entirety as necessary for its own use but not to distribute or publish it to any other person, or to make any derivative work.

AOL is a registered trademark of AOL LLC.

All trademarks, service marks, and copyrights are property of their respective owners.

Contents

1	Introduction	1
1.1	Overview	1
1.2	Document name and identification	1
1.3	PKI participants.....	2
1.3.1	Certification authorities.....	2
1.3.2	Registration authorities.....	2
1.3.3	Subscribers	2
1.3.4	Relying Parties	2
1.4	Certificate usage.....	2
1.4.1	Appropriate certificate uses.....	2
1.4.2	Prohibited certificate uses	2
1.5	Policy administration.....	2
1.5.1	Organization administering the document.....	2
1.5.2	Contact person	2
1.5.3	Person determining CPS suitability for the policy.....	3
1.5.4	CPS approval procedures	3
1.6	Definitions and acronyms	3
2	Publication and Repository Responsibilities	4
2.1	Repositories.....	4
2.2	Publication of certification information	4
2.3	Time or frequency of publication.....	5
2.4	Access controls on repositories	5
3	Identification and Authentication	5
3.1	Naming	5
3.1.1	Types of names.....	5
3.1.2	Need for names to be meaningful	5
3.1.3	Anonymity or pseudonymity of Subscribers	5
3.1.4	Rules for interpreting various name forms	5
3.1.5	Uniqueness of names.....	5
3.1.6	Recognition, authentication, and role of trademarks	6
3.2	Initial identity validation.....	6
3.2.1	Method to prove possession of private key	6
3.2.2	Authentication of organization identity.....	6
3.2.3	Authentication of individual identity	6
3.2.4	Non-verified Subscriber information	6
3.2.5	Validation of authority.....	6
3.3	Identification and authentication for re-key requests	6
3.3.1	Identification and authentication for routine re-key.....	6
3.3.2	Identification and authentication for re-key after revocation.....	6
3.4	Identification and authentication for revocation request	6
4	Certificate Life-cycle Operational Requirements.....	7
4.1	Certificate Application	7
4.1.1	Who can submit a certificate application	7
4.1.2	Enrolment process and responsibilities.....	7
4.2	Certificate application processing	7
4.2.1	Performing identification and authentication functions	7
4.2.2	Approval or rejection of certificate applications	7
4.2.3	Time to process certificate applications	7
4.3	Certificate issuance	7
4.3.1	AOL Root Certifier actions during certificate issuance	7
4.3.2	Notification to AOLCA by the AOL Root Certifier of issuance of certificate.....	8
4.4	Certificate acceptance	8
4.4.1	Conduct constituting certificate acceptance	8
4.4.2	Publication of the certificate by the AOL Root Certifier	8
4.4.3	Notification of certificate issuance by the AOL Root Certifier to other entities	8
4.5	Key pair and certificate usage	9
4.5.1	AOLCA private key and certificate usage.....	9
4.5.2	Relying party public key and certificate usage	9

4.6	Certificate renewal	9
4.6.1	Circumstance for certificate renewal	9
4.6.2	Who may request renewal.....	9
4.6.3	Processing certificate renewal requests.....	9
4.6.4	Notification of new certificate issuance to Subscriber	9
4.6.5	Conduct constituting acceptance of a renewal certificate	9
4.6.6	Publication of the renewal certificate by the AOL Root Certifier.....	9
4.6.7	Notification of certificate issuance by the AOL Root Certifier to other entities	9
4.7	Certificate re-key.....	9
4.7.1	Circumstance for certificate re-key	10
4.7.2	Who may request certification of a new public key	10
4.7.3	Processing certificate re-keying requests.....	10
4.7.4	Notification of new certificate issuance to Subscriber	10
4.7.5	Conduct constituting acceptance of a re-keyed certificate	10
4.7.6	Publication of the re-keyed certificate by the AOL Root Certifier	10
4.7.7	Notification of certificate issuance by the AOL Root Certifier to other entities	10
4.8	Certificate modification	10
4.9	Certificate revocation and suspension.....	10
4.9.1	Circumstances for revocation.....	10
4.9.2	Who can request revocation.....	11
4.9.3	Procedure for revocation request	11
4.9.4	Revocation request grace period	11
4.9.5	Time within which AOL Root Certifier must process the revocation request.....	11
4.9.6	Revocation checking requirement for relying parties	11
4.9.7	CRL issuance frequency	12
4.9.8	Maximum latency for CRLs	12
4.9.9	On-line revocation/status checking availability.....	12
4.9.10	On-line revocation checking requirements	12
4.9.11	Other forms of revocation advertisements available	12
4.9.12	Special requirements regarding key compromise	12
4.9.13	Circumstances for suspension	12
4.9.14	Who can request suspension	12
4.9.15	Procedure for suspension request	12
4.9.16	Limits on suspension period.....	13
4.10	Certificate status services.....	13
4.10.1	Operational characteristics.....	13
4.10.2	Service availability.....	13
4.10.3	Optional features.....	13
4.11	End of subscription	13
4.12	Key escrow and recovery	13
4.12.1	Key escrow and recovery policy and practices	13
4.12.2	Session key encapsulation and recovery policy and practices	13
5	Facility, Management, and Operational Controls.....	13
5.1	Physical controls.....	13
5.1.1	Site location and construction	13
5.1.2	Physical access.....	14
5.1.3	Power and air conditioning	14
5.1.4	Water exposures	14
5.1.5	Fire prevention and protection.....	14
5.1.6	Media storage.....	15
5.1.7	Waste disposal	15
5.1.8	Off-site backup	15
5.2	Procedural controls.....	15
5.2.1	Trusted roles	15
5.2.2	Number of persons required per task.....	15
5.2.3	Identification and authentication for each role	15
5.2.4	Roles requiring separation of duties.....	15
5.3	Personnel controls.....	16
5.3.1	Qualifications, experience, and clearance requirements.....	16
5.3.2	Background check procedures.....	16
5.3.3	Training requirements	16

5.3.4	Retraining frequency and requirements	17
5.3.5	Job rotation frequency and sequence	17
5.3.6	Sanctions for unauthorized actions	17
5.3.7	Independent contractor requirements	17
5.3.8	Documentation supplied to personnel	17
5.4	Audit logging procedures	17
5.4.1	Types of events recorded	17
5.4.2	Frequency of processing log	17
5.4.3	Retention period for audit log	18
5.4.4	Protection of audit log	18
5.4.5	Audit log backup procedures	18
5.4.6	Audit collection system (internal vs. external)	18
5.4.7	Notification to event-causing subject	18
5.4.8	Vulnerability assessments	18
5.5	Records archival	18
5.5.1	Types of records archived	18
5.5.2	Retention period for archive	19
5.5.3	Protection of archive	19
5.5.4	Archive backup procedures	19
5.5.5	Requirements for time-stamping of records	19
5.5.6	Archive collection system (internal or external)	19
5.5.7	Procedures to obtain and verify archive information	19
5.6	Key changeover	19
5.7	Compromise and disaster recovery	19
5.7.1	Incident and compromise handling procedures	20
5.7.2	Computing resources, software, and/or data are corrupted	20
5.7.3	AOL Root Certifier private key compromise procedures	20
5.7.4	Business continuity capabilities after a disaster	21
5.8	AOL Root Certifier termination	21
6	Technical Security Controls	21
6.1	Key pair generation and installation	21
6.1.1	Key pair generation	21
6.1.2	Private key delivery to Subscriber	21
6.1.3	Public key delivery to certificate issuer	22
6.1.4	AOL Root Certifier public key delivery to relying parties	22
6.1.5	Key sizes	22
6.1.6	Public key parameters generation and quality checking	22
6.1.7	Key usage purposes (as per X.509 v3 key usage field)	22
6.2	Private Key Protection and Cryptographic Module Engineering Controls	22
6.2.1	Cryptographic module standards and controls	22
6.2.2	Private key (n out of m) multi-person control	22
6.2.3	Private key escrow	23
6.2.4	Private key backup	23
6.2.5	Private key archival	23
6.2.6	Private key transfer into or from a cryptographic module	23
6.2.7	Private key storage on cryptographic module	23
6.2.8	Method of activating private key	23
6.2.9	Method of deactivating private key	23
6.2.10	Method of destroying private key	23
6.2.11	Cryptographic Module Rating	23
6.3	Other aspects of key pair management	23
6.3.1	Public key archival	23
6.3.2	Certificate operational periods and key pair usage periods	24
6.4	Activation data	24
6.4.1	Activation data generation and installation	24
6.4.2	Activation data protection	24
6.4.3	Other aspects of activation data	24
6.5	Computer security controls	24
6.5.1	Specific computer security technical requirements	24
6.5.2	Computer security rating	25
6.6	Life cycle technical controls	25

6.6.1	System development controls	25
6.6.2	Security management controls	26
6.6.3	Life cycle security controls	26
6.7	Network security controls	26
6.8	Time-stamping	26
7	Certificate, CRL, and OCSP Profiles	26
7.1	Certificate profile	26
7.1.1	Version number(s)	26
7.1.2	Certificate extensions	26
7.1.3	Algorithm object identifiers	27
7.1.4	Name forms	27
7.1.5	Name constraints	29
7.1.6	Certificate policy object identifier	29
7.1.7	Usage of Policy Constraints extension	29
7.1.8	Policy qualifiers syntax and semantics	29
7.1.9	Processing semantics for the critical Certificate Policies extension	29
7.2	CRL profile	29
7.2.1	Version number(s)	30
7.2.2	CRL and CRL entry extensions	30
7.3	OCSP profile	30
7.3.1	Version number(s)	30
7.3.2	OCSP extensions	30
8	Compliance Audit and other Assessments	31
8.1	Frequency or circumstances of assessment	31
8.2	Identity/qualifications of assessor	31
8.3	Assessor's relationship to assessed entity	31
8.4	Topics covered by assessment	31
8.5	Actions taken as a result of deficiency	31
8.6	Communication of results	31
9	Other Business and Legal Matters	32
9.1	Fees	32
9.1.1	Certificate issuance or renewal fees	32
9.1.2	Certificate access fees	32
9.1.3	Revocation or status information access fees	32
9.1.4	Fees for other services	32
9.1.5	Refund policy	32
9.2	Financial responsibility	32
9.2.1	Insurance coverage	32
9.2.2	Other assets	32
9.2.3	Insurance or warranty coverage for end-entities	32
9.3	Confidentiality of business information	32
9.3.1	Scope of confidential information	32
9.3.2	Information not within the scope of confidential information	32
9.3.3	Responsibility to protect confidential information	33
9.4	Privacy of personal information	33
9.4.1	Privacy plan	33
9.4.2	Information treated as private	33
9.4.3	Information not deemed private	33
9.4.4	Responsibility to protect private information	33
9.4.5	Notice and consent to use private information	33
9.4.6	Disclosure pursuant to judicial or administrative process	33
9.4.7	Other information disclosure circumstances	33
9.5	Intellectual property rights	33
9.5.1	Relying Party Obligations	33
9.5.2	Representations and warranties of other Participants	34
9.6	Disclaimers of warranties	34
9.7	Limitations of liability	34
9.8	Indemnities	35
9.9	Term and termination	35
9.9.1	Term	35
9.9.2	Termination	35

9.9.3	Effect of termination and survival	35
9.10	Individual notices and communications with Participants	35
9.11	Amendments.....	35
9.11.1	Procedure for amendment.....	35
9.11.2	Notification mechanism and period	35
9.11.3	Circumstances under which OID must be changed	35
9.12	Dispute resolution provisions	36
9.13	Governing law.....	36
9.14	Miscellaneous provisions.....	36
9.14.1	Entire agreement.....	36
9.14.2	Assignment.....	36
9.14.3	Severability	36
9.14.4	Enforcement (attorneys' fees and waiver of rights)	36
9.14.5	Force Majeure	36
9.15	Other provisions.....	36
10	References.....	36

AOL Root Certifier

Certificate Policy and Certification Practice Statement

1 Introduction

1.1 Overview

This document (termed the “CP/CPS”) is the combined certificate policy and certification practice statement of the AOL Root Certifier, which is the issuer of public key certificates to AOLCAs and possibly¹ other certifiers in the public key infrastructure of the AOL system. All certificates issued by an AOLCA for use in that public key infrastructure are ultimately verifiable by reference to a certificate issued by the AOL Root Certifier. The AOL Root Certifier does not issue any certificates to AOL Members or other end users; it issues only final root certificates and certificates listing AOLCAs as their subjects. Some certificates issued by the AOL Root Certifier are distributed in popular operating systems such as Microsoft Windows[®] and Apple Mac OS X[®].

For simplicity, all certificate-related policies and practices of the AOL Root Certifier appear in a single document, this CP/CPS. This document assumes a more limited and technically expert audience than comparable documents of AOLCAs serving Members and other end users.

This document is a statement of how AOL intends to conduct its activities as the AOL Root Certifier and specifies the overall framework for AOL’s public key certification services. The AOL Root Certifier does not prescribe or require compliance with any rules or policies². Rather, the AOL Root Certifier provides a means by which the authenticity of certificates issued by AOLCAs can be verified. More specifically, the authenticity of a certificate issued by an AOLCA is verifiable by reference to a certificate issued to the AOLCA. That AOLCA certificate is in turn verifiable by reference to another certificate, a final root certificate, which AOL publishes as described in section 2.2.

Certificates issued by the AOL Root Certifier are useful in verifying the authenticity of certificates issued by an AOLCA. Persons do have occasion to rely on a certificate issued by the AOL Root Certifier without also relying on a certificate issued by an AOLCA.

This CP/CPS is subject to change by AOL from time to time, as AOL deems appropriate in its sole discretion. Certain internal operational procedures relating to the AOL Root Certifier are not disclosed in order to avoid unnecessarily jeopardizing the security of the AOL root certification infrastructure.

1.2 Document name and identification

This CP/CPS applies to every certificate issued by the AOL Root Certifier regardless of whether this CP/CPS is expressly listed in such a certificate. In particular, it may not be listed in final root certificates.

If a certificate issued by the AOL Root Certifier lists this CP/CPS, it does so in one of the following ways:

- 1) By listing the object identifier of this CP/CPS (“1.3.6.1.4.1.1066.1.101.2”) in the *certificatePolicies* field, as defined in section 4.2.1.5 of [RFC 3280];³
- 2) By listing the URL of the applicable version of this CP/CPS in the certificate’s *cpsURI* subfield of its *certificatePolicies* field, as defined in section 4.2.1.5 of [RFC 3280].

In addition to AOL’s copyright in this document, AOL holds a copyright in each object identifier (“OID”) assigned by AOL. Only the AOL Root Certifier may use a copyrighted object identifier listed in this CP/CPS.

¹ The AOL public key infrastructure (PKI) may evolve to include certifiers other than AOLCAs and the AOL root certifier.

² AOL manages its certification processes and their quality through internal controls that are not publicly disclosed. AOL does not ordinarily disclose its internal security rules and management structures outside of its organization.

³ If an AOLCA does not wish to limit the set of policies under which it issues certificates, it may list the “anyPolicy” OID (“2.5.29.32.0”) instead, per [RFC 3280].

1.3 PKI participants

This CP adheres to the structure laid out in RFC 3647, "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework", © 2003 by the Internet Society, in order to facilitate comparison with other Certificate Policies and to ease interoperability between the certificates issued by different CAs, thereby promoting electronic commerce.

1.3.1 Certification authorities

A PKI Root is a special type of CA. A Root serves as a trust anchor for a PKI and its associated subordinate CAs by issuing certificates to CAs. In general, the Root of a PKI is self signed but it may be cross certified with other Roots or CAs.

The AOL Root Certifier does not issue certificates to end users. It issues only:

- Final root certificates, in which both subject and issuer are the AOL Root Certifier; and
- Certificates listing an AOLCA as the subject.

An AOLCA is defined as: AOL in its role as certification service provider for AOL PKI services, as well as any other entity authorized by AOL to perform that role. The AOLCAs issue certificates to their participants.

1.3.2 Registration authorities

There are no dedicated registration authorities. Registration is performed by the AOL Root Certifier.

1.3.3 Subscribers

Subscribers to the AOL Root Certifier are the AOLCAs.

1.3.4 Relying Parties

A person or system that receives a certificate identifying a subject and that is in a position to act in reliance upon that certificate and/or information verified using the certificate.

1.4 Certificate usage

1.4.1 Appropriate certificate uses

The AOL Root Certifier issues two types of certificates:

- **Certificates issued by the AOL Root Certifier to itself:** These are either final root certificates or certificates used for the internal operation of the AOL system.
- **Certificates issued to AOLCAs:** These enable a participant to check the authenticity of the certificates issued to them by AOLCAs.

Certificates issued by the AOL Root Certifier shall be used by the AOLCAs for issuing end entity certificates.

1.4.2 Prohibited certificate uses

No stipulation.

1.5 Policy administration

1.5.1 Organization administering the document

AOL has adopted this CP/CPS through its PKI Policy Management Authority.

1.5.2 Contact person

Any notices or correspondence relative to this CP/CPS may be sent to the

AOL Root Certifier Administrator,
pki-info@aol.net.

1.5.3 Person determining CPS suitability for the policy

AOLs PKI Policy Management Authority is responsible for the suitability of this CP/CPS.

1.5.4 CPS approval procedures

This CP/CPS is under continuous review and is subject to amendment by the AOL PKI Policy Management Authority.

1.6 Definitions and acronyms

Within this CP/CPS and in any contract, certificate profile, or other document incorporating these definitions by reference, the following terms have the meanings indicated:

(1) **AOL**. "AOL" means AOL LLC, a Delaware corporation, and any entity in which AOL LLC controls directly or indirectly at least 50% of the equity or ownership interest.

(2) **AOLCA**: AOL in its role as certification service provider for AOL PKI services, as well as any other entity authorized by AOL to perform that role.

(3) **AOL Member Security PKI**: The name for the particular AOL system used to enable certain security-related products and services that rely on the issuance, management and/or use of digital certificates and other cryptographic capabilities described in the AOL Member Security PKI CP/CPS.

(4) **AOL system**: The network and related infrastructure managed and/or operated by or for AOL in order to provide information, entertainment, communications, and transactional services to Members, including without limitation the AOL Member Security PKI. The AOL system also consists of the network and infrastructure used to extend any such services (or portion thereof) to its customers, partners and affiliates.

(5) **Certificate**: A digital record which:

- (a) contains a public key (possibly in a form encoded pursuant to applicable technical standards);
- (b) either lists a subject or refers to a subject listed in other records available to its issuer; and
- (c) is digitally signed by its issuer.

(6) **Certificate request**: A data record containing information to be included in a certificate and signed by the subject-to-be of that certificate using the private key corresponding to the public key to be certified.

(7) **Certificate revocation list (CRL)**: A time-stamped and digitally signed list identifying revoked certificates issued by a certifier.

(8) **Certifier**: A person (including a company) that issues a certificate.

(9) **Confirm**: To substantiate through the exercise of reasonable care the accuracy of a factual representation to be included in a certificate.

(10) **CP/CPS**: This document, which specifies the policies and practices of the public key infrastructure of AOL.

(11) **Final root certificate**: A certificate which:

- (a) is issued by a root certifier to itself (*i.e.* the root certifier is issuer and subject);
- (b) is signed by the root certifier as issuer, and thus verifiable by the public key listed in the certificate's own *subjectPublicKeyInfo* field; and
- (c) terminates a certificate verification chain (*i.e.* is not verifiable by reference to another certificate); except that a certificate issued by the AOL Root Certifier to itself and used for internal AOL operations is not a final root certificate for purposes of this document.

(12) **Member**: A person who has registered to use any service or product offered through the AOL system pursuant to a Member Agreement, e.g. Terms of usage, Terms of Service.

(13) **Member Agreement**: A written contract establishing the terms and conditions under which a user may obtain access to and/or use any product or service offered through the AOL system.

(14) **Participant**: A Subscriber or Relying Party.

(15) **Publish**: To make information widely available for reference and retrieval, such as by posting it on the World Wide Web.

(16) **Relying party**: A person or system that receives a certificate identifying a subject and that is in a position to act in reliance upon that certificate and/or information verified using the certificate.

(17) **Revoke a certificate**: To include the certificate in a class of certificates that are no longer valid regardless of when they expire. See section 4.9.

(18) **Subject**: A person or device that is the subject of a certificate, *i.e.* listed in the *subject* field of the certificate as described in section 7.1.4.2.

(19) **Valid certificate**: A certificate which, at a given time:

- (a) Has been issued by the issuer listed in it;
- (b) Has not yet expired as indicated by its *validity:notAfter* field; and
- (c) Has not been revoked.

2 Publication and Repository Responsibilities

Because final root certificates are the ultimate reference point for verifying the authenticity of other certificates (see 1.3.1), it is important that they be available throughout the public key infrastructure(s) that AOL provides to participants.

2.1 Repositories

AOL's root certifier operates a repository to support the PKI operations. AOL shall ensure interoperability with common standards so that Relying Parties may obtain certificates and CRLs from or through that repository.

The repository shall be available as required by the certificate information posting and retrieval stipulations of this CP/CPS.

The repository shall be subject to access control mechanisms to protect its availability and information as described in later sections.

2.2 Publication of certification information

The AOL Root Certifier makes its final root certificates widely available by publishing them in at least one of the following ways:

- As part of the process of installing other AOL software;
- By download when Members log into the AOL Service;
- By download from <https://pki-info.aol.com/AOL>;
- By inclusion with applications such as Java and OpenSSL, or operating systems such as Microsoft Windows® and Apple Macintosh OS® X.

The content of the AOL Root Certifier's final root certificates can be checked by comparing the content of a copy of the certificate against the content published at <https://pki-info.aol.com/AOL>. It may also be possible to corroborate the authenticity of a final root certificate using the operating system in which it is distributed or its distribution media; this depends on the features of the operating system.

Certificates issued from the AOL Root Certifier to AOLCAs are published in the repository.

This CP/CPS shall be published in the repository.

2.3 Time or frequency of publication

AOLs root certifier issues certificates to AOLCAs only. Therefore, it is sufficient to update the information in the repository and the CRLs on a yearly basis.

In addition, updates are performed whenever a certificate is issued to an AOLCA, or when such a certificate is revoked.

This CP/CPS and any subsequent changes shall be made publicly available within one week of approval.

2.4 Access controls on repositories

Only authorized personnel shall be able to publish or modify any information referred to in section 2.2.

The repository shall not contain information not intended for public dissemination.

The repository shall be made publicly available through the Internet.

3 Identification and Authentication

In order to obtain a certificate, any AOLCA must apply for a certificate, and identify and authenticate itself to the AOL Root Certifier. This section covers these topics.

3.1 Naming

3.1.1 Types of names

The AOL Root Certifier shall only generate and sign AOLCA certificates that contain a non-null subject Distinguished Name (DN) complying with the X.500 standard. Details may be found in the certificate profiles set forth later in this CP/CPS.

3.1.2 Need for names to be meaningful

Names used in the AOLCA certificates shall unambiguously identify the AOLCAs to which they are assigned.

The Common Name (CN) shall observe name space uniqueness requirements.

Names shall never be misleading. This does not preclude the use of pseudonymous Certificates as defined in Section 3.1.3.

3.1.3 Anonymity or pseudonymity of Subscribers

The AOL Root Certifier shall not issue anonymous certificates. The AOL Root Certifier may issue pseudonymous certificates to AOLCAs to support their operations. However, it is required that the CN of an AOLCA is an unambiguous name identifying the subject in the records of the AOL Root Certifier. This name may not be meaningful to anyone but the AOL Root Certifier.

3.1.4 Rules for interpreting various name forms

No stipulation.

3.1.5 Uniqueness of names

Any AOLCA DN in a X.509 certificate issued by the AOL Root Certifier must uniquely identify a single AOLCA among all of the AOLCAs. If necessary, the AOL Root Certifier may append additional numbers or letters to an actual name in order to ensure the name's uniqueness.

The same AOLCA may have different certificates all bearing the same subject DN, but no two separate AOLCAs may share a common DN. In any case, there must not be two X.509 certificates having the same issuer DN and serial number

3.1.6 Recognition, authentication, and role of trademarks

N/A.

The AOL Root Certifier issues certificates only to AOLCAs.

3.2 Initial identity validation

3.2.1 Method to prove possession of private key

In order to prove an AOLCA's possession of the Private Key corresponding to the Public Key contained in a certificate application, any certificate request submitted for a signature certificate shall be self-signed. Upon generating a key pair, an AOLCA creates a certificate request, signs it with the newly generated private key, and forwards it to the AOL Root Certifier.

3.2.2 Authentication of organization identity

Requests for AOLCA certificates must include the organization name, address, documentation of the existence of the organization, identity-proofing of the requesting organization agent, and proof of the agent's authorization to act on behalf of the organization. The AOL Root Certifier shall verify the information, the authenticity of the requesting representative and the representative's authorization to act in the name of the organization.

3.2.3 Authentication of individual identity

N/A.

The AOL Root Certifier issues certificates only to AOLCAs.

3.2.4 Non-verified Subscriber information

Information that is not verified will not be included in AOLCA certificates.

3.2.5 Validation of authority

The AOL Root Certifier shall issue certificates to AOLCAs only after ascertaining that the (human) applicant has the authorization to act on behalf of the organization in the asserted capacity.

3.3 Identification and authentication for re-key requests

Certificate re-key may be performed in case the existing key can no longer be used. Examples are:

- The key is comprised and the certificate has to be revoked,
- The existing certificate has expired.

Rekey means changing the Public Key for an existing certificate by issuing a new certificate with a *different* (usually new) Public Key. The certificate name stays the same. It is different from renewal, which means issuing a new certificate, with an extended validity period, for the *same* Public Key.

3.3.1 Identification and authentication for routine re-key

AOLCAs shall identify themselves through by using the initial identity-proofing process described in section 3.2.2 above.

3.3.2 Identification and authentication for re-key after revocation

After an AOLCA certificate has been revoked, the AOLCA shall generate a new key pair and reapply for a new certificate by going through the initial identity-proofing process described in section 3.2.2 to obtain a new certificate.

3.4 Identification and authentication for revocation request

The AOL Root Certifier revokes a certificate issued to an AOLCA when the AOLCA requests it and after confirming the authenticity of the request. The identification and authentication is identical to the initial certificate application. See section 3.2.

4 Certificate Life-cycle Operational Requirements

4.1 Certificate Application

4.1.1 Who can submit a certificate application

The AOL root certifier issues certificates only to AOLCAs (except for final root certificates). It retains absolute discretion to determine whether to issue a certificate to a prospective AOLCA or a company wishing to be an AOLCA. The exercise of its discretion whether to certify is objective but not subject to disclosure or review.

4.1.2 Enrolment process and responsibilities

When applying for certification the prospective AOLCA shall be responsible for providing accurate information in their application for certification. Upon creation, each AOL Root Certifier certificate and AOLCA certificate shall be manually checked to ensure each field and extension is properly populated with the correct information before the certificate is delivered and published.

A prospective AOLCA shall provide all required information by completing and submitting a certificate application.

After receiving the application the AOL Root Certifier shall check the application for errors and omissions. Pursuant to section 3.2.1, the CA shall perform the proof of possession of the private key (e.g., verify digital signature on the self-signed AOLCA certificate request).

All prospective AOLCAs must follow industry best practices for maintaining secure operations of their CA and protecting the data they store. AOLCAs should also endeavor to make their CPS available to their Relying Parties and Participants.

The AOL Root Certifier does not issue a certificate to an AOLCA if the report of the AOLCA's most recent Webtrust® for Certification Authorities (or equivalent) audit was unsatisfactory or indicated substantial noncompliance with the AOL Member Security PKI CP/CPS.

The AOL Root Certifier shall then initiate the identification and authentication process as described in section 3.2.

4.2 Certificate application processing

Having received an application an AOLCA shall begin to process the application. This shall include the verification of accuracy and correctness of all relevant data.

4.2.1 Performing identification and authentication functions

The identity-proofing for AOLCAs shall meet the requirements specified in this CP/CPS in section 3.2.

4.2.2 Approval or rejection of certificate applications

The AOL Root Certifier shall either approve the application and issue the prospective AOLCA's certificate upon successful completion of the identity-proofing process or reject the application and inform the prospective AOLCA about any problems or inconsistencies. If in doubt the AOL Root Certifier may contact the AOL PKI Policy Management Authority.

4.2.3 Time to process certificate applications

No stipulation.

4.3 Certificate issuance

4.3.1 AOL Root Certifier actions during certificate issuance

The AOL Root Certifier issues certificates only to AOLCAs (except for final root certificates). It retains absolute discretion to determine whether to issue a certificate to an AOLCA or a company wishing to be an AOLCA. The exercise of its discretion whether to certify is objective but not subject to

disclosure or review. Nevertheless, all prospective AOLCAs must follow industry best practices for maintaining secure operations of their CA and protecting the data they store.

Upon receiving a certificate request from a prospective AOLCA, the AOL Root Certifier confirms the accuracy of the information to be certified, as described in section 3. If the AOL Root Certifier can complete that confirmation and determines in its discretion to issue the requested certificate, it creates and signs a certificate using one of its certified private keys. It then sends the certificate to the AOLCA that requested it. That AOLCA accepts the certificate and then can begin issuing certificates signed by the corresponding private key.

The AOL Root Certifier shall verify, as set forth in section 3.2.1, that the applying AOLCA is in possession of the Private Key and that the certificate request has the proper contents. The AOL Root Certifier verifies the data contained in the request according to this CP/CPS.

The AOL Root Certifier generates certificates using the appropriate certificate format, and sets validity periods and extension fields in accordance with relevant standards, such as X.509.

All certificates are checked to ensure that all fields and extensions are properly populated.

After generation, verification, and acceptance, the AOL Root Certifier posts the certificate as set forth in section 4.4.2 and publishes it in the repository.

4.3.2 Notification to AOLCA by the AOL Root Certifier of issuance of certificate

The AOL Root Certifier either issues the AOLCA's certificate upon successful completion of the vetting process and notifies the AOLCA about the issuance of the certificate, or informs the AOLCA about any problems or inconsistencies.

After a certificate has been issued, the AOL Root Certifier informs the AOLCA that the certificate is available and makes the certificate available to the AOLCA.

Certificates are made available to AOLCAs either by allowing them to download the certificates from a web site or via a message containing the certificate. For example, a URL may be sent, describing where the AOLCA can obtain the certificate. The certificate may also be sent to the AOLCA in an e-mail message.

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

Downloading a certificate or installing a certificate from a message (see section 4.3.2) constitutes the AOLCA's receipt of the certificate.

Usage of the Private Key by the AOLCA, corresponding to a certificate issued under this CP/CPS, shall be deemed to be acceptance of the certificate.

By accepting a certificate the AOLCA warrants that all of the information provided by the AOLCA (and by its organization, where applicable) and included in the certificate, and all representations made by the AOLCA (and by its organization, where applicable) as part of the application and identification process, are true and not misleading.

4.4.2 Publication of the certificate by the AOL Root Certifier

As specified in section 2.2, the AOLCA certificates shall be published in a publicly accessible repository.

The AOL Root Certifier makes issued certificates available to participants immediately after the certificate has been issued. This includes the AOL Root Certifier certificates.

4.4.3 Notification of certificate issuance by the AOL Root Certifier to other entities

There is no explicit notification to other entities. Certificates are published as specified in section 4.4.2.

4.5 Key pair and certificate usage

4.5.1 AOLCA private key and certificate usage

AOLCAs shall generate, store, and protect their private keys as specified in their respective CP and/or CPS and other documentation.

AOLCAs shall use their keys in accordance with the applicable CP and/or CPS.

4.5.2 Relying party public key and certificate usage

The AOL Root Certifier issues information specifying the current status of all unexpired AOLCA certificates. Relying Parties must process and comply with this information.

Certificates issued by the AOL Root Certifier are useful in verifying the authenticity of certificates issued by an AOLCA. Persons do have occasion to rely on a certificate issued by the AOL Root Certifier without also relying on a certificate issued by an AOLCA. AOLCAs issue certificates that are typically tied to a particular service or feature that uses these certificates. Relying parties of these certificates are required to comply with the terms of service or other agreements of the respective service.

4.6 Certificate renewal

Certificate renewal consists of issuing a new certificate with a new validity period and serial number while retaining all other information in the original certificate including the Public Key.

Certificate renewal is not supported.

4.6.1 Circumstance for certificate renewal

Certificate renewal is not supported.

4.6.2 Who may request renewal

Certificate renewal is not supported.

4.6.3 Processing certificate renewal requests

Certificate renewal is not supported.

4.6.4 Notification of new certificate issuance to Subscriber

Certificate renewal is not supported.

4.6.5 Conduct constituting acceptance of a renewal certificate

Certificate renewal is not supported.

4.6.6 Publication of the renewal certificate by the AOL Root Certifier

Certificate renewal is not supported.

4.6.7 Notification of certificate issuance by the AOL Root Certifier to other entities

Certificate renewal is not supported.

4.7 Certificate re-key

Re-keying a certificate consists of creating new certificates with a different Public Key (and serial number) while retaining the remaining contents of the old certificate that describe the subject. The new certificate may be assigned a different validity period, key identifiers, specify a different CRL distribution point, and/or be signed with a different key.

4.7.1 Circumstance for certificate re-key

The AOL Root Certifier may issue a new certificate to an AOLCA when the AOLCA has generated a new key pair and is entitled to a certificate in accordance with this CP/CPS.

4.7.2 Who may request certification of a new public key

An AOLCA may request re-key of its certificate.

4.7.3 Processing certificate re-keying requests

An AOLCA replaces its CA certificate by generating a new key pair and requesting a new certificate (section 4.1). AOL may arrange for or facilitate replacement of the certificate using one or more of the publication methods explained in section 4.4.2. The timing and sequence of these actions may vary depending on the circumstances.

4.7.4 Notification of new certificate issuance to Subscriber

Identical to section 4.3.2.

4.7.5 Conduct constituting acceptance of a re-keyed certificate

Identical to section 4.4.1.

4.7.6 Publication of the re-keyed certificate by the AOL Root Certifier

Identical to section 4.4.2.

4.7.7 Notification of certificate issuance by the AOL Root Certifier to other entities

Identical to section 4.4.3.

4.8 Certificate modification

Certificate modification is not supported.

4.9 Certificate revocation and suspension

If an AOLCA certificate is revoked, it becomes invalid as soon as the AOL Root Certifier has processed the revocation request. The certificate's serial number and time of revocation shall be included in the Certificate Revocation List, and subsequent status inquiries to the certificate repository shall result in a response citing the certificate as invalid.

Certificate suspension is not supported for certificates issued by the AOL Root Certifier.

4.9.1 Circumstances for revocation

The AOL Root Certifier revokes a certificate issued to an AOLCA when the AOLCA requests it and after confirming the authenticity of the request.

The AOL Root Certifier also revokes a certificate that it has issued if it has sufficient reason to believe that the certificate is unreliable or if the AOLCA that is the subject of the certificate ceases to participate in the AOL PKI.

In the event that the AOL Root Certifier revokes a certificate that it has issued, the AOL Root Certifier publishes notice that the certificate is revoked by posting a certificate revocation list at the URL listed in the *CRLdistributionPoints* field of the certificate in question. Access to this certificate revocation list is unrestricted.

4.9.2 Who can request revocation

The AOL PKI Policy Management Authority may request revocation of the AOL Root Certifier certificate and any AOLCA certificate issued by the AOL Root Certifier as stipulated in section 4.9.1.

An AOLCA may request the revocation of its CA certificate.

4.9.3 Procedure for revocation request

A request to revoke a certificate shall identify the certificate to be revoked, explain the reason for revocation, and allow the request to be authenticated (e.g., digitally or manually signed). The AOL Root Certifier shall authenticate the request as well as the authorization of the requester.

There are several ways to submit a revocation request:

1. The AOLCA may call the AOL Root Certifier by phone and authenticate by using a pre-shared secret (e.g. revocation password) chosen when submitting the initial certificate application.
2. If the AOLCA provided the signature of one or more representatives during the initial application process, the AOLCA may request its certificate to be revoked by writing a letter to the AOL Root Certifier stating this request. Authentication is then provided by the signature of an authorized representative of the AOLCA. The AOLCA representative's signature on the revocation request must match a signature provided during the initial application process.
3. Additional procedures may be agreed upon between the AOL Root Certifier and AOLCAs.

4.9.4 Revocation request grace period

There is no revocation grace period. The AOL Root Certifier and AOLCAs or their authorized representatives are required to request the revocation of a certificate immediately after the need for revocation comes to their attention.

4.9.5 Time within which AOL Root Certifier must process the revocation request

The unreliability of a certificate issued by the AOL Root Certifier may affect the reliability of other certificates depending on the time when the certificate became unreliable in relation to the validity period of the other certificates. For example, if a certificate's authenticity is verifiable by reference to a root certificate and that root certificate becomes questionable, the first certificate's authenticity may thereby become questionable as well. The seriousness of that sort of consequent unreliability and the relative timing of the unreliable effect of one certificate on another may be uncertain and depend a great deal on the circumstances. The AOL Root Certifier may advise or require an AOLCA to revoke certificates issued by it if their reliability is compromised. However, which certificates are affected by problems with an AOLCA certificate or key, and the seriousness of those problems, may vary considerably and will depend on the circumstances.

The timing and sequence of these actions may vary depending on the circumstances.

4.9.6 Revocation checking requirement for relying parties

Any relying party's reliance on a certificate issued by the AOL Root Certifier must be reasonable and exercise ordinary business prudence under the circumstances and must conform to the following obligations:

- Validate the certificate (i.e., confirm that it has not expired or been revoked or suspended), by checking the published revocation list;
- Verify that a valid certificate chain is established between the relying party and the subject. A valid chain means that the certificate signatures have been validated back to a final root certificate and the revocation list has been checked to determine the validity of each certificate.

4.9.7 CRL issuance frequency

Certificate status information shall be made available to all relevant entities through Certificate Revocation Lists (CRLs) that shall be available from the repository of the CA that issued the certificate (AOL Root Certifier or AOLCA).

Each CRL shall be digitally signed so that entities can validate the integrity of the CRL and the date of issuance, and it shall include a monotonically increasing sequence number.

The AOL Root Certifier shall issue CRLs at least once per year.

In addition, a new CRL shall be published immediately whenever an AOLCA certificate is revoked.

If the AOL Root Certifier key is compromised, an emergency CRL shall be issued within 24 hours.

4.9.8 Maximum latency for CRLs

No stipulation.

4.9.9 On-line revocation/status checking availability

The AOL Root Certifier issues CRLs.

Any changes committed to the repository shall be immediately available to any Participant and / or Relying Party.

The certificate status can be checked on-line from the relevant certificate repository. The AOL Root Certifier's Web sites shall contain information about additional means for validating a certificate's status, if such additional means are available.

4.9.10 On-line revocation checking requirements

It is the responsibility of the Relying Party to obtain the latest CRL from the AOL Root Certifier and check the revocation status of an AOLCA.

In order to check the integrity and authenticity of a CRL a Relying Party must be in possession of or obtain the appropriate AOL Root Certifier's CRL signing certificate. This certificate may differ from the certificate that issued the AOLCA certificate being checked, and if so, it shall be available from the web site of the AOL Root Certifier.

4.9.11 Other forms of revocation advertisements available

No stipulation.

4.9.12 Special requirements regarding key compromise

No stipulation.

4.9.13 Circumstances for suspension

Suspension of AOL Root Certifier certificates is not supported.

Suspension of AOLCA certificates is not supported.

4.9.14 Who can request suspension

Suspension of AOL Root Certifier certificates is not supported.

Suspension of AOLCA certificates is not supported.

4.9.15 Procedure for suspension request

Suspension of AOL Root Certifier certificates is not supported.

Suspension of AOLCA certificates is not supported.

4.9.16 Limits on suspension period

Suspension of AOL Root Certifier certificates is not supported.

Suspension of AOLCA certificates is not supported.

4.10 Certificate status services

No stipulation beyond section 4.9.9.

4.10.1 Operational characteristics

No stipulation.

4.10.2 Service availability

Relying Parties are bound to their obligations and the stipulations of this CP/CPS irrespective of the availability of the certificate status service.

4.10.3 Optional features

No stipulation.

4.11 End of subscription

Certificates that have expired prior to or upon termination of an AOLCA are not required to be revoked.

Unexpired AOLCA certificates shall be revoked upon termination of the AOLCA.

4.12 Key escrow and recovery

This CP/CPS prohibits escrow or recovery of CA signing keys.

4.12.1 Key escrow and recovery policy and practices

Key escrow is not supported.

4.12.2 Session key encapsulation and recovery policy and practices

Not supported.

5 Facility, Management, and Operational Controls

5.1 Physical controls

The AOL Root Certifier endeavours to operate according to the generally accepted practices and procedures in the internet service industry. More specifically, it substantially complies with the Webtrust® for Certification Authorities Criteria and the requirements imposed by ETSI TS 102042.

The AOL Root Certifier shall impose physical security requirements specified in Section 5.1.2.

5.1.1 Site location and construction

The location and construction of the facility housing AOL Root Certifier equipment shall be consistent with facilities used to house high value, sensitive information. The site location and construction, when combined with other physical security protection mechanisms such as guards and intrusion sensors, shall provide robust protection against unauthorized access to the AOL Root Certifier and records.

5.1.2 Physical access

AOL Root Certifier equipment is always protected from unauthorized access. The equipment is protected from unauthorized access at any time. Physical access controls are implemented to reduce the risk of equipment tampering even when cryptographic equipment is not installed and activated.

The security mechanisms shall be commensurate with the level of threat in the equipment environment.

Physical security mechanisms are in place to:

- Permit no unauthorized access to the hardware;
- Store all removable media and paper containing sensitive plain-text information in secure containers;
- Monitor, either manually or electronically, for unauthorized intrusion at all times;
- Maintain and periodically inspect an access log; and
- Require two-person physical access control to all sensitive computer systems and cryptographic equipment as Hardware Security Modules (HSMs).

Removable HSMs must be inactivated prior to storage. When not in use, removable cryptographic hardware and activation information used to access or enable HSMs used by the AOL Root Certifier is placed in secure containers. Activation data must either be memorized, or recorded and stored in a manner commensurate with the security afforded by the HSMs, and shall not be stored with HSMs.

Whenever the facility is left unattended (e.g. during the night) a security check of the facility housing the AOL Root Certifier equipment shall occur. At a minimum, the check shall verify the following:

- All equipment is in a state appropriate to the current mode of operation;
- Any security containers are properly secured;
- Physical security systems (e.g., door locks, windows,...) are functioning properly; and
- The area is secured against unauthorized access.

A group of persons is made explicitly responsible for making such checks. A log identifying the last person leaving the location is maintained.

The last person to depart has to activate all peripheral alarming systems. The alarming system is configured in such a way that it can only be activated if all necessary physical protection mechanisms are in place and activated (e.g. all windows and relevant doors are locked and all sensors are active).

The alarming system in combination with the access control system automatically logs date and time of its activation.

When activated the alarming system is directly connected to a security company and the next police station.

5.1.3 Power and air conditioning

No stipulation.

The AOL Root Certifier is an off-line CA. Permanent availability is not required.

On-line servers (e.g., those hosting the repository and CRLs) are provided with uninterruptable power supply to support either a smooth shutdown of their operations or to re-establish commercial power.

5.1.4 Water exposures

The AOL Root Certifier and the systems hosting the repository have reasonable precautions taken to minimize the impact of water exposure.

5.1.5 Fire prevention and protection

The AOL Root Certifier and the systems hosting the repository have industry standard fire prevention and protection mechanisms in place.

5.1.6 Media storage

AOL Root Certifier media is stored so as to protect it from accidental damage (such as water, fire, electromagnetic, etc.). Media that contains audit, archive, or backup information is duplicated and stored in a location separate from the AOL Root Certifier.

5.1.7 Waste disposal

Sensitive waste material is disposed of in a secure fashion.

5.1.8 Off-site backup

No stipulation.

5.2 Procedural controls

The AOL Root Certifier's operating procedures are documented and maintained. Procedural controls ensure that no single person acting by itself will be able to circumvent the security measure taken.

Formal management responsibilities and procedures exist to control all changes to CA equipment, software, and operating procedures.

Development and testing facilities are separated from operational facilities. Procedures exist and are followed for reporting software malfunctions. Procedures exist and are followed to ensure that faults are reported and corrective action is taken. Users of CA systems are required to note and report observed or suspected security weaknesses in or threats to systems or services. System documentation is protected from unauthorized access.

Capacity demands are monitored and projections of future capacity requirements made to ensure that adequate processing power and storage are available.

Detection and prevention controls to protect against viruses and malicious software and appropriate user awareness procedures are implemented.

A formal reporting procedure exists and is followed, together with an incident response procedure, setting out the action to be taken on receipt of an incident report. Incident management responsibilities and procedures exist and are followed to ensure a quick, effective, and orderly response to security incidents.

5.2.1 Trusted roles

Duties and areas of responsibility are segregated in order to reduce opportunities for unauthorized modification or misuse of information or services. This is achieved, for example, by defining different roles so that performing certain essential tasks requires multiple individuals from different roles. Examples of roles are: System Operator, System Administrator, CA Manager, CA Operator, CA Administrator, Auditor, and IT Security Officer.

5.2.2 Number of persons required per task

All activities at the AOL Root Certifier system require (at least) dual control. Backup and activation of the AOL Root Certifier CA certificate signing Private Key requires dual control.

Generation of AOL Root Certifier certificate signing Private Keys requires at least participation of three individuals.

5.2.3 Identification and authentication for each role

An individual in a trusted role must identify and authenticate him/herself before being permitted to perform any actions related to operating the AOL Root Certifier system.

5.2.4 Roles requiring separation of duties

The role concept is enforced by the AOL Root Certifier system. Especially for activation the HSM protecting the AOL Root Certifier signing keys at least two different roles are required.

Individual personnel are specifically designated to the roles.

Individuals may not assume more than one role except for the following restrictions:

- An individual assigned an IT Security Officer role may also be assigned an Auditor role, and vice versa.
- An individual assigned the CA Operator role may also be assigned a System Operator role, and vice versa.
- An individual assigned the CA Administrator role may also be assigned a System Administrator role, and vice versa.

No individual shall be assigned more than one identity.

Under no circumstances shall any PKI entity perform its own compliance auditor function.

5.3 Personnel controls

5.3.1 Qualifications, experience, and clearance requirements

All persons filling trusted roles and personnel involved in issuing, managing, and revoking certificates and managing related data and information are selected on the basis of loyalty, trustworthiness, and integrity.

This includes, but is not limited to, requiring a certificate issued by the police or other qualified entity, stating that the individual in question has no criminal record whatsoever. Persons filling trusted roles must have proper knowledge and experience related to CA operations and must have demonstrated security consciousness and awareness regarding their duties for the AOL Root Certifier. Periodic reviews occur to verify the continued trustworthiness of all personnel. Employees have to sign a confidentiality (nondisclosure) agreement as part of their initial terms and conditions of employment.

All employees involved in the operation of the AOL Root Certifier receive appropriate training in organizational policies and procedures.

A formal disciplinary process exists and is followed for employees who have violated organizational security policies and procedures. The AOL Root Certifier's corporate policies and procedures specify the sanctions against personnel for unauthorized actions, unauthorized use of authority, and unauthorized use of systems.

Appropriate and timely actions are taken when an employee is terminated so that controls and security are not impaired by such an occurrence.

5.3.2 Background check procedures

Relevant personnel involved in the operation of the AOL Root Certifier shall, at a minimum, pass a background investigation covering the following areas:

- Employment;
- Education;
- Place of residence;
- Law Enforcement; and
- References.

The extent to which these investigations are performed is restricted by the applicable local legislation.

5.3.3 Training requirements

All personnel performing duties with respect to the operation of the CA shall receive comprehensive training. Training shall be conducted in the following areas:

- CA security principles and mechanisms;
- Use and operation of all PKI associated equipment;

- PKI software versions in use on the AOL Root Certifier;
- All PKI duties an individual is expected to perform.

5.3.4 Retraining frequency and requirements

Individuals responsible for trusted roles regarding the AOL Root Certifier shall be aware of changes in the AOL Root Certifier's operation. Any significant change to the operations shall have a training (awareness) plan, and the execution of such plan shall be documented. Examples of such changes are software or hardware upgrade, changes in automated security systems, and relocation of equipment.

5.3.5 Job rotation frequency and sequence

No stipulation.

5.3.6 Sanctions for unauthorized actions

Appropriate administrative and disciplinary actions are taken against personnel who perform unauthorized actions (i.e., not permitted by this CP/CPS or other policies) involving the AOL Root Certifier and its repository.

5.3.7 Independent contractor requirements

Contractor personnel employed to perform functions pertaining to the AOL Root Certifier is subject to the same requirements as AOL staff performing similar functions (c.f. section 5.3 and subsections thereof).

5.3.8 Documentation supplied to personnel

The AOL Root Certifier makes available to its personnel this CP/CPS, applicable system operations documents, operations procedures documents, and any relevant statutes, policies or contracts required to perform their jobs.

5.4 Audit logging procedures

As part of the scheduled system back up procedures, audit trail files are backed up to WORM media. Audit trail files are archived by the system administrator before system shutdown. Event journals are reviewed when the system is powered up.

No single person may modify or even delete audit trails or system log files, and access to them is strictly restricted.

5.4.1 Types of events recorded

The AOL Root Certifier keeps audit trails and system log files that document actions taken as part of its services. These include, but are not limited to: issuance of certificates, issuance of CRLs, notification of key compromise, revocation of certificates, establishment of trusted roles and actions of trusted personnel, changes of AOL root keys.

In addition, system access and use is monitored and recorded in audit logs or written down in event journals. Thus all personnel are accountable for their activities. Audits logs and event journals are reviewed regularly and archived to assist in future investigations of security-related incidents.

5.4.2 Frequency of processing log

The AOL Root Certifier is an off-line CA. It is activated only if a new AOLCA certificate has to be issued, if a new CRL has to be issued due to the regular CRL schedule (once per year), or if an AOLCA certificate has to be revoked and a new CRL must be issued to reflect this revocation.

Most of the time the AOL Root Certifier is shut down and does not generate any logs.

There is no fixed frequency for processing logs. Log files are inspected whenever the AOL Root Certifier is activated.

5.4.3 Retention period for audit log

Audit logs are retained for 1 year to comply with necessary external audit efforts. Logs may be retained shorter or longer as deemed necessary by the AOL Policy Management Authority.

5.4.4 Protection of audit log

System configuration and operating procedures shall ensure that:

- Only authorized people have read access to the logs;
- Audit logs are not modified.

The entity performing audit log archive (in general, this is the Auditor role) need not have modify access, but procedures must be implemented to protect archived data from destruction prior to the end of the audit log retention period (note that deletion may require modification access). Audit logs shall be moved to a safe, secure storage location separate from the component equipment.

5.4.5 Audit log backup procedures

Audit logs shall be backed up immediately before the AOL Root Certifier system is shutdown.

5.4.6 Audit collection system (internal vs. external)

Audit collection is internal because the AOL Root Certifier is an off-line CA. Audit processes are invoked at system startup, and cease at system shutdown. Should it become apparent that the system audit has failed, and the integrity of the system or confidentiality of the information protected by the system is at risk, then the IT Security Officer (see section 5.2.1) shall be notified, and the AOL Root Certifier's operation shall be suspended until the problem is remedied.

5.4.7 Notification to event-causing subject

No stipulation.

5.4.8 Vulnerability assessments

No stipulation because the AOL Root Certifier is an off-line system.

5.5 Records archival

AOL Root Certifier archive records shall be sufficiently detailed to establish the proper operation of the AOL Root Certifier, or the validity of any AOLCA certificate (including those revoked or expired) issued by the AOL Root Certifier.

5.5.1 Types of records archived

At a minimum, the following data shall be recorded for archive:

- This CP/CPS
- Contractual obligations
- System and equipment configuration
- Modifications and updates to system or configuration
- Certificate requests
- Revocation requests
- All certificates issued or published

- Record of AOL Root Certifier re-key
- All CRLs issued and/or published
- All Audit Logs
- Documentation required by compliance auditors

5.5.2 Retention period for archive

AOL Root Certifier archive records are retained for a period of at least 10 years.

5.5.3 Protection of archive

Only authorized individuals are permitted to add to or delete from the archive. The archived records may be moved to another medium when authorized by the Auditor.

The contents of the archive shall not be released except as determined by the AOL PKI Policy Management Authority, the AOL Root Certifier, or as required by law.

5.5.4 Archive backup procedures

Audit trails and system log files (see section 5.4) are backed up regularly on WORM (write once, read multiple) media and archived in a safe facility. Backup is performed before an AOL Root Certifier system is shutdown.

5.5.5 Requirements for time-stamping of records

No stipulation.

5.5.6 Archive collection system (internal or external)

No stipulation.

5.5.7 Procedures to obtain and verify archive information

Archive information is automatically created by the AOL Root Certifier system. Archive information is held on the AOL Root Certifier system and, additionally, backed up to WORM media (see section 5.5.4). Archive information is verified before and after issuance of an AOLCA certificate and before and after issuance of a CRL.

5.6 Key changeover

To minimize risk from compromise of AOL Root Certifier's signing private key, that key shall be changed from time to time. Once changed, only the new key shall be used for AOLCA certificate signing purposes. The older, but still valid, certificate will be available to verify old signatures until all of the AOLCA certificates signed by the associated private key have expired.

Upon the end of the AOL Root Certifier private key's lifetime, a new AOL Root Certifier signing key pair is generated and all subsequently issued certificates and CRLs will be signed with the new private AOL Root Certifier signing key.

Aside from minimizing the risk of key compromise, changing the AOL Root Certifier's keys enables AOL to adjust key parameters, taking into account advances in science and / or technology.

Any new AOL Root Certifier public key is available by request via e-mail or from AOL's repository at <https://pki-info.aol.com/AOL> and <https://pki-info.aol.com/AOLTW>.

5.7 Compromise and disaster recovery

This CP/CPS does not define the period of time that is an acceptable system outage time in the event of a major natural disaster or other technical malfunction. The AOL Root Certifier is an off-line system, which is activated only if a new AOLCA certificate or a new CRL are to be issued. Both functions are not time-critical.

Backups of essential business information and AOL Root Certifier system software are performed before the AOL Root Certifier is shutdown (compare section 5.5.4).

5.7.1 Incident and compromise handling procedures

AOL, and any third party managed service providers for AOLCAs shall be required to notify the AOL PKI Policy Management Authority and all AOLCAs if any of the following cases occur:

- suspected or detected compromise of the AOL Root Certifier;
- physical or electronic attempts to penetrate the AOL Root Certifier;
- denial of service attacks on the AOL Root Certifier;
- any incident preventing the AOL Root Certifier from issuing a CRL within 24 hours of the time specified in the next update field of its currently valid CRL.

The AOL Root Certifier shall re-establish operational capabilities as quickly as practical in accordance with procedures set forth this CP/CPS.

If the AOL Root Certifier detects a potential hacking attempt or other form of compromise, it shall perform an investigation in order to determine the nature and the degree of damage. If the AOL Root Certifier signing key is suspected of compromise, the procedures outlined in Section 5.7.3 will be followed. Otherwise, the scope of potential damage shall be assessed in order to determine if the AOL Root Certifier needs to be rebuilt, only some certificates need to be revoked, and/or the AOL Root Certifier key needs to be declared compromised.

5.7.2 Computing resources, software, and/or data are corrupted

The AOL Root Certifier shall maintain backup copies of its databases and private keys in order to rebuild the signing capability in case of software and/or data corruption.

Because the AOL Root Certifier is an off-line system with no guaranteed response time, redundant system hardware is not required.

When computing resources, software, and/or data are corrupted, the AOL Root Certifier shall respond as follows:

- If the AOL Root Certifier signature keys are not destroyed, operation shall be re-established, giving priority to the ability to generate certificate status information within the CRL issuance schedule specified in section 4.9.7.
- If the AOL Root Certifier signature keys are destroyed, operation shall be re-established as quickly as possible, giving priority to the generation of a new AOL Root Certifier key pair.

5.7.3 AOL Root Certifier private key compromise procedures

In case of a key compromise of the AOL Root Certifier, the AOLCAs shall be informed about this fact.

The unreliability of a certificate issued by the AOL Root Certifier (i.e. the self-signed AOL Root Certifier certificate or an AOLCA certificate signed by the AOL Root Certifier) may affect the reliability of other certificates depending on the time when the certificate became unreliable in relation to the validity period of the other certificates. For example, if a certificate's authenticity is verifiable by reference to the AOL Root Certifier and that root certificate becomes questionable, the first certificate's authenticity may thereby become questionable as well.

The seriousness of that sort of consequent unreliability and the relative timing of the unreliable effect of one certificate on another may be uncertain and depend a great deal on the circumstances. The AOL Root Certifier may advise or require an AOLCA and its end-users to remove the trusted self-signed AOL Root Certifier certificate and to install a new one (distributed via secure out-of-band mechanisms).

However, which certificates are affected by problems with the AOL Root Certifier certificate or key, and the seriousness of those problems, may vary considerably and will depend on the circumstances. The AOL Root Certifier and AOLCAs have absolute discretion in determining the extent to which the unreliability of a root certificate affects other certificates and in determining whether and when to replace those certificates.

5.7.4 Business continuity capabilities after a disaster

In the case of a disaster whereby the AOL Root Certifier installation is physically damaged and all copies of the AOL Root Certifier signing key are destroyed as a result, the AOL Root Certifier shall inform all AOLCAs that it will not be able to issue a new CRL with the same CRL signing key as before. The AOL Root Certifier shall generate a new self-signed root key; the AOLCAs and their users will have to install this root key and the associated certificate as a new trust anchor.

If any CA equipment is damaged or rendered inoperative, but the CA signing keys are not destroyed, the CA operation shall be re-established as quickly as possible and in a secure fashion, giving priority to the ability to generate a new CRL.

Directories containing certificates and certificate status information are deployed so as to provide high availability. Features are implemented to provide high levels of directory reliability.

5.8 AOL Root Certifier termination

The AOL Root Certifier can only be terminated by AOL. In the case of termination, AOL shall inform all associated AOLCAs that were certified by the AOL Root Certifier. The AOLCAs shall be given as much advance notice as circumstances permit. The AOLCAs shall react in a manner defined in their respective CPSs.

Before the AOL Root Certifier terminates its services, all AOLCA certificates that have not expired or have not been revoked by the respective AOLCA shall be revoked by the AOL Root Certifier. A final CRL shall be published and made available for at least as long as the validity period of the AOLCA certificate with the longest validity period indicates. The CRL nextUpdate date of this final CRL shall be past the expiration dates of all certificates issued by the AOL Root Certifier.

6 Technical Security Controls

Only a FIPS 140-1/2 module may be used to protect AOL Root Certifier and AOLCA key materials. Before a FIPS 140-1/2 module is first used, the module shall be validated.

6.1 Key pair generation and installation

AOLCAs generate their own key pairs and store their private keys as specified in their respective CP/CPS and other documentation. The AOL Root Certifier generates its own key pair.

6.1.1 Key pair generation

The AOL Root Certifier generates its key pairs used for signing and verifying AOLCA certificates:

- In accordance with its operational standards listed in section 5;
- By means of hardware security modules certified under FIPS 140-1/2 Level 3 or greater and which are operated by authorized AOL personnel or, in some cases, contractors acting under their supervision; and
- In a procedure documented in a key generation script carried out by or under the supervision of AOL personnel and archived securely for as long as the corresponding certificate is valid.

The private keys are retained either in the hardware security module in which they were generated or are stored in secure hardware tokens to which access is limited to AOL personnel and contractors. The private keys are also backed up and stored offline in a secure facility.

Immediately after generating a key pair, the hardware security module creates a certificate request and signs it, using the private key just created. The AOL Root Certifier receives and verifies that certificate request, and then issues a certificate to itself with the content specified in section 7.1.

6.1.2 Private key delivery to Subscriber

N/A.

AOLCAs generate their own keys.

6.1.3 Public key delivery to certificate issuer

An AOLCA generates its key pairs and stores its private keys as specified in its CP/CPS and other documentation.

Upon generating a key pair, an AOLCA creates a certificate request, signs it with the newly generated private key, and forwards it to the AOL Root Certifier in a secure way.

6.1.4 AOL Root Certifier public key delivery to relying parties

Because final root certificates are the ultimate reference point for verifying the authenticity of other certificates, it is important that they be available throughout the public key infrastructure(s) that AOL provides to Participants. The AOL Root Certifier makes its final root certificates widely available by publishing them in at least one of the following ways:

- As part of the process of installing other AOL software;
- By download when Members log into the AOL Service;
- By download from <https://pki-info.aol.com/AOL>;
- By inclusion with applications such as Java and OpenSSL, or operating systems such as Microsoft Windows® and Apple Macintosh OS® X.

The content of the AOL Root Certifier's final root certificates can be checked by comparing the content of a copy of the certificate against the content published at <https://pki-info.aol.com/AOL>. It may also be possible to corroborate the authenticity of a final root certificate using the operating system in which it is distributed or its distribution media; this depends on the features of the operating system.

6.1.5 Key sizes

All AOL Root Certifier and AOLCA keys shall be at least 2048 bit RSA.

6.1.6 Public key parameters generation and quality checking

Public key parameters prescribed in the Digital Signature Standard (DSS) shall be generated in accordance with FIPS 186-2 or equivalent.

Parameter quality checking (including primality testing for prime numbers) shall be performed in accordance with FIPS 186 or equivalent.

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

AOL Root Certifier and AOLCA certificates must set the following key usage bits: *cRLSign* and *keyCertSign*.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic module standards and controls

The relevant standard for cryptographic modules is FIPS PUB 140-2, *Security Requirements for Cryptographic Modules*.

The minimum requirement for cryptographic modules storing AOL Root Certifier keys or AOLCA keys is Level 3; higher levels may be used.

6.2.2 Private key (n out of m) multi-person control

Use of AOL Root Certifier private signing keys requires action by at least two persons in accordance with requirements of Section 5.2.2.

6.2.3 Private key escrow

Under no circumstances shall AOL Root Certifier signing keys be escrowed.

6.2.4 Private key backup

Under no circumstances shall the AOL Root Certifier signing private keys be backed up in clear.

The AOL Root Certifier signing private keys shall be backed up under the same multi-person control as the original signing key. A backup copy of any private keys shall be kept at the CA backup location using a FIPS 140-2 Level 3 (or higher) HSM.

Procedures for AOLCA signing private key backup shall be identified in the relevant CPS.

6.2.5 Private key archival

Signing private keys shall not be escrowed or archived by the AOL Root Certifier.

6.2.6 Private key transfer into or from a cryptographic module

AOL Root Certifier private keys must be generated in FIPS 140-1/2 Level 3 (or equivalent) compliant Hardware Security Modules and remain in the same HSM. The AOL Root Certifier private keys may be backed up in accordance with section 6.2.4.

6.2.7 Private key storage on cryptographic module

Hardware cryptographic modules may store private keys in any form as long as the keys are accessible only with a FIPS 140-2, Level 2 authentication mechanism.

6.2.8 Method of activating private key

The private key user has to be authenticated to the cryptographic module before the activation of any private key(s). Acceptable means of authentication include but are not limited to pass-phrases, PINs and/or tokens. Entry of activation data such as passwords and PINs is to be protected from disclosure (i.e., the data is not to be displayed while it is entered; where video surveillance is present, cameras are positioned in such a way that they do not record PINs and passwords).

6.2.9 Method of deactivating private key

After use, private keys are deactivated by deactivating the cryptographic module and the AOL Root Certifier.

6.2.10 Method of destroying private key

The AOL Root Certifier's signing private keys will be destroyed when they are no longer needed or when the certificates to which they correspond expire or are revoked.

Destruction may be achieved by executing a "zeroize" command on the hardware cryptographic module storing the private key or by physical destruction of the hardware cryptographic module.

6.2.11 Cryptographic Module Rating

See section 6.2.1.

6.3 Other aspects of key pair management

6.3.1 Public key archival

All public keys are archived as part of the certificate archive process.

6.3.2 Certificate operational periods and key pair usage periods

The AOL Root Certifier's private keys and associated certificates shall have a maximum validity period of 35 years.

The AOLCA'S private keys and associated certificates shall have a maximum validity period of 25 years.

6.4 Activation data

6.4.1 Activation data generation and installation

The activation data used to unlock the AOL Root Certifier's private keys, in conjunction with any other access control, has a level of strength appropriate for a trust anchor. It consists of a combination of user-selected passwords/PINs and one or more unique hardware tokens. Activation data is split between at least two disjoint groups of trusted roles.

Each group has to present its token to the crypto device and must enter a PIN that is associated with the token before the crypto device can be activated. If the activation data – more precisely: splits of activation data– must be transmitted, it shall be via an appropriately protected channel, and distinct in time and place from the associated cryptographic module.

AOL Root Certifier's activation data shall be changed when the AOL Root Certifier re-keys.

6.4.2 Activation data protection

As part of the AOL Root Certifier's activation data, hardware tokens are stored in a secure manner under dual control.

Activation data shall be written down and secured at the level appropriate for the data that the associated cryptographic module protects. Activation data shall not be stored with the cryptographic module.

Activation data for the AOL Root Certifier is split among dedicated trusted roles, such that no single person has knowledge of or access to all activation data.

To allow other members of the same trusted role access to activation data, activation data for each trusted role is stored separately in tamper-evident packaging and under dual control in a safe location.

Staff involved in the AOL Root Certifier certificate issuance process may write down activation data on a sheet of paper, which the owner of the activation data shall then keep at all times (e.g. in his briefcase) or, alternatively, activation data may be stored electronically. If stored electronically, the activation data shall be encrypted using appropriate algorithms, parameters, and passwords.

6.4.3 Other aspects of activation data

No stipulation.

6.5 Computer security controls

6.5.1 Specific computer security technical requirements

The following computer security functions shall be provided by the operating system used by the AOL Root Certifier:

- Authenticated logins
- Discretionary Access Control
- Security audit capability
- Access control restrictions to CA services based on authenticated identity
- Operating system self-protection.

6.5.2 Computer security rating

No stipulation.

6.6 Life cycle technical controls

6.6.1 System development controls

The AOL Root Certifier's CA, RA, and certificate status validation systems are infrastructure components that support a range customer related applications. The design, installation, and operation are documented by qualified personnel and in a qualified manner. This documentation establishes that all relevant systems are properly installed and configured, and operate in accordance with their own technical specifications and the technical requirements imposed by business best practice, common standards (e.g. ETSI TS 102 042, ETSI TS 101 456, etc.) and governmental regulations (e.g. the German Digital Signature Act).

This documentation includes:

- Installation manuals, procedures/scripts/data, acceptance criteria, and results.
- Operation manuals, procedures/scripts/data, acceptance criteria, certifications, and test results.

The AOL Root Certifier's CA system development process meets the following requirements:

- The CA shall use software that has been designed and developed under a formal, documented development methodology.
- All hardware and software shall be purchased in a fashion to reduce the likelihood that any particular component was tampered with (e.g., by ensuring the equipment was randomly selected at time of purchase or the vendor uses tamper-evident packaging).
- If a CA develops its own software for the CA system or certificate status validation system, this development shall take place in a controlled environment, and the entire development process shall defined and documented.
- Whenever possible CAs shall use tamper-evident packaging in combination with courier services for shipping or delivery of hardware and software in order to obtain a continuous chain of accountability, from the purchase location to the operations location.
- CA platform (server hardware, operating system software, and CA application software) shall be dedicated to performing CA functions. There shall be no non-CA applications installed on the CA platform.
- Certificate validation system platform (server hardware, operating system software, and certificate validation application software) shall be dedicated to performing certificate validation functions. Applications which are not related to certificate validation shall not be installed on the certificate validation system platform.
- RA system platform (server hardware, operating system software, and RA application software) shall be dedicated to performing RA functions. There shall be no non-RA applications installed on the RA platform.
- CAs shall use centralized as well as host based firewalls in combination with local virus scanning software and intrusion detection/prevention systems to prevent malicious software from being loaded. Applications required to perform PKI relevant operations shall either have been developed in-house or shall have been obtained from reliable sources.
- Hardware and software updates shall be purchased or developed in the same manner as original equipment. Installation of hardware and software shall be performed by trusted and trained personnel in a defined manner.
- CA, RA, and validation system platform shall be scanned for malicious code before first use and periodically thereafter.

6.6.2 Security management controls

The configuration of the AOL Root Certifier system as well as any modifications and upgrades are documented and controlled. There are mechanisms in place for detecting unauthorized modification to the AOL Root Certifier software or configuration. A formal configuration management methodology is used for installation and ongoing maintenance of AOL Root Certifier system.

The CRLs are manually checked when issued. Since they are signed they can not be altered unnoticed.

6.6.3 Life cycle security controls

Cryptographic hardware may be transported between locations in tamper evident packaging only.

Upon receipt of cryptographic hardware, authorized AOL Root Certifier personnel inspect the tamper evident packaging to determine whether seals are intact. This is followed by acceptance testing.

After acceptance testing the cryptographic hardware is added to an inventory list. To prevent tampering, AOL Root Certifier cryptographic hardware is stored in a secure site, with access limited to authorized personnel.

Each piece of cryptographic hardware is tracked during its life cycle; any change in its state (removal from storage, integration into the production environment, removal from service etc.) is reflected in an event journal.

The handling, installation and removal of cryptographic hardware are performed in the presence of no less than two trusted individuals. The same controls apply to service or repair being performed on the AOL Root Certifier site. AOL Root Certifier cryptographic hardware is never serviced or repaired off-site and subsequently put back into production.

6.7 Network security controls

The AOL Root Certifier is an off-line system; network security does not apply.

The systems providing repository and CRLs employ appropriate security measures to ensure they are guarded against denial of service and intrusion attacks. Such measures include the use of firewalls and filtering routers. No unused network ports and services are activated.

Facilities housing the AOL Root Certifiers have installed adequate protection from both inside and outside attacks (firewalls, intrusion detection mechanisms, etc.). Computer systems directly involved in issuing certificates have no LAN or WAN connection.

Access to all servers is subject to authentication. Users are provided direct access only to the services that they have been specifically authorized to use.

6.8 Time-stamping

Not provided.

7 Certificate, CRL, and OCSP Profiles

7.1 Certificate profile

7.1.1 Version number(s)

The AOL Root Certifier issues X.509 v3 certificates.

7.1.2 Certificate extensions

All extensions shall be interoperable in their intended community of use.

7.1.3 Algorithm object identifiers

The subfield *algorithmIdentifier:algorithm* must contain the object identifier (specified in [RFC 3280]) for SHA-1 with RSA encryption.

The subfield *algorithmIdentifier:algorithm* contains the object identifier for SHA-1 with RSA encryption. The length of the public key in *subjectPublicKey* is not less than 1024 bits.

7.1.4 Name forms

7.1.4.1 Fields Identifying the Issuer

Certificates issued by the AOL Root Certifier contain the following in the *issuer* field:

Identifier Type:	With data content of:	Indicates:
OrganizationName (O)	"America Online Inc."	AOL LLC ⁴ acts as the AOL Root Certifier ⁵
CountryName (C)	"US"	The AOL Root Certifier is incorporated in the United States (specifically, Delaware)
CommonName (CN)	"America Online Root Certification Authority" followed by a numeral	The company listed in the <i>OrganizationName</i> field is the AOL Root Certifier. The numeral indicates the particular private keyID used to sign the certificate

7.1.4.2 Fields Identifying the Subject

A certificate issued by the AOL Root Certifier identifies its subject in the *subject* field. The *subjectAltName* field is not used. The AOL Root Certifier's final root certificates have the same content in the *subject* field as in the *issuer* field (section 7.1.4.1 above) because the subject and the issuer are the same entity.

Certificates issued by the AOL Root Certifier to an AOLCA contain the following in the *subject* field:

Identifier Type:	With data content of:	Indicates:
OrganizationName (O)	Alphanumeric text	The full company name of the AOLCA that is the subject of the certificate
LocalityName (L)	Alphanumeric text	The city or town in which that AOLCA's principal place of business is located
StateOrProvinceName (ST)	Alphanumeric text	The state or province in which that AOLCA's principal place of business is located. This field may be left blank for an AOLCA incorporated in a country without states or provinces.
CountryName (C)	A standard two-letter abbreviation listed [ISO 3166] for a country, such as "US" for the United States	The country in which that AOLCA's principal place of business is located
CommonName (CN)	Alphanumeric text	An unambiguous name identifying the subject in the records of the AOL Root Certifier. This name may not be meaningful to anyone but the

⁴ America Online, Inc. formally changed its name to AOL LLC on April 3, 2006. References to America Online, Inc. are embedded in certificates issued by the AOL root certifier. It is important to note that America Online, Inc. and AOL LLC refer to the same organization.

⁵ AOL LLC acts as the root certifier for the entire public key infrastructure of the worldwide AOL system. National or regional AOLCA's provide more localized services to some markets.

	AOL Root Certifier
--	--------------------

7.1.4.3 Other Supported Fields

Certificates issued by the AOL Root Certifier also contain the following fields. “Critical” indicates for an extension whether an application is required to be able to process the content of the field.

It is not applicable (“n/a”) for fields that are not extensions. See [ITU-T X.509] and [RFC 3280] for more information about certificate content.

Field Name	Critical?	Data Content Requirements	Significance
version	n/a	V3 only	Indicates the version of [ITU-T X.509] to which the certificate conforms
serialNumber	n/a	An integer unique to the certificate among the range of all serial numbers in certificates issued by the same issuer	Certificate serial number. The combination of issuer and serial number comprises a unique identifier for the certificate
signature	n/a	The subfield <i>algorithmIdentifier</i> : <i>algorithm</i> must contain the object identifier (specified in [RFC 3280]) for SHA-1 with RSA encryption	Indicates the algorithm used by the issuer to sign the certificate, which must be SHA-1 with RSA
validity	n/a	The subfields <i>notBefore</i> and <i>notAfter</i> contain dates in the form specified for UTC in [RFC 3280]	<i>NotBefore</i> indicates the date on which the certificate begins to be valid and <i>notAfter</i> indicates when it ceases to be valid. Years are listed as specified in [RFC 3280]
subject	n/a	Contains at least one identifier specified in section 7.1.4.2	As specified in section 7.1.4.2
subjectPublicKeyInfo	n/a	The subfield <i>algorithmIdentifier</i> : <i>algorithm</i> contains the object identifier for SHA-1 with RSA encryption. The length of the public key in <i>subjectPublicKey</i> is not less than 1024 bits	<i>SubjectPublicKey</i> is the subject’s public key, and <i>algorithmIdentifier</i> lists the algorithm to use with it.
authorityKeyIdentifier	No	The subfield <i>keyIdentifier</i> contains the SHA-1 hash of the public key by which the issuer’s signature on the certificate can be verified	Indicates which public key to use in verifying the authenticity of the certificate
subjectKeyIdentifier	No	The subfield <i>keyIdentifier</i> contains the SHA-1 hash of the public key listed in <i>subjectPublicKeyInfo:subjectPublicKey</i> . The other subfields of <i>subjectKeyIdentifier</i> are not used	The subfield <i>keyIdentifier</i> labels the public key of this certificate for convenient reference and to prevent confusion with other key pairs the same subject may have.
keyUsage	Yes	Bits 0 and 5 of the bitstring are set to true; all others are set to false, except that bit 6	Indicates to software applications using the key that the key is to be used for

		is set to true if the certificate is for use in verifying the digital signature on a certificate revocation list	authentication and certification (see [ITU X.509] and [IETF 3280])
certificatePolicies	No	As stated in section 1.2	As stated in section 1.2
subjectAltName	No	Not used	Not used
basicConstraints	Yes	The subfield CA is set to true. The <i>pathLenConstraint</i> is generally omitted	The subfield CA with a value of "true" indicates that the certificate may be used to issue and verify other certificates. The <i>pathLenConstraint</i> subfield is interpreted as specified in [RFC 3280] section 4.2.1.10. Omission indicates that no limit is imposed
CRLDistribution-Points	No	The subfield <i>DistributionPointName</i> contains a URL. The <i>reasonFlags</i> subfield is not used (<i>i.e.</i> bit 0 is true)	Points to a URL where more information about the post-issuance validity or reliability of a certificate may be available

7.1.5 Name constraints

No stipulation.

7.1.6 Certificate policy object identifier

Certificates issued by the AOL Root Certifier under this CP/CPS shall assert the OID listed in section 1.2.

7.1.7 Usage of Policy Constraints extension

No stipulation.

7.1.8 Policy qualifiers syntax and semantics

No stipulation.

7.1.9 Processing semantics for the critical Certificate Policies extension

Processing semantics for critical certificate policy extensions shall conform to X.509 certification path processing rules.

7.2 CRL profile

The fields in AOL certificate revocation lists are the following:

Field Name	Critical?	Data Content Requirements	Significance
version	n/a	V2 only (indicated by the integer "1")	Indicates the version of [ITU-T X.509] to which the certificate revocation list (CRL) conforms
signature	n/a	Same as specified for certificates in section 7.1.4.1	
issuer	n/a	The distinguished name of the issuer (see section 7.1.4.1) of the revoked certificate	Identifies the AOLCA that issued the CRL (and the revoked certificate)
ThisUpdate	n/a	A date and time specified according to section 5.1.2.4 of [RFC 3280] (<i>i.e.</i> in UTCtime)	The date and time when the certificate revocation list was issued

NextUpdate	n/a	A date and time specified according to section 5.1.2.5 of [RFC 3280] (<i>i.e.</i> in UTCtime). Except for device authentication certificates, the time indicated is 24 hours from the time listed in <i>ThisUpdate</i>	If this field is present, it represents the date and time when the issuer anticipates issuing an update to the current CRL
RevokedCertificates	n/a	If present, this field contains the following subfields: <i>userCertificate</i> contains a subfield containing an integer <i>revocationDate</i> contains a date and time specified as UTCtime	If this field is present, <i>userCertificate</i> indicates the serial number of the unexpired, revoked certificate and <i>revocationDate</i> <i>i.e.</i> the time when the certificate was revoked. If this field is absent in a particular certificate revocation list (CRL) ⁶ a user can infer that no certificates have been revoked as of the issue date of the CRL
authorityKeyIdentifier	No	The subfield <i>keyIdentifier</i> contains the SHA-1 hash of the public key by which the issuer's signature on the CRL can be verified	Indicates which public key to use in verifying the authenticity of the certificate
CRLnumber	No	A long integer not exceeding 20 octets in length	The serial number of this CRL in an incrementally increasing sequence of CRLs

7.2.1 Version number(s)

The AOL Root Certifier issues X.509 version two (v2) CRLs.

7.2.2 CRL and CRL entry extensions

No stipulation.

7.3 OCSP profile

OCSP is not supported.

7.3.1 Version number(s)

OCSP is not supported.

7.3.2 OCSP extensions

OCSP is not supported.

⁶ CRLs are ordinarily issued as a result of a revocation event and are processed manually. If no certificates have been revoked, the *RevokedCertificates* field will be absent as required in section 5.1.2.6 of [RFC 3280]

8 Compliance Audit and other Assessments

If an AOL Root Certifier system is hosted by a third party provider, the provider shall be subject to regular external audits. These include audits pursuant to the *WebTrust™ for Certification Authorities*, or the ETSI TS 102 042 compliance audit.

These audits require demonstration of a specific level of security and conformity to documented policies and practices. The respective provisions supplement one another and serve to enhance the overall security controls, which are audited regularly by independent third parties.

This CP/CPS in combination with any relevant third party provider's organization, processes, and procedures has been assessed by independent auditors to be compliant to the standard "ETSI TS 102 042 – Policy requirements for certification authorities issuing public key certificates", Version 1.3.4, of the European Telecommunications Standards Institute (ETSI).

As a result the AOL Root Certifier has been certified by an independent party as conforming to ETSI TS 102 042. Periodic audits ensure the AOL Root Certifier's continuing conformity with this standard.

ETSI TS 102 042 is typically accepted as equivalent to *WebTrust™ for Certification Authorities*.

8.1 Frequency or circumstances of assessment

"ETSI TS 102 042 – Policy requirements for certification authorities issuing public key certificates" specifies the frequency and other requirements for periodic audits.

These periodic audits ensure the AOL Root Certifier's continuing conformity with ETSI TS 102 042 requirements.

8.2 Identity/qualifications of assessor

The auditor performing the ETSI TS 102 042 audit demonstrates competence in the field of compliance audits for security and PKIs. The auditor is thoroughly familiar with requirements for the issuance and management of certificates.

The compliance auditor performs such compliance audits as a primary responsibility.

8.3 Assessor's relationship to assessed entity

The compliance auditor is a private firm, which is independent from AOL LLC (in the role as the owner of the AOL Root Certifier).

8.4 Topics covered by assessment

The purpose of a compliance audit regarding ETSI TS 102 042 is to verify that the AOL Root Certifier is complying with the requirements of this CP/CPS as well as with the requirements specified in ETSI TS 102 042. Thus all applicable aspects of this CP/ CPS and the ETSI standard have to be covered by the compliance audit.

8.5 Actions taken as a result of deficiency

AOL shall make commercially reasonable effort to rectify deficiencies identified in any given audit in accordance with applicable requirements and standards.

8.6 Communication of results

An Audit Compliance Report, including identification of corrective measures taken or being taken, shall be provided to the AOL PKI Policy Management Authority. The report shall identify the CP/CPS used in the assessment, including their dates and version numbers.

9 Other Business and Legal Matters

9.1 Fees

The AOL Root Certifier issues certificates only to itself or to AOLCAs.

The AOL Root Certifier does not issue certificates to the public.

A fee structure is not applicable.

9.1.1 Certificate issuance or renewal fees

No stipulation.

9.1.2 Certificate access fees

No stipulation.

9.1.3 Revocation or status information access fees

No stipulation.

9.1.4 Fees for other services

No stipulation.

9.1.5 Refund policy

No stipulation.

9.2 Financial responsibility

9.2.1 Insurance coverage

No stipulation.

9.2.2 Other assets

No stipulation.

9.2.3 Insurance or warranty coverage for end-entities

No stipulation.

9.3 Confidentiality of business information

9.3.1 Scope of confidential information

The AOL system does not forward confidential member information to the AOL Root Certifier or to an AOLCA for inclusion in a certificate. What information is confidential is determined in accordance with the applicable Member Agreement, AOL privacy policy, and applicable law.

AOL and AOLCAs may disclose confidential Member information to law enforcement officials or private litigants in order to comply with valid legal process such as a search warrant, subpoena or court order, to protect the company's rights and property, or during emergencies when we believe physical safety is at risk.

9.3.2 Information not within the scope of confidential information

Certificates are designed to circulate widely in technological systems, and restricting their dissemination is impractical. In accordance with standards, most applications include a copy of the relevant certificate with each digital signature or block of encrypted data. Consequently, information in

a certificate is not treated as confidential as a practical matter. In addition, expiration and revocation status of a certificate must, by design, be published and is therefore not treated as confidential.

9.3.3 Responsibility to protect confidential information

The AOL Root Certifier is responsible for protecting the confidential information in its possession in accordance with AOL Member Agreements, AOL privacy policy, AOL internal policies, and applicable law.

9.4 Privacy of personal information

The AOL Root Certifier does not issue certificates to end users. Therefore, it does not process personal information.

9.4.1 Privacy plan

N/A.

9.4.2 Information treated as private

N/A.

9.4.3 Information not deemed private

N/A.

9.4.4 Responsibility to protect private information

N/A.

9.4.5 Notice and consent to use private information

N/A.

9.4.6 Disclosure pursuant to judicial or administrative process

N/A.

9.4.7 Other information disclosure circumstances

N/A.

9.5 Intellectual property rights

Members agree and acknowledge that AOL and its suppliers own and shall retain all respective rights, title and interest in and to, and all intellectual property rights embodied in or associated with any AOL product or service. Such right, title and interest shall extend without limitation to any content, software, graphics, design materials, technology, methods, architecture, publications, business plans and other tangible or intangible intellectual property-based assets of any kind in machine readable, printed or other form and all revisions, enhancements, improvements, technical know-how, patents, copyrights, moral rights and trade secrets associated with any AOL product or service. Except as expressly stated in this CP/CPS or an applicable Member Agreement, Participants and relying parties will have no rights of any kind in or to any certificate, key pairs, trademarks or other intellectual property, PKI documents or the AOL system. There are no implied licenses under this Agreement, and any rights not expressly granted under this Agreement are reserved by AOL.

9.5.1 Relying Party Obligations

Any Relying Party's reliance on a certificate issued by the AOL Root Certifier must be reasonable and exercise ordinary business prudence under the circumstances and must conform to the following obligations:

- Ensure that use of a certificate is appropriate as set forth in this CP/CPS, or any applicable Member Agreement;
- Validate the certificate (i.e., confirm that it has not expired or been revoked or suspended), by checking the published revocation list;
- Trust and make use of the certificate only if a valid certificate chain is established between the Relying Party and the subject. A valid chain means that the certificate signatures have been validated back to a final root certificate and the revocation list has been checked to determine the validity of each certificate;
- Verify that the digital signature in question was created by the private key corresponding the public key in the certificate during the certificate's validity period;
- Confirm that any document signed with a digital signature has not been altered; and
- Act in good faith, in light of all the circumstances that were known or should have been known at the time of reliance.

A Relying Party assumes all risks and liability arising from any decision to rely on a certificate in a manner inconsistent with these obligations.

9.5.2 Representations and warranties of other Participants

No stipulation.

9.6 Disclaimers of warranties

Except as expressly provided otherwise in a Member Agreement, any reliance on a certificate issued by the AOL Root Certifier is at the Relying Party's own risk. This CP/CPS describes certain aspects of the public key infrastructure employed in AOL Root Certifier services, but that description is not relevant or applicable to non-Participants except as promotional literature to persuade them to sign up and participate in AOL PKI products or services. Similarly, any information in certificates is only promotional in relation to non-Participants.

AOL AND ITS SUPPLIERS DISCLAIM ANY AND ALL WARRANTIES, BOTH EXPRESS AND IMPLIED, INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTY OF MERCHANTABILITY, ANY WARRANTY OF FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OF ACCURACY OF INFORMATION PROVIDED WITH RESPECT TO AN AOL PKI, INCLUDING USE OF KEY PAIRS, CERTIFICATES, OR ANY OTHER GOODS OR SERVICES PROVIDED BY THE AOL ROOT CERTIFIER OR AN AOLCA TO ANY PERSON.

AOL AND ITS SUPPLIERS FURTHER DISCLAIM ANY AND ALL WARRANTIES, BOTH EXPRESS AND IMPLIED, THAT PARTICIPATION IN AN AOL PKI WILL AFFECT IN ANY MANNER THE LEGAL RECOGNITION OR ENFORCEABILITY OF A DIGITAL SIGNATURE.

9.7 Limitations of liability

IN NO EVENT SHALL AOL, THE AOL ROOT CERTIFIER, AN AOLCA OR THEIR SUPPLIERS BE LIABLE FOR INDIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES, INCLUDING, WITHOUT LIMITATION, ANY LOSS OF PROFITS, LOSS OF DATA, COST OF PROCUREMENT OF SUBSTITUTE SERVICES, OR ANY OTHER INDIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES, HOWSOEVER CAUSED, AND ON ANY THEORY OF LIABILITY, WHETHER FOR BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE AND STRICT LIABILITY), OR OTHERWISE. THESE LIMITATIONS WILL APPLY WHETHER OR NOT AOL, THE AOL ROOT CERTIFIER, AN AOLCA OR THEIR SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, WHETHER OR NOT SUCH DAMAGES COULD HAVE BEEN FORESEEN AND NOTWITHSTANDING ANY FAILURE OF ESSENTIAL PURPOSE OF ANY LIMITED REMEDY. SUBJECT TO THE FOREGOING, AOL'S, THE AOL ROOT CERTIFIER'S, AOLCA'S, AND THEIR SUPPLIERS' LIABILITY FOR DIRECT DAMAGES OF ANY KIND OR NATURE IN CONNECTION WITH THIS AGREEMENT AND AOL PKI SERVICES SHALL IN NO EVENT EXCEED US\$50.

9.8 Indemnities

No stipulation.

9.9 Term and termination

9.9.1 Term

This CP/CPS shall become effective when approved by the AOL PKI Policy Management Authority. This CP/CPS has no specified term.

9.9.2 Termination

The AOL Root Certifier can only be terminated by the AOL PKI Policy Management Authority. The AOL Root Certifier will inform AOLCAs with valid certificates (i. e., neither revoked nor expired). They will be given as much advance notice as circumstances permit, and attempts to provide alternative sources of interoperation will be sought.

9.9.3 Effect of termination and survival

Despite the fact that this CP/CPS may eventually no longer be in effect, the following obligations and limitations of the CP/CPS shall survive: section 9.5 (Intellectual Property Rights), section 9.7 (Limitation of Liability), and section 9.3 (Confidentiality).

If the AOL Root Certifier is terminated all certificates that have not expired or have not been revoked by the respective AOLCAs will be revoked by AOL. A final CRL will be published and made available for at least as long as the validity period of the certificate with the longest validity period indicates. AOLCAs will be notified of such action.

9.10 Individual notices and communications with Participants

No stipulation.

All communications between the AOL Root Certifier and AOLCAs is handled internally by AOL.

9.11 Amendments

9.11.1 Procedure for amendment

AOL has adopted this CP/CPS through its PKI Policy Management Authority. It is under continuous review as AOL develops and is subject to amendment by the PKI Policy Management Authority. This CP/CPS is subject to change without notice at the discretion of the AOL root certifier.

Any notices or correspondence relative to this CP/CPS may be sent to the AOL Root Certifier Administrator, pki-info@aol.net.

9.11.2 Notification mechanism and period

This CP/CPS and any subsequent changes shall be made publicly available within one week of approval.

All policy changes under consideration by the AOL PKI Policy Management Authority shall be disseminated to AOLCAs and other parties designated by the AOL PKI Policy Management Authority.

9.11.3 Circumstances under which OID must be changed

The policy OID (see section 1.2) shall only change if the change in the CP/CPS results in a material change to the trust by the relying parties, as determined by the AOL PKI Policy Management Authority.

9.12 Dispute resolution provisions

The AOL Root Certifier issues certificates only to itself or to AOLCAs. The AOL Root Certifier does not issue certificates to the public. Therefore, dispute resolution with the AOL Root Certifier, if necessary, is handled internally by AOL. AOLCAs define their dispute resolution provisions in their CPSSs.

9.13 Governing law

The laws of the Commonwealth of Virginia, excluding its conflicts-of-law rules, govern this CP/CPS. The exclusive jurisdiction for any claim or dispute with AOL or relating in any way to this CP/CPS or AOL Member Security PKI services resides in the courts of Virginia. Members, Participants, and Relying Parties, further agree and expressly consent to the exercise of personal jurisdiction in the courts of Virginia in connection with any such dispute or claim. This CP/CPS shall not be governed by the United Nations Convention on Contracts for the International Sale of Goods.

9.14 Miscellaneous provisions

9.14.1 Entire agreement

No stipulation.

9.14.2 Assignment

No stipulation.

9.14.3 Severability

If parts of any of the provisions in this CP are incorrect or invalid, this shall not affect the validity of the remaining provisions until the CP is updated. The process for updating this CP is described in section 9.11.

9.14.4 Enforcement (attorneys' fees and waiver of rights)

No stipulation.

9.14.5 Force Majeure

No stipulation.

9.15 Other provisions

No stipulation.

10 References

The following documents were used in part to develop this CP/CPS:

[AOL Member Security PKI CP/CPS]: AOL Member Security PKI: Certificate Policy and Certification Practice Statement (2004). This document is adopted and published by each AOLCA in cooperation with AOL Information Technology Security.

[ETSI TS 102042] Policy requirements for certification authorities issuing public key certificates, Version 1.2.3, 2006, European Telecommunications Standards Institute (ETSI).

[FIPS 140-2]: National Institute for Standards and Technology, Federal Information Processing Standard 140-1: Security Requirements for Cryptographic Modules -- 01 May 25 (Supersedes FIPS PUB 140-1, 1994 January 11)

[ITU-T X.509]: International Telecommunication Union, Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks version 3 (2000).

[ITU-T X.520]: Information technology - Open Systems Interconnection - The directory: Selected attribute types (1997).

[ITU-T X.690] Information technology - ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER) (2002).

[RFC 3280]: R. Housley, W. Polk, W. Ford, D. Solo, Internet X.509 Public Key Infrastructure: Certificate and Certificate Revocation List (CRL) Profile (2002).

[RFC 3647]: S. Chokhani, W. Ford, R. Sabett, C. Merrill, S. Wu, Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework (2003).

[Webtrust® Criteria]: American Institute of Certified Public Accountants, Inc. and Canadian Institute of Certified Public Accountants, Suitable Trust Services Criteria and Illustrations for Security Availability, Processing Integrity, Online Privacy, and Confidentiality (Including Webtrust® and SysTrust®) version 3.0 (2003).