



Adobe Systems Incorporated
Root Certificate Policy

Revision #4

Revision History

Rev #	Date	Author	Description of Change(s)
1	02/24/03	Deloitte & Touche	First draft.
2	04/02/03	Deloitte & Touche Cooley Godward	Significant wording changes throughout the document.
3	01/16/04	Adobe	Further refinements.
4	06/20/04	Adobe	Further refinements.

1. INTRODUCTION	8
1.1 Overview	8
1.2 Identification	8
1.3 Community and Applicability.....	8
1.3.1 Certification Authorities	9
1.3.2 Registration Authorities	9
1.3.3 End Entities	9
1.3.4 Applicability	9
1.3.5 Policy Authority.....	9
1.4 Contact Details.....	9
1.4.1 Specification Administration Organization	9
1.4.2 Contact Person	10
1.4.3 Person Determining CP Suitability for the Policy	10
2. GENERAL PROVISIONS	10
2.1 Obligations.....	10
2.1.1 Root CA Obligations.....	10
2.1.2 Root RA Obligations.....	10
2.1.3 End Entity obligations.....	11
2.1.3.1 Trusted Roles	11
2.1.3.2 Test CAs.....	11
2.1.4 Relying Party Obligations.....	12
2.1.5 Repository Obligations	12
2.2 Liability.....	12
2.2.1 Root CA Liability	12
2.2.2 RA Liability	12
2.3 Financial Responsibility.....	13
2.3.1 Indemnification by Relying Parties	13
2.3.2 Fiduciary Relationships	13
2.3.3 Administrative Processes	13
2.4 Interpretation and Enforcement	13
2.4.1 Governing Law	13
2.4.2 Severability, Survival, Merger, Notice	14
2.4.3 Dispute Resolution Procedures	14
2.5 Fees	14
2.5.1 Certificate Issuance or Renewal Fees	14
2.5.2 Certificate Access Fees	14
2.5.3 Revocation or Status Information Access Fees	14
2.5.4 Fees for Other Services Such as Policy Information	14
2.5.5 Refund Policy.....	14
2.6 Publication and Repository	14
2.6.1 Publication of CA Information	15
2.6.2 Frequency of Publication	15
2.6.3 Access Controls	15
2.6.4 Repositories.....	15
2.7 Compliance Audit	15

2.7.1	Frequency of Entity Compliance Audit	15
2.7.2	Identity/qualifications of Auditor	15
2.7.3	Auditor's Relationship to Audited Party.....	15
2.7.4	Topics Covered by Audit	15
2.7.5	Actions Taken as a Result of Deficiency	16
2.7.6	Communication of Results.....	16
2.8	Confidentiality	16
2.8.1	Types of Information to be Kept Confidential.....	16
2.8.2	Types of Information not Considered Confidential	16
2.8.3	Disclosure of Certificate Revocation/Suspension Information.....	16
2.8.4	Release to Law Enforcement Officials	16
2.8.5	Release as Part of Civil Discovery.....	16
2.8.6	Disclosure upon Owner's Request	16
2.8.7	Other Information Release Circumstances	16
2.9	Intellectual Property Rights	16
3.	IDENTIFICATION AND AUTHENTICATION.....	16
3.1	Initial Registration	16
3.1.1	Types of Names	16
3.1.2	Need for Names to be Meaningful.....	17
3.1.3	Rules for Interpreting Various Name Forms	17
3.1.4	Uniqueness of Names	17
3.1.5	Name Claim Dispute Resolution Procedure	17
3.1.6	Recognition, Authentication and Role of Trademarks	17
3.1.7	Method to Prove Possession of Private Key	17
3.1.8	Standard Authentication of Organization Identities	18
3.1.9	Authentication of Individual Identity.....	18
3.2	Routine Rekey.....	18
3.3	Rekey after Revocation.....	18
3.4	Revocation Request	19
4.	OPERATIONAL REQUIREMENTS.....	19
4.1	Certificate Application.....	19
4.1.1	Subordinate CA Certificate Application.....	19
4.1.2	Trusted Role Certificate Application.....	19
4.2	Certificate Issuance.....	20
4.3	Certificate Acceptance.....	20
4.4	Certificate Suspension and Revocation	20
4.4.1	Circumstances for Revocation	20
4.4.2	Who can Request Revocation	20
4.4.3	Procedure for Revocation Request.....	20
4.4.4	Revocation Request Grace Period	21
4.4.5	Circumstances for Suspension	21
4.4.6	Who can Request Suspension	21
4.4.7	Procedure for Suspension Request.....	21
4.4.8	Limits on Suspension Period	21
4.4.9	ARL/CRL Issuance Frequency (if applicable)	21
4.4.10	ARL/CRL Checking Requirements	21

4.4.11 On-line Revocation/Status Checking Availability.....	21
4.4.12 On-line Revocation Checking Requirements.....	22
4.4.13 Other Forms of Revocation Advertisements Available.....	22
4.4.14 Checking Requirements for other Forms of Revocation Advertisements.....	22
4.4.15 Special Requirements Re Key Compromise.....	22
4.5 Security Audit Procedures.....	22
4.5.1 Types of Event Recorded.....	22
4.5.2 Frequency of Processing Log.....	22
4.5.3 Retention Period for Audit Log.....	23
4.5.4 Protection of Audit Log.....	23
4.5.5 Audit Log Backup Procedures.....	23
4.5.6 Audit Collection System (internal vs. external).....	23
4.5.7 Notification to Event-causing Subject.....	23
4.5.8 Vulnerability Assessments.....	23
4.6 Records Archival.....	24
4.6.1 Types of Event Recorded.....	24
4.6.2 Retention Period for Archive.....	24
4.6.3 Protection of Archive.....	24
4.6.4 Archive Backup Procedures.....	24
4.6.5 Requirements for Time-stamping of Records.....	24
4.6.6 Archive Collection System (internal or external).....	24
4.6.7 Procedures to Obtain and Verify Archive Information.....	24
4.7 Key Changeover.....	25
4.8 Compromise and Disaster Recovery.....	25
4.8.1 Computing Resources, Software, and/or Data are corrupted.....	25
4.8.2 Entity Public Key is revoked.....	25
4.8.3 Entity Key Compromise.....	25
4.8.3.1 Suspected Compromise.....	25
4.8.3.2 Key is Compromised.....	25
4.8.4 Secure Facility after a Natural or Other Type of Disaster.....	26
4.9 CA Termination.....	26
5. PHYSICAL, PROCEDURAL, AND PERSONNEL SECURITY CONTROLS.....	26
5.1 Physical Controls.....	26
5.1.1 Site Location and Construction.....	26
5.1.2 Physical Access.....	26
5.1.3 Power and Air Conditioning.....	27
5.1.4 Water exposures.....	27
5.1.5 Fire prevention and protection.....	27
5.1.6 Media Storage.....	27
5.1.7 Waste Disposal.....	27
5.1.8 Off-Site Backup.....	27
5.2 Procedural Controls.....	27
5.2.1 Trusted Roles.....	27
5.2.2 Number of Persons Required per Task.....	28
5.2.3 Identification and Authentication for Each Role.....	28

5.3 Personnel Controls	28
5.3.1 Background, Qualifications, Experience, and Clearance.....	28
Requirements	28
5.3.2 Background Check Procedures	28
5.3.3 Training Requirements.....	28
5.3.4 Retraining Frequency and Requirements.....	28
5.3.5 Job Rotation Frequency and Sequence	28
5.3.6 Sanctions for Unauthorized Actions	28
5.3.7 Contracting Personnel Requirements.....	29
5.3.8 Documentation Supplied to Personnel.....	29
6. TECHNICAL SECURITY CONTROLS	29
6.1 Key Pair Generation and Installation.....	29
6.1.1 Key Pair Generation.....	29
6.1.2 Private Key Delivery to Entity.....	29
6.1.3 Public Key Delivery to Certificate Issuer	29
6.1.4 CA Public Key Delivery to Users.....	30
6.1.5 Key Sizes	30
6.1.6 Public Key Parameters Generation	30
6.1.7 Parameter Quality Checking.....	30
6.1.8 Hardware/Software Key Generation.....	30
6.1.9 Key Usage Purposes (as per X.509 v3 key usage field)	30
6.2 Private Key Protection	30
6.2.1 Standards for Cryptographic Module.....	30
6.2.2 Private Key (n out of m) Multi-person Control	31
6.2.3 Private Key Escrow.....	31
6.2.4 Private Key Backup	31
6.2.5 Private Key Archival.....	31
6.2.6 Private Key Entry into Cryptographic Module.....	31
6.2.7 Method of Activating Private Key	31
6.2.8 Method of Deactivating Private Key	31
6.2.9 Method of Destroying Private Key	31
6.3 Public Key Archival.....	32
6.3.1 Public Key Archival.....	32
6.3.2 Usage Periods for the Public and Private Keys	32
6.4 Activation Data	32
6.4.1 Activation Data Generation and Installation.....	32
6.4.2 Activation Data Protection.....	33
6.4.3 Other Aspects of Activation Data	33
6.5 Computer Security Controls	33
6.5.1 Specific Computer Security Technical Requirements	33
6.5.2 Computer Security Rating.....	33
6.6 Life Cycle Technical Controls	33
6.6.1 System Development Controls	33
6.6.2 Security Management Controls.....	33
6.6.3 Life Cycle Security Ratings.....	33
6.7 Network Security Controls	34
6.8 Cryptographic Module Engineering Controls.....	34

7. CERTIFICATE AND CRL PROFILES	34
7.1 Root Certificate Profile	34
7.1.1 Version Number(s).....	35
7.1.2 Certificate Extensions	35
7.1.3 Algorithm Object Identifiers.....	35
7.1.4 Name Forms.....	35
7.1.5 Name Constraints.....	35
7.1.6 Certificate Policy Object Identifier	35
7.1.7 Usage of Policy Constraints Extension.....	35
7.1.8 Policy Qualifiers Syntax and Semantics	35
7.1.9 Processing Semantics for the Critical Certificate Policy Extension	36
7.2 CRL Profile.....	36
7.2.1 Version Number(s).....	36
7.2.2 CRL and CRL Entry Extensions.....	36
7.3 CDS Subordinate CA Certificate Profile	36
7.3.1 Version Number(s).....	38
7.3.2 Certificate Extensions	38
7.3.3 Algorithm Object Identifiers.....	358
7.3.4 Name Forms.....	358
7.3.5 Name Constraints.....	358
7.3.6 Certificate Policy Object Identifier	358
7.3.7 Usage of Policy Constraints Extension.....	358
7.3.8 Policy Qualifiers Syntax and Semantics	358
7.3.9 Processing Semantics for the Critical Certificate Policy Extension	368
8. SPECIFICATION ADMINISTRATION	39
8.1 Specification Change Procedures	39
8.2 Publication and Notification Policies.....	39
8.3 CP Approval Procedures.....	39
Appendix A – Terms and Definitions	40

1. INTRODUCTION

1.1 Overview

Adobe Systems Incorporated (Adobe) established a Public Key Infrastructure (PKI) to manage the issuance of digital certificates. The Adobe PKI is managed by the Adobe Policy Authority.

Central to the Adobe PKI is a root certificate hierarchy put in place by Adobe to provide digital certificates to partners, test CAs and employees. This certificate hierarchy is called the Adobe Root CA (Adobe Root CA). Its hierarchy is depicted in Figure 1 and described in Section 1.3.1.

The Adobe CA Root CA hierarchy was established in January 2003, when Adobe generated a self-signed root Certificate (Adobe CA Root).

This document is the Certificate Policy (CP) for and describing the policies of the Adobe Root Certification Authority (CA) operating within the Adobe Root CA hierarchy (Adobe Root CA). This CP is applicable to all entities with relationships to the Adobe CA hierarchy including Trusted Roles and Subordinate CAs. This CP provides a statement of the required practices and responsibilities of the Adobe Root CA, as well as the responsibilities of each entity participating in the Adobe Root CA's community of trust. While this document references operational aspects of the Adobe PKI, its specific purpose is to prescribe the practices within the Adobe Root CA hierarchy.

This document follows the "Chokhani-Ford framework" for such documents, as outlined in Internet Engineering Task Force's IETF PKIX Working Group Internet Draft - Internet X.509 Public Key Infrastructure – Certificate Policy and Certification Practices Framework, Part 4, version April 25, 1998. For consistency with that document's format, as well as for adaptability, all sections of the framework are included, with appropriate section headings. When no stipulation has been made for a section with regard to this CP, "No Stipulation" is indicated below the related section heading.

1.2 Identification

This CP is called the Adobe Systems Incorporated Root Certificate Policy.

The Attribute Object Identifier (OID) for this CP is: 1.2.840.113583.1.2.1

1.3 Community and Applicability

The Adobe Root CA has been established to provide certificate services for Adobe Systems Incorporated.

1.3.1 Certification Authorities

The Adobe Root CA issues certificates according to the hierarchy of CAs as shown in Figure 1 below. At the top of the hierarchy is the Adobe Root CA. Currently, the Adobe Root CA provides certificates to its Trusted Roles, Level 1 Subordinate CAs, and Adobe Test Subordinate CAs. The Adobe Test Subordinate CAs issue End-Entity Certificates for test purposes only. Currently, the Adobe PKI is implemented using the Entrust Authority suite of products and services. (Version 6.0)

1.3.2 Registration Authorities

Registration Authorities (RAs) evaluate and either approve or reject certificate applications. This evaluation includes verification of the identity of End-entities.

1.3.3 End Entities

End-entities for Trusted Roles and subordinate Test CAs are Adobe employees whose identities are bound to a particular certificate issued by the Adobe CA.

1.3.4 Applicability

All certificates issued by the Adobe Root CA are supported by this CP. Certificates issued by the Test CAs are intended to be used for testing, and therefore, do not include any assurance.

1.3.5 Policy Authority

The policies used to manage the Adobe Root CA are developed, maintained and enforced by the Adobe Policy Authority. The Adobe Policy Authority is made up of the following people:

- VP, Information Services
- Senior Manager, Information Security
- Corporate Counsel

1.4 Contact Details

1.4.1 Specification Administration Organization

No stipulation.

1.4.2 Contact Person

Adobe Policy Authority
c/o Information Security and Risk Management
Adobe Systems Incorporated
345 Park Ave
San Jose, CA 95110

1.4.3 Person Determining CP Suitability for the Policy

No stipulation.

2. GENERAL PROVISIONS

2.1 Obligations

2.1.1 Root CA Obligations

In general, the Adobe Root CA must:

- utilize the Adobe Root CA software and hardware required to initiate and operate the Adobe PKI as shown in Figure 1 above;
- use commercially reasonable efforts to generate key material in a manner that ensures reasonable trust and integrity;
- sign a root certificate for the Adobe PKI in a high assurance environment;
- issue certificates to itself, and other entities in accordance with this CP;
- as required, revoke certificates; and
- publish CRL's as needed or at least once per year.

2.1.2 Root RA Obligations

The Adobe Root RA is operated by the Trusted Roles. The Trusted Roles shall ensure the identity and authentication of entities to which the Adobe Root CA issues certificates (e.g., Trusted Roles, Level 1 Subordinate CAs, and test CAs), and shall issue requests that cause the Adobe Root CA to issue certificates to those entities that are compliant with this CP/CPS.

The Trusted Roles operating the Root RA verify, by their appearance, the accuracy and authenticity of the information provided by the Test CA and Level 1 Subordinate CA applicants, along with other Trusted Roles, at the time of application for a certificate. The Adobe Root RA also validates revocation requests and communicates authorized revocation requests to the Adobe Root CA.

2.1.3 End Entity obligations

2.1.3.1 Trusted Roles

Any entity performing in a Trusted Role shall:

- Maintain its private keys in a secure manner according to this CP and other established Adobe procedures for handling or accessing such keys;
- Not disclose to anyone any information needed to access its private keys, including, without limitation, the PINs, passwords, pass phrases, or other information or mechanisms used to protect their private keys;
- Request revocation of its certificate if it has reasonable reason to suspect that its private keys or any information used to access its private keys have been compromised;
- Conform to all requirements and follow all instructions during the Root Key Generation Ceremony; and
- Conform to all other requirements as may be specified from time to time by Adobe.

When an Adobe employee who is performing in a Trusted Role leaves Adobe, that employee's certificates are revoked as soon as possible after leaving the company.

2.1.3.2 Test CAs

In general, and as specified in greater detail in this CP, test CAs shall:

- Provide test CA capabilities as needed to test the Adobe PKI;
- Maintain their private keys in a secure manner;
- Implement and maintain administrative procedures (including personnel and procedural requirements), as well as physical and technological security mechanisms appropriate for a basic assurance CA;
- Issue certificates for test purposes only;
- Revoke certificates that it issues as soon as possible after issuance;
- Take reasonable steps to ensure that certificates it issues never leave the test environment within the Adobe PKI; and
- Issue and publish Test CA Certificate Revocation Lists.

2.1.4 Relying Party Obligations

No stipulation.

2.1.5 Repository Obligations

No stipulation.

2.2 Liability

2.2.1 Root CA Liability

2.2.1.1 Warranty Disclaimers

Other than specified in the CDS CP or any CDS Provider Agreement, the Adobe Root CA disclaims any and all warranties related to any certificates issued in the Adobe Test PKI, including warranties:

- related to the accuracy, authenticity, reliability, completeness, currentness, merchantability, or fitness of any information contained in certificates or otherwise compiled, published, or disseminated by or on behalf of the Adobe Root CA;
- related to the security provided by any cryptographic process implemented by the Adobe Root CA;
- for representations of information contained in a certificate;
- of non-repudiation of any messages; and
- related to any software or applications.

2.2.1.2 Limitations on Liability

Under no circumstances will Adobe be liable to any purported Relying Parties, or any other person or entity, for any loss of use, revenue or profit, lost or damaged data, or other commercial or economic loss or for any other indirect, incidental, special, punitive, exemplary or consequential damages whatsoever, even if advised of the possibility of such damages or if such damages are foreseeable. This limitation shall apply even in the event of a fundamental breach or a breach of the fundamental terms of this CP.

2.2.2 RA Liability

Other than specified in the CDS CP or any CDS Provider Agreement, the Adobe Root CARA disclaims any and all warranties related to any certificates issued in the Adobe Test PKI, including warranties:

- related to the accuracy, authenticity, reliability, completeness, currentness, merchantability, or fitness of any information contained in certificates or

otherwise compiled, published, or disseminated by or on behalf of the Adobe Root CA;

- related to the security provided by any cryptographic process implemented by the Adobe Root CA;
- for representations of information contained in a certificate;
- of non-repudiation of any messages; and
- related to any software or applications.

2.2.2.1 Limitations on Liability

Other than specified in the CDS CP or any CDS Provider Agreement, under no circumstances will Adobe be liable to any purported Relying Parties, or any other person or entity, for any loss of use, revenue or profit, lost or damaged data, or other commercial or economic loss or for any other indirect, incidental, special, punitive, exemplary or consequential damages whatsoever, even if advised of the possibility of such damages or if such damages are foreseeable. This limitation shall apply even in the event of a fundamental breach or a breach of the fundamental terms of this CP.

2.3 Financial Responsibility

2.3.1 Indemnification by Relying Parties

Any purported Relying Parties in the Adobe Test PKI agree to indemnify and by the use of any certificates issued by the Adobe Root CA or any Test CA do indemnify Adobe, the Adobe Root CA, and any other parties for any third party losses or damages caused by any use of any of the certificates issued by the Adobe Root CA or any Test CA.

2.3.2 Fiduciary Relationships

No fiduciary relationships are created as a result of any of the activities of the Adobe Root CA.

2.3.3 Administrative Processes

No stipulation

2.4 Interpretation and Enforcement

2.4.1 Governing Law

Unless specified otherwise in an Adobe PKI Partner Agreement, or other Subordinate CA Agreement, this CP shall be governed by the laws of the State of California, USA, without giving effect to: (i) the principles of conflicts of law and that body of law applicable to choice of law; (ii) the United Nations Convention on

Contracts for the International Sale of Goods, and/or its implementing and/or successor legislation and/or regulations; (iii) the Uniform Commercial Code and/or its implementing and/or successor legislation and/or regulations; and/or (iv) the Uniform Computer Information Transactions Act and/or its implementing and/or successor legislation and/or regulations, as applicable respectively. Any party involved with the Adobe Test PKI agrees that the State and Federal courts located in Santa Clara County, California constitute a convenient forum for any litigation and submits to the jurisdiction of such courts. Except to the extent required by law, any party involved in the Adobe PKI waives trial by jury. All parties hereby agree to comply with all applicable laws, regulations and government orders in performing their obligations.

2.4.2 Severability, Survival, Merger, Notice

No stipulation.

2.4.3 Dispute Resolution Procedures

No stipulation.

2.5 Fees

2.5.1 Certificate Issuance or Renewal Fees

No stipulation.

2.5.2 Certificate Access Fees

No stipulation.

2.5.3 Revocation or Status Information Access Fees

No stipulation.

2.5.4 Fees for Other Services Such as Policy Information

No stipulation.

2.5.5 Refund Policy

No stipulation.

2.6 Publication and Repository

2.6.1 Publication of CA Information

The repository of the Adobe Root CA operating under this CP contains at least the following information:

- All certificates issued by the Adobe Root CA which reference the policies identified in Section 1;
- Applicable certificate revocation lists (CRL's) (if any) as published in accordance with the Operational Requirements section of this CP; and
- The certificate of the Adobe Root CA, containing the public key corresponding to its private signing key.

Since the Adobe Root CA is an off-line root, the contents of the repository are only made available upon approved request.

2.6.2 Frequency of Publication

The Adobe Root CA immediately publishes the certificates it issues. Information relating to the revocation of a certificate is published in accordance with Section ~~4.4~~.

2.6.3 Access Controls

No stipulation.

2.6.4 Repositories

No stipulation.

2.7 Compliance Audit

2.7.1 Frequency of Entity Compliance Audit

No stipulation.

2.7.2 Identity/qualifications of Auditor

No stipulation.

2.7.3 Auditor's Relationship to Audited Party

No stipulation.

2.7.4 Topics Covered by Audit

No stipulation.

2.7.5 Actions Taken as a Result of Deficiency

No stipulation.

2.7.6 Communication of Results

No stipulation.

2.8 Confidentiality

2.8.1 Types of Information to be Kept Confidential

No stipulation.

2.8.2 Types of Information not Considered Confidential

No stipulation.

2.8.3 Disclosure of Certificate Revocation/Suspension Information

No stipulation.

2.8.4 Release to Law Enforcement Officials

No stipulation.

2.8.5 Release as Part of Civil Discovery

No stipulation.

2.8.6 Disclosure upon Owner's Request

No stipulation.

2.8.7 Other Information Release Circumstances

No stipulation.

2.9 Intellectual Property Rights

No stipulation.

3. IDENTIFICATION AND AUTHENTICATION

3.1 Initial Registration

3.1.1 Types of Names

Names for certificate issuers and certificate subjects are of the X.500 Distinguished Name (DN) form in accordance with PKIX Part 1. Certificates issued as part of this PKI shall have an OrganizationName attribute with a value “Adobe Systems Incorporated” (o=Adobe Systems Incorporated).

The Root CA certificate shall have an OrganizationalUnit attribute with a value “Adobe Trust Services” (ou=Adobe Trust Services).

The Root CA certificate shall have a CommonName attribute with a value “Adobe Root CA” (cn=Adobe Root CA).

All subordinate CA certificates issued by the Adobe Root CA shall have a DN structure that is meaningful.

3.1.2 Need for Names to be Meaningful

Names used in certificates issued by the Adobe Root CA must be meaningful in that they can be understood and used by Relying Parties and linked to a Subscriber, an Organizational Unit or a specific individual operating in a certain role.

3.1.3 Rules for Interpreting Various Name Forms

No stipulation

3.1.4 Uniqueness of Names

Names used within the Adobe PKI must be unique.

3.1.5 Name Claim Dispute Resolution Procedure

The Adobe Policy Authority will use reasonable efforts to resolve any name claim disputes brought to its attention.

3.1.6 Recognition, Authentication and Role of Trademarks

No stipulation

3.1.7 Method to Prove Possession of Private Key

Proof of possession of the private key is provided by:

- Using password protected FIPS 140-1 Level 3 cryptographic hardware tokens (Chrysalis Luna CA3);
- Using RFC 2510 PKIX-CMP; and
- Using PKCS #10: Certification Request Syntax

3.1.8 Standard Authentication of Organization Identities

Organizations external to Adobe wishing to have an Adobe Root CA certificate issued to them must be represented, in-person, by an authorized employee of the Organization named in the certificate.

The Adobe Policy Authority shall validate all application requests prior to approving them.

3.1.9 Authentication of Individual Identity

3.1.9.1 Trusted Roles

Only Adobe employees will be given End-Entity Certificates issued by the Adobe Root CA. The individual must also receive approval from the Adobe Policy Authority. At the time of certificate issuance, the individual must produce a valid piece of approved identification from the following list, one of which must have a recent photograph:

- Driver's License
- Passport

3.1.9.2 Subordinate CAs

The Adobe Policy Authority shall review and approve all applications for certificate issuance submitted by Level 1 Subordinate CAs prior to any certificate being issued by the Adobe Root CA.

A Level 1 Subordinate CA wishing to have an Adobe Root CA certificate issued to it must be represented, in-person, by an authorized employee of the Organization or Organizational Unit named in the certificate.

The Adobe Policy Authority shall validate all application requests prior to approving them.

3.2 Routine Rekey

No stipulation

3.3 Rekey after Revocation

The Adobe Root CA shall not permit rekeying after a certificate has been revoked.

3.4 Revocation Request

All requests for revocation must be authenticated by the Adobe Policy Authority prior to any action being taken.

4. OPERATIONAL REQUIREMENTS

4.1 Certificate Application

4.1.1 Subordinate CA Certificate Application

4.1.1.1 Adobe Managed Subordinate CAs

All Adobe employees wishing to create Level 1 Subordinate CAs under the Adobe Root CA must follow the application process as defined by the Adobe Policy Authority including completing and submitting an application.

4.1.1.2 Externally Managed Subordinate CAs

All entities wishing to become a Level 1 Subordinate CA must follow the application process as defined by the Adobe Policy Authority including completing and submitting an application and entering into a fully executed CDS Provider Agreement. The Adobe Policy Authority will review and approve (if so decided) all applications for CAs applying for certificates issued by the Root CA. All other applications must be reviewed and approved (if so decided) by the Adobe Policy Authority.

4.1.2 Trusted Role Certificate Application

Each person desiring to act in a Trusted Role shall adhere to the following procedures when making application for an Adobe Root CA issued certificate:

- Follow the identification and authentication procedures specified in Section 3.1.9 of this CP;
- Read and sign the Trusted Roles Agreement, which indicates understanding and acceptance of the obligations required to act as a Trusted Role for the Adobe Root CA; ~~and~~
- Obtain the signature of the person's immediate supervisor, a member of the Adobe Internal Audit staff, or an External Auditor.

4.2 Certificate Issuance

Certificates are issued to subordinate CA's during a scripted and externally audited process.

4.3 Certificate Acceptance

Certificates must be accepted in a manner that positively confirms the receipt of the certificate by the applicant. As Adobe Root CA Trusted Role certificates are maintained on the Root CA system, no confirmation of receipt is required.

4.4 Certificate Suspension and Revocation

The Adobe PKI does not support certificate suspension.

4.4.1 Circumstances for Revocation

Any Subscriber's certificate shall be revoked when the certificates are no longer trusted, needed or if the employee acting in a Trusted Role leaves Adobe. Some of the specific reasons for certificate revocation include, but are not limited to:

- Compromise or suspected compromise of private keys;
- Corporate mergers or take-overs;
- Termination of business relationship; and
- Failure of the Subordinate CA to meet their obligations.

4.4.2 Who can Request Revocation

No stipulation.

4.4.3 Procedure for Revocation Request

A request for revocation of a certificate issued by the Adobe Root CA certificate requires approval from the Adobe Policy Authority. After approval from the Policy Authority, three of five members of the Trusted Roles are required to bring up the Adobe Root CA (if not already running).

After the Adobe Root CA is brought into operation, the Third Security Officer logs in by providing the appropriate credentials. If the Third Security Officer is not available and the Policy Authority deems it necessary to perform the revocation immediately, the First Security Officer will fill in for the Third Security Officer and

complete the revocation. But in this in case, the revocation procedures must be witnessed by an independent third party (e.g., external auditor).

4.4.4 Revocation Request Grace Period

No stipulation.

4.4.5 Circumstances for Suspension

No stipulation.

4.4.6 Who can Request Suspension

No stipulation.

4.4.7 Procedure for Suspension Request

No stipulation.

4.4.8 Limits on Suspension Period

No stipulation.

4.4.9 ARL/CRL Issuance Frequency (if applicable)

The Adobe Root shall issue a routine Authority Revocation Lists (ARL) at least once every year even if there are no changes to the list. In the case of a certificate being revoked due to a private key being compromised, the Adobe Root CA shall issue an updated ARL within 24 hours of the revocation.

4.4.10 ARL/CRL Checking Requirements

Each certificate issued by the Adobe Root CA includes the full DN of the Root CA, as well as the URL where the CRL can be found during the verification of the certificate.

Relying Parties shall check the most current ARL/CRL prior to relying on a certificate.

4.4.11 On-line Revocation/Status Checking Availability

No stipulation.

4.4.12 On-line Revocation Checking Requirements

No stipulation.

4.4.13 Other Forms of Revocation Advertisements Available

No stipulation.

4.4.14 Checking Requirements for Other Forms of Revocation Advertisements

No stipulation.

4.4.15 Special Requirements Re Key Compromise

Should a key compromise occur involving the Adobe Root CA or any of the Subordinate CA's, the Policy Authority shall, upon notification, immediately organize and conduct an investigation into the circumstances surrounding the cause of the compromise.

4.5 Security Audit Procedures

4.5.1 Types of Event Recorded

Significant security-event on the Adobe Root CA, as determined by Adobe, in its sole discretion, are automatically time-stamped and recorded in audit trail files. These include, but are not limited to, such events as:

- Successful and failed attempts to initialize, remove, enable, disable, update, and recover users, their keys and certificates;
- Successful and failed attempts to create, remove, login as, set, reset, and change passwords of, revoke privileges of, and create, update, and recover keys and certificates for Master Users and Security Officers;
- Failed interactions with the directory including successful and failed connection attempts, and read and write operations by the Adobe Root CA; and
- Events related to certificate revocation, security policy modification and validation, Adobe Root CA software start-up and stop, database backup, certificate and certificate chain validation, attribute certificate management, user upgrade, DN change, database and audit trail management, certificate life-cycle management and other miscellaneous events.

4.5.2 Frequency of Processing Log

The Root CA's audit logs are to be reviewed by a Trusted Role or Internal Auditor each time the Root CA is brought on-line. The Security Officer should confirm that the last entry on the audit log coincides with documentation generated externally from the Root CA (e.g. scripts, approval forms, etc.).

4.5.3 Retention Period for Audit Log

Audit logs shall be retained for 20 years.

4.5.4 Protection of Audit Log

Access to the Adobe Root CA system audit logs is restricted to authorized Adobe personnel by a combination of physical and IT security controls as described in Sections 5 and 6.

The Adobe Root CA system audit log is stored in regular operating system flat files. Each audit trail file consists of an audit header which contains information about the audits in the file and list of events. A Message Authentication Code (MAC) is created for each of the audit events and the audit header. Each audit trail file has a different audit key used to generate the MAC. The Entrust Master Integrity key for the Adobe Root CA is used to protect the audit key which is stored in the audit header. Security Officers are capable of viewing and processing audit log files.

4.5.5 Audit Log Backup Procedures

The audit log of Adobe Root CA shall be backed up after a significant event. Significant events include, but are not limited to, certificate issuances, revocations, and changes in the Trusted Roles.

4.5.6 Audit Collection System (internal vs. external)

With respect to CA (and subsidiary CAs) key generation and usage, manual audit trails of such activity are created by Adobe personnel. With respect to End-Entity Certificate application, validation, issuance, acceptance and revocation, audit logs are created and processed by the Entrust software.

4.5.7 Notification to Event-causing Subject

No stipulation.

4.5.8 Vulnerability Assessments

Adobe shall perform regular self assessments of security controls.

4.6 Records Archival

4.6.1 Types of Event Recorded

The types of events recorded in the audit trail files are described in section 4.5.1 of this CP.

4.6.2 Retention Period for Archive

Archives of the Adobe Root CA database and audit log files shall be retained for the life of the Adobe Root CA.

4.6.3 Protection of Archive

The same methods used to protect backups shall also be used to protect archives. In addition, archived materials shall be protected by being stored separately from the backups (different geographical location).

4.6.4 Archive Backup Procedures

Archives shall be backed up and securely stored. Considerations shall be given to the possibility of degradation of media used for storage of records in accordance with the CA's archive process and manufacturer's recommendations for the media at issue.

4.6.5 Requirements for Time-stamping of Records

No stipulation

4.6.6 Archive Collection System (internal or external)

The archive collection system (backup facility) for the Adobe Root CA database is internal to the Adobe Root CA system. The archive collection system (backup facility) for the audit trail files is described in this CP.

The archiving of both data stores onto separate media and secure storage of that media is external from the Adobe Root CA system.

4.6.7 Procedures to Obtain and Verify Archive Information

No stipulation.

4.7 Key Changeover

The Adobe Root CA root key has a life of 20 years. The Adobe Policy Authority handles all aspects of CA key changeover in accordance with its prescribed key management process. With respect to Subordinate CA key changeover, the Adobe PKI Policy Authority shall use commercially reasonable efforts to notify a Subordinate CA with appropriate notice prior to the expiration of a certificate. Note that since key renewal is not allowed, Subordinate CA's must regenerate and resubmit a newly generated Public Key with the renewal request.

4.8 Compromise and Disaster Recovery

4.8.1 Computing Resources, Software, and/or Data are corrupted

Appropriate software and data shall be backed up after significant changes are made to the system, which can be used to restore corrupted software or data, or to recover from a hardware failure.

4.8.2 Entity Public Key is revoked

If the Adobe Root CA Public Key is revoked, the CRL shall be updated and published, the CA may be brought down and a new root CA key generation process may occur. The Adobe Policy Authority shall notify Subordinate CA that a CA key changeover has occurred and Subordinate CA shall notify each applicable Subscriber that a CA key changeover has occurred.

4.8.3 Entity Key Compromise

4.8.3.1 Suspected Compromise

The Policy Authority shall meet to discuss any suspected key compromises. If a key compromise is confirmed, the steps in 4.8.3.2 shall be followed.

4.8.3.2 Key is Compromised

Once it is confirmed that the Adobe Root CA Private Key has been compromised, all certificates issued by the Root CA shall be revoked in a timely manner and the CRL shall be updated and published to the appropriate repository. Subscribers shall be notified of the compromise by the CA that issued their respective certificates. In the event that a new Adobe Root CA is established, Subscribers shall be required to regenerate new Key Pairs and to repeat the application process.

4.8.4 Secure Facility after a Natural or Other Type of Disaster

Detailed procedures shall be contained in the Adobe IS Disaster Recovery Plan, or in a suitable alternative document or combination of documents.

4.9 CA Termination

In the event that the Adobe Root CA ceases operation, all End-Entity Certificates shall be revoked.

5. PHYSICAL, PROCEDURAL, AND PERSONNEL SECURITY CONTROLS

The focus of physical security controls is to minimize exposure from environmental hazards and malicious actions that could harm data or information, severely delay the timeliness of processing or threaten the safety of personnel.

5.1 Physical Controls

The Adobe Root CA shall impose physical security requirements that provide similar levels of protection as those specified below.

The Root CA equipment shall be protected from unauthorized access while the cryptographic module is installed and activated. The Policy Authority shall implement physical access controls to reduce the risk of equipment tampering even when the cryptographic module is not installed and activated.

5.1.1 Site Location and Construction

The location and construction of the facility housing the Adobe Root CA 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 Adobe Root CA equipment and records.

5.1.2 Physical Access

The Adobe Root CA equipment shall be always protected from unauthorized access, and especially while the cryptographic module is installed and activated. Physical access controls shall be implemented to reduce the risk of equipment tampering even when the cryptographic module is not installed and activated.

These security mechanisms shall be commensurate with the level of threat in the equipment environment. Even though the Adobe Root CA plans to issue certificates at different levels of assurance, it shall be always operated and controlled at a level offering reasonably high assurances.

5.1.3 Power and Air Conditioning

No stipulation.

5.1.4 Water exposures

No stipulation.

5.1.5 Fire prevention and protection

No stipulation.

5.1.6 Media Storage

All media used to generate the Adobe Root CA shall be stored securely.

5.1.7 Waste Disposal

Paper documents and electronic media containing trusted elements of the Adobe Root CA or commercially sensitive or confidential information shall be securely disposed of as follows:

- Cryptographic devices are physically destroyed or zero-ized in accordance with the manufacturers' guidance prior to disposal;
- Electronic media is physically destroyed; and
- Paper documents are destroyed by using an approved secure shredding service.

5.1.8 Off-Site Backup

No stipulation.

5.2 Procedural Controls

5.2.1 Trusted Roles

All Adobe personnel performing functions critical to the trustworthiness of the Adobe Root CA are defined as Trusted Roles. Such roles include but are not limited to System Administrators, Security Officers, Master Users and Adobe executive personnel.

All personnel wishing to act as a Trusted Role must complete a Trusted Role Agreement and have it counter-signed by their immediate supervisor, a member of Adobe's Internal Audit staff, or an External Auditor.

5.2.2 Number of Persons Required per Task

As the Adobe Root CA is stored off-line, three of the five Master Users must present their credentials and be authenticated by the CA equipment before any actions can be taken on the Adobe Root CA system.

5.2.3 Identification and Authentication for Each Role

Each person performing a Trusted Role within the Adobe Root CA must be authorized to perform such functions. Approval as a trusted employee shall be documented by use of the Trusted Role Agreement.

5.3 Personnel Controls

5.3.1 Background, Qualifications, Experience, and Clearance

Requirements

All Adobe employees operating in a Trusted Role shall be approved by the Adobe Policy Authority.

5.3.2 Background Check Procedures

Adobe's Human Resource department shall perform background checks on all regular and intern employment candidates prior to offers being extended.

5.3.3 Training Requirements

No stipulation.

5.3.4 Retraining Frequency and Requirements

No stipulation.

5.3.5 Job Rotation Frequency and Sequence

No stipulation.

5.3.6 Sanctions for Unauthorized Actions

Contravention of the Adobe Root CA CP is subject to appropriate disciplinary actions.

5.3.7 Contracting Personnel Requirements

Short-term contractors must be authorized prior to being given access to the Adobe Root CA.

5.3.8 Documentation Supplied to Personnel

The Adobe Root CA Trusted Roles shall be provided with hard and/or soft copies of:

- Entrust/PKI Administration Guide;
- The Adobe Root CP (this document);
- The Adobe Root CPS or other suitable documentation detailing the operation of the Adobe Root CA; and
- Other guidelines and procedures necessary for operation of the Adobe Root CA.

6. TECHNICAL SECURITY CONTROLS

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

The key pair of the Adobe Root CA shall be generated in a hardware token that meets the requirements of FIPS 140-1 Level 3. The key pair of the Adobe Root CA shall be generated in a secure environment during a scripted and audited process.

Trusted Role key pairs shall be generated in software or hardware that is designed to meet FIPS 140-1 Level 1 requirements.

6.1.2 Private Key Delivery to Entity

For Adobe Root CA Trusted Roles, the private decryption key shall be provided securely to the user via PKIX-CMP protocol exchange between the Adobe Root CA and the Registration Authority. An Entrust authorization code is used to derive a MAC key which is then used to provide authentication and integrity protection on the session. For the digital signature key pair, no delivery of the private key is required, since the key pair is generated by the End-Entity.

Since subordinate CA signing key pairs are generated by the subordinate CAs, delivery of the private key is not required.

6.1.3 Public Key Delivery to Certificate Issuer

For Adobe Root CA Trusted Roles, are delivered securely by the Adobe Root CA using the PKIX-CMP protocol.

Subordinate CA's wishing to have a certificate issued by the Adobe Root CA must submit their request electronically through the use of a PKCS # 10 Certificate Signing Request (CSR).

6.1.4 CA Public Key Delivery to Users

The Adobe Root CA public key is delivered to the End-Entity using the PKIX-CMP protocol. Authenticity and integrity protection is based on a MAC key derived from the Entrust authorization code.

6.1.5 Key Sizes

The Adobe Root CA shall use RSA key pairs with a 2048-bit prime modulus.

6.1.6 Public Key Parameters Generation

Generation parameters shall be consistent with those of FIPS 140-1 Level 1.

6.1.7 Parameter Quality Checking

Generation parameters shall be consistent with those of FIPS 140-1 Level 1.

6.1.8 Hardware/Software Key Generation

Adobe's Root CA key pair shall be generated in hardware (e.g., a Luna CA3 tokens) that meets or exceeds FIPS 140-1 Level 3 requirements.

6.1.9 Key Usage Purposes (as per X.509 v3 key usage field)

The Adobe Root CA signing key shall be used to sign certificates and ARL/CRL's.

6.2 Private Key Protection

6.2.1 Standards for Cryptographic Module

At a minimum, FIPS 140-1 Level 3 rated cryptographic modules shall be used to store the Adobe Root CA key pair.

6.2.2 Private Key (n out of m) Multi-person Control

The Adobe Root CA shall enforce multi-person control (3 of 5) for highly sensitive operations such as generating Subordinate CAs and cloning the tokens.

6.2.3 Private Key Escrow

Private keys shall not be escrowed.

6.2.4 Private Key Backup

A backup of the Adobe Root CA's private key shall be created during the Root Key Generation Ceremony and stored in a FIPS 140-1 Level 3 hardware token.

6.2.5 Private Key Archival

See section 6.2.4 of this document.

6.2.6 Private Key Entry into Cryptographic Module

The Root CA's private keys shall be generated in cryptographic modules that meet or exceed FIPS 140-1 level 3 requirements.

6.2.7 Method of Activating Private Key

Three of five secret shares held by separate custodians on removable media shall be required for logical activation of the Adobe Root CA Private Key. The Adobe Root CA Private Key shall not be maintained online and shall only be utilized to sign its own Certificate and the Certificates of Subordinate CA's and Trusted Roles. The key for each Trusted Role is activated at the time of logon to the online Registration Authority administration system.

6.2.8 Method of Deactivating Private Key

The following are methods of deactivating private keys: logging out of the private key module, private key life span expiration, private key module timeout, and removal of the private key's hardware device.

6.2.9 Method of Destroying Private Key

All sensitive keys in memory shall be overwritten with zeros when no longer used. Permanent destruction of private keys is achieved with secure delete operations.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

No stipulation.

6.3.2 Usage Periods for the Public and Private Keys

The Adobe Root CA signing key lifetime is set to 20 years.

Test CA signing key lifetimes are set to 5 years.

Subordinate CA signing key lifetimes are set to 10 years.

Trusted Role certificates issued by the Adobe Root CA will have a validity period not to exceed two (2) years. End-Entities may use their private keys only during the validity period of the corresponding certificate. Additionally, they may not use their private keys before they have accepted the certificate from the Adobe Root CA (i.e., during the period between key generation and certificate acceptance). Public keys on expired certificates may be used to validate signatures on objects that were signed during the validity period of the certificate.

The maximum key lifetimes for End-Entities shall be:

- Encryption public key: 36 months (3 years).
- Verification public key 36 months (3 years).
- Signing private key 70% of the verification public key lifetime.

The signing private key lifetime must be less than or equal to the corresponding verification public key expiration date.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

Activation Data for the Adobe Root CA is maintained in secret shares as defined in section 6.2.7, Method of Activating Private Key. The Activation Data, in the form of passwords, is held secretly by the authorized individuals.

The Entrust software enforces the requirement that individuals performing trusted roles have passwords that meet the following requirements:

- It must have at least ten characters;
- It must have at least one upper-case letter
- It must have at least one digit;
- It must have at least one lower-case letter; and
- It must not contain many occurrences of the same character.

6.4.2 Activation Data Protection

The Adobe Root CA Trusted Roles choose passwords that meet the criteria specified in Section 6.4.1 of this document. Upon initial entry, the Entrust Authority software puts password through numerous hashing iterations, producing a password token. Only the password token is stored in the Trusted Role's client profile.

6.4.3 Other Aspects of Activation Data

No stipulation.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

The Adobe Root CA system information is protected from unauthorized access through a combination of operating system, PKI application, and physical controls.

6.5.2 Computer Security Rating

No stipulation.

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

The following controls are utilized to protect the development and operations of the Adobe Root CA:

- Commercial hardware and software (including updates, patches, etc.) is acquired from reliable sources using methods that ensure that hardware and software is not tampered with during shipment; and
- Hardware and software (including updates, patches, etc.) components are installed by trained and trusted personnel.

6.6.2 Security Management Controls

No stipulation.

6.6.3 Life Cycle Security Ratings

No stipulation.

6.7 Network Security Controls

Not applicable.

6.8 Cryptographic Module Engineering Controls

The Adobe Root CA utilizes a FIPS 140-1 level 3 using cryptographic hardware modules.

7. CERTIFICATE AND CRL PROFILES

7.1 Root Certificate Profile

The following fields of the X.509 version 3 certificate format are used in the Adobe Root CA certificate:

X.509 v3 Certificate Attributes/ Extensions	Critical / Non Critical	Value / Notes
Attributes		
Version		<ul style="list-style-type: none"> v3
SerialNumber		<ul style="list-style-type: none"> integer; unique to each certificate issued in the Adobe PKI domain
Signature		<ul style="list-style-type: none"> sha-1 w/ RSAEncryption – {1.2.840.113549.1.1.5}
Issuer		<ul style="list-style-type: none"> cn=Adobe Root CA , ou=Adobe Trust Services,, o=Adobe Systems Incorporated , c=US
Validity		<ul style="list-style-type: none"> 20 years notBefore and notAfter are specified
Subject		<ul style="list-style-type: none"> cn=Adobe Root CA , ou=Adobe Trust Services,, o=Adobe Systems Incorporated, c=US
SubjectPublicKeyInfo		<ul style="list-style-type: none"> rsaEncryption – {1.2.840.113549.1.1.1} RSA public key is 2048 bit public key
Extensions		
PrivateKeyUsagePeriod	Non-critical	<ul style="list-style-type: none"> N/A
AuthorityKeyIdentifier	Non-critical	<ul style="list-style-type: none"> contains a 20 byte SHA-1 hash of the subjectPublicKey in this certificate
SubjectKeyIdentifier	Non-critical	<ul style="list-style-type: none"> contains a 20 byte SHA-1 hash of the subjectPublicKey in this certificate
BasicConstraints		<ul style="list-style-type: none"> Subject Type = CA Path Length = 0
KeyUsage	Non-critical	<ul style="list-style-type: none"> Certificate Signing Off-line CRL Signing CRL Signing (06)
CRLDistributionPoints	Non-critical	<ul style="list-style-type: none"> http://crl.adobe.com/cds.crl cn=CRL1, cn=Adobe Root CA, OU=Adobe Trust Services, o=Adobe Systems Incorporated, c=US

X.509 v3 Certificate Attributes/ Extensions	Critical / Non Critical	Value / Notes
Netscape-cert-type	Non-critical	<ul style="list-style-type: none"> • SSL CA, SMIME CA, Signature CA (07)
EntrustVersInfo	Non-critical	<ul style="list-style-type: none"> • V6

7.1.1 Version Number(s)

See Section 7.1.

7.1.2 Certificate Extensions

See Section 7.1.

7.1.3 Algorithm Object Identifiers

See Section 7.1.

7.1.4 Name Forms

Certificates issued by the Adobe Root CA contain the full X.500 distinguished name of the certificate issuer and certificate subject in the issuer name and subject name fields.

7.1.5 Name Constraints

Name constraints may be utilized by the Adobe Root CA for certain subordinate CA classes.

7.1.6 Certificate Policy Object Identifier

See Section 7.1.

7.1.7 Usage of Policy Constraints Extension

The Policy Constraint extension is utilized when deemed necessary by the Policy Authority.

7.1.8 Policy Qualifiers Syntax and Semantics

No stipulation.

7.1.9 Processing Semantics for the Critical Certificate Policy Extension

No stipulation

7.2 CRL Profile

The Adobe PKI uses x.509v2 Certificate Revocation Lists (CRL's). The Entrust CA supports the issuing of full CRL's as well as CRL distribution points.

7.2.1 Version Number(s)

The Adobe Root CA issues X.509 Version 2 CRL's and supports the following fields:

- Version: Set to v2;
- Signature: Identifier of the algorithm used to sign the CRL;
- Issuer: The distinguished name of the Root CA;
- This update: Time of CRL issue;
- Next update: Time of the next CRL update;
- User certificate: Certificate serial number of a revoked certificate; and
- Revoked certificates: List of revoked certificates.

7.2.2 CRL and CRL Entry Extensions

The Adobe Root CA uses the following X.509 Version 2 CRL and CRL entry extensions:

- Authority Key Identifier: Contains a 20 byte hash of the CA certificate's subject public key information field; and
- CRL Number: A CRL number, which is incremented each time a CRL is created.

7.3 CDS SUBORDINATE CA CERTIFICATE PROFILE

The following fields of the X.509 version 3 certificate format must be used when issuing certificates to CDS Subordinate CA's:

X.509 v3 Certificate Attributes/ Extensions	Critical / Non Critical	Value / Notes
Attributes		
Version		<ul style="list-style-type: none"> v3
SerialNumber		<ul style="list-style-type: none"> integer; unique to each certificate issued in the Adobe PKI domain
Signature		<ul style="list-style-type: none"> sha-1 w/ RSAEncryption – {1.2.840.113549.1.1.5}
Issuer		<ul style="list-style-type: none"> cn=Adobe Root CA , ou=Adobe Trust Services, o=Adobe Systems Incorporated , c=US
Validity		<ul style="list-style-type: none"> 11 years notBefore and notAfter are specified
Subject		<ul style="list-style-type: none"> cn=TBD CDS CA , ou=TBD, o=TBD, c=US
SubjectPublicKeyInfo		<ul style="list-style-type: none"> rsaEncryption – {1.2.840.113549.1.1.1} RSA public key is 2048 bit public key
Extensions		
AuthorityKeyIdentifier	Non-critical	<ul style="list-style-type: none"> contains a 20 byte SHA-1 hash of the Root CA public key
KeyUsage	Non-critical	<ul style="list-style-type: none"> Certificate Signing Off-line CRL Signing CRL Signing (06)
SubjectKeyIdentifier	Non-critical	<ul style="list-style-type: none"> contains a 20 byte SHA-1 hash of the subjectPublicKey in this certificate
BasicConstraints	Critical	<ul style="list-style-type: none"> Subject Type=CA Path Length = 1
CertificatePolicies	Non-critical	<ul style="list-style-type: none"> 1.2.840.113583.1.2.1
ExtendedKeyUsage	Non-critical	<ul style="list-style-type: none"> 1.2.840.113583.1.1.5
CRLDistributionPoints	Non-critical	<ul style="list-style-type: none"> http://crl.adobe.com/cds.crl CN=CRL1, CN=Adobe Root CA, OU=Adobe Trust Service, O=Adobe Systems Incorporated, C=US
Entrust Version Info 1.2.840.113533.7.65.0	Non-critical	<ul style="list-style-type: none"> V6

7.3.1 Version Number(s)

See Section 7.3.

7.3.2 Certificate Extensions

See Section 7.3.

7.3.3 Algorithm Object Identifiers

See Section 7.3.

7.3.4 Name Forms

Certificates issued within the CDS PKI contain the full X.500 distinguished name of the certificate issuer and certificate subject in the issuer name and subject name fields, respectively.

7.3.5 Name Constraints

See Section 7.3.

7.3.6 Certificate Policy Object Identifier

See Section 7.3.

7.3.7 Usage of Policy Constraints Extension

No stipulation.

7.3.8 Policy Qualifiers Syntax and Semantics

The policy qualifier syntax is an IA5String that contains the URI for this CP. The semantics of this policy qualifier is that the application, under user control, can display part or all of the CP document as defined by the URI.

7.3.9 Processing Semantics for the Critical Certificate Policy Extension

Processing semantics is according to IETF RFC 3280.

8. SPECIFICATION ADMINISTRATION

8.1 Specification Change Procedures

Changes to items within this CP which, in the judgment of the Policy Authority, will have no or minimal impact on the End-Entities and Subordinate CA's using certificates and CRL's issued by the Adobe Root CA, may be made with no change to the CP or CPS version number and no notification to the users.

Changes to this CP or the CPS which, in the judgment of the Policy Authority that have a significant impact on the End-Entities and Subordinate CA's using certificates and CRL's issued by the Adobe Root CA, will be made with 90 days notice to the End-Entities and Subordinate CA communities and the version number of this CP or the CPS will be increased accordingly.

8.2 Publication and Notification Policies

No stipulation.

8.3 CP Approval Procedures

This CP and any subsequent changes are approved by the Adobe Policy Authority.

Appendix A – Terms and Definitions

Term	Definition
Adobe PKI	The policy, process and technology required to manage, use and rely on certificates that chain to the Adobe Root CA.
Adobe Policy Authority	Selected members of Adobe's management that define, review and approve polices related to the Adobe PKI.
Adobe Root CA	Adobe's root Certification Authority.
ARL	Authority Revocation List. Also known as CARL or Certification Authority Revocation List
CDS	Certified Document Services
Certificate Custodian	The individual responsible for the safe-keeping of a
Certified Document Services	A service offered by Adobe partners in which an Adobe .pdf document can be digitally signed by its author using a signature private key generated within the CDS PKI.
CRL	Certificate Revocation List
Directory	A system (hardware and software) used to store issued certificates and CRLs.
End Entity	End entity is a Subscriber
HSM	Hardware Security Module. See Token
Issuing CA	The Certification Authority that issues a certificate to either a subordinate CA or a Subscriber.
Level 1 CA	A CDS Level 1 Root CA or a CDS Level 1 Subordinate CA
Level 2 CA	A CDS Subordinate CA that has been issued its Certificate by a Level 1 Root CA or a CDS Level 1 Subordinate CA.
Organization	A legally recognized company, enterprise or governmental agency that has applied for or has been issued a certificate in the CDS PKI.
Partner Agreement	An agreement between Adobe Systems Incorporated and partners that details the terms and conditions in which both parties operate within the CDS PKI.
Registration Authorities	An entity that is responsible for identification and authentication of certificate subjects, but that does not sign or issue certificates.

Term	Definition
Relying Parties	An individual who uses an Adobe Acrobat product to validate a certified document.
Relying Party Agreement	Any agreement between a Relying Party and a CDS Subordinate CA or the Adobe Root CA.
Repository	A Directory or other mechanism for storing information related to the CDS PKI.
Root CA	The Adobe Root CA
Root RA	The Adobe Root CA's registration authority
Subscriber	An individual or organization that has been issued a certificate in the CDS PKI.
Subscriber Agreement	An agreement between CDS Subordinate CAs and Subscribers that binds Subscribers to certain terms and conditions for using CDS certificates.
Test CA	A Certification Authority managed by Adobe to issue Certificates used for testing purposes only
Token	A hardware device that is used to store either a Certification Authority's or a Subscriber's key pair and certificate chain and perform signing ...
Trusted Role	An individual tasked with managing a root CA's RA functionality.