Adobe Systems Incorporated

CDS Certificate Policy

October 2005
Revision #14

Revision History

Rev #	Date	Author	Description of Change(s)
0.1	2/7/03	Outside Counsel	First draft
0.2	2/10/03	Outside Counsel	Incorporate comments received from v0.1
0.3	2/13/03	Outside Counsel	Incorporate comments from v0.1 and v0.2 reviews.
0.4	2/14/03	Outside Counsel	Add comments from 2/13 review session
0.5	2/14/03	Outside Counsel	Minor revisions from status call and work on Section 2
0.6	2/27/03	Outside Counsel	Modifications based on discussions w/ potential partner(s)
0.7	3/10/03	Outside Counsel	Modifications based on discussions w/ potential partner(s)
0.8	3/27/03	Outside Counsel	Modifications based on discussions w/ potential partner(s)
0.9	11/14/03	Outside Counsel	Modifications based on discussions w/ potential partner(s)
10	12/04/03	Adobe Legal	Modifications based on discussions with potential partner
11	12/22/03	Outside Consultant	Modifications to the glossary and to section 7.1.7
12	01/08/04	Outside Consultant and Adobe Legal	Modifications to section 7.1.
13	01/16/04	Adobe Legal	Modifications based on discussions with partner in preparation for Subordinate CA generation ceremony
14	10/11/05	Adobe Legal	Modifications to Section 4.4.10 and 6.1.5.

1. INTRODUCTION

1.1 Overview

Certified Document Services (CDS) is a new platform offering first available in the Acrobat 6.0 product family. Using digital signature technology, CDS provides recipients with assurances that certified PDF documents are authentic – that they did originate from their stated author and the portion of the document signed by the author have not been modified since authoring.

While digital signature technology is not new, Adobe is taking a leadership position working with security partners to provide a solution that is easy to use for document authors and recipients on the Adobe PDF platform. Document recipients using the free Adobe Reader on supported platforms will have the ability to automatically validate a certified document without additional software or configuration.

Adobe Systems Incorporated (Adobe) has contracted with one or more 3rd parties to provide Certification Authority (CA) services including all registration authority (RA) functionality. Authors interested in creating certified documents will register with one of these authorized 3rd parties, have their identification information verified and then be provided with a certificate used in Adobe Acrobat Standard or Professional to certify documents.

All 3rd parties providing CA services for Certified Document Services will be governed by the following policy.

1.2 Identification

This Certificate Policy (CP or Policy) is called the CDS Certificate Policy.

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

The extended key usage OID for the CDS PKI is: 1.2.840.113583.1.1.5.

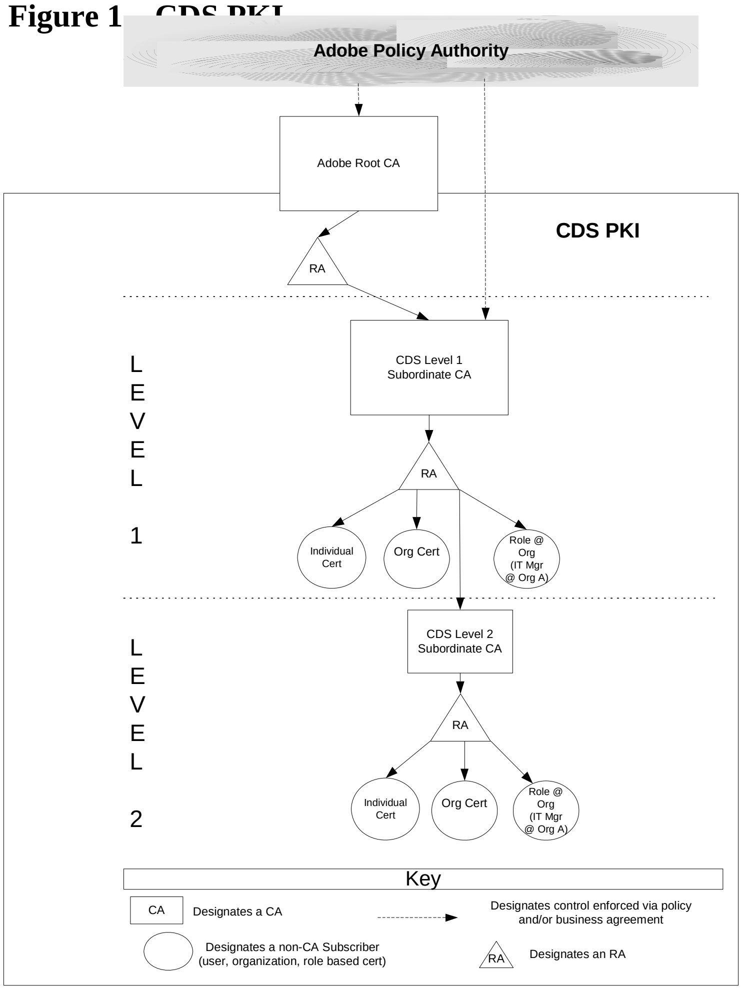
1.3 Community and Applicability

The community for this Policy includes all CDS Subordinate CAs, RAs, and Subscribers whose certificates chain to the Adobe Root CA embedded in Acrobat® by Adobe, along with all Relying Parties who rely on such certificates.

Certificates issued within the CDS PKI community shall have the certificate policy extension populated with the OID identified in Section 1.2

Subscriber certificates issued by CDS Subordinate CAs are to be used only for digitally signing Adobe Acrobat documents.

Figure 1 CDS PKI


Adobe Policy Authority
Adobe Root CA
CDS PKI
RA
CDS Level 1 Subordinate CA
LEVEL 1
RA
Individual Cert
Org Cert
Role @ Org (IT Mgr @ Org A)
CDS Level 2 Subordinate CA
LEVEL 2
RA
Individual Cert
Org Cert
Role @ Org (IT Mgr @ Org A)
Key
CA
Designates a CA
Designates control enforced via policy and/or business agreement
Designates a non-CA Subscriber (user, organization, role based cert)
RA
Designates an RA

1.3.1 Certification Authorities

Certification Authorities (CAs) are authorized 3rd parties that create and issue CDS certificates to Subscribers under this Policy.

1.3.2 Registration Authorities

Registration Authorities (RAs) manage the certificate lifecycle for their respective CAs. RAs are responsible for requesting the CA to issue and revoke certificates in accordance with this Policy, as well as any additional relevant policies and procedures including their respective CPSs, operating procedures, etc.

1.3.3 End Entities

End Entities are Subscribers and Relying Parties.   A Subscriber is any authorized individual, hardware device or organization that has a CDS certificate issued to them and uses that certificate to sign a CDS document.

Relying Parties are recipients of CDS documents who wish to verify the Subscriber's signature.

1.3.4 Applicability

CDS signing certificates may only be issued by authorized CAs to Subscribers in accordance with this Policy. CDS certificates may only be used to digitally sign and verify Adobe Acrobat documents.

1.3.5 Policy Authority

This Policy is managed by the Adobe Policy Authority. The Adobe Policy Authority consists of selected members of Adobe's management team.

1.4 Contact Details

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

2. GENERAL PROVISIONS

2.1.1 CA Obligations

2.1.1.1 Root CA Obligations

In general, the Root CA shall:

- utilize the appropriate software and hardware required to initiate and operate the Root CA within the CDS PKI (see Figure 1)
- use commercially reasonable efforts to generate keying material in a manner that ensures reasonable trust and integrity;
- sign a root certificate for the CDS PKI in a high assurance (offline) environment;
- issue certificates to itself, and other entities in accordance with the Root Authority Certificate Policy;
- as required, revoke certificates; and
- publish CRLs as needed or at least once per year.

2.1.1.2 Level 1 CA Obligations

In general, each Level 1 CA shall:

- represent and warrant to all Relying Parties placing reasonable reliance on a CDS CA-issued Certificate that chains up to the Level 1 CA that the (a) Level 1 CA took reasonable steps (no less than the procedures set forth in Sections 3.1.8 and 3.1.9) to verify the information contained in the Certificate is accurate, (b) information in the Certificate accurately reflects the information provided to the Level 1 CA by the Subscriber in all material respects, (c) Subscriber has accepted the Certificate according to the provisions of this policy, (d) Level 1 CA has complied in all material respects with this policy and its CPS, and (e) Level 1 CA has auditing procedures in place to ensure that all Level 2 CAs signed by such Level 1 CA has complied in all material respects with this policy and the applicable CPS;
- represent and warrant to the Adobe Root CA that all Level 2 CAs are and will be compliant with this policy;
- maintain records (including without limitation CRLs) of the users and documents necessary to respond to requests concerning its operation for as

long as the applicable record or document is valid but in no event less than three (3) years;

- revoke certificates that it issues according to the provisions in this policy regarding revocation, including, without limitation, the provisions of Section 4.4;
- ensure that all potential Subscribers are bound to a Subscriber Agreement (see also Section 2.1.3.2.1 and Section 2.1.3.2.2);
- ensure that each potential Subscriber is notified that a Certificate has been issued;
- upon revocation of a Certificate, ensure that the Subscriber is notified of the revocation by email, postal mail, telephone, or facsimile;
- provide notification of Certificate revocation via CRLs in a Repository, as more fully specified in Section 2.6;
- provide renewal and replacement of Certificates; and
- publish and adhere to a privacy policy.

2.1.1.3 Level 2 CA Obligations

In general, each Level 2 CA shall:

- represent and warrant to all Relying Parties placing reasonable reliance on a CDS CA-issued Certificate that chains up to the Level 2 CA that the (a) Level 2 CA took reasonable steps (no less than the procedures set forth in Sections 3.1.8 and 3.1.9) to verify the information contained in the Certificate is accurate, (b) information in the Certificate accurately reflects the information provided to the Level 2 CA by the Subscriber in all material respects, (c) Subscriber has accepted the Certificate according to the provisions of this policy, and (d) CDS Subordinate CA has complied in all material respects with this policy and its CPS;
- maintain records (including without limitation CRLs) of the users and documents necessary to respond to requests concerning its operation for as long as the applicable record or document is valid but in no event less than three (3) years;
- revoke certificates that it issues according to the provisions in this policy regarding revocation, including, without limitation, the provisions of Section 4.4;
- ensure that all potential Subscribers are bound to a Subscriber Agreement (see also Section 2.1.3.2.1 and Section 2.1.3.2.2);
- ensure that each potential Subscriber is notified that a Certificate has been issued;

- upon revocation of a Certificate, ensure that the Subscriber is notified of the revocation by email, postal mail, telephone, or facsimile;
- provide notification of Certificate revocation via CRLs in a Repository, as more fully specified in Section 2.6;
- provide renewal and replacement of Certificates; and
- publish and adhere to a privacy policy.

2.1.2 RA Obligations

2.1.2.1 Root RA Obligations

Trusted Roles manage each Root RA. The Trusted Roles shall ensure the identity and authentication of entities to which it issues certificates (e.g., Trusted Roles and CDS Subordinate CAs), and shall issue requests that cause the Root CA to issue CDS Subordinate CA certificates to those entities that are compliant with this Policy.

The Trusted Roles shall verify the accuracy and authenticity of the information provided by applicants for CDS Subordinate CA certificates and other Trusted Roles at the time of application for a certificate. The Root RA shall validate revocation requests and communicate authorized revocation requests to the Root CA.

2.1.2.2 CDS RA Obligations

A CDS Subordinate CA may delegate specific registration activities to one or more CDS RAs, provided that the CDS Subordinate CA remains responsible for the services provided by its CDS RAs and the CDS CA warrants that the activities of its CDS RAs will be conducted in accordance with this policy. A CDS RA shall perform all delegated registration functions in accordance with the requirements of this policy, and comply with a CPS approved by the Adobe Policy Authority for use with this policy.

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 policy 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, passphrases, or other information or mechanisms used to protect their private keys;

- Request revocation of its certificate if it has any 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 Subscribers

In general and as specified in a Subscriber Agreement between the CDS Subordinate CA and the Subscriber, a Subscriber shall:

- accurately represent itself in all communications with the CDS Subordinate CA;
- at all times, protect the private key associated with the public key in any certificates issued by a CDS Subordinate CA in accordance with this policy;
- notify, in a timely manner, the CDS Subordinate CA that issued its certificate of suspicion that its private key is compromised or is reasonably believed to have been compromised. Such notification shall be made with the CDS Subordinate CA as specified in the CDS Subordinate CA's CPS; and
- abide by all the terms, conditions, and restrictions in this policy and in the applicable Subscriber Agreement.

The Root CA and CDS Subordinate CAs reserve the right to revoke the certificate of any Subscriber who violates the obligations specified in this Section 2.1.3.2 of this policy or in the applicable Subscriber Agreement. If such a violation occurs, the certificate of the Subscriber shall immediately be revoked by the CDS Subordinate CA and other appropriate actions taken.

Subscribers may either apply for certificates directly or an organization acting on behalf of a Subscriber or group of Subscribers may apply for certificate(s).

2.1.3.2.1 Applicant is an individual

When the applicant is an individual Subscriber applying for a certificate in the name of that individual or in the name of the role of that individual within an organization, the CDS Subordinate CA shall require that the Subscriber enter into a binding Subscriber Agreement which obligates the Subscriber to:

(a) generate a public key pair using a trustworthy system, or use a key pair generated in a secure hardware token by the CDS Subordinate CA or its RA and take all reasonable precautions to prevent any loss, disclosure, or unauthorized use of the private key;
(b) warrant that all information and representations made by the Subscriber that are included in the certificate application are true;
(c) use the certificate exclusively for CDS purposes, consistent with this policy; and
(d) request certificate revocation immediately upon any actual or suspected loss, disclosure, or other compromise of the Subscriber's private key.

2.1.3.2.2 Applicant is an organization acquiring a certificate on behalf of an individual Subscriber

When the applicant is an organization acquiring and managing a certificate on behalf of an individual Subscriber (in the name of that individual or in the name of the role of that individual within the organization), the CDS Subordinate CA shall require the organization to:

(a) maintain processes that assure that the private key can be used only with the knowledge and explicit action of the Subscriber;
(b) maintain information that permits a determination of who signed a particular document;
(c) assure that the certificate subject has received security training appropriate for the purposes for which the certificate is issued;
(d) notify the CDS Subordinate CA immediately upon any actual or suspected loss, disclosure, or other compromise of the Subscriber's private key;
(e) ensure that the Subscriber named in the certificate or responsible for the use of the private key corresponding to the public key in the certificate enters into a binding Subscriber Agreement which obligates the Subscriber to:

    i. generate a public key pair using a trustworthy system, or use a key pair generated in a secure hardware token by the CDS Subordinate CA or its RA and take all reasonable precautions to prevent any loss, disclosure, or unauthorized use of the private key;
    ii. acknowledge that the information identifying the Subscriber in the certificate is true and accurate, or notify the CDS Subordinate CA immediately upon any inaccuracies in that information;
    iii. use the certificate exclusively for CDS purposes, consistent with this policy; and

iv. request certificate revocation immediately upon any actual or suspected loss, disclosure, or other compromise of the Subscriber's private key.

2.1.3.2.3 Applicant is an organization acquiring a certificate on behalf of the organization

When the applicant is an organization acquiring and managing a certificate on behalf of the organization (i.e., an organizational certificate), the CDS Subordinate CA shall require the organization to:

(a) maintain processes, including, without limitation, changing of activation data, that assure that each private key can be used only with the knowledge and explicit action of only one human being within the organization (the certificate custodian);

(b) maintain information that permits a determination of who signed a particular document;

(c) assure that the certificate custodian has received security training appropriate for the purposes for which the certificate is issued;

(d) prevent sharing of organizational certificates amongst members of the organization;

(e) acknowledge that the information identifying the organization in the certificate is true and accurate, or notify the CDS Subordinate CA immediately upon any inaccuracies in that information;

(f) ensure that the certificate custodian enters into a binding Subscriber Agreement which obligates the certificate custodian to:

i. generate a public key pair using a trustworthy system, or use a key pair generated in a secure hardware token by the CDS Subordinate CA or its RA and take all reasonable precautions to prevent any loss, disclosure, or unauthorized use of the private key;

ii. use the certificate exclusively for CDS purposes, consistent with this policy;

iii. not share the certificate nor any activation data related to the private key corresponding to the public key in the organizational certificate; and

iv. request certificate revocation immediately upon any actual or suspected loss, disclosure, or other compromise of the Subscriber's private key;

(g) notify the CDS Subordinate CA immediately upon any actual or suspected loss, disclosure, or other compromise of the private key corresponding to the public key in the organizational certificate; and

(h) request revocation of an organizational certificate upon any actual or suspected loss, disclosure, or other compromise of the private key corresponding to the public key in the organizational certificate.

2.1.4 Relying Party Obligations

In addition to any other Relying Party obligations in the Acrobat End User License Agreement, the CDS Subordinate CA shall use commercially reasonable efforts to notify all relying parties that reliance on a CDS-signed document is only permitted if verified on a Supported Platform, including, without limitation, via the user Notice field within each Certificate it publishes. For the purposes of this policy, Supported Platform means those applications specified on the CDS information web page, currently http://www.adobe.com/security/partners_cds.html.

2.1.5 Repository Obligations

See Section 2.6.

2.2 Liability

2.2.1 Adobe Root CA Liability

2.2.1.1 Warranty Disclaimers by Adobe Root CA

In addition to any other warranty disclaimers in any CDS Provider Agreements, the Adobe Root CA disclaims any and all warranties related to any certificates issued in the CDS 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 any entities other than the Adobe Root CA;
- related to the security provided by any cryptographic process implemented by any entities other than 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 Adobe Root CA Liability

Under no circumstances will the Adobe Root CA 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 direct, 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 policy.

Adobe accepts no responsibility or liability for any transactions relying upon certificates issued by any CDS Subordinate CA. The CDS Subordinate CA issuing further subordinated CDS Subordinate CA certificates or Subscriber certificates that chain to the certificate of the Adobe Root CA accepts liability for those CDS Subordinate CA or Subscriber certificates according to the CPS of the CDS Subordinate CA, or the terms and conditions of any Subscriber Agreement, Relying Party Agreement, or other applicable contract with the CDS Subordinate CA.

2.2.2 CDS Subordinate CA Liability

A CDS Subordinate CA is responsible to any Subscriber to whom it has issued a certificate, and to all relying parties who reasonably rely on such certificate in accordance with Section 2.1.4, for damages suffered by such persons that are caused by the failure of the CDS Subordinate CA to comply with the terms of its CPS, its Subscriber Agreement, or its Relying Party Agreement and sustained by such persons as a result of the use of or reliance on the certificate.

2.2.2.1 Warranty Disclaimers by a CDS CA

Except as expressly provided in this policy, or in a Subscriber Agreement or Relying Party Agreement, each CDS Subordinate CA may disclaim all other warranties and obligations of any type, including, without limitation, any warranties of merchantability, fitness for a particular purpose, or accuracy of information provided.

2.2.2.2 Limitations on CDS CA Liability

Each CDS Subordinate CA may limit its liability under this policy to an amount specified in the certificate or an applicable contract or its CPS, except in no cases shall such an amount be less than five thousand dollars ($5,000.00).

2.2.3 RA Liability

See Section 2.1.2.2.

2.3 Financial Responsibility

2.3.1 Indemnifications

2.3.1.1 By Subscribers

When a Subscriber accepts a certificate from a CDS Subordinate CA, the CDS Subordinate CA shall ensure that in its Subscriber Agreement each Subscriber indemnify the Root CA to which the Subscriber’s certificate chains and the CDS Subordinate CA for any and all third party liability, claims, demands (including direct, indirect, special and consequential damages), losses or damages, and all costs and expenses, including reasonable attorney's fees, caused by any breach of the Subscriber Agreement, including, without limitation, as a result of reliance on any misrepresentation of a material fact by that Subscriber.

2.3.1.2 By relying parties

In addition to any Relying Party agreements (including, without limitation the Adobe Acrobat EULA), when a Relying Party accepts a digitally signed CDS document from a Subscriber, the CDS Subordinate CA shall use all reasonable efforts to require the Relying Party to indemnify the Root CA and the CDS Subordinate CA for any third party losses or damages caused by any breach of any Relying Party Agreements, EULAs, or PKI Disclosure Statement, including, without limitation any failure to check the certificate status prior to any reliance on a digital signature from a Subscriber.

2.3.1.3 By CDS CAs

In addition to any other indemnities in any CDS Partner Agreements, each CDS Subordinate CA shall indemnify Adobe and the Adobe Root CA for any losses or damages caused as a result of (a) any erroneous issuing of certificates; and (b) any non-CDS Certificates issued by the CDS CA that verify up to the Adobe Root CA.

2.3.2 Fiduciary Relationships

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

2.3.3 Administrative Processes

No stipulation

2.4 Interpretation and Enforcement

2.4.1 Governing Law

No stipulation in this policy (since addressed in the applicable CDS Provider Agreement).

2.4.2 Severability, Survival, Merger, Notice

No stipulation in this policy (since addressed in the applicable CDS Provider Agreement).

2.4.3 Dispute Resolution Procedures

No stipulation in this policy (since addressed in the applicable CDS Provider Agreement).

2.5 Fees

2.5.1 Certificate Issuance or Renewal Fees

No stipulation in this policy (since addressed in the applicable CDS Subordinate CA Provider Agreement).

2.5.2 Certificate Access Fees

No stipulation in this policy (since addressed in the applicable CDS Subordinate CA Provider Agreement).

2.5.3 Revocation or Status Information Access Fees

No stipulation in this policy (since addressed in the applicable CDS Subordinate CA Provider Agreement).

2.5.4 Fees for Other Services Such as Policy Information

No stipulation in this policy (since addressed in the applicable CDS Subordinate CA Provider Agreement).

2.5.5 Refund Policy

No stipulation in this policy (since addressed in the applicable CDS Subordinate CA Provider Agreement).

2.6 Publication and Repository

2.6.1 Publication of CA Information

2.6.1.1 Publication of Root CA Information

The Repository of the Adobe Root CA operating under this policy shall contain 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 (CRLs) (if any) as published in accordance with the Operational Requirements section of this policy; 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.

2.6.1.2 Publication of CDS Subordinate CA Information

Each CDS Subordinate CA shall maintain a Repository that, at a minimum, contains the following:

- one or more Certificate Revocation Lists (CRLs) issued by the CDS Subordinate CA, such that notice is provided of all revoked Certificates within the CDS PKI;
- copies of past and current versions of its CPS, indicating the effective period of each copy of the CPS

2.6.2 Frequency of Publication

2.6.2.1 Frequency of Publication of Adobe Root CA Information

The Adobe Root CA shall immediately publish the certificates it issues. Information relating to the revocation of a CDS Subordinate CA certificate is published in accordance with the profile in Section 7.2.

2.6.2.2 Frequency of Publication of CDS Subordinate CA Information

Each certificate shall be published in the Repository by the CDS Subordinate CA following issuance and acceptance of the certificate in accordance with Section 4.2 and Section 4.3 of this policy.

A CRL shall be published by the CDS Subordinate CA in its Repository at least every 24 hours in accordance with Section 4.4 of this policy.

2.6.3 Access Controls

Each CDS Subordinate CA shall use reasonable efforts to make the Repository available to all parties 24 hours per day, seven days per week, subject to routine maintenance.

2.6.4 Repositories

See section 2.6.1.

2.7 Compliance Audit and Reporting

2.7.1 Frequency of Entity Compliance Audit

Each CDS Subordinate CA shall undergo an annual WebTrust for CAs audit to review (a) the compliance of the CDS Subordinate CA with its obligations under its CPS and (b) its compliance with this policy (“Annual Recurring Audit”).

2.7.2 Identity/Qualifications of Auditor

The auditor who performs the Annual Recurring Audit shall:

(a) be a licensed certified public accountant (CPA);
(b) hold an appropriate designation (including, without limitation, Certified Information Systems Auditor (CISA), Certified Information Systems Security Practitioner (CISSP), or other designation approved by the CDS PA); or
(c) have demonstrated expertise in computer and information security.

2.7.3 Auditor's Relationship to Audited Party

The auditor for a Webtrust audit shall be independent of the CDS Subordinate CA and shall have no other relationship that would impair its independence and objectivity under Generally Accepted Auditing Standards.

2.7.4 Topics Covered by Audit

The Annual Recurring Audit shall follow the then-current WebTrust for CAs audit program as published by the AICPA.

2.7.5 Actions Taken as a Result of Deficiency

CDS Subordinate CA management shall inform the Adobe Policy Authority of (a) each deficiency notice, (b) the CDS Subordinate CA proposed response to such deficiency notice and (c) the timeline for implementing such response. The Adobe Policy Authority and the CDS Subordinate CA shall mutually agree to each proposed response and the corresponding timeline for implementation.

2.7.6 Communication of Results

Upon completion of the Annual Recurring Audit, the CDS Subordinate CA shall communicate the Summary of WebTrust audit results, along with all sections of the WebTrust results that directly relate to the CDS PKI.

2.7.7 Quarterly Reporting

The CDS Subordinate CA shall submit an operational report quarterly to the Adobe Policy Authority in accordance with the requirements of the CDS Service Provider Agreement.

2.8 Confidentiality

2.8.1 Types of Information to be Kept Confidential

No stipulation in this policy (since addressed in the applicable CDS Service Provider Agreement).

2.8.2 Types of Information not Considered Confidential

No stipulation in this policy (since addressed in the applicable CDS Service Provider Agreement).

2.8.3 Disclosure of Certificate Revocation/Suspension Information

No stipulation in this policy (since addressed in the applicable CDS Service Provider Agreement).

2.8.4 Release to Law Enforcement Officials

No stipulation in this policy (since addressed in the applicable CDS Service Provider Agreement).

2.8.5 Release as Part of Civil Discovery

No stipulation in this policy (since addressed in the applicable CDS Service Provider Agreement).

2.8.6 Disclosure Upon Owner's Request

No stipulation in this policy (since addressed in the applicable CDS Service Provider Agreement).

2.8.7 Other Information Release Circumstances

No stipulation in this policy (since addressed in the applicable CDS Service Provider Agreement).

2.9 Intellectual Property Rights

No stipulation in this policy (since addressed in the applicable CDS Service Provider Agreement).

3. IDENTIFICATION AND AUTHENTICATION

3.1 Initial Registration

3.1.1 Types of Names

Names for Subordinate CAs and Subscribers are of the X.500 Distinguished Name (DN) form in accordance with PKIX Part 1. All certificates issued as part of this PKI shall have at a minimum a Country (c), OrganizationName (o) attribute, and a CommonName (cn) attribute. The cn may be an individual's name, an organization's name or the name of a specific role within an organization (e.g. Chief Financial Officer). Together, these attributes make up the Subscriber's distinguishedName (dn). Each dn must be unique.

All attributes are as defined in ITU-T Recommendation X.521.

3.1.2 Need for Names to be Meaningful

Names used in CDS certificates must be meaningful in that they can be understood and used by Rely Parties and linked to a Subscriber, an Organization 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

No stipulation.

3.1.5 Name Claim Dispute Resolution Procedure

The Adobe Policy Authority will 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

3.1.7.1 CDS Subordinate CA

CDS Subordinate CAs are required to prove possession of the private key that corresponds to the public key included in their certificate request. This is to be done by using the CDS Subordinate CA's private key to sign a certificate request and providing that request to the Issuing CA. The Issuing CA will validate the signature using the CDS Subordinate CA's public key included in the certificate request.

3.1.7.2 Subscriber

Subscribers generating their own private keys must prove possession of that private key by using it to sign a certificate request and providing that request to the Issuing CA. The Issuing CA will validate the signature using the Subscriber's public key.

Private keys generated outside the control of Subscribers must be generated in a secure and controlled manner and delivered to the certificate subject or an authorized representative via an accountable method (see Section 4.2).

3.1.8 Standard Authentication of Organization Identities

Organizations wishing to receive either CDS Subordinate CA or Subscriber certificates must include the organization name, address and Dun & Bradstreet number (or similar 3rd party verification) in their application to the Issuing CA.

In the case of an organization applying for a Level 1 CDS Subordinate CA certificate, the Adobe Policy Authority will be responsible for verifying the information, in addition to the authentication of the requesting representative and the representative's authorization to act in the name of the organization.

Level 2 CDS Subordinate CA certificate requests shall be verified by the Issuing CA receiving the request.

A CDS Subordinate CA's RA shall verify the organization's identity, in addition to the authentication of the requesting representative and the representative's authorization to act in the name of the organization.

3.1.9 Authentication of Individual Identity

CDS Subordinate CA shall authenticate individual identities in accordance with the practices set forth in the CPS (as approved by the Adobe Policy Authority).

3.2 Routine Rekey

3.2.1 Rekey of CDS Subordinate CAs

CDS Subordinate CAs may use their current signature key to sign a request for rekey. Upon receipt of a valid Rekey Request, the Issuing CA will issue a new certificate that includes the new key pair for the CDS Subordinate CA.

3.2.2 Rekey of Subscribers

Subscribers may use their current valid signature key to sign a request for rekey. Upon receipt of a valid Rekey Request, the CDS Subordinate CA that issued the original certificate will issue a new certificate that includes the new key pair for the Subscriber.

3.3 Rekey after Revocation

For CDS Subordinate CAs' and Subscribers' Certificates that have been revoked, rekey will not be permitted. The CDS Subordinate CA's and Subscriber's identity must be re-established through the existing registration process.

3.4 Revocation Request

Revocation requests must be authenticated prior to any action being taken.

4. OPERATIONAL REQUIREMENTS

4.1 Certificate Application

4.1.1 CDS Subordinate CA Certificate Application

All entities wishing to become a CDS Subordinate CA must follow the application process as defined by the Adobe Policy Authority including completing and submitting an application and executing any required CDS Service Provider Agreement. The Adobe Policy Authority will review and approve (if so decided) all applications for CAs applying for certificates issued by the Adobe Root CA.

4.1.2 Subscriber Certificate Application

All entities wishing to become Subscribers in the CDS PKI must follow the application process as approved by the Adobe Policy Authority including completing and submitting an application and agreeing to any required Subscriber Agreement. An authorized representative of the CDS Subordinate CA will review the application and make a decision as to whether or not a certificate should be issued to the applicant.

4.2 Certificate Issuance

Certificates must be issued to applicants in a secure manner only after the application has been approved. The issuing CA or its RA is responsible for the accurate transfer of data supplied by Subscribers into the applicable Certificates so that the Certificates accurately reflect the data supplied. The issuing CA shall issue certificates in accordance with the certificate profile set forth in the applicable CPS.

4.3 Certificate Acceptance

Certificate acceptance must be performed in accordance with the CDS Service Provider Agreement and/or the Subscriber Agreement.

4.4 Certificate Suspension and Revocation

4.4.1 Circumstances for Revocation

A certificate may be revoked for any of the following reasons:

a) The Adobe Policy Authority requests that the CDS Subordinate CA or Subscriber certificate be revoked.

b) The CDS Subordinate CA management team receives an authorized request for revocation.

c) The Subscriber is no longer authorized to represent the Organization or the Subscriber losses control of the private key.

d) The Subscriber has violated the Subscriber Agreement.

4.4.2 Who can Request Revocation

A certificate issued under this Policy may be revoked upon receipt of a request from an authorized representative of the Adobe Policy Authority, a CDS Subordinate CA, a Subscriber, or an authorized representative of a Subscriber.

4.4.3 Procedure for Revocation Request

Procedures for requesting revocations shall be addressed in the each CDS Subordinate CA's CPS.

4.4.4 Revocation Request Grace Period

No stipulation

4.4.5 Circumstances for Suspension

Suspension of certificates is not supported in the CDS PKI environment.

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.

CDS Subordinate CAs shall issue routine ARLs once every year and CRLs at least once every 24 hours. If issuing combined ARL/CRLs, then issuance of the combined ARL/CRL shall occur at least once every 24 hours. In the case of a certificate being revoked due to a private key being compromised, the CDS Subordinate CA shall issue an updated ARL/CRL within 24 hours of the revocation.

4.4.10 ARL/CRL Checking Requirements

Relying parties must retrieve ARL/CRLs at least once every 24 hours before relying on a document signed using a CDS certificate except for CDS certificates issued for the purpose of Time-stamping services.

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 Key Compromise

In the case that a CDS Subordinate CA's key is compromised, the Issuing CA will issue an updated ARL. The issuance of the ARL shall be authorized by the Issuing CA's management as soon as the compromise has been confirmed.

4.5 Security Audit Procedures

4.5.1 Types of Event Recorded

All material security events must be automatically recorded in audit logs.

4.5.2 Frequency of Processing Log

The Adobe Root and Subordinate CAs shall establish procedures for the regular review of audit logs.

4.5.3 Retention Period for Audit Log

Audit logs shall be maintained on-site as specified in the Adobe Root CPS and CDS Subordinate CAs' CPS.

4.5.4 Protection of Audit Log

Access to audit logs shall be protected by a combination of physical and logical controls as specified in the Adobe Root CPS and each CDS Subordinate CA's CPS.

4.5.5 Audit Log Backup Procedures

As specified in the Adobe Root CPS and each CDS Subordinate CA's CPS, a backup of the audit log shall be made prior to any log being sent off-site for storage.

4.5.6 Audit Collection System (internal vs. external)

No stipulation

4.5.7 Notification to Event-causing Subject

No stipulation

4.5.8 Vulnerability Assessments

Partners managing CDS Subordinate CAs shall perform regular self assessments of security controls.

4.6 Records Archival

4.6.1 Types of Event Recorded

The Adobe Root and each CDS Subordinate CA shall archive records with sufficient detail so that proper operation of the CA can be established.

Item / Data to be Archived	Required (Yes/No)
Certificate Policy	Yes
Certification Practice Statement	Yes
Contractual Obligations	Yes

Item / Data to be Archived	Required (Yes/No)
System & Equipment Configurations	Yes
Modification & Updates to System or Configuration (Scripts)	Yes
Revocation Requests	Yes
Subscriber Identity Authentication (per Section 3.1.9)	Yes
Documentation of Receipt and Acceptance of Certificates	Yes
Documentation of Receipt of Tokens	Yes
All Certificates Issued or Published	Yes
A Complete Listing of All Certificates Revoked	Yes
All Audit Logs	Yes
Other Data or Applications Needed to Verify Archive Contents	Yes
Documentation Required by Compliance Auditors	Yes

4.6.2 Retention Period for Archive

Archives shall be kept for a minimum of three (3) years but may be required to be kept for a longer period of time as provided for in an applicable CDS Service Provider Agreement.

4.6.3 Protection of Archive

Archives shall be protected in a manner that prevents unauthorized users from writing to, modifying or deleting them. Additionally, the archive media will be provided adequate protection from environmental threats such as temperature, humidity, and magnetism.

4.6.4 Archive Backup Procedures

Archive backup procedures are to be followed as prescribed in the Adobe Root CPS and each CDS Subordinate CA’s CPS.

4.6.5 Requirements for Time-stamping of Records

No stipulation

4.6.6 Archive Collection System (internal or external)

No stipulation

4.6.7 Procedures to Obtain and Verify Archive Information

Procedures to obtain and verify archive information are to be followed as prescribed in the Adobe Root CPS and each CDS Subordinate CA’s CPS.

4.7 Key Changeover

The Adobe Root and each CDS Subordinate CA shall establish key changeover procedures in its CPS. Consideration should be given to the level of protection used to secure the signing private key when determining specific key changeover procedures.

4.8 Compromise and Disaster Recovery

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

Procedures detailing how to recover from corrupted hardware, software and/or data shall be established by the Adobe Root and each CDS Subordinate CA.

4.8.2 Entity Public Key is Revoked

CDS Subordinate CAs shall have a process for reestablishing a secure environment after their public key is revoked. These procedures shall address the steps necessary to provide the new public key to the necessary users and how to recertify them.

4.8.3 Entity Key is Compromised

If the Adobe Root CA’s or a CDS Subordinate CA’s signature key is compromised or suspected of being compromised, the Adobe Policy Authority shall be notified immediately.

Procedures to generate a new key pair will be followed in accordance with the compromised CA’s CPS.

4.8.3.1 Suspected Compromise

See Section 4.8.3

4.8.3.2 Key is Compromised

See Section 4.8.3

4.8.4 Secure Facility after a Natural or Other Type of Disaster

In the case where the facility housing either the Adobe Root CA or a CDS Subordinate CA is destroyed; thus disrupting the CA’s ability to manage certificates, the Adobe Policy Authority shall be notified immediately.

Disaster recovery procedures will be followed in accordance with the affected CA’s CPS.

4.9 CA Termination

The Adobe Policy Authority shall be notified prior to any CDS Subordinate CA terminating its services. The Adobe Policy Authority and the terminating CDS Subordinate CA must agree on what procedures are required to properly cease operations. This may include archiving and/or escrowing relevant data if the company operating the terminating CA is deemed to be distressed.

5. PHYSICAL, PROCEDURAL, AND PERSONNEL SECURITY CONTROLS

5.1 Physical Controls

CDS Subordinate CAs shall impose physical security requirements that provide similar levels of protection as those specified below.

5.1.1 Site Location and Construction

The location and construction of the facility housing CDS Subordinate 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, provides robust protection against unauthorized access to the CA equipment and records.

5.1.2 Physical Access

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

CDS Subordinate CAs shall operate their PKI at the highest level of assurance as to which they plan to issue certificates (present and future). At a minimum, the following physical controls shall be present:

- Physical access to CDS Subordinate CA equipment shall be monitored either manually or electronically at all times;
- Access logs shall be maintained and reviewed periodically; and
- Two person physical access controls to both the cryptographic module and computer system shall be required.

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 a CDS Subordinate CA will be stored securely.

5.1.7 Waste Disposal

Paper documents and electronic media containing trusted elements of a CDS Subordinate CA or commercially sensitive or confidential information are 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 shedding service.

5.1.8 Off-Site Backup

CDS Subordinate CAs shall make full system backups that are sufficient to recover from system failure on a regular basis and any time a significant change is made to the system. The backup schedule shall be documented in each CDS Subordinate CA's CPS. Offsite storage of CDS Subordinate CA backup material must be protected in a secure location with two person physical access control.

5.2 Procedural Controls

5.2.1 Trusted Roles

Trusted roles shall be assigned by CDS Subordinate CAs in a manner that provides as much assurance as possible that integrity of the CA cannot be compromised without collusion.

5.2.2 Number of Persons Required per Task

CDS Subordinate CAs shall implement multi-person control via physical and/or logical controls for sensitive operations. These controls shall be addressed in each CDS Subordinate CA's CPS.

5.2.3 Identification and Authentication for Each Role

Each person performing a Trusted Role within the CDS PKI must be authorized and authenticated to perform such functions as described in each CDS Subordinate CA's CPS.

5.3 Personnel Controls

5.3.1 Background, Qualifications, Experience, and Clearance Requirements

No stipulation

5.3.2 Background Check Procedures

No stipulation

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

No stipulation

5.3.7 Contracting Personnel Requirements

No stipulation

5.3.8 Documentation Supplied to Personnel

No stipulation

6. TECHNICAL SECURITY CONTROLS

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

All CAs participating in the CDS PKI must document their key generating procedures in a manner that provides auditable evidence that said procedures were followed. An independent third party, as defined in Section 2.7.3, must witness the key generation ceremony of any CDS Subordinate CA. CDS Subordinate CA key pairs must be generated in hardware security modules (HSM) that meet or exceed FIPS 140-1 Level 3 certification standards.

Subscriber key pairs must be generated in a manner that ensures that the private key is not known by anybody other than the Subscriber or a Subscriber's authorized representative. Subscriber key pairs must be generated in a medium that prevents exportation or duplication and that meets or exceed FIPS 140-1 Level 2 certification standards.

Temporary key pairs and corresponding certificates may be generated by a CDS Subordinate CA for the limited purpose of testing such certificates so long as the test certificates do not contain actual identities and are clearly marked for testing purposes only. These temporary test key pairs are exempt from the requirement that hardware security modules (HSM) must meet or exceed FIPS 140-1 Level 3 certification standards.

6.1.2 Private Key Delivery to Entity

CDS Subordinate CAs generate their own private keys and therefore, no delivery is necessary.

Subscriber private keys must be delivered to the Subscriber in accordance with the appropriate CDS Subordinate CA's CPS.

6.1.3 Public Key Delivery to Certificate Issuer

Public keys will be delivered to the certificate issuer via a PKCS#10 request. The PKCS#10 request shall be signed using the Subscriber's private key. The Subscriber's signature must be authenticated by the Issuing CA prior to issuing the Subscriber a certificate.

6.1.4 CA Public Key Delivery to Users

No stipulation

6.1.5 Key Sizes

CDS Subordinate CAs shall use an RSA key pair with at least 2048 bits.

CDS Subscriber certificates shall use an RSA key pair with at least 2048 bits.

6.1.6 Public Key Parameters Generation

No stipulation

6.1.7 Parameter Quality Checking

No stipulation

6.1.8 Hardware/Software Key Generation

Key generation must meet the requirements of Sections 6.1.1 and 6.1.5.

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

No stipulation

6.2 Private Key Protection

6.2.1 Standards for Cryptographic Module

Standards for cryptographic modules to be adhered to in the CDS PKI are decided by the Adobe Policy Authority. CDS Subordinate CAs must use cryptographic hardware modules that meet or exceed FIPS 140-1 Level 3 standards. CDS Subscribers must use cryptographic hardware modules that (a) meet or exceed FIPS 140-1 Level 2 standards or (b) for which the cryptographic hardware module manufacturer has applied for FIPS 140-1 Level 2 status within the previous year without receiving a notice of noncompliance or other communication indicating that such device fails to meet such standard.

Temporary key pairs generated by a CDS Subordinate CA for testing purposes pursuant to Section 6.1.1 are exempt from the requirement of using cyrptographic hardware modules that meet or exceed FIPS 140-1 Level 3 certification standards.

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

Multiple people are required to access all CDS Subordinate CAs' private keys.

6.2.3 Private Key Escrow

Private keys shall not be escrowed.

6.2.4 Private Key Backup

Backups of Subscribers' private keys shall not be made.

6.2.5 Private Key Archival

Private keys shall not be archived.

6.2.6 Private Key Entry into Cryptographic Module

Private keys are either generated by the Cryptographic Module or securely imported to it.

6.2.7 Method of Activating Private Key

In order to activate a private key, Subscribers or Trusted Roles must authenticate to the medium housing the private key. Forms of authentication include but are not limited to passwords, PINS, pass-phrases, and biometrics.

6.2.8 Method of Deactivating Private Key

Private keys must be deactivated when not in use. Procedures for deactivation shall be specified in CDS Subordinate CAs' CPS.

6.2.9 Method of Destroying Private Key

Secure procedures for the destruction of private keys shall be followed when a private key is no longer needed or the certificate in which it corresponds has expired. Secure procedures shall dictate how private keys are destroyed. These secure procedures shall be included in the Adobe Root's CPS, each Subordinate CA's CPS and any applicable Subscriber Agreements. An example of such procedures is overwriting the key with zeros.

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

See section 6.1.9

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

Activation data used to unlock private keys shall have an appropriate level of strength for keys being protected. User created activation data or stronger access controls shall be used.

6.4.2 Activation Data Protection

Activation data shall be protected from disclosure. Activation data should not be written down. Cryptographic hardware shall have a mechanism to lock the hardware (at least temporarily) after a certain number of failed attempts to login.

6.4.3 Other Aspects of Activation Data

No stipulation

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

No stipulation

6.5.2 Computer Security Rating

No stipulation

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

System development controls shall be enforced by CDS Subordinate CA management.

6.6.2 Security Management Controls

Initial CA system (hardware, application, operating system) builds and modifications thereafter shall be documented and controlled.

6.6.3 Life Cycle Security Ratings

No stipulation

6.7 Network Security Controls

Should a CDS Subordinate CA be located on a network it must employ the appropriate security measure to ensure that the CA is protected from intrusion and other attacks that could enable it inoperative.

6.8 Cryptographic Module Engineering Controls

See Section 6.2.1.

7. CERTIFICATE AND CRL PROFILES

7.1 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		- v3
SerialNumber		- integer; unique to each certificate issued in the Adobe PKI domain
Signature		- sha-1 w/ RSAEncryption – {1.2.840.113549.1.1.5}
Issuer		- cn=Adobe Root CA , ou=Adobe Trust Services, o=Adobe Systems Incorporated , c=US
Validity		- 11 years - notBefore and notAfter are specified
Subject		- cn=TBD CDS CA , ou=TBD, o=TBD, c=US
SubjectPublicKeyInfo		- rsaEncryption – {1.2.840.113549.1.1.1} - RSA public key is 2048 bit public key
Extensions		
AuthorityKeyIdentifier	Non-critical	- contains a 20 byte SHA-1 hash of the Root CA public key
KeyUsage	Non-critical	- Certificate Signing - Off-line CRL Signing - CRL Signing (06)
SubjectKeyIdentifier	Non-critical	- contains a 20 byte SHA-1 hash of the subjectPublicKey in this certificate
BasicConstraints	Critical	- Subject Type=CA - Path Length = 1
CertificatePolicies	Non-critical	- 1.2.840.113583.1.2.1
ExtendedKeyUsage	Non-critical	- 1.2.840.113583.1.1.5
CRLDistributionPoints	Non-critical	- 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	- V6

7.1.1 Version Number(s)

See section 7.1 of this document.

7.1.2 Certificate Extensions

See section 7.1 of this document.

7.1.3 Algorithm Object Identifiers

See section 7.1 of this document.

7.1.4 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.

7.1.5 Name Constraints

See Section 7.1.

7.1.6 Certificate Policy Object Identifier

See Section 7.1

7.1.7 Usage of Policy Constraints Extension

No stipulation

7.1.8 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.

7.1.9 Processing Semantics for the Critical Certificate Policy Extension

Processing semantics is according to IETF RFC 3280.

7.2 CRL Profile

The CDS PKI requires x.509v2 Certificate Revocation Lists (CRL’s).

7.2.1 Version Number(s)

The Adobe Root CA and CDS Subordinate CAs issue X.509 Version 2 CRL’s and support the following fields:

- Version: Set to v2;
- Signature: Identifier of the algorithm used to sign the CRL;
- Issuer: The distinguished name of the Issuing 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

CDS Subordinate CA’s shall use 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 unique to each CRL issued.

8. SPECIFICATION ADMINISTRATION

8.1 Specification Change Procedures

The Adobe Policy Authority maintains this Policy. All proposed changes to this Policy shall be communicated to all CDS Subordinate CAs ninety (90) days prior to the change being made. The Adobe Policy Authority will consider comments in favor or opposition of the proposed changes as long as they are submitted in writing and within 30 days of the proposed change being published.

8.2 Publication and Notification Policies

This Policy and subsequent changes shall be made available to CDS Subordinate CAs within one week of approval.

8.3 CPS Approval Procedures

Each CDS Subordinate CA shall develop and publish a Certification Practice Statement (CPS) that provides details of their CDS PKI implementation in accordance to this Policy. All CDS Subordinate CA CPSs must be reviewed by the Adobe Policy Authority prior to a CA receiving a certificate and when a significant change is made to an existing CPS that may affect its ability to comply with this Policy. The Adobe Policy Authority reserves the right to disapprove of CDS Subordinate CA’s CPS if it feels it is direct conflict with this Policy.

Appendix A – CDS PKI 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.
Annual Recurring Audit	A formal review of a CDS CA’s operations by an independent and AICPA accredited service organization to be conducted at least once per year.
ARL	Authority Revocation List. Also known as CARL or Certification Authority Revocation List
CDS	Certified Document Services
CDS Certificate	A signing certificate issued within the CDS PKI for the purposes of digitally signing Acrobat documents.
CDS Document	An Acrobat document signed using a CDS certificate.
CDS PKI	The policy, process and technology required to manage, use and rely on certificates that chain to a root CA embedded in Acrobat by Adobe and used in connection with Certified Document Services.
CDS Service Provider Agreement	An agreement between Adobe Systems Incorporated and partners that details the terms and conditions in which both parties operate within the CDS PKI.
CDS Subordinate CA	Any authorized Certification Authority that chains to a root CA embedded in Acrobat by Adobe.
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.
CPS	Certification Practice Statement

Term	Definition
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.
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.
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 …

Term	Definition
Trusted Role	An individual tasked with managing a root CA’s RA functionality.