VeriSign
Certified Document Service (CDS)
for Adobe PKI

Certification Practice Statement

Version 1.0

13 September 2010

(Portions of this document have been redacted.)

VeriSign, Inc.
487 East Middlefield Road
Mountain View, CA 94043
+1 650.527.8000
http//:www.verisign.com

Revision History

Version	Date	Description
Version 1.0	13 September, 2010	Initial approval by Adobe PMA

VeriSign Certified Document Service (CDS) for Adobe PKI Certificate Practice Statement

Initial Publication Date: September 13, 2010

Trademark Notices

VeriSign, Inc.
487 East Middlefield Road
Mountain View, CA 94043 USA
Attn: Practices Development.
Tel: +1 650.527.8000
Fax: +1 650-527.8050
practices@verisign.com

TABLE OF CONTENTS

1. INTRODUCTION

Certified Document Services (CDS) is an offering 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.

VeriSign, Inc. (VeriSign) is contracted with Adobe Systems Incorporated (Adobe) as a 3rd party PKI Services Provider to provide Certification Authority (CA) services including all Registration Authority (RA) functionality. VeriSign may also offer CDS services through a global network of affiliates ("Affiliates") throughout the world.

Organizations interested in creating certified documents may register with the VeriSign CDS PKI, have their identification information verified and then be provided with a certificate used in Adobe Acrobat Standard or Professional to certify documents.

This VeriSign Certified Document Services (CDS) PKI Certification Practice Statement (CPS) in conjunction with the Adobe Certified Document Services Certification Policy (CP) defines the practices that VeriSign, and VeriSign Affiliates, will employ in issuing and managing certificates and in maintaining a certificate-based CDS PKI for Adobe clients.

1.1 Overview

This CPS is the statement of practices that VeriSign employs when issuing digital certificates from the VeriSign CDS PKI ("VeriSign CDS"). This CPS is structured in accordance with RFC 2527 of the Internet Engineering Task Force (IETF).

The VeriSign CDS PKI operates under the Adobe CDS Certificate Policy (CP) as a subordinate CA and provides complete certificate life-cycle support and certificate repository services for Adobe client entities.

The architecture and functional solution for the VeriSign CDS PKI is based on VeriSign's Managed PKI (MPKI) service offering.

The VeriSign CDS PKI provides medium assurance or confidence in the validity of the asserted identity.

The VeriSign CDS PKI primary location is at a VeriSign data center and a disaster recovery site with full backup and data mirroring located outside a one hundred (100) mile perimeter of the primary site. All customer transactions are copied between the primary and disaster recovery systems over a secure VPN connection. VeriSign may also offer CDS CAs and certificate services through Affiliate Processing Centers at locations throughout the world. Such facilities shall provide an equivalent level of security and disaster recovery in compliance with this CPS.

Authorized VeriSign personnel perform the CA functions as described in this CPS. The RA functions, including control over the registration process and identity proofing are performed by trusted entities at organizations that purchase the services of the CDS PKI.

The VeriSign CDS PKI issues X.509 Version 3 certificates compliant with the certificate profiles listed in Appendix A of this CPS. The certificates can be used by subscribers and relying parties for digital signature validation of electronic documents using only Adobe approved applications.

1.2 Policy Identification

This CPS describes VeriSign's practices for VeriSign CDS PKI services delivered in accordance with the Adobe Systems Incorporated CDS CP. The Adobe CDS CP Object Identifier is shown below:

1.2.840.113583.1.2.1	Adobe Certificate Policy Attribute Object Identifier (OID)

Certificates issued to a VeriSign CDS CA will contain the Adobe CDS Policy OID. Certificates issued by a VeriSign CDS PKI service to end entities will contain the Adobe CDS Policy OID asserting user identity with hardware cryptographic module storage and digital signature key usage.

The Policy Object Identifiers are populated in accordance with CPS § 7.1.6.

1.3 Community and Applicability

This CPS describes a PKI community of components comprising the Adobe PKI hierarchy including CDS Subordinate CAs and Subscribers whose certificates chain to the Adobe Root CA embedded in Acrobat® by Adobe, along with all Relying Parties who will rely on such certificates.

This CPS describes the rights and obligations of persons and entities authorized under this CPS and the CP to fulfill any of the following roles: Certification Authority, Registration Authority, Trusted Agent, Repository, and the end-entity roles of Subscriber and Relying Party.

This CPS defines the policies and procedures that will be followed for the creation and management of X.509 Version 3 public-key certificates for use in Adobe-approved applications only, for digitally signing and signature verification of Adobe Acrobat documents.

Certificates issued within the CDS PKI community has the certificate policy extensions populated with the OIDs identified in Section 1.2.

1.3.1 Certification Authority (CA)

VeriSign has established a multi-level CDS CA hierarchy within the Adobe Trust Hierarchy under the Adobe Root CA. The first level Subordinate CA is a single VeriSign Intermediate CA authorized by the Adobe PA to create, sign and issue one or more Level 2 Subordinate CA digital certificates. Level 2 Subordinate CAs are entities authorized by VeriSign under the Adobe CDS CP to create, sign and issue end-entity digital certificates that conform to the requirements of the Adobe CP and this CPS.. Organizations may have a dedicated CDS CA or may use a shared CDS CA.

The Adobe Root CA serves as the "trust anchor" for all certificates issued by the VeriSign CDS CA hierarchy. The VeriSign subordinate Level 2 CDS CAs are entities authorized by the VeriSign PMA to create, sign and issue digital certificates that conform to the requirements of the CP and this CPS.

The VeriSign CDS PKI is responsible for all aspects of the issuance and management of CDS certificates including the certificate management process, publication of certificates, revocation of certificates and re-key; generation and destruction of CA signing keys, and for ensuring that all aspects of the CA services, operations and infrastructure related to CDS certificates are performed in accordance with the requirements, representations, and warranties of this CPS.

The VeriSign CDS CA is responsible to use all reasonable efforts to notify relying parties, at minimum, using the user Notice within each end-entity certificate published, that reliance on a CDS-signed document is only permitted if verified on an Adobe-approved application.

1.3.1.1 Other Participants

An Affiliate is a leading trusted third party, for example in the technology telecommunications, or financial services industry that has entered into an agreement with VeriSign to operate a Level 2 CA under the VeriSign Intermediate CDS CA within a specific territory.

Processing Centers (i.e, VeriSign or certain Affiliates) are entities that create a secure facility housing, among other things, the cryptographic modules used for the issuance of certificates. Processing Centers act as CAs within the VeriSign CDS CA hierarchy and perform all certificate lifecycle services of issuing, managing, revoking and renewing certificates. Affiliates who outsource the backend functionality to VeriSign but retain the RA responsibilities are called Service Centers.

The Affiliate Processing Centers operate as a dedicated CA within the VeriSign CDS CA hierarchy, as depicted in Figure 1. . The Affiliate and any Affiliate customer organization shall establish an Organization PMA to ensure compliance of the organization CA components in accordance with section 2.1.

1.3.1.2 Related Authorities

1.3.1.2.1 Compliance Auditor

VeriSign retains the services of an independent security auditing firm, (e.g. KPMG), which conducts a yearly examination of the controls associated with VeriSign's operations as set forth in VeriSign's practices documentation and described in section 2.7.

1.3.1.2.2 Repository

VeriSign operates a CDS Repository from its secure data facility. This LDAP-compliant directory contains the CDS CA certificates and associated CRLs. Updates to information contained in the VeriSign CDS Repository are limited to authorized VeriSign personnel and processes. Subscribers and relying parties may query, view, and download certificate, certificate status and CRL entries in the repository via an http query.

1.3.2 Registration Authority (RA)

VeriSign personnel and designated client organization personnel perform the RA functions for the VeriSign CDS PKI. The Organization RA may rely on a manual identity validation process performed by a Trusted Agent.

VeriSign establishes a contractual relationship with an organization prior to the authorization of an Organization RA to perform identity verification of employees/associates of the organization. The Organization RA will be bound by contract with VeriSign to comply with the requirements of the CP and this CPS. The Organization RA personnel are issued VeriSign Class 3 administrator certificates to enable secure authenticated privileged access to their organization's subordinate CDS CA. The RA certificate is stored on a FIPS 140 Level 2 Hardware Security Module (HSM).

VeriSign shall require the organization to bind Trusted Agents by contract to comply with the requirements of the CP and this CPS.

1.3.2.1 Trusted Agent

A Trusted Agent is a person who satisfies all the trustworthiness requirements of an Organization RA and who performs the identity proofing function as a proxy for the Organization RA. A Trusted Agent is responsible for validating a subscriber's identity based on the presentation of a government-issued photo ID and other identity documents.

Authorized employees of the organization or Affiliate may also serve as Trusted Agents. Trusted Agents are holders of CDS subscriber certificates, but they do not have privileged access to CA registration functions.

1.3.3. End Entities

1.3.3.1 Subscribers

A CDS Subscriber is an entity whose name appears as the subject in a CDS certificate and who asserts it protects and uses its key and certificate in accordance with the CDS CPS. Subscribers include any authorized individual, organization or organization role that has a CDS certificate issued to them and uses that certificate to sign a Portable Document File (PDF) document.

Although a CDS CA is a subscriber, the term Subscriber, as used in this document, refers only to those entities who request certificates for uses other than signing and issuing certificates.

1.3.3.2 Relying Parties

Relying parties are recipients of CDS documents who wish to verify the subscriber's signature.

A relying party relies on the validity of the binding of the subscriber's name to a public key. The relying party is responsible to use Adobe-approved applications for deciding whether the document or signature has been tampered with and whether the signer's certificate has been compromised.

1.3.4 Applicability

CDS digital signature certificates may only be issued by authorized VeriSign CDS CAs to Subscribers in accordance with this Policy. CDS certificates issued may only be used to digitally sign and verify the authenticity of Adobe Acrobat documents.

CDS certificates issued do not provide confidentiality of the content of the Adobe document. The decision to produce certain textual content within the Adobe Acrobat documents is solely the responsibility of the organization, based on organizational security policy and data sensitivity classifications. This evaluation is done by the organization and is not controlled by this CPS.

The CDS PKI is classified as a medium assurance PKI and certificates issued by this PKI are suitable for signature of Adobe documents that correspond to a medium assurance risk. Risk analysis is solely the responsibility of the organization based on organizational security policy, risk assessment and data sensitivity classifications.

1.3.5 PKI Policy Authority (PA)

The Adobe Systems Policy Authority (PA) is responsible maintaining the CP, approving the CPS and Compliance Audit for each CA that issues certificates under the CP. The Adobe Policy Authority consists of selected members of Adobe's management team.

The VeriSign Policy Management Authority (PMA) is established to manage the PKI implementation in accordance with CP. This body is responsible to develop the CPS, conduct Compliance Audits for each CA implemented, and provide regular reporting and escalation of significant events to the Adobe PA. This body is referred to as the VeriSign PMA.

1.3.5.1 Organization Policy Management Authority (PMA)

Organizations that contract for CDS PKI services under this CPS also establish a management body to manage any organization components (e.g., RAs or repositories) and resolve name space collisions. This body is referred to as an Organization Policy Management Authority, or Organization PMA.

1.4 Contact Details

1.4.1 Specification Administration Organization

The organization responsible for administering this CPS is the VeriSign Practices Development group. Questions or correspondence related to this CPS should be addressed as specified in section 1.4.2:

1.4.2 Contact Persons

Parties having questions as to the content, applicability, or interpretation of this CPS may address their comments to:

VeriSign, Inc.
487 East Middlefield Road
Mountain View, CA 94043
Attn: Practices Development – CPS
+1 650-527.8000
+1 650-527.8050 (fax)
practices@verisign.com

1.4.3 Person Determining CPS Suitability for the Policy

The VeriSign Certification Practice Statement (CPS) document(s) are approved by the VeriSign PMA based on independent review and subject to a compliance audit as specified in section 2.7.

The Adobe Policy Authority (PMA) has the final authority for approving the suitability of the subordinate CDS CA CPS and asserts its compliance with the Adobe CDS CP.

2. GENERAL PROVISIONS

This Section sets forth general provisions of obligations and defines and allocates specific responsibilities among the various parties participating in the CDS PKI described in this CPS. These parties are:

- Policy Authority (PA)
- Organization Policy Management Authority (PMA)
- Certification Authority (CA)
- Registration Authority (RA)
- Trusted Agent (TA)
- Subscriber
- Relying Party (RP)
- Repository

The parties are hereby notified of the following rules and obligations governing the respective rights and obligations of the parties among themselves. These rules and obligations are deemed to be agreed by the parties effective:

- Upon publication of this CPS in the case of the CA, RA, Trusted Agent;
- Upon submission of an application for a certificate, in the case of a Subscriber; and
- Upon reliance of a certificate or digital signature verifiable with reference to a public key listed in the certificate, in the case of a Relying Party or other recipient of a certificate issued under this CPS.

Additional obligations are set forth in other provisions of this CPS and the Subscriber Agreement.

2.1 Obligations

2.1.1 PMA Obligations

The VeriSign PMA shall—

- Approve the VeriSign CDS CPS applicable to all CAs that issue certificates under this policy;
- Review periodic compliance audits to ensure that the Intermediate CA and Subordinate CAs are operating in compliance with their approved CPSes;
- Notify appropriate entities in the event of disaster, CA compromise or termination;
- Review name space control procedures to ensure that distinguished names are uniquely assigned for all certificates issued under this CPS; and
- Coordinate modifications to the CPS to ensure continued compliance by CAs operating under the Adobe CDS CP.

2.1.2 Organization PMA Obligations

The VeriSign Affiliate and customer organization shall appoint an Organization PMA. The Organization PMA shall—

- Review periodic compliance audits to ensure that RAs and CA components operated by the organization are operating in compliance with their approved CPSes;
- Notify appropriate entities in the event of disaster, compromise or termination; and
- Review name space control procedures to ensure that distinguished names are uniquely assigned within their organization.

2.1.3 CA Obligations

VeriSign shall provide to the Adobe PA this CPS document, as well as any subsequent changes, for conformance assessment. All CAs in the VeriSign CDS CA hierarchy shall conform to the stipulations of this document, including—

- Maintaining its operations in conformance to the stipulations of the approved CPS;
- Maintaining records of the users and operations of the CA to respond to requests concerning its operation over the validity period of the applicable record or document, but not less than three (3) years;
- Ensuring that registration information is accepted only from approved RAs operating under an approved CPS;
- Providing notification to the Subscriber of the issuance and the revocation of a Certificate as described in Section 4;
- Revoking the certificates of Subscribers and RAs found to have acted in a manner counter to their obligations in accordance with Section 2.1.6 and 2.1.4 respectively, and according to the provisions regarding revocation in Section 4.4;
- Operating or providing for the services of an online repository that satisfies the obligations under Section 2.1.8, and informing the repository service provider of their obligations if applicable;
- Represent and warrant to all Relying Parties about the CDS CA-issued certificate—
    - that due diligence was exercised in validating the information contained in the certificates, and evidence is maintained;
    - information included in certificates accurately reflects the information provided by the Subscriber in all material respects, and
    - the Subscriber has accepted the Certificate according to the provisions of policy and are bound to a Subscriber Agreement.
- Represent to all Relying Parties about the CDS-signed document—
    - notification, at minimum via the User Notice qualifier within the certificate, that reliance is only permitted if the document is verified on an Adobe supported platform.
- Providing the re-key and replacement of certificates; and
- Publishing and adhering to a privacy policy.

The Level 1 CA shall —

- have auditing procedures in place to ensure that all Level 2 CAs signed by the Level 1 CA, has complied in all material respects with this policy and the applicable CPS; and
- represent and warrant to the Adobe Root CA that all level 2 CAs are and will be compliant with the Adobe CDS CP.

The Level 2 CA shall —

- represent and warrant that it has complied in all material respects with the Adobe CDS CP and this CPS;

The Affiliate Processing Centers operating a dedicated CA within the VeriSign CDS CA hierarchy may choose to develop their own CPS in accordance with their national law. These CPS must at minimum comply with all the requirements set forth by the Adobe CDS CP and this CPS, and is subject to approval in accordance with section 1.4.3.

2.1.4 RA Obligations

An RA who performs registration functions as described in this CPS shall comply with the stipulations of this CPS and the governing CP. An RA who is found to have acted in a manner inconsistent with these obligations is subject to revocation of RA responsibilities. An RA supporting this policy shall conform to the stipulations of this document, including:

- Performing identify verification of certificate applicants in accordance with Section 3.1.10;
- Including only valid and appropriate information in certificate requests, and maintaining evidence that due diligence was exercised in validating the information contained in the certificate; and
- Ensuring that obligations are imposed on subscribers in accordance with Section 2.1.6, and that Subscribers are informed of the consequences of not complying with those obligations; and
- Maintaining its operations in conformance to the stipulations of the approved CPS.

The distinction between the VeriSign RA and the Organization RA entities is described in section 5.2.1.2.

2.1.4.1 Trusted Agent Obligations

A Trusted Agent who performs identification and authentication functions as described in this CPS shall comply with the stipulations of this CPS and the governing CP. A Trusted Agent who is found to have acted in a manner inconsistent with these obligations is subject to revocation of Trusted Agent responsibilities. A Trusted Agent supporting this CPS shall conform to the stipulations of this document, including:

- Performing manual identify verification of certificate applicants in accordance with Section 3.1.10;
- Including only valid and appropriate information in certificate requests, and maintaining evidence that due diligence was exercised in validating the information contained in the certificate; and
- Ensuring that obligations are imposed on subscribers in accordance with Section 2.1.3, and that Subscribers are informed of the consequences of not complying with those obligations.

2.1.5 End Entity Obligations

2.1.5.1 Trusted Roles Obligations

An individual serving in the capacity of a Trusted Role shall:

- Protect their private keys at all times, in accordance with this CPS, and as set forth in the applicable subscriber agreements;
- Protect the information needed to access its private keys, including without limitation, the PIN, password, passphrase or other information or mechanism employed to protect the private key;
- Notify the VeriSign CA, in a timely manner, if the individual believes or has reason to believe that their private keys are compromised or lost. Such notification shall be made directly or indirectly through mechanisms consistent with the CP and this CPS;
- Abide by all the terms, conditions, and restrictions levied upon the use of their private keys and certificates as prescribed in this CPS and in the applicable Subscriber Agreement;
- Agree not to monitor, interfere with, or reverse engineer the technical implementation of the VeriSign CDS PKI except as explicitly permitted by this CPS or upon written approval by VeriSign; and
- Conform to all requirements and procedures of the Key Generation Ceremony.

2.1.5.2 Subscriber Obligations

Subscribers shall:

- Accurately represent themselves and ensure the accuracy of information provided in all communications with the CDS CA, RA, and/or TA;
- Abide by all the terms, conditions, and restrictions levied upon the use of their private keys and certificates as prescribed in this CPS and in the applicable Subscriber Agreement;
- Agree not to monitor, interfere with, or reverse engineer the technical implementation of the VeriSign CDS except as explicitly permitted by this CPS or upon written approval by VeriSign; and
- Agree not to submit to VeriSign or the VeriSign CDS repository any materials that contains statements that are (i) libelous, defamatory, obscene, pornographic, abusive, bigoted, hateful, or racially offensive, (ii) advocate illegal activity or discuss illegal activities with the intent to commit them, or (iii) otherwise violate any law.

Subscribers shall enter into a binding Subscriber Agreement which, at minimum 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;

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

e) agree to Subscriber Liability and Indemnifications as set forth in section 2.3.1.

2.1.5.3 Sponsor Obligations

Subscribers apply for certificates either directly, or indirectly in those cases where the subscriber is sponsored by an organization or representing an organization, as described in sections 3 and 4. Applications submitted indirectly on behalf of another, constitutes sponsorship.

PKI Sponsors (as described in Section 5.2.1.6) assume the obligations of Subscribers for the certificates associated with their applications in accordance with section 2.1.5.2. Additionally, the subscriber organization that utilizes PKI Sponsors assumes the following responsibilities:

- maintain processes that assure that the private key can be used only with the knowledge and explicit action of the subscriber;
- When the subscriber represents an organizational entity maintain at minimum, processes to change the activation data that assures that the private key can be used only with the knowledge and explicit action of a single individual within the organization (ie, the *certificate custodian*);
- maintain information that permits a determination of who signed a particular document;
- assure that the individual interpreted as the certificate subject (i.e., the *certificate custodian*) has received security training appropriate for the purposes for which the certificate is issued;
- prevent sharing of the organizational certificate among members of the organization;
- notify the CDS CA immediately upon any actual or suspected loss, disclosure, or other compromise of the Subscriber's private key;

- ensure that the certificate subject ((i.e., the *certificate custodian*) has entered into a binding Subscriber Agreement.

2.1.6 Relying Party Obligations

The relying party shall receive and abide by User Notices directing limitations on their reliance of a digitally signed document. The relying party shall rely upon a document signature derived from a certificate issued by the VeriSign CDS only if the digital signature is verified using an Adobe supported platform.

Relying parties that do not perform the obligations in this section assume all risks with regard to the digital signature and/or certificate on which they are relying.

2.1.7 Repository Obligations

The VeriSign CDS Repository is obligated to provide certificates, CRLs, and other revocation information. No confidential subscriber data not intended for public dissemination is published in the VeriSign CDS Repository. Therefore, the VeriSign CDS Repository provides unrestricted read-only access to subscribers, relying parties, and other interested parties. The VeriSign CDS repository is accessible via methods described in Section 2.6.4. VeriSign may replicate certificates and CRLs in additional repositories for performance enhancement. Such repositories may be operated by VeriSign or other parties.

2.2 Liability

2.2.1 Warranties and Limitations on Warranties

This section sets forth the warranties, disclaimers of warranties, and limitations of liability provided by all levels of CAs in the VeriSign CDS hierarchy to Subscribers and Relying Parties pursuant to this CPS.

2.2.1.1 Certificate Authority Warranties

VeriSign, warrants to subscribers that:

- There are no material misrepresentations of fact in such certificate known to or originating from VeriSign;
- There are no errors in the information in the certificate that were introduced by VeriSign as a result of its failure to exercise reasonable care in creating the certificate;
- Such certificate meets all material requirements of this CPS; and
- Revocation services and use of a repository conform to this CPS in all material respects.

VeriSign warrants to Relying Parties who reasonably rely on a certificate that:

- VeriSign has materially complied with the CPS when issuing the certificate; and
- All information in or incorporated by reference in such certificate is accurate as of the date of issue.

2.2.1.2 Subscribers' Representations

By accepting a CDS certificate issued by VeriSign, the subscriber certifies to and agrees with VeriSign and to all who reasonably rely on the information contained in the certificate that at the time of acceptance and throughout the operational period of the certificate, until notified otherwise by the subscriber:

- each digital signature created using the private key corresponding to the public key listed in the certificate is the digital signature of the Subscriber and the certificate has been accepted and is operational (not expired, suspended or revoked) at the time the digital signature is created;
- no unauthorized person has ever had access to the subscriber's private key;

- all representations made by the subscriber to VeriSign regarding the information contained in the certificate are true;
- all information contained in the certificate is true to the extent that the subscriber had knowledge or notice of such information and does not promptly notify VeriSign of any material inaccuracies in such information as set forth in CPS § 2.3.1;
- the certificate is being used exclusively for authorized and legal purposes, consistent with this CPS; and
- the Subscriber is an end-user and will not use the private key corresponding to any public key listed in the certificate for purposes of signing any certificate (or any other format of certified public key) or CRL.

By accepting a certificate, the Subscriber acknowledges that they agree to the terms and conditions contained in this CPS and the applicable subscriber agreement.

2.2.2 Disclaimers of Warranty and Liability

2.2.2.1 Specific Disclaimers

Adobe Root CA Disclaimers

In addition to any other warranty disclaimers in any CDS Provider Agreements, the Adobe Root CA disclaims any and all warrantees 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.

VeriSign Disclaimers

Except as otherwise set forth in this CPS, VeriSign:

a) Shall not incur liability to any person or entity for representations contained in a certificate, provided the certificate was prepared substantially in compliance with the CPS, and provided further that the foregoing disclaimer shall not apply to VeriSign's liability in tort for negligent, reckless, or fraudulent conduct;

b) Does not warrant "non-repudiation" for any VeriSign certificate or any message (because non-repudiation is determined exclusively by law and the applicable final dispute resolution mechanism); and

c) Does not warrant the standards or performance of any hardware or software not under exclusive ownership of, exclusive control of, or licensed to VeriSign.

See also CPS § 2.3.3 (Disclaimer of Fiduciary Relationship).

2.2.2.2 General Disclaimer

Except as set forth in this CPS and the applicable subscriber agreement, and to the extent permitted by applicable law, VeriSign disclaims any and all other express or implied warranties and obligations of any type

to any person or entity, including any warranty of merchantability, any warranty of fitness for a particular purpose, and any warranty of the accuracy of information provided by certificate applicants, subscribers, and third parties, and further disclaims any and all liability for any acts by VeriSign that constitute or may be held to constitute strict liability, whether sole or jointly with any other person or entity.

2.2.3 Limitations of Liability

2.2.3.1 Limitations on Amount of Damages

Adobe Root CA Limitations on Liability

Under no circumstances will the Adobe Root CA be liable to any purported relying parties or any other person or entity, or an 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 of fundamental terms of the certificate policy.

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

VeriSign Limitations on Liability

In the event a subscriber or relying party initiates any claim, action, suit, arbitration, or other proceeding separate from a request for payment under this CPS and to the extent permitted by applicable law, VeriSign's liability shall be limited as follows:

The total liability of VeriSign to any party for general contract, tort or any other damages for negligent, reckless, or fraudulent conduct by the VeriSign CDS CA, its RAs or Trusted Agents for any incident (aggregate of all transactions) involving the use or reliance on a VeriSign CDS certificate shall be limited to five thousand dollars U.S. dollars ($5,000 USD). The liability cap shall be the same regardless of the number of digital signatures, acts of authentication, or encrypted messages related to, or claims arising out of such transaction.

2.2.3.2 Exclusion of Certain Elements of Damages

Except as expressly provided in this CPS, and to the extent permitted by applicable law, VeriSign shall not be liable in contract to any person or entity for any indirect, special, reliance, incidental, or consequential damages (including but not limited to any loss of profits or loss of data), arising from or in connection with the use, delivery, license, performance, or nonperformance of certificates, digital signatures, or any other transactions, products, or services offered or contemplated by this CPS, even if VeriSign has been advised of the possibility of such damages.

To the extent permitted by applicable law, VeriSign shall not be liable to any person or entity for any punitive damages arising from or in connection with the use, delivery, license, performance, or nonperformance of certificates, digital signatures, or any other transactions or services offered or contemplated by this CPS.

2.2.4 Third Party Beneficiary

Adobe Systems Incorporated is intended to be a third party beneficiary for the purposes of section 2.2.2 (Disclaimers of Warranty and Liability).

2.3 Financial Responsibility

VeriSign has sufficient financial resources to maintain its operations and perform its duties, and it is reasonably able to bear the risk of liability to Subscribers and recipients of certificates and other persons who may rely on the certificates and time stamps it issues. VeriSign also maintains professional liability insurance.

2.3.1 Subscriber's Liability and Indemnity

Without limiting other Subscriber obligations stated in this CPS, subscribers are liable for any misrepresentations they make in certificates to third parties who, having verified one or more digital signatures with the certificate, reasonably rely on the representations contained therein.

By accepting a certificate, the Subscriber agrees to indemnify and hold the Adobe Root CA, VeriSign and its agent(s) and contractors harmless from any acts or omissions resulting in liability, any loss or damage, and any suits and expenses of any kind, including reasonable attorneys' fees, that the Root CA, VeriSign and its agents and contractors may incur, that are caused by the use or publication of a certificate, and that arises from (i) falsehood or misrepresentation of fact by the subscriber (or a person acting upon instructions from anyone authorized by the Subscriber); (ii) failure by the Subscriber to disclose a material fact, if the misrepresentation or omission was made negligently or with intent to deceive VeriSign or any person receiving or relying on the certificate; or (iii) failure to protect the subscriber's private key, to use a trustworthy system, or to otherwise take the precautions necessary to prevent the compromise, loss, disclosure, modification, or unauthorized use of the subscriber's private key.

2.3.2 Relying Party's Liability and Indemnity

Without limiting other Relying Party obligations stated in this CPS, relying parties are liable for reliance upon a CDS-signed document that has not been verified on a platform approved by Adobe Systems, or otherwise has failed to check the certificate status prior to any reliance on the digital signature.

By accepting a CDS-signed document, the relying party agrees to indemnify and hold the Adobe Root CA, VeriSign and its agent(s) and contractors harmless from any breach of the relying party obligations.

2.3.3 Fiduciary Relationships

The VeriSign CDS CA is not the agent, fiduciary, trustee, or other representative of the Adobe Root CA.

The VeriSign CDS CA or RA is not the agent, fiduciary, trustee, or other representative of subscribers or relying parties. The relationship between VeriSign and Subscribers and that between VeriSign and relying parties is not that of agent and principal. Neither Subscribers nor relying parties have any authority to bind VeriSign, by contract or otherwise, to any obligation. VeriSign shall make no representations to the contrary, either expressly, implicitly, by appearance, or otherwise.

2.3.4 Administrative Processes

An annual report of VeriSign can be obtained by submitting a written request to the address specified in section 1.4. VeriSign's financial resources are set forth in disclosures appearing at:
http://corporate.verisign.com/investor/sec-filings.html

2.4 Interpretation and Enforcement

2.4.1 Interpretation

2.4.1.1 Governing Law

The laws of the Commonwealth of Virginia, U.S.A., shall govern the enforceability, construction, interpretation, and validity of this CPS, irrespective of contract or other choice of law provisions and without the requirement to establish a commercial nexus in Virginia. This choice of law is made to ensure uniform procedures and interpretation for all users, no matter where they reside or use their certificates.

2.4.1.2 Conflict of Provisions

To the extent not inconsistent with the CDS Subordinate CA PKI Provider Agreement, the provisions set forth in this CPS apply to the VeriSign CDS hierarchy. In the event of a conflict between this CPS and the CDS Subordinate CA PKI Provider Agreement, the CDS Subordinate CA PKI Provider Agreement shall take precedence.

In the event of a conflict between this CPS and other rules, guidelines, or contracts, the subscriber shall be bound by the provisions of this CPS except to the extent that the provisions of this CPS are prohibited by law. In the event of a conflict between the Adobe CDS CP and this CPS, the Adobe CDS CP shall take precedence over this CPS.

2.4.1.3 Interpretation

Unless otherwise provided, this CPS shall be interpreted consistently with what is commercially reasonable under the circumstances.

2.4.1.4 Headings and Appendices of this CPS

The headings, subheadings, and other captions in this CPS are for convenience and reference only and shall not be used in interpreting, construing, or enforcing any of the provisions of this CPS. The appendices, including the definitions to this CPS, are an integral and binding part of the CPS.

2.4.2 Severability, Survival, Merger, and Notice

2.4.2.1 Severability

If any provision of this CPS, or the application thereof, is for any reason and to any extent found to be invalid or unenforceable, the remainder of this CPS (and the application of the invalid or unenforceable provision to other persons or circumstances) shall be interpreted so as best to reasonably effect the intent of its parties. It is expressly understood and agreed that each and every provision of this CPS that provides for a limitation of liability, disclaimer of or limitation upon any warranties or other obligations, or exclusion of damages is intended to be severable and independent of any other provision and is to be enforced as such.

2.4.2.2 Survival

The obligations and restrictions contained within CPS § 2.7 (Audit), 2.8 (Confidential Information), CPS §§ 2.2.2, 2.2.3 (Disclaimers of Warranty and Limitations of Liability), and CPS § 2.4 (Interpretation and Enforcement) shall survive the termination of this CPS.

2.4.2.3 Merger

No term or provision of this CPS directly affecting the respective rights and obligations of VeriSign may be orally amended, waived, supplemented, modified, or terminated, except by an authenticated message or document of such affected party, except to the extent provided otherwise herein.

2.4.2.4 Notice

Whenever any person hereto desires or is required to give any notice, demand, or request with respect to this CPS, such communication shall be made either using digitally signed messages consistent with the requirements of this CPS, or in writing. Electronic communications shall be effective upon the sender's receiving a valid, digitally signed acknowledgment of receipt from the recipient. Such acknowledgment must be received within five (5) days, or else written notice must then be communicated. Communications in writing must be delivered by a courier service that confirms delivery in writing or via certified or registered mail, postage prepaid, return receipt requested, addressed as follows:

To VeriSign:

> VeriSign, Inc.
> 487 East Middlefield Road Mountain View, CA 94043 USA
> Attn: Certification Services
> (+1 650-961-8820)

By VeriSign to another person:

> To the most recent address of record to another person on file with VeriSign, Inc.

2.4.3 Dispute Resolution Procedures and Choice of Forum

The VeriSign PA shall facilitate the resolution between entities when conflicts arise as a result of the use of certificates issued under this CPS.

2.4.3.1 Notification among Parties to a Dispute

Before invoking any dispute resolution mechanism (including litigation or arbitration, as detailed below) with respect to a dispute involving any aspect of this CPS or a certificate issued by VeriSign under this CPS, aggrieved persons shall notify VeriSign and any other party to a dispute for the purpose of seeking dispute resolution among themselves.

2.4.3.2 Formal Dispute Resolution

Disputes shall be resolved in accordance with the following provisions:

(i) When each indispensable party to a dispute is a Canadian or U.S. resident or organization situated or doing business in Canada or the United States except where each indispensable party to a dispute agrees to an alternative dispute resolution mechanism (such as arbitration), all suits to enforce any provision of this CPS or arising in connection with the CPS or any related business relationship between the parties hereto shall be brought in the federal or state court encompassing Fairfax County, Virginia, U.S.A. Each person hereby agrees that such courts shall have exclusive in personam jurisdiction and venue with respect to such person and each person hereby submits to the exclusive in personam jurisdiction and venue of such courts. The parties hereby waive any right to a jury trial regarding any action brought in connection with this CPS. Where an alternative dispute resolution is chosen by the parties, Virginia law shall govern arbitability and procedure.

(ii) Where one or more parties to a dispute is not a Canadian or U.S. resident or organization situated or doing business in Canada or the United States. All disputes arising in connection with the CPS shall be finally settled under the Rules of Conciliation and Arbitration of the International Chamber of Commerce (ICC) modified as necessary to reflect the provisions herein by one or more arbitrators. The place of arbitration shall be in New York or San Francisco, U.S.A., and the proceedings shall be conducted in English. In cases involving a single arbiter, that single arbiter shall be appointed by mutual agreement of the parties. If the parties fail to agree on an arbiter within fifteen (15) days, the ICC shall choose an arbiter knowledgeable in computer software law,

information security, and cryptography or otherwise having special qualifications in the field, such as a lawyer, academician, or judge in a common law jurisdiction.

2.4.4 Successors and Assigns

This CPS inures to the benefit of, and shall be binding upon the successors, executors, heirs, representatives, administrators, and assigns, whether express, implied, or apparent, of the parties. The rights and obligations detailed in this CPS are assignable by the parties, by operation of law (including as a result of merger or a transfer of a controlling interest in voting securities) or otherwise, provided such assignment is undertaken consistent with CPS § 4.9, concerning termination or cessation of CA operations; and provided further, that such assignment does not effect a novation of any other debts or obligations the assigning party owes to other parties at the time of such assignment.

2.4.5 No Waiver

Failure by any person to enforce a provision of this CPS will not be deemed a waiver of future enforcement of that or any other provision.

2.4.6 Compliance with Export Laws and Regulations

Export of certain software used in conjunction with the VeriSign CDS may require the approval of appropriate government authorities. The parties shall conform to applicable export laws and regulations.

2.4.7 Choice of Cryptographic Methods

All persons acknowledge that they (not VeriSign) are solely responsible for and have exercised independent judgment in choosing security software, hardware, and encryption/digital signature algorithms, including their respective parameters, procedures, and techniques.

2.4.8 Force Majeure

VeriSign shall not be responsible for any breach of warranty, delay, or failure in performance under this CPS that results from events beyond its control including, but not limited to, acts of God, acts of war, epidemics, power outages, fire, earthquakes, and other disasters.

2.5 Fees

2.5.1 Certificate Issuance or Renewal Fees

VeriSign is entitled to charge end-user Subscriber for the issuance, management and renewal of certificates.

2.5.2 Certificate Access Fees

VeriSign CDS certificates are available to relying parties at no charge.

2.5.3 Revocation or Status Information Access Fees

VeriSign CDS certificate revocation lists (CRLs) are available to relying parties at no charge. The VeriSign CDS may charge a fee for access to certificate status information via OCSP.

2.5.4 Fees for Other Services

No stipulation.

2.5.5 Refund Policy

The VeriSign CDS adheres to, and stands behind, rigorous practices and policies in undertaking certification operations and in issuing certificates. Nevertheless, if for any reason a subscriber is not completely satisfied

with the certificate issued to him, her, or it, the subscriber may request the VeriSign revoke the certificate within thirty (30) days of issuance and provide the subscriber with a refund. Following the initial thirty (30) day period, a subscriber may request that VeriSign revoke the certificate and provide a refund if VeriSign has breached a warranty or other material obligation under this CPS relating to the Subscriber or the Subscriber's certificate. Subscribers may request a refund in accordance with VeriSign's refund policy at *http://www.verisign.com/repository/refund*. This refund policy is not an exclusive remedy and does not limit other remedies that may be available to Subscribers.

2.6 Publication and Repositories

2.6.1 Publication of CA Information

The CDS Repository contains or provides access to the following minimum information published:

1. All valid and un-expired VeriSign CDS Certificates;
2. Certificate status information, including revocation;
3. The most recently issued CRL;
4. The VeriSign CDS certificate(s) needed to validate the signature on VeriSign CDS subscriber certificates;
5. Any other relevant information the VeriSign CDS considers relevant regarding the use of VeriSign CDS certificates by its subscribers or relying parties; and
6. A copy of an abridged version of this CPS including at least the following topics:
    - Effective period of the published CPSes;
    - Section 1.4, CDS CA Contact Information;
    - Section 2, General Provisions;
    - Sections 3.1 to 3.4, Initial Registration, Certificate Re-Key and Certificate Revocation;
    - Section 4.4, Certificate Suspension and Revocation;
    - Section 8, Certificate Practices Administration; and
    - Any additional information that the CDS CA deems to be of interest to the relying parties (e.g., mechanisms to disseminate CDS Root trust anchor, to provide notification of revocation of Adobe CDS Policy Root or CDS CA certificate).

The VeriSign CDS CPS is considered VeriSign Proprietary information.

2.6.2 Frequency of Publication

All information to be published in the repository is published promptly after such information is available to the VeriSign CDS.

Upon the subscriber's acceptance of the certificate, the VeriSign CDS immediately changes the status of the certificate in the CDS Repository from pending to valid.

Upon revoking a certificate, the VeriSign CDS immediately changes the status of the certificate indicated in the CDS Repository from valid to revoked.

CRLs are created and published as described in Section 4.4.3.

2.6.3 Access Controls

No confidential subscriber data not intended for public dissemination is published in the CDS Repository. Therefore the VeriSign CDS PKI shall not impose any read access restrictions to public information published

in its repository. Subscribers and relying parties may access certificate, certificate status and CRL information via HTTP queries.

The VeriSign CDS PKI shall protect any data in the repository or otherwise maintained by the CDS that is not intended for public dissemination or modification. Updates to information contained in the VeriSign CDS repository shall be limited to authorized CDS personnel.

2.6.4 Repositories

The VeriSign CDS PKI operates an online Repository available to Subscribers and Relying Parties. The VeriSign CDS Repository is implemented using LDAP technology. End users may search for CDS certificates, certificate status or CRLs using HTTP queries.

All reasonable efforts are used to make the repository available 24 hours per day, seven days per week ("24x7") subject to routine maintenance.

2.7 Compliance Audit

The compliance audit is performed in accordance with standards established by the American Institute of Certified Public Accounts (AICPA) as defined in the Statement of Auditing Standards (SAS) 70 and the WebTrust for CA guidelines. The VeriSign CDS CPS is based on its existing commercial practices and controls. As such, the yearly independent SAS 70 and WebTrust for CA audits provide the assurance of VeriSign's compliance with the CDS CPS.

2.7.1 Frequency of Compliance Audit

The VeriSign CDS shall undergo an annual compliance audit as part of the VeriSign annual recurring PKI audit.

2.7.2 Identity/Qualifications of Reviewer

The VeriSign CDS auditor is a member of the AICPA and licensed to perform WebTrust audits. To audit the CDS, VeriSign uses the same professional independent auditing firm that is responsible for conducting VeriSign's commercial PKI audit. The VeriSign CDS auditor is professionally qualified and intimately familiar with VeriSign's practices and policies, as it has been performing these services for VeriSign for more than five years. The auditing team has extensive experience in all relevant matters of physical, personnel, technical, and logical security. Specifically, the compliance audit team has the following applicable experience:

- a minimum of 5 years experience performing security audits;
- a minimum of 3 year PKI engineering/design experience;
- a minimum of 6 years cryptography engineering experience; and
- a minimum of 6 years computer security experience.

2.7.3 Auditor's Relationship to Audited Party

The VeriSign CDS auditor is under a contractual relationship to VeriSign for its security audit services and has no role or responsibility relating to the VeriSign CDS operation.

The Organization PMA is responsible for identifying and engaging a qualified auditor of its operations implementing aspects of this CPS.

2.7.4 Topics Covered by Compliance Audit

The Compliance Audit constitutes a WebTrust for CAs audit to verify that VeriSign has in place a system to assure the quality of the CDS services that it provides and that it complies with the requirements of the CP and

this CPS. All aspects of the VeriSign CA/RA operations are subject to compliance audit inspections. Compliance Audit shall include Level 1, and Level 2.

In addition to these compliance audits, VeriSign and Affiliates are entitled to perform other reviews and investigations to ensure the trustworthiness of the CDS PKI.

2.7.5 Actions Taken as a Result of Deficiency

When the compliance auditor finds a discrepancy between the requirements of the CP or the stipulations in the CPS and the design, operation, or maintenance of the PKI Authorities, the following actions shall be performed:

- The compliance auditor shall note the discrepancy;
- The compliance auditor shall notify the parties identified in Section 2.7.6 of the discrepancy;
- The party responsible for correcting the discrepancy will propose a remedy, including expected time for completion, to the PA for mutual agreement.

Depending upon the nature and severity of the discrepancy, and how quickly it can be corrected, the PA may decide to temporarily halt operation of the CA or RA, to revoke a certificate issued.

2.7.6 Communication of Results

The compliance auditor reports the results of a compliance audit to VeriSign and the VeriSign CDS communicates a Summary and pertinent sections of the WebTrust audit results to the Adobe PA.

After 30 days, the Audit Compliance report and identification of corrective measures taken or being taken by the CA or RA are provided to the Adobe PA. A special compliance audit may be required to confirm the implementation and effectiveness of the remedy.

2.8 Confidentiality

2.8.1 Types of Information to Be Kept Confidential

All non-certificate information received from Subscribers is treated as confidential by the VeriSign CDS and is not posted in the VeriSign CDS Repository. This information including: Dun and Bradstreet numbers, business or home addresses, telephone numbers and credit card data are handled as sensitive. This information is stored locally on the CDS equipment and access limited to authorized personnel.

The VeriSign CDS does not disclose or sell applicant names or other identifying information, and does not share such information, except in accordance with this CPS.

2.8.2 Information Release Circumstances

VeriSign does not disclose confidential information to any third party unless required by law, government rule or regulation, or order of a court of competent jurisdiction. VeriSign does not release or be required to release any confidential information without authorization by VeriSign Legal of an authenticated, reasonably specific request prior to such release.

2.9 Intellectual Property Rights

Unless otherwise agreed, property interests in the following security-related information materials and data are regarded as the property of the parties indicated below:

- Certificates and CRLs: Certificates and CRLs are the personal property of the VeriSign CDS. VeriSign licenses relying parties to use certificates and CRLs.

- CPS: This CPS is personal property of VeriSign, Inc.
- Distinguished Names: Distinguished names are the personal property of the persons named (or their employer or principal).
- Subscriber Private Keys: Subscriber private keys are the personal property of the subscribers who rightfully use or are capable of using them (or their employer or principal), regardless of the physical medium within which they are stored or protected.
- Subscriber Public Keys: Subscriber public keys are the personal property of subscribers (or their employers or principal), regardless of the physical medium within which they are stored or protected.
- VeriSign Private Keys: VeriSign CDS private keys are the personal property of VeriSign, Inc.
- VeriSign Public Keys: VeriSign CDS public keys are the property of VeriSign Inc. VeriSign licenses relying parties to use such keys.

3. IDENTIFICATION AND AUTHENTICATION

3.1 Initial Registration

3.1.1 Types of Names

Certificates issued by a CDS CA have a non-null DN name and use the X.500 DN name format for subject and issuer name fields. These distinguished names are in the form of an X.501 distinguished name specifying a geo-political name.

The X.501 distinguished name assigned to the Adobe CDS Root CA is:

- C=US, o=Adobe Systems Incorporated, ou=Adobe Trust Services, cn=Adobe Root CA

The X.501 distinguished name assigned to the VeriSign CDS CAs and dedicated organizational CAs is:

- C=US, o=VeriSign Inc., ou=Adobe Trust Services, cn=VeriSign Intermediate CA for Adobe CDS *(a Level 1 CA)*
- C=US, o=VeriSign Inc., ou=CDS Signing, cn=VeriSign CA for Adobe CDS *(a Level 2 CA for shared CA services)*
- C=US, o=<organization name>, ou=<TBD>, <(optional) ou=TBD,> cn=<Organization name> for Adobe CDS *(a Level 2 CA for dedicated CA services)*

An organization can utilize either a shared VeriSign CA or a CA dedicated to the organization. Depending on their choice, X.501 distinguished names assigned to subscribers are assigned from one of the following directory information trees as follows:

- C=US, o=VeriSign Inc., ou=CDS Signing, cn=<common name>
- C=US, o=<organization name>, ou=<TBD>, <(optional) ou=TBD,> cn=<common name>

The common name of the subscriber will have one of the following three values and the entire subscriber DN shall constitute a unique value:

- cn=<individual's name>
- cn=<organization's name>
- cn=<organizational role (eg, Chief Financial Officer)>

When the subscriber is an individual, the common name will take one of the following forms:

- cn=firstname initial. lastname
- cn=firstname middlename lastname
- cn=firstname middlename lastname, dnQualifier=integer

In the last form, dnQualifier is an integer value that makes the name unique. The last form may be used if the other two name forms have already been assigned to subscribers.

A VeriSign Affiliate Processing Center operates as a dedicated CA. The X.501 distinguished names assigned to the Affiliate CDS CA and their dedicated organizational CAs are:

- C=US, o=<Affiliate name>, ou=TBD, <(optional) ou=TBD,> cn=<Affiliate name> CA for Adobe CDS *(a Level 2 CA)*

Affiliate customers can utilize either a shared Affiliate CA or a CA dedicated to the customer organization. Depending on their choice, X.501 distinguished names assigned to subscribers are assigned from one of the following directory information trees as follows:

- C=US, o=<Affiliate name>, ou=TBD, <(optional) ou=TBD,> cn=<common name>

- C=US, o=<Affiliate's customer name >, ou=TBD, <(optional) ou=TBD,> cn=<common name>

Certificates issued include a non-null subject name field. The subject alternative name field may be used if marked non-critical.

VeriSign CDS certificates may assert an alternate name form in the subjectAltName field.

3.1.2 Need for Names to be Meaningful

The subscriber certificates issued pursuant to this CPS contain names that can be understood and used by relying parties. Names used in the certificates must identify in a meaningful way the subscriber to which they are assigned.

The common name in the DN must represent the subscriber in a way that is easily understandable for humans. For people, this will typically be a legal name, with the following preferred common name form:

cn=firstname initial lastname

While the issuer name in CA certificates is not generally interpreted by relying parties, this CP requires use of meaningful names by CAs. If included, the common name shall describe the issuer, such as:

cn=<Organization name> CA for Adobe CDS.

The subject name in CA certificates must match the issuer name in certificates issued by the subject, as required by RFC 5280, even if the subject's name is not meaningful.

3.1.3 Rules for Interpreting Various Name Forms

Rules for interpreting distinguished name forms are contained in the applicable certificate profiles (See Section 7.1.2. and Appendix A).

3.1.4 Uniqueness of Names

The Organization RA ensures the uniqueness of names for all certificates issued within the CDS Issuing CA domain. Information contained in certificate enrollment requests is automatically checked against the VeriSign CDS database to prevent duplication and to ensure the uniqueness of CDS certificate distinguished names and serial numbers.

3.1.5 Name Claim Dispute Procedure

The VeriSign PA investigates and corrects, if necessary, any name collisions brought to its attention. If appropriate, Organization PMAs resolves name collisions within their own space.

3.1.6 Recognition, Authentication, and Role of Trademarks

The VeriSign CDS shall not knowingly issue a certificate including a name that a court of competent jurisdiction has determined infringes the trademark of another. Certificate Applicants are prohibited from using names in their Certificate Applications that infringe upon the Intellectual Property Rights of others. VeriSign, however, does not verify whether a Certificate Applicant has Intellectual Property Rights in the name appearing in a Certificate Application or arbitrate, mediate, or otherwise resolve any dispute concerning the ownership of any domain name, trade name, trademark, or service mark. VeriSign is entitled, without liability to any Certificate Applicant, to reject or suspend any Certificate Application because of such dispute.

3.1.7 Method to prove possession of private key

For all Digital Signature certificate requests the subscriber generates the key pair and the VeriSign CDS PKI shall require proof of possession of the private key that corresponds to the public key in the certificate request. The technical mechanism to establish this proof is verification that the Subscriber's certificate enrollment request containing their public key is digitally signed with the corresponding private key.

For smart card issuance, certificate enrollment requests are sent from a CMS workstation to the CDS CA as signed and encrypted messages over an HTTP link.

For all certificate enrollment requests, the VeriSign CDS CA performs the digital signature validation checks to ensure it is a properly formed message and that its integrity has not been altered.

In cases where key generation is performed under the CA or RA's direct control, proof of possession is not required.

Private keys generated outside the control of the Subscriber are generated in a secure and controlled manner and delivered to the certificate subject or an authorized representative via an accountable method as described in Section 4.2.

Subscriber key pair generation is further described in Section 6.1.1.2.

3.1.8 Authentication of CA Certificate Issuance

An organization or Affiliate may request a CDS Subordinate CA certificate in order to have a dedicated CDS CA under the VeriSign Intermediate CDS CA to sign all Subscriber certificates for the organization. The organization applicant authentication is performed by the VeriSign RA in accordance with section 3.1.9.

An Affiliate customer organization may request a CDS Subordinate CA certificate to have a dedicated CDS CA under the Affiliate Subordinate CDS CA to sign all Subscriber certificates for the organization. The organization applicant authentication is performed by the Affiliate RA in accordance with section 3.1.9.

An audit shall examine the operations of the CA to verify compliance with this CPS in accordance with section 2.7.

The VeriSign PMA will have the final authority for verifying the information, and approving the requesting representative and the representative's authorization to act in the name of the organization.

The CA subscriber shall provide proof of possession of the private key in accordance with Section 3.1.7.

3.1.9 Authentication of Organization Identity

The RA authenticates the organization identity in a certificate request. Such authentication includes–

- Organization name, address and Dun & Bradstreet number (or similar trusted 3rd party verification); and
- Authentication and authorization of the requesting representative to act in the name of the organization.

Authentication is performed by the Issuing CA receiving the request (either Level 1 or 2).

In the case of an organization request for a dedicated subordinate CA certificate, the request is processed as per section 3.1.8. In the case of an organization request for a CDS Subscriber certificate for use on behalf of the organization, the Organization RA processes the request in accordance with section 3.1.11.

3.1.10 Authentication of Individual Identity

The Organization RA ensures that the applicant's identity information is verified. Identity is established no more than 30 days before initial certificate issuance.

Manual Authentication

RAs may accept a fax or email copy of an official form of government-issued photo identification, or notarized authentication of an applicant's identity to support identity proofing of remote applicants. Minimal procedures for RA authentication and notarized authentication of applicants are detailed below.

At a minimum, authentication procedures for applicants include the following steps:

1) Verify that the request by the applicant was authorized by the organization by performing a callback to the organization;

2) Applicant's information is verified through use of official organization records.

3) Applicant's identity is established by the Organization RA, based on the following processes:

   i) The applicant submits a minimum of one currently valid government-issued photo ID as proof of identity (possession of an official form of government-issued photo id substantiates proof of identity), and,

   ii) The credential presented in step 3) i) above shall be verified by the Organization RA for currency and legitimacy (e.g., the organization ID is verified as valid). Typically this is accomplished by querying a database maintained by the organization that issued the credential, but other equivalent methods may be used. Receipt of a notarized identity authentication is preferred whereby the currency and legitimacy of the credential is verified by the notary public.

4) The applicant signature is recorded and maintained by the Organization RA. This establishes an audit trail for dispute resolution.

Additionally, the Organization RA records the process that was followed for issuance of each certificate by recording the following information:

- The identity of the Organization RA or Trusted Agent performing the identification;
- A signed declaration by that person that he or she verified the identity of the Applicant as required by the CPS using the format set forth at 28 U.S.C. 1746 (declaration under penalty of perjury);
- Unique identifying number(s) from the ID(s) of the applicant, or a facsimile of the ID(s);
- The date and time of the verification; and
- A declaration of identity signed by the applicant using a handwritten signature using the format set forth at 28 U.S.C. 1746 (declaration under penalty of perjury). The Subscriber shall also attests that he or she understands and acknowledges the obligations contained in the Subscriber Agreement including use and protection of the private key and the need to report suspicion of loss or compromise of the private key.

A Trusted Agent may serve as proxy for the Organization RA. The Trusted Agent forwards the Subscriber Enrollment Form and all information collected from the applicant directly to the Organization RA in a secure manner either by first class postal mail, Federal Express or other similar means. The Trusted Agent notarizes a copy of the photo ID as well as the Subscriber Enrollment Form for transmission to the Organization RA.

Authentication by a Trusted Agent does not relieve the Organization RA of its responsibility to perform steps 1), 2), the verification of identifying information (e.g., by checking official records) in step 3), above.

Automated Authentication

The organization may deploy an Automated Administration process ("RA process") that performs the authentication procedure without administrator intervention. This automated procedure validates the identity of the applicant in real time through validation against the organization's existing knowledge of the identity of the applicant (ie, a pre-existing identity check). This is achieved by submission of shared secret information that is known only by the applicant. The RA process verifies the shared secret against antecedent identification held within secure organizational data stores and validates that an ongoing relationship exists with the applicant.

3.1.11 Authentication for Group Certificates

Normally, a certificate is issued to a single Subscriber. However, in some cases, a certificate is issued to an identity representing an organization or organizational role (eg, Chief Financial Officer). In these cases there are several entities acting in one capacity, and a certificate may be issued that corresponds to a private key that is shared by multiple possible custodians.

Organization RAs records the information identified in Section 3.1.10 for the designated sponsor before issuing a group certificate. In addition to the authentication of the sponsor, the following procedures are performed for members of the group:

- The Organization RA is responsible for ensuring control of the private key, including maintaining a list of Subscribers who have access to use of the private key, and accounting for which Subscriber had control of the key at what time;
- The subjectName DN must not imply that the subject is a single individual, e.g. by inclusion of a human name form;
- The certificate does assert the *nonRepudiation* bit;
- The list of those holding the shared private key is provided to, and retained by, the applicable CA or its designated representative; and
- The procedures for issuing HSMs for use in shared key applications must comply with all other stipulations of the CP (e.g., key generation, private key protection, and Subscriber obligations).

3.2 Certificate Renewal, Update, and Routine Re-Key

3.2.1 Certificate Renewal/Modification

Renewing a certificate means creating a new certificate with the same name, key, and authorizations as the old one, but a new, extended validity period and a new serial number. Certification modification means creating a new certificate with the same key as the old one, but with a new name or authorization.

The VeriSign CDS does not implement certificate renewal or modification for Subscriber certificates.

Modification of CDS CA certificates is permitted after the Issuing CA verifies proof of any subject information changes.

In the event of a CA compromise, Subscribers are required to repeat the initial certificate application process.

3.2.2 Certificate Re-key

The VeriSign CDS supports re-key for subscriber and CA certificates. Re-keying a certificate means that a new certificate is created that is identical to the old one, except that the new certificate has a new, different public key (corresponding to a new, different private key); a different serial number; and may be assigned a different validity period. After certificate re-key, the old certificate is be further re-keyed, but may be revoked.

A Subscriber, whose certificate has not expired and whose initial subscriber enrollment data has not changed, may re-key his or her certificate based on electronic authentication of a currently valid signature certificate. If the current certificate has expired or been revoked, a Subscriber obtains a new key only through the same procedures as initial certificate issuance.

The VeriSign CDS provides an SSL-protected web page for re-keying of the Signature certificate. Electronic authentication methods include proof of possession of the current, active private key or through the use of a challenge phrase (or the equivalent thereof). During original enrollment, subscribers choose and submit a challenge phrase (or the equivalent thereof). Upon renewal of a certificate, if a subscriber correctly submits the subscriber's challenge phrase (or the equivalent thereof) with the subscriber's reenrollment information, and the enrollment information (including contact information) has not changed, a renewal certificate is automatically issued.

Certificate re-key of the CDS CA certificate is described in Section 4.7.

3.2.3 Certificate Update

The VeriSign CDS does not implement certificate update for Subscriber certificates. If an individual's name, authorizations or privileges change, the subscriber must enroll for a new certificate using the procedures defined in Section 3.1.10, and the old certificate shall be revoked.

Update of the CDS CA certificate is governed by key changeover procedures specified in section 4.7.

3.3 Re-Key after Revocation

Subscribers must repeat the initial registration requirements, including identity verification, for re-key after revocation.

3.4 Revocation Request

The VeriSign CDS provides an online SSL-secured Web page at which subscribers may request revocation of their CDS certificate(s). The Subscriber authenticates by presenting his or her challenge phrase selected during the certificate enrollment process. The subscriber may also request revocation of his or her certificate by sending a digitally signed e-mail message to the Organization RA. The Organization RA authenticates the request by verifying the digital signature on the signed-mail. If the subscriber is unable to submit the challenge phrase or his or her certificate, the subscriber may communicate with the Organization RA by telephone, facsimile, e-mail, postal mail, or courier service. The Organization RA authenticates the communication before revoking the subscriber's certificate(s). Depending on the originator of the request and the method used, the request information is scrutinized and a callback performed to verify request authenticity.

A Trusted Agent may request revocation of a sponsored subscriber's certificate by sending a digitally signed e-mail message to VeriSign. The Organization RA authenticates the request by validating the digital signature on the signed e-mail and checks that the Trusted Agent is requesting revocation for a subscriber certificate that is associated with his or her organization.

An Organization RA may revoke a Subscriber's certificate only for Subscribers associated with his or her organization.

The VeriSign RA or Organization RA may revoke a Subscriber's certificate for cause.

4. OPERATIONAL REQUIREMENTS

4.1 Certificate Application

CDS PKI Authorities perform the following steps when processing a certificate enrollment request from an applicant:

- Establish the applicant's authorization (by the employing or sponsoring organization) to obtain a certificate (per sections 3.1.9–3.1.11).
- Establish and record identity of the applicant (per sections 3.1.9–3.1.11)
- Obtain the applicant's public key and verify the applicant's possession of the private key for each certificate required (per Section 3.1.7)
- Verify any information to be included in the certificate.

All communications with the CDS PKI in processing certification applications are electronic and are protected by SSL. Details of the certificate application process for a certificate issued by the CDS CA are as follows:

1) Applicants enrolling for a CDS certificate must complete an enrollment form and obtain enrollment authorization from an authorized organization official.
2) The Applicant must acknowledge acceptance of the terms of the Subscriber Agreement (by a query display of the agreement text and an acknowledgement check box) and submit the enrollment form to the Organization RA and provide accompanying identification information in accordance with sections 3.1.9–3.1.11.
3) After obtaining a hardware device, the subscriber receives a pre-authorized Passcode from the Organization RA which is presented to an organization-hosted, SSL-protected web page for receipt of the certificate.
4) Public/private key pairs for signature certificates are generated on the hardware device and a certificate signing request (CSR) is generated which includes the public key, the subscriber name, e-mail address and organizational data necessary to populate a certificate in accordance with the end entity certificate profile specified in Appendix A.

   The CSR is submitted over an SSL session to the CDS CA, which checks for proof of possession of the private key. The CDS CA then signs the request, posts the certificate to the CDS Repository and returns the certificate to the hardware issuance system where it is then downloaded onto the Subscriber's device.

Alternatively the organization may deploy an Automated Administration server that performs the steps of the application process without administrator intervention. This process validates the applicant's submission of secret information shared between the subscriber and the RA process that leverages antecedent identification by the organization (at least equivalent to that described in section 3.1) and confirms an ongoing relationship with the organization. The shared secret information is verified against approved organizational data stores to create the identity bind.

Upon successful authentication, the CDS CA issues a certificate as described at step 3) above.

4.1.1 Delivery of Subscriber's Public Key to Certificate Issuer

The Subscriber's identity information and public key are delivered from the FIPS 140 Level 2 compliant HSM to the CDS CA in an encrypted format using the CSR (PKCS#10) protocol.

4.2 Certificate Issuance

All information included in the certificate is verified prior to certificate issuance. The CDS CA signs the request and transmits the certificate to the hardware issuance system where it is downloaded onto the subscriber's hardware device.

The certificate is issued within a FIPS 140 Level 2 HSM in accordance with section 6.2.1. The VeriSign CDS may issue subscriber certificates with either a one (1), two (2) or three (3) year lifetime.

Secure delivery/exchange of the private key and public keys is described in sections 6.1.2 - 6.1.4.

4.3 Certificate Acceptance

Notification of certificate generation is an integral part of the certificate issuance/acceptance process. The applicant action in submitting a certificate enrollment request is sufficient to constitute acceptance of the resulting certificate and the corresponding certificate obligations in accordance with the Subscriber Agreement and responsibilities outlined in section 2.1.6.

4.4 Certificate Suspension and Revocation

4.4.1 Revocation

4.4.1.1 Circumstances for Revocation

A CDS certificate shall be revoked when the binding between the subject and the subject's public key defined within the certificate is no longer considered valid. Under the following circumstances a certificate will be revoked:

- Identifying information including the organizational affiliation in the Subscriber's certificate changes before the certificate expires;
- The certificate subject can be shown to have violated the requirements of this CPS or the Subscriber Agreement;
- The private key is suspected of compromise;
- The subscriber or other authorized party asks for his/her certificate to be revoked;
- The continued use of the certificate may be harmful to the CDS PKI; or
- On request by the Adobe Policy Authority.

Whenever any of the above circumstances occur, the associated certificate is revoked and placed on the CRL. A revoked certificate will appear on at least one CRL.

4.4.1.2 Who Can Request Revocation

The Subscriber is authorized to request the revocation of his or her own certificate. The Adobe Policy Authority, the VeriSign RA, the Organization RA, or other authorized party including a Trusted Agent can request the revocation of a Subscriber's certificate on the Subscriber's behalf.

A Trusted Agent can only request revocation of a certificate for a subscriber that is associated with the Trusted Agent's organization. Written notice including a reason for the revocation is also provided, via email, postal mail, telephone or facsimile, to a subscriber whose certificate has been revoked.

4.4.1.3 Procedure for Revocation Request

The revocation request must identify the certificate to be revoked and must include the reason for revocation. The revocation requests may be manually or digitally signed and must be authenticated by an Organization RA.

If the revocation is being requested for reason of key compromise or suspected fraudulent use, then the subscriber's and the RA's revocation request must so indicate. The processes for revocation are as follows:

Certificate Revocation Request by Subscriber: A CDS Subscriber may request revocation of a certificate by sending a digitally signed message to the Organization RA. The message must include a reason for the revocation. The Organization RA validates the request by verifying the signature on the signed message. If the Subscriber is not in possession of their private Signature key, he or she may also request revocation of his or her certificate by presenting the unique challenge phrase selected during certificate enrollment to a revocation Web page hosted by VeriSign. The Web page is protected using SSL. Upon successful validation of the revocation request by the Organization RA, the CDS PKI changes the certificate status in the repository from "valid" to "revoked" and places the revoked certificate's serial number on the next published CRL.

Certificate Revocation Request by Trusted Agent: A Trusted Agent may request revocation of a Subscriber's certificate by sending a digitally signed message to the Organization RA. The Organization RA validates the request by verifying the signature on the signed message and confirming that the affiliation in the Subscriber certificate is the same as the Trusted Agent affiliation. The message must identify the name and e-mail address of the subscriber whose certificate(s) is to be revoked and the reason for the revocation. Upon successful validation of the revocation request by the Organization RA, the CDS changes the certificate status in the repository from "valid" to "revoked" and places the revoked certificate's serial number on the next published CRL.

Certificate Revocation Request by RA: An Organization RA requests revocation of any CDS subscriber certificate associated with their organization. Access to the CDS to request revocation is protected using SSL and requires presentation of a valid RA certificate. The CDS validates the RA certificate and checks that the RA affiliation is the same as the organizational affiliation in the certificate to be revoked. If these checks are successful, the CDS changes the certificate status in the repository from "valid" to "revoked" and places the revoked certificate's serial number on the next published CRL.

The CDS aggregates all revoked certificates, digitally signs a new CRL, and posts the CRL to the repository per the frequency specified in Section 4.4.3.

4.4.1.4 Revocation Request Grace Period

There is no grace period for a request for revocation of the certificate by the CDS CA. The Subscriber or Organization RA is obligated to request that the CDS CA revoke the certificate as soon as possible after the need for revocation has been determined. The CDS CA revokes certificates as quickly as practical upon receipt of a proper revocation request. Revocation requests are processed before the next CRL is published, excepting those requests received within two hours of CRL issuance. Revocation requests received within two hours of CRL issuance are processed before the next CRL is published.

4.4.2 Suspension

Certificate suspension is not supported.

4.4.3 Certificate Revocation Lists

The CDS PKI issues CRLs at least every twenty-four (24) hours, and these CRLs have a twenty-four (24) hour validity interval (nextUpdate). Superceded CRLs are removed from the repository upon posting of the latest CRL. The latest CRL contains all revoked certificates.

The VeriSign Level 1 Intermediate CA is operated offline and used only for issuing certificates to other CAs and signing CRLs. CRLs for the offline CA shall be published every 365 days.

The CDS PKI publishes information on how to obtain information on revoked certificates and advises relying parties via the CDS CPS of the need to check certificate revocation status. If a relying party is unable to obtain revocation information for a CDS certificate, the relying party must either reject use of the certificate, or make

an informed decision to accept the risk, responsibility, and consequences of using a certificate whose authenticity cannot be guaranteed.

4.4.4 Online Status Checking

The VeriSign CDS will provide an online CSA to enable certificate status checking using the Online Certificate Status Protocol (OCSP compliant with RFC 5019). The OCSP responder certificate will be issued on a FIPS 140 Level 3 hardware token. The OCSP responder certificate is signed by the same CA using the same key that signed the certificates whose status is to be checked.

The OCSP responder shall ensure that accurate and up-to-date information is provided in the revocation status response and shall digitally sign all responses. Distribution of OCSP status information will meet or exceed the CRL issuance requirements specified in section 4.4.3.

Where a certificate is revoked for key compromise, the status information will be updated and made available to relying parties without delay. Client software using online status checking need not obtain or process CRLs.

4.4.5 Other Forms of Revocation Advertisements Available

The VeriSign CDS also provides a Web page protected with a VeriSign Class 3 certificate at which relying parties may query the revocation status of a subscriber certificate.

4.4.6 Checking Requirements for Other Forms of Revocation Advertisements

No stipulation.

4.4.7 Special Requirements Regarding Key Compromise

In the event of a CA key compromise, the VeriSign PMA is immediately be informed. The CDS PKI initiates procedures to notify subscribers affected depending on the scope of the compromise:

- the Adobe Root CA will communicate the revocation of the CDS Level 1 CA certificate to all relying parties by publishing an ARL.
- the VeriSign Level 1 CA will assist in communicating the revocation of a Level 2 CDS CA certificate to all relying parties by publishing an ARL;

Subsequently, the compromised CA will generate a new signing key pair and reconstitute its operation using the same procedures that were performed during initial system initialization and re-key all subscriber certificates. The new CDS CA certificate will be distributed as defined in section 4.2.2.

4.5 Security Audit /Audit Logging Procedures

4.5.1 Types of Events Recorded

All material security events are recorded in audit logs. Electronic-based audit data is automatically collected. Manual data may be recorded in the absence of electronic data as appropriate to the process being audited.

4.5.7 Notification to Event-Causing Subject

No notification is provided to an event-causing subject.

4.5.8 Vulnerability Assessments

VeriSign has instituted a multi-faceted, proactive approach to ensuring a trustworthy CDS operation.

VeriSign conducts quarterly vulnerability assessments to determine its ability to protect against external network threats. VeriSign personnel, in addition to external consultants, perform this routine assessment.

Finally, VeriSign undergoes a yearly extensive SAS 70 Type 2-security audit and a WebTrust audit to validate its operation in accordance with this practice documentation.

4.6 Records Archival

4.6.1 Types of Data/Records Archived

The VeriSign CDS audit process records the following information, in either paper or electronic record format, upon initialization of a CA key pair:

- CA system equipment configuration files,
- CA accreditation (if necessary),
- CDS CPS and any contractual agreements to which the CA is bound.

The following data is recorded for archive during CMA operation:

- CA accreditation (if applicable)
- Certificate Policy
- Certification Practice Statement
- Contractual obligations
- Other agreements concerning operations of the CA
- System and equipment configuration
- Modifications and updates to system or configuration
- Security audit data (in accordance with Section 4.5)
- Revocation requests and all certificates revoked
- All CARLs and CRLs issued and/or published
- Certificate requests and subscriber identity authentication data as per Section 3.1.10
- Subscriber Agreements
- All certificates issued and/or published
- Record of Re-key
- Other data or applications to verify archive contents
- Documentation required by compliance auditors

4.6.2 Retention Period for Archive

CDS archive records, including certificates, CRLs and CDS public keys, are retained for a period of at least ten (10) years and six (6) months. Currently, all database records are retained online for immediate access. Offsite storage of full system backups is maintained to ensure recovery of the online system in the event of a catastrophic system fault. System backups are stored at an offsite third party facility.

Media used for archiving CDS records can support the retention periods noted above.

4.7 Key Changeover

The CDS CA uses its private signature keys for signing certificates and CRLs only. CA key pairs established under this CPS will be prevented by technical means from signing subscriber certificates whose validity periods would extend beyond the expiration dates of the CA certificate's validity interval. When a CDS CA key is changed, the old CDS CA key pair is retained to issue CRLs for Subscribers that have been issued certificates signed with the old CDS CA signing key.

The CDS CA does not support key rollover certificates. Re-keying of a CA requires the new certificate to be issued for the CA public key.

4.8 Compromise and Disaster Recovery

VeriSign maintains a Disaster Recovery Facility (DRF) located at a VeriSign-owned facility located at a distance from the primary site as specified in section 5.1.1. The VeriSign DRF is operated under the same security policies and procedures as the primary facility.

VeriSign has developed a Disaster Recovery Plan for all of its managed PKI services including the CDS PKI service. The Disaster Recovery Plan defines the procedures for the VeriSign Disaster Recovery Team to reconstitute VeriSign CDS operations using backup data and backup copies of the CDS keys.

4.9 CA Termination

The Adobe PA shall be notified prior to any CDS Subordinate CA termination within the VeriSign CDS CA hierarchy. The Adobe PA and VeriSign will agree on appropriate procedures to properly cease operations.

In the event that it is necessary for a VeriSign CDS CA to cease operation, the VeriSign CDS makes a commercially reasonable effort to notify Subscribers, Relying Parties, and other affected entities of such termination in advance of the CA termination. In the event of termination of a CDS CA, certificates signed by the CDS CA will also be revoked.

A termination plan will be developed that minimizes disruption to Subscribers and Relying Parties. Such termination plans may address the following, as applicable:

- Provision of notice to parties affected by the termination, such as Subscribers, Relying Parties, and Customers, informing them of the status of the CA,
- Handling the cost of such notice,
- The revocation of the Certificate issued to the CA by VeriSign,
- The preservation of the CA's archives and records for the time periods required in this CPS,
- The continuation of Subscriber and customer support services,
- The continuation of revocation services, such as the maintenance of online status checking services,
- The revocation of unexpired un-revoked Certificates of end-user Subscribers if necessary,
- Refunding (if necessary) Subscribers whose unexpired un-revoked Certificates are revoked under the termination plan or provision, or alternatively, the issuance of replacement Certificates by a successor CA,
- Disposition of the CA's private key and the hardware modules containing such private key, and
- Provisions needed for the transition of the CA's services to a successor CA.

Dissemination of revocation notice will be performed as discussed in CPS section 4.8.

5. PHYSICAL, PROCEDURAL AND PERSONNEL SECURITY CONTROLS

5.1 Physical Controls

The VeriSign CDS equipment is dedicated to CA functions and does not perform non-CA related functions.

5.2 Procedural Controls

5.2.1 Trusted Roles

All employees, contractors, and consultants of the VeriSign CDS that have access to or control cryptographic operations that may materially affect the issuance, use, suspension, or revocation of certificates, including access to restricted operations of the CDS Repository, are considered as serving in a trusted position.

5.2.1.2 Officer

The Officer role is fulfilled by the following entities for the VeriSign CDS PKI:

The *VeriSign RA* is responsible for validating Organization RA identity and processing the RA certificate enrollment requests from a client organization. The VeriSign RA approves certificate enrollment requests, processes certificate revocation requests and also assists the RA subscribers during the enrollment process (as required). All persons filling the *VeriSign RA* role shall satisfy a complete background investigation.

An *Organization RA* is a representative of an organization that has entered into a contract with VeriSign for CDS PKI services. The Organization RA performs the equivalent functions of the VeriSign CDS RA for end entity Subscribers of the user community associated with that organization. The Organization RA has a secure, remote interface to the VeriSign CDS. All communications between the Organization RA and the VeriSign CDS are via an SSL session with certificate-based access control. The Organization RA certificate is stored on a FIPS 140 Level 2 HSM.

The Affiliate Organization RA perform the equivalent functions of the VeriSign CDS RA.

5.2.1.5 Trusted Agent

A *Trusted Agent* is a person authorized to act as a representative of the Organization RA in providing subscriber identity verification during the registration process. Trusted Agents do not have login access to the CDS PKI.

5.2.1.6 PKI Sponsor

A *PKI Sponsor* fills the role of a subscriber for another entity that is named as the public key certificate subject. The PKI Sponsor is an applicant requesting a certificate on behalf of:

- another individual subscriber, such as a contractor or other associated personnel;
- an organizational role; or
- an organization.

The PKI Sponsor works with the Organization RA and, when appropriate, Trusted Agents, to register entities in accordance with Sections 3.1.9, 3.1.10 and 3.1.11, and is responsible for meeting the obligations of subscribers as defined throughout this document. .

The individual within the sponsoring organization that is given custodial possession of the HSM containing the certificate is referred to as the *certificate custodian* with obligations as described in section 2.1.6.3.

5.3 Personnel Controls

5.3.1 Background, Qualifications, Experience and Clearance Requirements

All persons with unattended access to the VeriSign CDS and CDS Repository are expressly approved and must be of unquestionable loyalty, trustworthiness, and integrity.

The VeriSign CDS institutes an extensive personnel security program that identifies specific "high risk" duties and requires "trusted personnel" to be assigned to these duties. The trusted status is only granted upon successful completion of a background investigation, performed by an independent investigation firm. Employees are trained and made fully aware of their responsibilities to maintain compliance with corporate security, unique program security, and personal security/integrity requirements as a condition of continued employment as a trusted employee.

Personnel appointed to operate CMA equipment shall:

- Have successfully completed an appropriate training course;
- Have demonstrated the ability to perform their duties;
- Be trustworthy;
- Have no other duties that would interfere with their duties as a CMA;
- Have not knowingly been previously relieved of CMA or other trusted duties for reasons of negligence or non-performance of duties;
- Have not knowingly been denied a security clearance, or had a security clearance revoked;
- Have not been convicted of a felony offense; and
- Be appointed in writing by an approving authority, or be a party to a contract for PKI services.

5.3.3 Training Requirements

Operations personnel are sufficiently trained prior to performing independent, unattended duties.

6. TECHNICAL SECURITY CONTROLS

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

Key pairs are generated in such a way that the private key is not known by anyone other than the authorized user of the key pair. Private keys do not appear outside of the modules in which they are generated unless encrypted for local transmission or for processing or storage by a key recovery mechanism.

6.1.1.1 CA Key Pair Generation

CDS CA key pairs are generated within a secure Key Ceremony room on hardware tokens. The ceremony is video taped to evidence the valid execution of the key generation procedures. A full audit record is created to ensure that all security requirements, including separation of roles were followed.

6.1.1.2 Subscriber Key Pair Generation

Subscriber key pairs for CDS Digital Signature certificates are generated in a FIPS 140 Level 2 HSM and may not be exported from the module that generated the key pairs (e.g., smart card).At no time does the subscriber private key appear in plain-text form outside the hardware protection boundary of the cryptographic module.

VeriSign RA and Organization RA keys are generated in a FIPS 140 Level 2 HSM.

6.1.2 Private Key Delivery to Subscriber

Key generation for digital signature certificates stored on FIPS 140 Level 2 HSM is performed on the device. The private key never leaves the cryptographic boundary of the hardware device and thus, there is no need to deliver the subscriber's private key.

The CDS CA only issues certificates to a single Subscriber. In certain cases, the CDS issues a group certificate for use by several entities acting in one capacity and will allow end users to share the group certificate (e,g., an organization or an organizational role) only as noted in section 3.1.11. Such certificates indicate an organizational name or role name in the Subject of the certificate and do not set the *nonRepudiation* bit. Such group certificates have a certificate custodian identified who "acts" as the primary Subscriber as described in section 2.1.6.3.

When a key is generated for a non-specific end user, the custodian ensures that the following controls are met in the delivery of the certificate and handling of the HSM:

- The private key must be protected from inadvertent activation, compromise, or loss while in the possession of any certificate custodian;
- The private key must be protected from inadvertent activation, compromise or loss during the delivery of the HSM to another certificate custodian; and
- The certificate custodian shall acknowledge receipt of the HSM.

The Organization RA ensures that the correct HSM and activation data are provided to the correct certificate custodian without interception based on a careful matching against information contained in the corresponding application.

The Organization RA maintains a record of the custodian acknowledgement of receipt of the correct HSM.

6.1.3 Public Key Delivery to Certificate Issuer

The Subscriber's identity information and public key are delivered to the certificate issuer simultaneously in an SSL-protected session via a PKCS #10 request.

The format for the delivery of this data is dependent on the type of web browser used. For all browser types, the public key is signed by the corresponding private key as the mechanism to prove possession of the private key.

6.1.4 CA Public Key Delivery to Relying Parties

The Root CA certificates are available within Adobe approved components for signature verification by relying parties.

6.1.5 Key Sizes and Signature Algorithms

Signature algorithms conform to RSA PKCS#1. Key sizes and hash algorithms are detailed below:

- The key pairs for all VeriSign CDS CAs, including the Level 1 and Level 2 CAs are 2048-bit RSA key pairs.
- The key pairs for all end entity certificates shall be 2048-bit RSA key pairs and shall be stored on FIPS 140 Level 2 cryptographic hardware devices.

The trust anchor for the CDS CAs, is the Adobe CDS Root CA, which contains a public key of at least 2048 bits.

6.1.6 Public Key Parameters

Prime numbers for use with the RSA algorithm defined in [PKCS-1] are generated and checked in accordance with [PKCS-1].

6.1.7 Parameter Quality Checking

Public key parameters for signature algorithms defined in the Digital Signature Standard (DSS) are generated in accordance with FIPS 186. Parameter checking (including primarily testing for prime numbers) is performed in accordance with FIPS 186-2.

6.1.8 Hardware/Software Key Generation

Validated FIPS 140 Level 2 HSMs are used to generate all subscriber key pairs, as well as pseudo-random numbers and parameters used in key pair generation. Any pseudo-random numbers used for key generation material are generated by a FIPS-approved method. Symmetric keys may be generated by means of either software or hardware mechanisms.

6.1.9 Key Usage Purposes

The VeriSign CDS CA issues client Digital Signature certificates with the key usage extension for digital signature.

Public keys that are bound into end-entity Subscriber certificates are used only for digital signatures and assert the *digitalSignature* and *nonRepudiation* bits. Shared group certificates do not assert the *nonRepudiation* bit.

Public keys that are bound into the CDS CA certificates are used only for signing certificates and status information (e.g., CRLs). CDS CA certificates whose subject public key is to be used to verify other certificates assert the *keyCertSign* bit. CDS CA certificates whose subject public key is to be used to verify CRLs assert the *cRLSign* bit. For CDS CA certificates used to verify both certificate and CRLs, both the *keyCertSign* and *cRLSign* bits are asserted.

All certificates meet the certificate profiles defined in Appendix A.

6.2 Private Key Protection

6.2.1 Standards for Cryptographic Modules

All cryptographic modules meet the requirements of FIPS 140, Security Requirements for Cryptographic Modules.

The VeriSign CDS RA, Organization RAs and Subscribers are obligated to use the FIPS 140 Level 2 HSM for all cryptographic operations.

The VeriSign CDS CA use a FIPS 140 Level 3 hardware cryptographic module.

All cryptographic modules dedicated to management of VeriSign CDS certificate signing key pairs are operated such that the private asymmetric cryptographic keys are never output in plain-text.

The CDS RA key and certificates are contained on FIPS 140 Level 2 HSM. The RA function, either performed by VeriSign or an Organization RA, is physically separated from the CDS CA in the secure facility.

6.2.3 Private Key Escrow

CDS CA private keys are not escrowed. Subscriber private signature keys are not escrowed.

6.2.4 Private Key Backup

6.2.4.1 Backup of CA Private Signature Key

Backup copies of the VeriSign CDS CA private keys are made to facilitate disaster recovery.

6.2.4.2 Backup of Subscriber Private Keys

VeriSign CDS subscribers are obligated to prevent unauthorized disclosure of their private keys.

Subscriber private signature keys may not be backed up or copied.

6.2.5 Private Key Archival

CDS CA private signature keys and Subscriber private signature keys are not archived. See Section 6.2.3 and Section 6.2.4 for additional details.

6.2.6 Private Key Entry into Cryptographic Module

When the VeriSign CDS CA makes a backup copy of its private key, the key is transferred to a hardware token in encrypted form. At no time does the key exist in plaintext form outside the hardware protection boundary.

Private keys for RAs and Subscribers are generated by and in a FIPS 140 Level 2 HSM. RA and Subscriber private keys never exist in plaintext form outside of the boundary of the HSM.

6.2.7 Method of Activating Private Key

The VeriSign CDS CA hardware tokens utilize a PIN-based activation mechanism.

VeriSign CDS subscribers are obligated to select a password or PIN during key generation. Entry of the password or PIN is required to activate the private key. The subscriber is the only entity that knows the password; at no time does the VeriSign CDS become aware of the subscriber's password. The subscriber shall protect the entry of activation data from disclosure. Similarly, the RA is the only entity that knows the password for the RA HSM.

6.2.8 Method of Deactivating Private Key

The VeriSign CDS CA hardware tokens are operated within an access-controlled secure facility. Access to the data center is strictly controlled. The token deactivates its private key upon removal from its reader. When not in use, the token is stored in a vault.

RA HSMs are deactivated by removing them from the RA workstation. Subscriber HSMs are automatically deactivated after a time out period or by removing them from the reader.

6.2.9 Method of Destroying Private Key

Private signature keys are destroyed when they are no longer needed or when the certificates to which they correspond expire or are revoked. In the event the VeriSign CDS CA private key requires destruction, the hardware token's initialization operation will be performed to do so. In the event the RA private key requires destruction, the RA module "initialize" command is used to overwrite the private key. In the event the Subscriber's private key stored on a smart card requires destruction, the Organization RA may re-initialize the card to overwrite the private key

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

The public key is archived as part of the certificate archival.

6.3.2 Usage Periods for the Public and Private Keys

The usage period for a VeriSign Level 1 and 2 CDS CA key pair is a maximum of eleven (11) years.

Subscriber public keys and private keys have a maximum usage period of either one (1), two (2), or three (3) years.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

VeriSign CDS subscribers are requested to select their own password/PIN to protect their private key. Guidance regarding the selection of is provided during the enrollment process.

RAs are also required to choose their own PINs. Guidance regarding the selection of a PIN is provided during the enrollment process.

6.4.2 Activation Data Protection

The VeriSign CDS CA activation data PINs are split into shares, each portion of which is written to a separate non-volatile storage medium (hardware token). Shares are provided to designated trusted employees, one share per employee. 3 of 12 shares are required to reconstitute a PIN.

6.4.3 Other Aspects of Activation Data

See Section 6.4.1.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

The VeriSign CDS employs an operating system that has been evaluated for security functionality, including audit requirements, identification and authentication, domain integrity enforcement, and discretionary access controls.

6.6 Life Cycle Technical Controls

Equipment (hardware and software) procured to operate the VeriSign CA and RA is purchased in a fashion to reduce the likelihood that any particular component was tampered with, such as random selection.

Software applications for the VeriSign CDS and RA are developed in-house in a controlled environment in accordance with VeriSign systems development and change management procedures.

VeriSign developed software, when first loaded, provides a method to verify that the software originated from VeriSign, has not been modified prior to installation, and is the version intended for use. Procured CDS CA and RA software, when first loaded, is verified as being that supplied by the vendor, with no modifications, and the correct version.

Equipment updates are purchased or developed in the same manner as original equipment, and are installed by trusted and trained personnel in a controlled and audited manner.

6.7 Network Security Controls

The VeriSign CDS is designed to mitigate risk to external threats.

6.8 Cryptographic Module Engineering Controls

See Section 6.2.

7. CERTIFICATE AND CRL PROFILES

Appendix A contains the formats for the various certificates and CRLs.

7.1 Certificate Profile

7.1.1 Version Numbers

CDS issue X.509 Version 3 certificates only.

7.1.2 Certificate Extensions

The VeriSign CDS uses the certificate profiles as described in Appendix A of this CPS. These profiles, comply with RFC 5280.

The VeriSign CDS issues certificates that include non-critical Adobe private extensions, *TimeStamp* and *ArchiveRevInfo*. No critical private extensions are included in certificates issued by the VeriSign CDS.

7.1.3 Algorithm Object Identifiers

Certificates under this CPS use the following OIDs for signatures:

sha-1WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5}
Sha256WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}

Certificates under this CPS use the following OIDs for identifying the algorithm for which the subject key was generated.

rsaEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1}

The VeriSign CDS certifies only public keys associated with the crypto-algorithms identified above, and only uses the signature crypto-algorithms described above to sign certificates, certificate revocation lists and any other PKI product, including other forms of certificate status information such as OCSP responses .

7.1.4 Name Forms

The subject field in certificates is populated with an X.500 Distinguished Name, with the attribute type as further constrained by RFC 5280.

The issuer field of certificates issued under the policies in this document is populated with an X.500 Distinguished Name, with the attribute type as further constrained by RFC 5280.

7.1.5 Name Constraints

The VeriSign CDS does not enforce name constraints; however, Organization RAs are limited to the jurisdictional name space assigned to their RA domain.

7.1.6 Certificate Policy Object Identifier

Certificates issued by the VeriSign CDS CA assert the OID as defined in Section 1.2.

7.1.7 Usage of Policy Constraints

The VeriSign CDS does not enforce policy constraints.

7.1.8 Policy Qualifiers Syntax and Semantics

The policy qualifier syntax is an IA5String that contains the URI for the Adobe CDS CP.

The certificate contains at minimum the User Notice qualifier that represents to the relying party, that reliance is only permitted if the document is verified on an Adobe supported platform.

7.1.9 Processing Semantics for the Critical Certificate Policy Extension

Certificates issued by the CDS CA do not contain a critical certificate policy extension.

7.2 CRL Profile

CRLs issued by the CDS CA conform to the CRL profile specified in Appendix A.

7.2.1 Version numbers

CRLs issued under this CPS are X.509 version 2 CRLs. The CDS CA does not issue Authority Revocation Lists (ARLs) or any other partitioned CRLs.

7.2.2 CRL and CRL Entry Extensions

The CDS CA shall issue CRLs that comply with the extensions specified in the CRL profiles detailed in Appendix A.

7.3 OCSP PROFILE

CDS CSAs shall sign OCSP responses using algorithms designated for CRL signing. The OCSP Responder certificate shall comply with the extensions specified in the OCSP profile detailed in Appendix A.

8. SPECIFICATION ADMINISTRATION

8.1 Specification Change Procedures

Comments or issues with this CPS should be directed to the parties identified in Section 1.4.2 of this document.

The Adobe PA, prior to enactment, must approve material amendments to this CPS.

8.2 Publication and Notification Procedures

Upon approval of a CPS modification by the PA, an updated version of this document is provided to the PA.

An abridged version of this CDS CPS is posted in the VeriSign document repository at *http://www.verisign.com/repository/index.html*. Applicable updates to this CPS that affect Subscribers and relying parties are posted on the VeriSign corporate web site.

8.3 CPS Approval Procedures

The Adobe PA is the final approval authority of any proposed changes to this CPS.

The CDS CA and Organization RA meet all of the requirements of the approved CDS CPS before commencing operations.

8.4 CPS Waivers

The Adobe PA is the final approval authority of any proposed waiver to the CP which with this CPS is compliant.

APPENDIX A: CERTIFICATE AND CRL FORMATS

The certificates and CRLs associated with the CDS PKI utilize the certificate and CRL formats specified in the following X.509 Certificate and Certificate Revocation List Extensions Profile.

APPENDIX B: DEFINITIONS

access	Ability to make use of any information system (IS) resource.
access control	Process of granting access to information system resources only to authorized users, programs, processes, or other systems.
accreditation	Formal declaration by a Designated Approving Authority that an IS is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk.
applicant	The Subscriber is sometimes also called an "applicant" after applying to a certification authority for a certificate, but before the certificate issuance procedure is completed.
archive	Long-term, physically separate storage.
Attribute Authority	An entity, recognized by a CMA, as having the authority to verify the association of attributes to an identity.
audit	Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures.
audit data	Chronological record of system activities to enable the reconstruction and examination of the sequence of events and changes in an event.
authenticate	To confirm the identity of an entity when that identity is presented.
authentication	Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information.
backup	Copy of files and programs made to facilitate recovery if necessary.
binding	Process of associating two related elements of information.
biometric	A physical or behavioral characteristic of a person.
certificate	A digital representation of information which at least (1) identifies the CA issuing it, (2) names or identifies its subscriber, (3) contains the subscriber's public key, (4) identifies its operational period, and (5) is digitally signed by the CA issuing it. As used in this CP, the term "Certificate" refers to certificates that expressly reference the OID of this CP in the "Certificate Policies" field of an X.509 v.3 certificate.
Certificate Management Authority (CMA)	A Certification Authority or a Registration Authority.
Certification Authority (CA)	An authority trusted by one or more users to create and assign certificates. [ISO9594-8]
CA facility	The collection of equipment, personnel, procedures and structures that are used by a Certification Authority to perform certificate issuance and revocation.
certificate-related information	Information, such as a Subscriber's postal address, that is not included in a certificate, but that may be used by a CA in certificate management.
client (application)	A system entity, usually a computer process acting on behalf of a human user that makes use of a service provided by a server.
compromise	Disclosure of information to unauthorized persons, or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred.
Computer Security Objects Registry (CSOR)	Computer Security Objects Registry operated by NIST

confidentiality	Assurance that information is not disclosed to unauthorized entities or processes.
cryptographic module	The set of hardware, software, firmware, or some combination thereof that implements cryptographic logic or processes, including cryptographic algorithms, and is contained within the cryptographic boundary of the module.
cryptoperiod	Time span during which each key setting remains in effect.
data integrity	Assurance that the data are unchanged from creation to reception
e-commerce	The use of network technology (especially the Internet) to buy or sell goods and services
erroneous issuance	Issuance of a certificate not materially in accordance with the procedures required by the CPS, issuance of a certificate to a person other that the one named as the subject of the certificate, or issuance of a certificate without the authorization of the person named as the subject of such certificate.
firewall	Gateway that limits access between networks in accordance with local security policy.
Hardware Security Module (HSM)	A tamper-resistant hardware device used to store digital private keys to protect the generation of digital signatures. The HSM is a form of secure crypto-processor that provides a secure environment for storing keys and conducting sensitive cryptographic operations.
impersonation	Requesting and being issued a certificate issued under this CPS based on false or falsified information relating to naming or identity.
integrity	Protection against unauthorized modification or destruction of information.
intellectual property	Useful artistic, technical, and/or industrial information, knowledge or ideas that convey ownership and control of tangible or virtual usage and/or representation.
intermediate CA	A CA that is subordinate to another CA, and has a CA subordinate to itself.
key escrow	The retention of the private component of the key pair associated with a subscriber's encryption certificate to support key recovery.
key exchange	The process of exchanging public keys (and other information) in order to establish secure communication.
key generation material	Random numbers, pseudo-random numbers, and cryptographic parameters used in generating cryptographic keys.
Local Registration Authority (LRA)	An RA with responsibility for a local community.
naming authority	An organizational entity responsible for assigning distinguished names (DNs) and for assuring that each DN is meaningful and unique within its domain.
non-repudiation	Assurance that the sender is provided with proof of delivery and that the recipient is provided with proof of the sender's identity so that neither can later deny having processed the data.
Non-verified Subscriber Information	Information submitted by a Certificate Applicant to a CA or RA, and included within a Certificate, that has not been confirmed by the CA or RA and for which the applicable CA and RA provide no assurances other than that the information was submitted by the Certificate Applicant.
Object Identifier (OID)	A specialized formatted number that is registered with an internationally recognized standards organization; the unique alphanumeric/numeric identifier registered under the ISO registration standard to reference a specific object or object class. In the federal government PKI OIDs are used to uniquely identify each of the four policies and cryptographic algorithms supported.
Out-of-Band	Communication between parties using a means or method that differs from the current method of communication (e.g., one party uses U.S. Postal Service mail to communicate with another party where current communication is occurring online).
PKI Sponsor	Fills the role of a Subscriber on behalf of an organizational role or organizations that are named as public key certificate subjects, and is responsible for meeting the obligations of Subscribers as defined throughout this document.

Policy Authority (PA)	Authority that oversees the creation and update of Certificate Policies, reviews Certification Practice Statements, reviews the results of CA audits for policy compliance, evaluates non-domain policies for acceptance within the domain, and generally oversees and manages the PKI certificate policies. Also referred to as Policy Management Authority (PMA).
privacy	State in which data and system access is restricted to the intended user community and target recipient(s).
Private key compromise	A loss, theft or modification, or unauthorized access of a private key corresponding to the public key listed in a certificate governed by this CPS, including without limitation by cryptographic analysis or key extraction.
Public Key Infrastructure (PKI)	Framework established to issue, maintain, and revoke public key certificates.
Registration Authority (RA)	Entity responsible for identification and authentication of certificate subjects that has automated equipment for the communication of applicant data to Certification Authorities and does not sign or directly revoke certificates.
Root CA	In a hierarchical PKI, the CA whose public key serves as the most trusted datum (i.e., the beginning of trust paths) for a security domain.
re-key (a certificate)	To change the value of a cryptographic key that is being used in a cryptographic system application.
Relying Party	A person who has received a certificate and a digital signature verifiable with reference to a public key listed in the certificate, and is in a position to rely on them. [ABADSG]
renew (a certificate)	The act or process of extending the validity of the data binding asserted by a public key certificate by issuing a new certificate.
repository	A trustworthy system for storing and retrieving certificates or other information relevant to certificates. [ABADSG]
revocation	The act or process of prematurely ending the operational period of a certificate effective at a specific date and time.
risk	An expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular harmful result.
risk tolerance	The level of risk an entity is willing to assume in order to achieve a potential desired result.
server	A system entity that provides a service in response to requests from clients.
Signature certificate	A public key certificate that contains a public key intended for verifying digital signatures rather than encrypting data or performing any other cryptographic functions. Also referred to as an Identity Certificate.
subordinate CA	In a hierarchical PKI, a CA whose certificate signing key is certified by another CA, and whose activities are constrained by that other CA. (see superior CA)
Subscriber	An entity that (1) is the subject named or identified in a certificate issued to such an entity, and (2) holds a private key that corresponds to a public key listed in that certificate. [ABADSG]. **Current subscribers** possess valid CDS-issued certificates.
superior CA	In a hierarchical PKI, a CA who has certified the certificate signing key of another CA, and who constrains the activities of that CA. (see subordinate CA)
system equipment configuration	A comprehensive accounting of all system hardware and software types and settings.
technical non-repudiation	The contribution public key mechanisms make to the provision of technical evidence supporting a non-repudiation security service.
threat	Any circumstance or event with the potential to cause harm to an information system in the form of destruction, disclosure, adverse modification of data, and/or denial of service.
trust list	Collection of Trusted Certificates used by Relying Parties to authenticate other certificates.

tier	A barrier such as a locked door or closed gate that provides mandatory access control for individuals and requires a positive response (e.g., door unlocks or gate opens) for each individual to proceed to the next area. Each successive tier provides more restricted access and greater physical security against intrusion or unauthorized access. Moreover, each physical security tier encapsulates the next inner tier, such that an inner tier must be fully contained in an outside tier and cannot have a common outside wall with the outside tier, the outermost tier being the outside wall of the building.
Trusted Agent	Entity authorized to act as a representative of a Certificate Management Authority in providing Subscriber identification during the registration process. Trusted Agents do not have automated interfaces with Certification Authorities.
Trusted Certificate	A certificate that is trusted by the Relying Party on the basis of secure, authenticated delivery. The public keys included in Trusted Certificates are used to start certification paths. Also known as a "trust anchor".
Trusted Timestamp	A digitally signed assertion by a trusted authority that a specific digital object existed at a particular time.
two person control	Continuous surveillance and control of positive control material at all times by a minimum of two authorized individuals, each capable of detecting incorrect and/or unauthorized procedures with respect to the task being performed and each familiar with established security and safety requirements.
update (a certificate)	The act or process by which data items bound in an existing public key certificate, especially authorizations granted to the subject, are changed by issuing a new certificate.
unauthorized revocation	Revocation of a certificate without the authorization of the subscriber.

APPENDIX C: REFERENCES

The following documents contain information that provides background, examples, or details about the contents of this policy.

Number	Title	Revision	Date
ABADSG	*Digital Signature Guidelines* http://www.abanet.org/scitech/ec/isc/dsgfree.html		1 August 1996
FIPS140	*Security Requirements for Cryptographic Modules* http://csrc.nist.gov/publications/index.html		21 May 2001
FIPS112	*Password Usage* http://csrc.nist.gov/		5 May 1985
FIPS186-2	*Digital Signature Standard* http://csrc.nist.gov/fips/fips186-2.pdf		27 January 2000
NS4009	*NSTISSI 4009, National Information Systems Security Glossary*		January 1999
PACS	*Technical Implementation Guidance: Smart Card Enabled Physical Access Control Systems* http://smart.gov/information/TIG_SCEPACS_v2.2.pdf	2.2	27 July 2004
PKCS-1	*PKCS #1 v2.1: RSA Cryptography Standard* http://www.rsasecurity.com/rsalabs/node.asp?id=2125	2.1	14 June 2002
PKCS-12	*Personal Information Exchange Syntax Standard* http://www.rsasecurity.com/rsalabs/node.asp?id=2138	1.0	24 June 1999
RFC2527	*Certificate Policy and Certification Practices Framework*, Chokhani and Ford http://www.ietf.org/rfc/rfc2527.txt		March 1999
RFC3647	*Certificate Policy and Certification Practices Framework, Chokhani and Ford* *http://www.ietf.org/rfc/rfc3647.txt*		November 2003
RFC5019	The Lightweight Online Certificate Status Protocol (OCSP) Profile for High-Volume Environments, *http://www.rfc-editor.org/pipermail/rfc-dist/2007-September/001760.html*		
RFC5280	*Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*		May 2008

APPENDIX D: ACRONYMS AND ABBREVIATIONS

CA	Certification Authority
CDS	Certified Document Services
CMA	Certificate Management Authority
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSOR	Computer Security Objects Registry
DES	Data Encryption Standard
DN	Distinguished Name
DSA	Digital Signature Algorithm
DSS	Digital Signature Standard
FIPS	Federal Information Processing Standard
I&A	Identification and Authentication
ID	Identity (also, a credential asserting an identity)
ISO	International Organization for Standards
NIST	National Institute of Standards and Technology
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PA	Policy Authority
PIN	Personal Identification Number
PKCS	Public Key Certificate Standard
PKI	Public Key Infrastructure
PMA	Policy Management Authority
RA	Registration Authority
RFC	Request For Comment
RSA	Rivest, Shamir, Adelman (encryption and digital signature algorithm)
S/MIME	Secure Multipurpose Internet Mail Extensions
SSL	Secure Socket Layer
USC	United States Code
USD	United States Dollar

* * * End of Document * * *