



CP (Certificate Policy)

DocuSign, Inc.
Version 1.0
2014-02-01

221 Main Street
Suite 1000
San Francisco, CA 94105
Tel: 1-866-219-4318
Email: pma@DocuSign.com
URL: www.DocuSign.com

Version	Release Date	Author	Status + Description
V.1.0	February 1, 2014	DocuSign	Initial version, published to the DocuSign Repository in February 2014. The initial version of the DocuSign CP was authored in support of the DocuSign Express Digital Signature service, commercially available starting in early 2014.

TABLE OF CONTENTS

1	Introduction	1
1.1	Overview	1
1.2	Document Name and Identification	1
1.3	PKI Participants	1
1.3.1	<i>Policy Management Authority</i>	1
1.3.2	<i>Certification Authority</i>	1
1.3.3	<i>Registration Authority</i>	2
1.3.4	<i>Subscriber</i>	2
1.3.5	<i>Relying Party</i>	2
1.3.6	<i>Certificate Applicant</i>	2
1.3.7	<i>Other Participants</i>	2
1.4	Certificate Usage	2
1.5	Policy Administration	7
1.5.1	<i>Organization Administering the Policy</i>	7
1.5.2	<i>Contact Person</i>	7
1.5.3	<i>Person Determining CP Suitability for the Policy</i>	7
1.5.4	<i>CP Approval Procedures</i>	7
1.6	Definitions and Acronyms	7
2	Publication and Repository Responsibilities	9
2.1	Repositories	9
2.2	Publication of certification information	9
2.3	Time or Frequency of Publication	9
2.4	Access Controls on Repositories	9
3	Identification and Authentication	10
3.1	Naming	10
3.1.1	<i>Types of Names</i>	10
3.1.2	<i>Meaningfulness</i>	10
3.1.3	<i>Anonymity or Pseudonymity of Certificate Subjects</i>	10
3.1.4	<i>Rules for Interpreting Various Name Forms</i>	10
3.1.5	<i>Uniqueness of Names</i>	10
3.1.6	<i>Recognition, Authentication, and Role of Trademarks</i>	10
3.2	Initial Identity Validation	11
3.2.1	<i>Method to Prove Possession of Private Key</i>	11
3.2.2	<i>Authentication of Organization Identity</i>	11
3.2.3	<i>Authentication of Subject Identity</i>	11
3.2.4	<i>Non-verified Certificate Subject Information</i>	11
3.2.5	<i>Validation of Authority</i>	11
3.2.6	<i>Criteria for Interoperation</i>	11
3.3	Identification and Authentication for Re-key Requests	11
3.3.1	<i>Identification and Authentication of Re-Key and Renewal Requests</i>	11
3.3.2	<i>Identification and Authentication of Re-Key and Renewal After Revocation</i>	11
3.4	Identification and Authentication for Revocation Request	12

4	Certificate Life-Cycle.....	13
4.1	Certificate Application.....	13
4.1.1	Who Can Submit a Certificate Application.....	13
4.1.2	Enrollment Process and Responsibilities.....	13
4.2	Certificate Application Processing.....	13
4.2.1	Performing Identification and Authentication Functions.....	13
4.2.2	Approval or Rejection of Certificate Applications.....	13
4.2.3	Time to Process Certificate Applications.....	13
4.3	Certificate Issuance.....	13
4.3.1	RA Actions During Certificate Issuance.....	13
4.3.2	CA Actions During Certificate Issuance.....	14
4.3.3	Notification to Certificate Subject of Certificate Issuance.....	14
4.4	Certificate Acceptance.....	14
4.4.1	Conduct Constituting Certificate Acceptance.....	14
4.4.2	Publication of the Certificate by the CA.....	14
4.4.3	Notification of Certificate Issuance by the CA to Other Entities.....	14
4.5	Key Pair and Certificate Usage.....	14
4.5.1	Certificate Subject Private Key and Certificate Usage.....	14
4.5.2	Relying Party Public Key and Certificate Usage.....	14
4.6	Certificate Renewal.....	15
4.6.1	Circumstance for Certificate Renewal.....	15
4.6.2	Who May Request Renewal.....	15
4.6.3	Processing Certificate Renewal Requests.....	15
4.6.4	Notification of New Certificate Issuance to Certificate Subject.....	15
4.6.5	Conduct Constituting Acceptance of a Renewal Certificate.....	15
4.6.6	Publication of the Renewal Certificate by the CA.....	15
4.6.7	Notification of Certificate Issuance by the CA to Other Entities.....	15
4.7	Certificate Re-Key.....	15
4.7.1	Circumstance for Certificate Re-key.....	15
4.7.2	Who May Request Certification of a New Public Key.....	16
4.7.3	Circumstance for Certificate Re-key.....	16
4.7.4	Who May Request Certification of a New Public Key.....	16
4.7.5	Processing Certificate Re-keying Requests.....	16
4.7.6	Notification of New Certificate Issuance to Certificate Subject.....	16
4.7.7	Conduct Constituting Acceptance of a Re-keyed Certificate.....	16
4.7.8	Publication of the Re-keyed Certificate by the CA.....	16
4.7.9	Notification of Certificate Issuance by the CA to Other Entities.....	16
4.8	Modification.....	16
4.8.1	Circumstance for Certificate Modification.....	16
4.8.2	Who May Request Certificate Modification.....	16
4.8.3	Processing Certificate Modification Requests.....	16
4.8.4	Notification of New Certificate Issuance to Certificate Subject.....	16
4.8.5	Conduct Constituting Acceptance of Modified Certificate.....	16
4.8.6	Publication of the Modified Certificate by the CA.....	16
4.8.7	Notification of Certificate Issuance by the CA to Other Entities.....	17
4.9	Certificate Revocation and Suspension.....	17
4.9.1	Circumstances for Revocation.....	17

4.9.2	Who Can Request Revocation	17
4.9.3	Procedure for Revocation Request	17
4.9.4	Revocation Request Grace Period.....	17
4.9.5	Time within which CA Must Process the Revocation Request	17
4.9.6	Revocation Checking Requirements for Relying Parties	17
4.9.7	CRL Issuance Frequency.....	17
4.9.8	Maximum Latency for CRLs.....	17
4.9.9	On-line Revocation/Status Checking Availability.....	17
4.9.10	On-line Revocation Checking Requirements	18
4.9.11	Other Forms of Revocation Advertisements Available	18
4.9.12	Special Requirements Re Key Compromise	18
4.9.13	Circumstances for Suspension	18
4.9.14	Who can Request Suspension	18
4.9.15	Procedure for Suspension Request	18
4.9.16	Limits on Suspension Period.....	18
4.10	Certificate Status Services.....	18
4.10.1	Operational Characteristics.....	18
4.10.2	Service Availability	18
4.10.3	Optional Features.....	18
4.11	End of Subscription	18
4.12	Key Escrow and Recovery	18
4.12.1	Key Escrow and Recovery Policy and Practices.....	18
4.12.2	Session Key Encapsulation and Recovery Policy and Practices.....	18
5	Management, Operational, and Physical Controls.....	19
5.1	Physical Controls	19
5.1.1	Site Location and Construction	19
5.1.2	Physical Access.....	19
5.1.3	Power and Air Conditioning	19
5.1.4	Water Exposures.....	20
5.1.5	Fire Prevention and Protection	20
5.1.6	Media Storage.....	20
5.1.7	Waste Disposal.....	20
5.1.8	Off-Site backup.....	20
5.2	Procedural Controls.....	21
5.2.1	Trusted Roles.....	21
5.2.2	Number of Persons Required Per Task.....	21
5.2.3	Identification and Authentication for Each Role	21
5.2.4	Roles Requiring Separation of Duties	21
5.3	Personnel Controls	22
5.3.1	Qualifications and Experience Requirements.....	22
5.3.2	Background Check Procedures.....	22
5.3.3	Training Requirements.....	22
5.3.4	Retraining Frequency and Requirements.....	22
5.3.5	Job Rotation Frequency and Sequence	22
5.3.6	Sanctions for Unauthorized Actions.....	22
5.3.7	Independent Contractor Requirements.....	22

5.3.8	<i>Documentation Supplied to Personnel</i>	22
5.4	<i>Audit Logging Procedures</i>	22
5.4.1	<i>Types of Events Recorded</i>	22
5.4.2	<i>Frequency of Processing Log</i>	23
5.4.3	<i>Retention Period for Audit Log</i>	23
5.4.4	<i>Protection of Audit Log</i>	23
5.4.5	<i>Audit Log Backup Procedures</i>	23
5.4.6	<i>Audit Collection System (Internal vs. External)</i>	24
5.4.7	<i>Notification to Event-Causing Subject</i>	24
5.4.8	<i>Vulnerability Assessments</i>	24
5.5	<i>Records Archive</i>	24
5.5.1	<i>Types of Events Archived</i>	24
5.5.2	<i>Retention Period for Archive</i>	24
5.5.3	<i>Protection of Archive</i>	24
5.5.4	<i>Archive Backup Procedures</i>	24
5.5.5	<i>Requirements for Time-Stamping of Records</i>	24
5.5.6	<i>Archive Collection System (Internal or External)</i>	24
5.5.7	<i>Procedures to Obtain and Verify Archive Information</i>	25
5.6	<i>Key Changeover</i>	25
5.7	<i>Compromise and Disaster Recovery</i>	25
5.7.1	<i>Incident and Compromise Handling Procedures</i>	25
5.7.2	<i>Computing Resources, Software, and/or Data Are Corrupted</i>	25
5.7.3	<i>CA Private Key Compromise Procedures</i>	25
5.7.4	<i>Business Continuity Capabilities After a Disaster</i>	25
5.8	<i>CA and RA Termination</i>	25
6	<i>Technical Security Controls</i>	26
6.1	<i>Key Pair Generation and Installation</i>	26
6.1.1	<i>Key Pair Generation</i>	26
6.1.2	<i>Private Key Delivery to Certificate Subject</i>	26
6.1.3	<i>Public Key Delivery to Certificate Issuer</i>	26
6.1.4	<i>CA Public Key Delivery to Relying Parties</i>	26
6.1.5	<i>Key Sizes</i>	26
6.1.6	<i>Public Key Parameters Generation and Quality Checking</i>	26
6.1.7	<i>Key Usage Purposes (as per X.509v3 key usage field)</i>	26
6.2	<i>Private Key Protection and Cryptographic Module Engineering Controls</i>	26
6.2.1	<i>Cryptographic Module Standards and Controls</i>	26
6.2.2	<i>Private Key Multi-Person Control</i>	26
6.2.3	<i>Private Key Escrow</i>	27
6.2.4	<i>Private Key Backup</i>	27
6.2.5	<i>Private Key Archival</i>	27
6.2.6	<i>Private Key Transfer into or from a Cryptographic Module</i>	27
6.2.7	<i>Private Key Storage on Cryptographic Module</i>	27
6.2.8	<i>Method of Activating Private Keys</i>	27
6.2.9	<i>Methods of Deactivating Private Keys</i>	27
6.2.10	<i>Method of Destroying Private Key</i>	27
6.2.11	<i>Cryptographic Module Rating</i>	27

6.3	Other Aspects of Key Management.....	28
6.3.1	Public Key Archival.....	28
6.3.2	Certificate Operational Periods/Key Usage Periods.....	28
6.4	Activation Data.....	28
6.4.1	Activation Data Generation and Installation.....	28
6.4.2	Activation Data Protection.....	28
6.4.3	Other Aspects of Activation Data.....	28
6.5	Computer Security Controls.....	28
6.5.1	Specific Computer Security Technical Requirements.....	28
6.5.2	Computer Security Rating.....	28
6.6	Life-Cycle Security Controls.....	29
6.6.1	System Development Controls.....	29
6.6.2	Security Management Controls.....	29
6.6.3	Life Cycle Security Ratings.....	29
6.7	Network Security Controls.....	29
6.8	Time Stamping.....	29
7	Certificate, CRL, SCVP, and OCSP Profiles Format.....	30
7.1	Certificate Profile.....	30
7.1.1	Root CA Certificate Profile.....	30
7.1.2	Sub-CA Certificate Profile.....	31
7.1.3	DocuSign Subscriber Certificate Profile.....	32
7.2	CRL Profile.....	33
7.2.1	DocuSign Root CRL Profile.....	33
7.2.2	DocuSign Sub-CA CRL Profile.....	34
7.3	OCSP Profile.....	34
7.4	SCVP Profile.....	34
8	Compliance Audit and Other Assessments.....	35
8.1	Frequency of Audit or Assessments.....	35
8.2	Identity and Qualifications of Assessor.....	35
8.3	Assessor’s Relationship to Assessed Entity.....	35
8.4	Topics Covered By Assessment.....	35
8.5	Actions Taken As A Result of Deficiency.....	35
8.6	Communication of Results.....	35
9	Other Business and Legal Matters.....	36
9.1	Fees.....	36
9.1.1	Certificate Issuance/Renewal Fees.....	36
9.1.2	Certificate Access Fees.....	36
9.1.3	Revocation or Status Information Access Fee.....	36
9.1.4	Fees for other Services.....	36
9.1.5	Refund Policy.....	36
9.2	Financial Responsibility.....	36
9.2.1	Insurance Coverage.....	36
9.2.2	Other Assets.....	36
9.2.3	Insurance/warranty Coverage for End-Entities.....	36
9.3	Confidentiality of Business Information.....	36

9.3.1	<i>Scope of Confidential Information</i>	36
9.3.2	<i>Information Not Within the Scope of Confidential Information</i>	37
9.3.3	<i>Responsibility to Protect Confidential Information</i>	37
9.4	<i>Privacy of Personal Information</i>	37
9.4.1	<i>Privacy Plan</i>	37
9.4.2	<i>Information Treated as Private</i>	37
9.4.3	<i>Information Not Deemed Private</i>	37
9.4.4	<i>Responsibility to Protect Private Information</i>	37
9.4.5	<i>Notice and Consent to use Private Information</i>	37
9.4.6	<i>Disclosure Pursuant to Judicial/Administrative Process</i>	37
9.4.7	<i>Other Information Disclosure Circumstances</i>	38
9.5	<i>Intellectual Property Rights</i>	38
9.6	<i>Representations and Warranties</i>	38
9.6.1	<i>PMA</i>	38
9.6.2	<i>Generally Applicable Representations and Warranties</i>	38
9.6.3	<i>CA Representations and Warranties</i>	38
9.6.4	<i>RA Representations and Warranties</i>	38
9.6.5	<i>Certificate Subject Representations and Warranties</i>	38
9.6.6	<i>Relying Parties Representations and Warranties</i>	38
9.6.7	<i>Subscriber Representation and Warranties</i>	38
9.6.8	<i>Representations and Warranties of Other Participants</i>	39
9.7	<i>Disclaimers of Warranties</i>	39
9.8	<i>Limitations of Liability</i>	39
9.8.1	<i>PMA</i>	39
9.8.2	<i>Other Participants</i>	39
9.9	<i>Indemnities</i>	40
9.9.1	<i>PMA</i>	40
9.9.2	<i>Other Participants</i>	40
9.10	<i>Term and Termination</i>	40
9.10.1	<i>Term</i>	40
9.10.2	<i>Termination</i>	40
9.10.3	<i>Effect of Termination and Survival</i>	40
9.11	<i>Individual Notices and Communications With participants</i>	41
9.12	<i>Amendments</i>	41
9.12.1	<i>Procedure for Amendment</i>	41
9.12.2	<i>Notification Mechanism and Period</i>	41
9.12.3	<i>Circumstances Under Which OID Must Be Changed</i>	41
9.13	<i>Dispute Resolution Provisions</i>	41
9.14	<i>Governing Law</i>	41
9.15	<i>Compliance with Applicable Law</i>	42
9.16	<i>Miscellaneous Provisions</i>	42
9.16.1	<i>Document Incorporated into CP</i>	42
9.16.2	<i>Entire agreement</i>	42
9.16.3	<i>Assignment</i>	42
9.16.4	<i>Severability</i>	42
9.16.5	<i>Waiver</i>	42
9.16.6	<i>Attorneys' Fees</i>	42

9.16.7 Force Majeure..... 42
9.17 Other Provisions..... 42

1 Introduction

1.1 Overview

The DocuSign® CP (Certificate Policy) defines the policies, procedures, and requirements that DocuSign requires participants (see Section 1.3) comply with when issuing and managing Digital Certificates. This CP is under the control by the DocuSign PMA (Policy Management Authority) (see Section 1.5). It complies with the content, layout, and format of the IETF (Internet Engineering Task Force) PKIX (Public Key Infrastructure X.509) Certificate Policy and Certification Practices Framework described in RFC 3647, as per industry standards.

1.2 Document Name and Identification

The official name of this document is the DocuSign Certificate Policy. The OID (Object Identifier) “1.3.6.1.4.1.42482.1.2.1.1.0” is included in subscriber certificates to indicate that they are issued in accordance with this CP.

1.3 PKI Participants

1.3.1 Policy Management Authority

The DocuSign PMA (Policy Management Authority) approves the CP and any changes to it. The PMA is comprised of the following members:

- At least one member of the DocuSign management team, and;
- At least two authorized agents directly involved in authoring the DocuSign CP.

The DocuSign PMA also approves all agreements that affect the DocuSign CAs (Certification Authorities) and RAs (Registration Authorities) services including, but not limited to, the following documents:

- CPS (Certification Practice Statements)
- SA (Subscriber Agreements)
- RPA (Relying Party Agreements)
- PMA bylaws
- ToU (Terms of Use)

1.3.2 Certification Authority

A DocuSign CA (Certification Authority) is the collection of technology and procedures that issues Digital Certificates in accordance with the DocuSign CP. A DocuSign CA Operator is the entity ultimately responsible for all aspects of the issuance and management of Digital Certificates: registration, identification and authentication, issuance, rekey, etc.

There are two types of CAs, the Root CA and one or more Subordinate CAs:

- The offline Root CA is responsible for issuing certificates to Sub-CAs. The Root also publishes status information about the Sub-CAs.
- Sub-CAs are responsible for issuance and management of subscriber certificates; this includes publication of certificate status information.

Unless otherwise noted, or explicitly stated, for the remainder of this document the term CA refers to both Root CA and Sub-CAs.

1.3.3 Registration Authority

A DocuSign RA (Registration Authority) is the process that enrolls Certificate Applicants, and performs identification and authentication of Certificate Applicants.

1.3.4 Subscriber

A Subscriber is an entity that digitally signs a document at the behest of the Relying Party. The Subscriber is the entity whose name appears in the DocuSign Digital Certificate's subject field, and who uses the DocuSign service in accordance with any current DocuSign Subscriber Agreement or any published Terms of Use governing the DocuSign Service.

In this document, the term Subscriber never applies to a CA or an RA.

1.3.5 Relying Party

A Relying Party is an entity that requires the Subscriber to digitally sign a document using the DocuSign Service. The Relying Party uses the Digital Certificate created by the DocuSign Service to validate the digital signature applied by the Subscriber, and who uses the DocuSign Service in accordance with any current DocuSign Relying Party Agreement.

In this document, the term Relying Party never applies to a CA or an RA.

1.3.6 Certificate Applicant

A Certificate Applicant is an entity for whom a digital signature has been requested by a Relying Party, but has not yet been issued a Digital Certificate from DocuSign.

1.3.7 Other Participants

No stipulation.

1.4 Certificate Usage

DocuSign Digital Certificates SHALL only be used for the following purposes:

- Any Root CA SHALL only issue Digital Certificates and status information in support of DocuSign Sub-CAs. All other uses of the Root CA's Private Key and Digital Certificate are expressly prohibited.
- Any Subordinate CAs SHALL only issue Digital Certificate and status information in support of DocuSign Subscribers. All other uses of a Subordinate CA's Private Key and Digital Certificate are expressly prohibited.
- Any Subscriber certificate SHALL only be used in the manner described in the remainder of this section.

The DocuSign Express Digital Signature service works as depicted in **Figure 1**, and is described below:

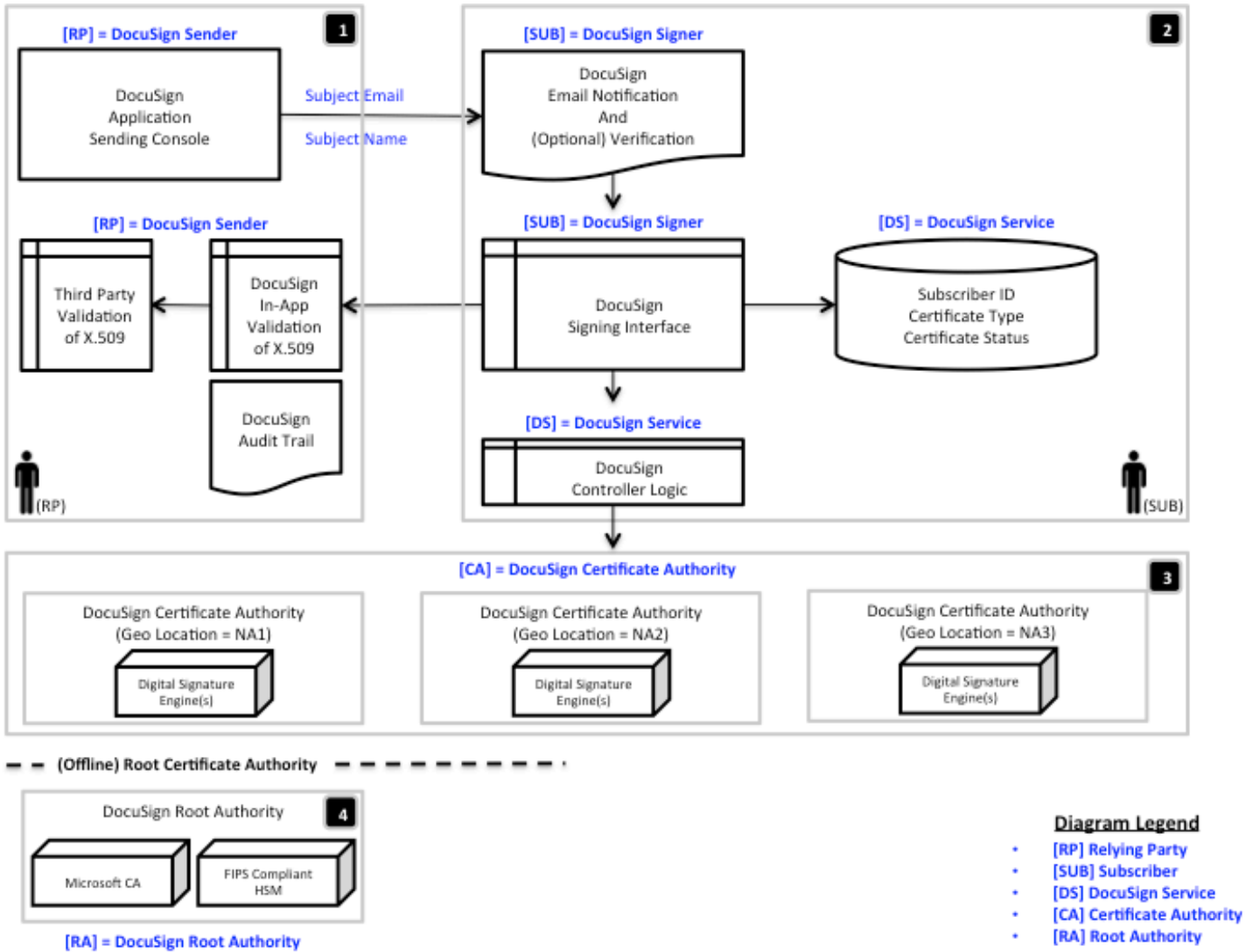


Figure 1 - The DocuSign Express Digital Signature Service

- Relying Party [RP]
 - Relying Parties determine the trust required for digital signing transactions managed by the DocuSign Service. The DocuSign Service executes against that determination.
 - Relying Parties are commonly referred to as “Senders” within the DocuSign Service.
 - Relying parties use "local methods" to pre-establish the “locally determined” identity of the Subscriber, which can include:
 - Internal systems like employee directories, customer databases, master contact lists, etc.,
 - Third party systems like LinkedIn, the Internet, etc.,
 - Paid professional databases,
 - Prior inter-personal communications (including emails, phone calls, etc.),
 - Personal connections, and
 - Other means.
 - Relying parties require the Subscriber to digitally sign documents within the DocuSign Service. Relying Parties engage Subscribers by inserting into the DocuSign Service the following locally determined Subscriber identification elements:
 - Subject’s Email Address, and
 - Subject’s Name (i.e., common name).
 - Relying parties may use features found within the DocuSign Service to help verify the locally determined Subscriber identification elements. Examples of available features are found below. The results of these verification events are stored in the DocuSign Service as part of the digital signing transaction:
 - None.
 - Access Code (a shared secret known by both Relying Party and Subscriber).
 - SMS Authentication (a randomly generated, One Time Password which is sent to a locally determined mobile phone number, assumed to be controlled by the Subscriber).
 - Phone Authentication (a phone call is placed to a locally determined mobile phone number, assumed to be controlled by the Subscriber).
 - Knowledge-Based Authentication (the Subscriber is required to answer out-of-wallet questions, provided by a third-party service).
 - Relying Party should expect the following from the DocuSign Service, when requiring a digital signature transaction:
 - A highly available transaction,
 - A secure transaction,
 - A historical record of the transaction (audit trail, certificate of completion, etc.),
 - A transaction that functions in accordance with the DocuSign CP/CPS,
 - A transaction that is backed by the DocuSign PMA,
 - A standards-based digitally signed document, in electronic format, and
 - A standards-based manifestation of Subscriber identity for that given transaction (an X.509 Digital Certificate issued by the DocuSign Service on behalf of the Subscriber).
- Subscriber (SUB)

- For the DocuSign Express Digital Signature Service, Subscribers are required by the Relying Party to digitally sign a document within the DocuSign Service.
- Subscribers are not required to obtain a signing Digital Certificate prior to transacting with the Relying Party. The DocuSign Service, as part of the digital signature transaction, issues the Subscriber's Digital Certificate.
- Subscribers must complete the transaction as defined by the Relying Party, or reject it entirely.
- Subscribers do not maintain direct control of their Private Key. Control is maintained by DocuSign and used via interactions with the DocuSign Service.
- Subscribers will perform the following actions during a transaction:
 - Acknowledge the identity of the Relying Party,
 - Acknowledge the intent of the Relying Party,
 - Confirm and attest they maintain control of the document,
 - Confirm and attest to their identity, as per the requirements of the Relying Party. Specifically, they confirm the email address and subject name that was locally determined by the Relying Party, and sent within the transaction,
 - Confirm and attest their agreement to digitally sign, and
 - Select a Signing Reason, if requested by the Relying Party.
- DocuSign Service [DS]
 - The service controls access to the DocuSign Express Digital Signature functionality.
 - The service controls access to the ability to use supported Digital Certificate Types, including the DocuSign Express certificate, for supported digital signature operations, which are described by this CP.
 - The Service manages interactions between Relying Party and Subscriber, including Email Notifications, SMS messages, phone calls, etc.
 - The Service consists of the following core components:
 - An Application UI for enabling the DocuSign Express capability within the DocuSign Service.
 - An Application UI that allows the Relying Party to require Subscriber(s) to digitally sign a document, using the Private Key associated with the DocuSign Express Digital Certificate.
 - Various Email Notifications that inform the Subscriber of their obligations, and inform the Relying Party of the transaction status.
 - An Application UI that guides the Subscriber through the digital signing process.
 - A Validation UI that shows the validity of the digital signature from within the DocuSign Service.
 - Completed and digitally signed documents, which can be exported from the platform. These documents are digitally signed by the Subscriber as per the requirements of the Relying Party, and include Sub-CA X.509 and Subscriber Digital Certificates.
 - High-availability Subordinate Certificate Authorities:
 - A cluster of Sub-CAs, architected for high-availability by way of failover mechanisms, monitoring, etc.
 - A sub-cluster of Sub-CAs in distinct geo-locations which are architected for disaster resilience and optimized performance.
 - Each Sub-CA runs on a FIPS 140-2 Level 3 compliant, evaluated, and certified Signature Engine.
 - An offline Root Certificate Authority:

- The Root CA is not on any network except the one used to connect the CA software to the HSM. It resides in a secure location, as described within this CP. The Root CA is only activated when authorized by the DocuSign PMA, and only in the multi-person manners described by DocuSign PMA procedural control documents.
- The Root CA consists of a server running Certification Authority software and utilizing an HSM for secure storage of keys. These two devices are connected during ceremonies, but never connected to any other devices on any public or private network.
- The Root CA utilizes a FIPS 140-2 Level 3 compliant, evaluated, and certified HSM for storage of all keys.
- The DocuSign Service maintains a secure database that contains information required to manage the transaction, including:
 - A Unique Subscriber Identifier, generated by DocuSign in a secure manner,
 - A Certificate Type, to distinguish the unique CA being asked to provide the Digital Certificate for a given digital signature transaction.
- The DocuSign Service controls access to the Certificate Authority, including:
 - The FIPS 140-2 Level 3 Signing Engine which power the Sub-CAs,
 - The FIPS 140-2 Level 3 cryptographic operations that run on the Signing Engines, and
 - The secured Subscriber Private Key, which resides in the signing engine's HSM.
- The Service maintains logs of activity related to the transaction.
- The service will produce evidence of all completed transactions:
 - Documents, digitally signed by the Service to provide tamper evidence,
 - Documents, digitally signed by the Subscriber to provide identity assurance and compliance with Relying Party requirement,
 - Documents, containing an X.509 Digital Certificate containing reliable information about the Service and the Subscriber,
 - An Audit Trail containing standard DocuSign transaction detail, and
 - A tamper-evident Certificate of Completion containing additional warranty stipulations and transaction detail.
- DocuSign Certificate Authority [CA]
 - The DocuSign Service includes the DocuSign Subordinate CAs, which interact with the DocuSign Application as described above, and operate in a manner compliant with the DocuSign CP and CPS.
- DocuSign Root Certificate Authority [CA]
 - The DocuSign Service includes the DocuSign Root CA, which interacts with the DocuSign Sub-CAs as described above in this section, and operates in a manner compliant with the DocuSign CP and CPS.
 - The DocuSign Root CA was created using a documented Key Cutting Ceremony, based on PKI best practices and policies.
 - All use of the DocuSign Root CA Private Keys require a documented and archived ceremony performed under the authority of the PMA.

1.5 Policy Administration

1.5.1 Organization Administering the Policy

The DocuSign PMA SHALL be responsible for all aspects of this CP and approval of all related agreements and amendments.

1.5.2 Contact Person

All communications regarding this CP SHALL be directed to:

DocuSign, Inc.
Attn: Security Council / Policy Management Authority
221 Main Street
Suite 1000
San Francisco, CA 94101
Tel: 1-866-219-4318
Email: pma@DocuSign.com

1.5.3 Person Determining CP Suitability for the Policy

The DocuSign PMA SHALL be the entity that determines whether a particular CPS conforms to this CP based on input for auditors. The DocuSign PMA is also responsible for acting upon any findings of the auditors.

1.5.4 CP Approval Procedures

The DocuSign PMA SHALL approve the CP and any amendments according to the PMA's bylaws. The DocuSign PMA determines whether an amendment to this CP requires notice or an OID change (see Section 9.10 and Section 9.12).

1.6 Definitions and Acronyms

"CA (Certificate Authority)" means a certificate authority authorized to issue and revoke Digital Certificates.

"CP (Certificate Policy)" means a document that establishes the requirements for how a CA is to be governed, managed, and operated.

"CPS (Certification Practice Statement)" means a document that articulates specific procedures and practices that adhere to the CP-defined requirements for how a CA is to be governed, managed, and operated.

"Certificate Applicant" means a person who is applying for a Digital Certificate

"Certificate Chain" means the chain of Digital Certificates, which arises due to the issuing of a Digital Certificate by a Root Certification Authority to a Subordinate Certification Authority, and from a Subordinate Certification Authority to a Subscriber.

"Certificate Path" means an ordered list of certificates that is used to validate the signature on the document and that is composed of the Subscriber's DocuSign Digital Certificate, a Sub-CA Digital Certificate, and the Root CA Digital Certificate.

"Cryptography" means the discipline which embodies principles, means and methods for the transformation of data in order to hide its information content, prevent its undetected modification and/or prevent its unauthorized use; (See ISO 7498-2)

"CSI" / "CRL" means DocuSign's certificate status information relied upon to validate the digital signature generated on behalf of the Subscriber. For this DocuSign PKI, it is a CRL (Certificate Revocation List).

"Digital Certificate" / "Certificate" means an IETF (Internet Engineering Task Force) PKIX (Public Key Infrastructure X.509) RFC 5280 (Request for Comments) digitally formatted data structure that binds a Public Key to an identity.

"Digital Signature" means an electronic data file which is attached to or logically associated with other electronic data, and which identifies and is uniquely linked to the signatory of the electronic data. The Digital Signature is created in manner ensuring that control is limited to the signatory, and is linked in a way so as to make any subsequent changes that have been made to the electronic data detectable.

"DocuSign Service" means a SaaS (Software as a Service) offering, hosted and managed by DocuSign, which for the purposes of this document is the sole technology governing interactions between RPs (Relying Parties), SUBs (Subscribers), and CAs (Certificate Authorities).

"HSM (Hardware Security Module)" means a physical computing device that safeguards and manages digital keys for strong authentication and provides cryptographic processing.

"PMA (Policy Management Authority)" means an advisory group, comprised of DocuSign staff members, authorized by DocuSign to govern various aspects of the CA as outlined in the CP and CPS.

"Private Key" means a confidential electronic data file designed to interface with a Public Key and which may be used to create Digital Signatures.

"Public Key" means a publicly available electronic data file designed to mathematically bind with a Private Key and which may be used to verify Digital Signatures.

"RA (Registration Authority)" means a process within the DocuSign Service that ensures that the Subscriber validates Subscriber identity elements, locally determined and provided to the RA by the Relying Party.

"RP (Relying Party)" means a person or business entity that is requiring the Subscriber to digitally sign a document using the DocuSign Service.

"Repository" means a publicly available collection Digital Certificates and other information relating to Digital Certificates and which may be accessed via DocuSign's website.

"Root CA (Root Certificate Authority)" means a certificate authority like DocuSign that issues its own certificate. All certificates chain up to a Root CA, meaning they are issued by a Root CA, or by a CA whose certificate was issued by a Root CA, or by a CA whose certificate was issued by a CA whose certificate was issued by a Root CA, or any number of layers of CA's deep but terminating at a Root CA.

"RPA (Relying Party Agreement)" means a document, authored by DocuSign, which defines the legal relationship between DocuSign and all Relying Parties.

"Signing Engine" means a dedicated device used for the purpose of digitally signing documents. In the case of the DocuSign Service, the Signing Engine device is a CA, a key manager, and an HSM that will generate and store Subscriber Private Keys, manage Subscriber keys and and Digital Certificates, and will use Subscriber Private Keys to sign documents.

"SUB (Subscriber)" means a person who is issued one or more Digital Certificates signed by DocuSign and who is capable of using, and is authorized to use, the Private Key that corresponds to the Public Key listed in the Digital Certificates at issue.

"SA (Subscriber Agreement)" means the agreement entered into between DocuSign and the Subscriber for the provisioning of a Digital Certificate

"Sub-CA (Subordinate Certificate Authority)" means a subordinate certificate authority like DocuSign or any third party appointed by DocuSign to act as a certification authority. It is a subordinate because it is issued by a Root CA or another Subordinate CA.

2 Publication and Repository Responsibilities

2.1 Repositories

Any CA governed by this CP, including the DocuSign CA, SHALL publish all CA certificates, certificate status information for all certificates, CP, and CPS as well as any SA, RPA, and references to ToU (Terms of Use) in online repositories. Repositories SHALL be available 24 hours a day, 7 days a week, with a minimum of 99% availability overall per year, and with a scheduled down-time that does not exceed 0.5% annually.

No stipulation for Subscriber DocuSign Express certificates (see Section 1.4); they are embedded in the signed document by the DocuSign Service and not distributed via the repository.

2.2 Publication of certification information

See Section 2.1.

2.3 Time or Frequency of Publication

For any CA governed by this CP, including the DocuSign CA, Root CA generated CRLs SHALL be produced at a frequency of no less than once every 7 months. If a compromise is detected the PMA will require an appropriate CRL publication. These CRLs will be generated within two business days of the PMA being notified of the compromise. The CRLs MUST be made available no later than one business day after they are generated.

For any CA governed by this CP, including the DocuSign CA, Sub-CA certificates SHALL be published within one business day of issuance.

For any CA governed by this CP, including the DocuSign CA, Sub-CA generated CRLs SHALL be produced at a frequency no less than every 7 days.

DocuSign makes no stipulation for Subscriber Digital Certificates; see Section 2.1.

For any CA governed by this CP, including the DocuSign CA, changes to documentation pertaining to the CA SHALL be published within one business day of approval by the DocuSign PMA. For the DocuSign CA, this includes documentation describing the DocuSign Service.

2.4 Access Controls on Repositories

No stipulation.

3 Identification and Authentication

3.1 Naming

3.1.1 Types of Names

Any CA governed by this CP, including the DocuSign CA, SHALL issue non-null subject names that are conformant with RFC 5280. Subject Alternative may be included but they must be marked as non-critical. The following forms SHALL be supported:

- Root CA:
 - o cn=DocuSign Inc Root CA
- Subordinate CA:
 - o cn=DocuSign NA# CA#, where # is an integer,
 - o ou=DocuSign Certification
 - o o=DocuSign, Inc.
 - o c=US
- Subscriber:
 - o cn=[name provided by RP]
 - o email=[email address provided by RP]
 - o o=DocuSign, Inc.

When the naming element is DirectoryString (i.e., O= and OU=) either PrintableString or UTF8String MUST be used. If the character set is ASCII, then PrintableString shall be used otherwise UTF8String is used.

3.1.2 Meaningfulness

For any CA governed by this CP, including the DocuSign CA, the Subscriber subject name and email address SHALL be meaningful to the Relying Party.

For the DocuSign CA, the Subscriber subject name and email address SHALL identify the Subscriber to the Relying Party adequately for the Relying Party's needs.

3.1.3 Anonymity or Pseudonymity of Certificate Subjects

No stipulation.

3.1.4 Rules for Interpreting Various Name Forms

See Section 3.1.1.

3.1.5 Uniqueness of Names

For any CA governed by this CP, including the DocuSign CA, CA names SHALL be unique across the whole DocuSign Service.

No stipulation for Subscriber names.

3.1.6 Recognition, Authentication, and Role of Trademarks

For any CA governed by this CP, including the DocuSign CA, the CA SHALL revoke any Digital Certificate containing a Subject Name that a court of competent jurisdiction has determined infringes on the trademark of another.

For any CA governed by this CP, including the DocuSign CA, the CA, RA, and Subscriber Digital Certificates all include the string “DocuSign”.

Relying Parties MUST NOT request subject names for Subscribers that infringe upon the Intellectual Property Rights of others. CAs and RAs are under no obligation to ensure that the Subscriber has Intellectual Property Rights in the name appearing in the certificate application or arbitrates, mediate or otherwise resolve any dispute concerning the ownership of any domain name, trademark, trade name or service mark. DocuSign is entitled without liability to any Relying Party or Subscriber, to reject any certificate application or to revoke any issued certificate because of such dispute.

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

For any CA governed by this CP, including the DocuSign CA, CAs SHALL generate their own keys and they MUST prove to the issuing CA that they possess the Private Key that corresponds to the Public Key in the certification request. PKCS#10 standard certificate requests are preferred.

For the DocuSign CA, Subscriber Private Keys are generated by the DocuSign Service on behalf of the Subscriber, at the behest of the Relying Party (see Section 1.4).

3.2.2 Authentication of Organization Identity

No stipulation.

3.2.3 Authentication of Subject Identity

No stipulation.

3.2.4 Non-verified Certificate Subject Information

No stipulation.

3.2.5 Validation of Authority

No stipulation.

3.2.6 Criteria for Interoperation

For any CA governed by this CP, including the DocuSign CA, CAs SHALL only issue Digital Certificates or generate status information in support of the DocuSign Service. All other uses of CA Digital Certificates are expressly prohibited.

For the DocuSign CA, Relying Parties SHALL only request Digital Certificates for Subscribers in connection with the DocuSign Service. All other uses of a DocuSign Digital Certificate, including the DocuSign Express Digital Certificate, are expressly prohibited.

3.3 Identification and Authentication for Re-key Requests

3.3.1 Identification and Authentication of Re-Key and Renewal Requests

For any CA governed by this CP, including the DocuSign CA, the Root CA SHALL be responsible for authentication of a Sub-CA’s request for re-key. The procedures for CA re-key are the same those for the original certificate.

For any CA governed by this CP, including the DocuSign CA, Sub-CAs SHALL support re-key and renewal of Subscriber Digital Certificates if the functional flow within the DocuSign Service requires these functions.

3.3.2 Identification and Authentication of Re-Key and Renewal After Revocation

No stipulation.

3.4 Identification and Authentication for Revocation Request

For any CA governed by this CP, including the DocuSign CA , the DocuSign PMA MUST authorize any requests for revocation of the Sub-CA.

For any CA governed by this CP, including the DocuSign CA, the Sub-CA SHALL process requests for revocation of Subscriber Digital Certificates. The following entities are the only entities who may request revocation of DocuSign Subscriber Digital Certificates: Relying Parties, Subscriber, Sub-CA Operator, Root CA Operator, and the DocuSign PMA.

4 Certificate Life-Cycle

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application

DocuSign technical representatives, as designated by the PMA, SHALL be the only entities from which certificate applications are accepted for additional Sub-CA Digital Certificates.

Relying Parties begin the certificate application process by requiring that Subscribers digitally sign a document in the DocuSign service. The DocuSign Service generates and digitally signs the certification request on behalf of the Subscriber once the Subscriber confirms the locally determined identity elements provided by the Relying Party.

4.1.2 Enrollment Process and Responsibilities

For any CA governed by this CP, the Root CA operator SHALL only issue certificates at the request of the PMA. The Root CA operator SHALL validate that the use of the issued certificates are consistent with the request of the PMA.

For non-DocuSign CAs, no stipulations at this time.

For the DocuSign CA, Sub-CAs SHALL only issue certificates as part of the DocuSign Service workflow (see Section 1.4) after the Subscriber confirms the locally determined identity elements provided by the Relying Party.

For the DocuSign CA, a Relying Party SHALL provide the Subscriber's subject name and email address to the RA through the DocuSign Service.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

For any CA governed by this CP, including the DocuSign CA, CAs and RAs SHALL verify and authenticate each Certificate Applicant, as described in Sections 1.4 and 3.2.

4.2.2 Approval or Rejection of Certificate Applications

For any CA governed by this CP, including the DocuSign CA, Sub-CA certificate applications SHALL be approved or rejected based on outcome of the procedures in Section 4.1.

For the DocuSign CA, the DocuSign Service SHALL approve applications for DocuSign Digital Certificates when the Subscriber validates the locally determined identity elements provided by the Relying Party, as described in Section 1.4. The Service may deny issuance if the Subscriber fails to pass any additional verification required by the Relying Party, also as described in Section 1.4

4.2.3 Time to Process Certificate Applications

For any CA governed by this CP, including the DocuSign CA, Sub-CA certificate applications SHALL be processed in a timely manner.

4.3 Certificate Issuance

4.3.1 RA Actions During Certificate Issuance

For any CA governed by this CP, including the DocuSign CA, the RA SHALL verify and authenticate the source of each Subscriber certification request.

For non-DocuSign CAs, no stipulations at this time.

For the DocuSign CA, see Section 1.4.

4.3.2 CA Actions During Certificate Issuance

For any CA governed by this CP, including the DocuSign CA, the CA SHALL ensure that the public and Private Keys are bound to the correct Certificate Applicant's name, as specified by the Relying Party, as detailed below, and generate a properly formed Digital Certificate.

Issuance:

- Root CAs SHALL issue Sub-CA certificates only during formal recorded, scripted, and PMA authorized ceremonies.
- Sub-CAs SHALL issue Subscriber certificates within FIPS 140-2 level 3 compliant appliances. Key generation, key management, certificate requests, and certificate issuance MUST all occur within this appliance.

After issuance:

- Root CAs SHALL publish Sub-CA certificates in the repository. Sub-CA certificates SHALL be provided along with downloaded signed documents. See Section 2.1.
- Subscriber certificates SHALL be stored with signed documents as part of the DocuSign service; see Section 1.4.

4.3.3 Notification to Certificate Subject of Certificate Issuance

For any CA governed by this CP, including the DocuSign CA, the CA SHALL notify the certificate subject when a certificate is being issued on their behalf.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

No stipulation.

4.4.2 Publication of the Certificate by the CA

See Section 2.1.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

For any CA governed by this CP, including the DocuSign CA, the PMA SHALL authorize all Sub-CA certificate issuance and be notified when a Sub-CA certificate is issued.

For the DocuSign CA, no stipulation for issuance of Subscriber Certificates.

4.5 Key Pair and Certificate Usage

4.5.1 Certificate Subject Private Key and Certificate Usage

For any CA governed by this CP, including the DocuSign CA, the CA SHALL protect all Private Keys from unauthorized use by or disclosure to third parties; see Section 6.

For the DocuSign CA, no stipulation beyond those in Section 1.4.

4.5.2 Relying Party Public Key and Certificate Usage

For any CA governed by this CP, including the DocuSign CA, Relying Parties SHALL be instructed, via the Relying Party agreement, to ensure that the Public Key in a Digital Certificate is used only for appropriate purposes as identified in critical certificate extensions (See Section 7).

For the DocuSign CA, no stipulation for certificate usage beyond that in Section 1.4.

4.6 Certificate Renewal

For any CA governed by this CP, including the DocuSign CA, Digital certificate renewal SHALL be defined as the issuance of a new Digital Certificate, without changing the Public Key or any other information other than the validity dates and the serial number within the Digital Certificate.

For the DocuSign CA, Digital certificate renewal is supported for Subscriber DocuSign Digital Certificates if the functional flow within the DocuSign Service requires these functions.

4.6.1 Circumstance for Certificate Renewal

For any CA governed by this CP, including the DocuSign CA, it is necessary for the renewal to take place prior to the expiration of an existing Digital Certificate to maintain continuity. An overlap period is recommended to ensure continuity.

For the DocuSign CAs, issued Digital Certificates SHALL NOT be renewed after expiration.

4.6.2 Who May Request Renewal

A recognized DocuSign technical representative may submit Sub-CA Digital Certificate renewal requests, which are approved by the PMA prior to the publication of the Sub-CA's Digital Certificate. Sub-CA renewal is a multi-person procedure as specified in Section 5.2.2 and requires a "Key Ceremony" as specified in Section 6.1.1 because of access to the Root CA's Private Key.

No stipulation for Subscriber certificate renewal requests.

4.6.3 Processing Certificate Renewal Requests

In accordance with Section 4.2.

4.6.4 Notification of New Certificate Issuance to Certificate Subject

In accordance with Section 4.3.2.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

In accordance with Section 4.4.1.

4.6.6 Publication of the Renewal Certificate by the CA

In accordance with Section 4.4.2.

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

4.7 Certificate Re-Key

For any CA governed by this CP, including the DocuSign CA, Digital Certificate re-key SHALL be defined as the issuance of a new Digital Certificate that certifies a new Public Key. Digital Certificate re-key is supported for Sub-CAs and for DocuSign Subscriber Digital Certificates if the functional flow within the DocuSign Service requires these functions.

4.7.1 Circumstance for Certificate Re-key

For any CA governed by this CP, including the DocuSign CA, it is necessary for the renewal to take place prior to the expiration of an existing Digital Certificate to maintain continuity. An overlap period is recommended to ensure continuity.

For the DocuSign CA, Subordinate CA Digital Certificates SHALL NOT be re-keyed after expiration.

4.7.2 Who May Request Certification of a New Public Key

DocuSign CAs will not re-key Digital Certificates.

4.7.3 Circumstance for Certificate Re-key

DocuSign CAs will not re-key Digital Certificates.

4.7.4 Who May Request Certification of a New Public Key

No stipulation.

4.7.5 Processing Certificate Re-keying Requests

No stipulation.

4.7.6 Notification of New Certificate Issuance to Certificate Subject

No stipulation.

4.7.7 Conduct Constituting Acceptance of a Re-keyed Certificate

No stipulation.

4.7.8 Publication of the Re-keyed Certificate by the CA

No stipulation.

4.7.9 Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

4.8 Modification

DocuSign CAs will not modify Digital Certificates.

4.8.1 Circumstance for Certificate Modification

Digital certificate modification is not be performed by DocuSign.

4.8.2 Who May Request Certificate Modification

No stipulation.

4.8.3 Processing Certificate Modification Requests

No stipulation.

4.8.4 Notification of New Certificate Issuance to Certificate Subject

No stipulation.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

No stipulation.

4.8.6 Publication of the Modified Certificate by the CA

No stipulation.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

4.9 Certificate Revocation and Suspension

The following specifies formal operational requirements of Digital Certificate revocation procedures.

4.9.1 Circumstances for Revocation

For any CA governed by this CP, including the DocuSign CA, a Digital Certificate SHALL be revoked when the binding between the subject and the subject's Public Key within the Digital Certificate is no longer considered valid (e.g., loss or compromise of the Private Key) or if it is determined that the Relying Party's locally determined identity elements for the Subscriber (Subject Name and Email) infringe upon a copyright.

4.9.2 Who Can Request Revocation

For any CA governed by this CP, including the DocuSign CA, any Digital Certificate issued can be revoked upon the direction of the DocuSign PMA. Additionally, CA operators can request revocation of their Sub-CA's Digital Certificate. Subscriber Digital Certificates may be revoked based on an authenticated request from the Relying Party, Subscriber, Sub-CA operator, Root CA operator, or DocuSign PMA. Revocation is subject to approval by the DocuSign PMA.

4.9.3 Procedure for Revocation Request

For any CA governed by this CP, including the DocuSign CA, Digital Certificates SHALL be revoked and included in a CRL upon receipt of sufficient evidence that shows the binding of between the subject and the subject's Public Key within the Digital Certificate is no longer considered valid. Requests to revoke Digital Certificates SHALL identify the Digital Certificate to be revoked, explain the reason for revocation, and allow the request to be authenticated (e.g., manually signed).

The DocuSign PMA SHALL approve Revocation requests for DocuSign CA issued certificates.

4.9.4 Revocation Request Grace Period

For any CA governed by this CP, including the DocuSign CA, the revocation request grace period SHALL be the time available to the Subordinate CA within which the Subordinate CA MUST make a revocation request after reasons for revocation have been identified.

4.9.5 Time within which CA Must Process the Revocation Request

For any CA governed by this CP, including the DocuSign CA, revocation requests SHALL be processed in a timely manner.

4.9.6 Revocation Checking Requirements for Relying Parties

Relying parties are RECOMMENDED to check that certificates are not revoked.

4.9.7 CRL Issuance Frequency

For any CA governed by this CP, including the DocuSign CA, CRLs SHALL be issued as described in Section 2.3.

4.9.8 Maximum Latency for CRLs

No stipulation.

4.9.9 On-line Revocation/Status Checking Availability

No stipulation.

4.9.10 On-line Revocation Checking Requirements

No stipulation.

4.9.11 Other Forms of Revocation Advertisements Available

No stipulation.

4.9.12 Special Requirements Re Key Compromise

No stipulation.

4.9.13 Circumstances for Suspension

Support for suspension is prohibited.

4.9.14 Who can Request Suspension

No stipulation.

4.9.15 Procedure for Suspension Request

No stipulation.

4.9.16 Limits on Suspension Period

No stipulation.

4.10 Certificate Status Services

4.10.1 Operational Characteristics

For any CA governed by this CP, including the DocuSign CA, the revocation status of Digital Certificate MUST be made available in a CRL through the online repository.

4.10.2 Service Availability

See Section 2.1.1.

4.10.3 Optional Features

No stipulation.

4.11 End of Subscription

For any CA governed by this CP, including the DocuSign CA, Subscriptions SHALL end when a Digital Certificate is revoked or the Digital Certificate's expiry time passes.

4.12 Key Escrow and Recovery

4.12.1 Key Escrow and Recovery Policy and Practices

No stipulation.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

No stipulation.

5 Management, Operational, and Physical Controls

5.1 Physical Controls

5.1.1 Site Location and Construction

For any CA governed by this CP, including the DocuSign CA, the location and construction of the facility that will house CA equipment and operations SHALL be in accordance with that afforded the most sensitive business and financial information. CA operations SHALL be conducted within a protected environment that deters, prevents, and detects unauthorized use of, access to, or disclosure of sensitive information and systems.

5.1.2 Physical Access

For any CA governed by this CP, including the DocuSign CA, the physical security requirements pertaining to CAs are:

- The CA MUST ensure that no unauthorized access to the hardware is permitted;
- The CA MUST provide manual or electronic monitoring for unauthorized intrusion at all times;
- The CA MUST ensure that an access log is maintained and inspected periodically
- The CA MUST ensure that only trained and authorized personnel can access the CA

When not in use:

- Paper containing sensitive plain-text information SHALL be stored in secure containers;
- The media and the activation information (see Section 6.4) for the Root CA Private Keys SHALL be stored in a secure container, and SHALL be encrypted. Activation data SHALL either be memorized, or recorded and stored in a manner commensurate with the security afforded by the DocuSign service, and SHALL NOT be stored with the cryptographic module.

If the facility is not continuously attended, the last person to depart SHALL initial a sign-out sheet that indicates the date and time, and asserts that all necessary physical protection mechanisms are in place and activated. A security check of the facility housing the CA equipment SHALL occur if the facility is to be left unattended. At a minimum, the check SHALL verify the following:

- The equipment is in a state appropriate to the current mode of operation (e.g., that cryptographic modules are in place when “open”, and secured when “closed”; and for the CA, that all equipment other than the repository is shut down);
- Any security containers are properly secured;
- Physical security systems (e.g., door locks, vent covers) are functioning properly; and,
- The area is secured against unauthorized access.

If at any time the Hardware Security Module (HSM) containing a CA’s Private Key is physically moved permanently from one location to another (i.e., not during normal activation), then:

- The HSM MUST be protected from destruction, unauthorized disclosure, and unauthorized modification.
- The DocuSign PMA MUST approve the movement.
- The DocuSign PMA or authorized representative MUST be present.

5.1.3 Power and Air Conditioning

For any CA governed by this CP, including the DocuSign CA, the facility that houses the CA equipment SHALL be supplied with power and air conditioning sufficient to create a reliable operating environment.

5.1.4 Water Exposures

For any CA governed by this CP, including the DocuSign CA, facilities that house CAs SHALL be installed such that it is not in danger of exposure to water (e.g., on tables or elevated floors).

5.1.5 Fire Prevention and Protection

For any CA governed by this CP, including the DocuSign CA, facilities that house CAs SHALL be constructed and equipped, and procedures SHALL be implemented, to prevent and extinguish fires or other damaging exposure to flame or smoke.

5.1.6 Media Storage

For any CA governed by this CP, including the DocuSign CA, when not in operation, the cryptographic modules storing the Root CA Private Key SHALL be stored in a secure container. When not in operation, the cryptographic modules storing the Sub-CA Private Key SHALL be stored in a secure room in encrypted form or in a secure container.

5.1.7 Waste Disposal

For any CA governed by this CP, including the DocuSign CA, CAs SHALL implement procedures for the disposal of waste (paper, media, or any other waste) to prevent the unauthorized use of, access to, or disclosure of waste containing Confidential/Private Information.

5.1.8 Off-Site backup

For any CA governed by this CP, including the DocuSign CA, System backups, sufficient to recover from system failure, SHALL be made on a periodic schedule. Backups SHALL be performed and stored off-site not less than annually or when the Root CA is operational, whichever is less frequent. At least one backup copy SHALL be stored at an offsite location (separate from the Root CA equipment). The backup SHALL be stored at a site with physical and procedural controls commensurate to that of the operational Root CA system.

For the DocuSign CA, the design of the DocuSign service is such that backup of Sub-CA and Subscriber keys is unnecessary; see Section 1.4.

5.2 Procedural Controls

5.2.1 Trusted Roles

A trusted role is one who performs functions that can introduce security problems if not carried out properly, whether accidentally or maliciously. For any CA governed by this CP, including the DocuSign CA, the people selected to fill these roles MUST be extraordinarily responsible or the integrity of the CA is weakened. The functions performed in these roles form the basis of trust for all uses of the CA. Two approaches are taken to increase the likelihood that these roles can be successfully carried out. The first ensures that the person filling the role is trustworthy and properly trained. The second distributes the functions among more than one person, so that any malicious activity would require collusion.

The following SHALL be the trusted Roles within the PKI:

- Administrator: trained technical operators that have been approved by the DocuSign PMA.
- CA Operator: installs, configures, and maintains the CA; configures Digital Certificate profiles and parameters; generates and performs backup of CA keys;
- Auditor: maintains and reviews audit logs; and,
- Operator: performs routine system backup and recovery.

Multi-Person control requirements are specified in Section 6.2.2.

5.2.2 Number of Persons Required Per Task

For any CA governed by this CP, including the DocuSign CA, Root CA Private Key actions MUST require at least “two-party” control. Actions include:

- Generation of CA keys;
- Access to CA Private Key;
- Backup of CA Private Key; and,
- Access to backup CA Private Key.

Where multi-person control is required, at least one of the participants SHALL be an Administrator. All participants MUST serve in a trusted role as defined in Section 5.2.1. Multi-person control SHALL NOT be achieved using personnel that serve in the Auditor Trusted Role.

No stipulation for Sub-CAs.

5.2.3 Identification and Authentication for Each Role

For any CA governed by this CP, including the DocuSign CA, a person occupying a trusted role SHALL have their identity and authorization verified, before being permitted to perform any action for that role or identity.

5.2.4 Roles Requiring Separation of Duties

For any CA governed by this CP, including the DocuSign CA, individuals MAY only assume one of the Officer, Administrator, and Auditor roles, but any individual MAY assume the Operator role. The CA software and hardware SHALL identify and authenticate its users. Procedures SHALL ensure that no user identity can assume both an Administrator and an Officer role, assume both the Administrator and Auditor roles, and assume both the Auditor and Officer roles. No individual SHALL have more than one identity.

5.3 Personnel Controls

5.3.1 Qualifications and Experience Requirements

For any CA governed by this CP, including the DocuSign CA, personnel engaged in the PKI SHALL be suitably qualified and experienced.

5.3.2 Background Check Procedures

Vetting process used for trusted personnel engaged in the PKI SHALL be described in the CPS.

5.3.3 Training Requirements

For any CA governed by this CP, including the DocuSign CA, CA Operators SHALL be appropriately trained. Topics SHALL include the operation of the CA software and hardware, operational and security procedures, and the stipulations of this policy and local guidance.

5.3.4 Retraining Frequency and Requirements

For any CA governed by this CP, including the DocuSign CA, refresher training will be provided to the extent and frequency required to ensure the required level of proficiency to perform job responsibilities competently.

5.3.5 Job Rotation Frequency and Sequence

No stipulation.

5.3.6 Sanctions for Unauthorized Actions

For any CA governed by this CP, including the DocuSign CA, if an unauthorized action takes place then appropriate action SHALL be taken to ensure disciplinary or other appropriate action is taken. In cases where an unauthorized action brings into question the security of the system, then recovery procedures will be followed (see Section 5.7).

5.3.7 Independent Contractor Requirements

For any CA governed by this CP, including the DocuSign CA, contractor personnel employed to perform functions pertaining to the CA SHALL meet the personnel requirements set forth in this CP.

5.3.8 Documentation Supplied to Personnel

For any CA governed by this CP, including the DocuSign CA, documentation sufficient to define duties and procedures for each role SHALL be provided to their personnel filling that role.

5.4 Audit Logging Procedures

5.4.1 Types of Events Recorded

For any CA governed by this CP, including the DocuSign CA, security auditing capabilities of the underlying CA equipment operating system SHALL be enabled during installation and operation. At a minimum, the following events SHALL be recorded:

For the Root CA:

- Root CA software admin activity;
- Root CA Signer Private Key generation;
- Root CA Digital certificate issuance;
- Root CA Digital certificate revocation request;
- Root CA Digital certificate revocation;
- Root CA Software and/or configuration updates to Root CA and account management;

- Root CA Clock Adjustments;
- Root CA Anomalies, error conditions, software integrity check failures, receipt of improper or misrouted messages; and,
- Root CA known or suspected violations of physical security, suspected or known attempts to attack the CA equipment via network attacks, equipment failures, power outages, network failures, or violations of this certificate policy

For the Sub-CA

- Sub-CA physical equipment access;
- Sub-CA Signer Private Key generation;
- Subscriber Digital certificate issuance;
- Subscriber Digital certificate revocation request;
- Subscriber Digital certificate revocation;
- Sub-CA Software and/or configuration updates to Sub-CA and account management;
- Sub-CA Anomalies, error conditions, software integrity check failures, receipt of improper or misrouted messages; and,
- Sub-CA Any known or suspected violations of physical security, suspected or known attempts to attack the CA equipment via network attacks, equipment failures, power outages, network failures, or violations of this certificate policy

At a minimum, for each auditable event the record SHALL include:

- The type of event;
- The time the event occurred;
- A success or failure indication for signing;

Audit logs SHALL be generated automatically and periodically backed up.

5.4.2 Frequency of Processing Log

For any CA governed by this CP, including the DocuSign CA, Offline CA audit logs SHALL be reviewed at least annually or any time the CA is brought online. Online CA audit logs SHALL be reviewed as needed to ensure integrity.

Action taken as a result of this review SHALL be documented.

Audit log reviews SHALL also be conducted when requested by the DocuSign PMA.

5.4.3 Retention Period for Audit Log

For any CA governed by this CP, including the DocuSign CA, the information generated on the CA equipment SHALL be kept on the CA equipment, or on a secure server that retrieves audit log information from the CA, until the information is moved to an appropriate archive facility. Audit logs SHALL be available for three months, at a minimum, and then moved offsite as archive records (See Section 5.5).

5.4.4 Protection of Audit Log

For any CA governed by this CP, including the DocuSign CA, only authorized personnel MAY archive audit logs. Audit logs MUST be protected against unauthorized viewing, modification, and deletion. Audit logs SHALL only be deleted from a system after it has been archived.

For the DocuSign CA, only personnel assigned to a trusted role, as designated by the PMA, have read access to the logs.

5.4.5 Audit Log Backup Procedures

For any CA governed by this CP, including the DocuSign CA, audit logs SHALL be backed up. A copy of the audit log SHALL be stored at a separate facility from the active audit log as required.

5.4.6 Audit Collection System (Internal vs. External)

For any CA governed by this CP, including the DocuSign CA, automated audit processes SHALL be invoked at system (or application) startup, and cease only at system (or application) shutdown.

5.4.7 Notification to Event-Causing Subject

No stipulation.

5.4.8 Vulnerability Assessments

For any CA governed by this CP, including the DocuSign CA, Trusted Roles SHALL routinely assesses the CA system and its components for malicious activity.

5.5 Records Archive

5.5.1 Types of Events Archived

For any CA governed by this CP, including the DocuSign CA, CA archive records SHALL be detailed enough to establish the validity of a signature and of the operation of the PKI. The following MUST be recorded at a minimum:

- CA accreditation;
- CPS;
- System equipment configuration;
- Modification and updates to system or configuration;
- Key Signing Ceremony video footage;
- Certificate Subject identity authentication data from 3.1.9;
- Documentation of receipt and acceptance of certificates;
- Audit logs from Section 5.4.1;
- All Digital Certificates issued;
- Other data or applications to verify archive contents; and,
- Documentation required by compliance auditors.

5.5.2 Retention Period for Archive

For any CA governed by this CP, including the DocuSign CA, archive data SHALL be maintained for a minimum of the period of validity of all Certificates issued by CA, plus one (1) year or such longer period as MAY be required by law.

5.5.3 Protection of Archive

For any CA governed by this CP, including the DocuSign CA, archive data SHALL be protected to ensure there is no unauthorized disclosure or modification. Archive media SHALL be stored in a safe, secure storage facility separate from the CA itself.

5.5.4 Archive Backup Procedures

For any CA governed by this CP, including the DocuSign CA, archive facility SHALL support backups.

5.5.5 Requirements for Time-Stamping of Records

For any CA governed by this CP, including the DocuSign CA, archive data SHALL indicate the date on which the archive was created.

5.5.6 Archive Collection System (Internal or External)

No stipulation.

5.5.7 Procedures to Obtain and Verify Archive Information

For any CA governed by this CP, including the DocuSign CA, DocuSign PMA or designated representative MUST be granted timely access to archive information when requested.

5.6 Key Changeover

For any CA governed by this CP, including the DocuSign CA, Root CA keys MAY be rekeyed (see Section 4.7). Sub-CAs MAY be rekeyed (Section 4.7) if the Root CA reconfirms the identity of the Sub-CA, which the Root CA either accepts or rejects. Re-keying requires multi-person control as specified in Section 5.2.2 and requires a "Key Ceremony" as specified in Section 6.1.1 for access to the Root CA's Private Key.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

In the event of suspected compromise of any CA governed by this CP, including the DocuSign CA, the CA SHALL be investigated in order to determine the nature and the degree of damage. If the CA suspected of being compromised (even if unable to be confirmed) or is actually compromised and the CA Digital Certificate is revoked, a new CA Digital Certificate MUST be issued.

Revoked CA Digital Certificates in Relying Party trust stores (Operating Systems, Browsers, Applications, etc.) MUST be replaced with a newly issued CA Digital Certificate. Root CA Digital Certificates will be distributed via an online publicly available repository referred to from the Sub-CAs certificate.

5.7.2 Computing Resources, Software, and/or Data Are Corrupted

For any CA governed by this CP, including the DocuSign CA, Backup or Archived data MUST be used when computing resources, software, and data are corrupted.

5.7.3 CA Private Key Compromise Procedures

For any CA governed by this CP, including the DocuSign CA, compromised CA Private Keys MUST be revoked. Compromised CA Private Keys MUST NOT be used to sign new Digital Certificates. CA with compromised Private Keys MUST generate new Private Keys, which SHALL be published to the Repository within one business day of revocation. Follow procedures in Section 5.3.6 if the CA operator is suspected of compromising the CA's Public Key.

5.7.4 Business Continuity Capabilities After a Disaster

For any CA governed by this CP, including the DocuSign CA, in the case of a disaster in which the CA equipment is damaged and inoperative:

- The Root CA operations SHALL be established as quickly as possible, giving priority to the ability to issue CA Digital Certificates.
- The Sub-CA operations SHALL be reestablished as quickly as possible, giving priority to the ability to issue Subscriber Digital Certificates.

5.8 CA and RA Termination

For any CA governed by this CP, including the DocuSign CA, in the event a CA terminates, or ceases operation, the CA MUST ship its HSM, which contains the CA's Private Key, and any backup copies and archival copies to a location specified by the DocuSign PMA.

6 Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

For any CA governed by this CP, including the DocuSign CA, CA keys MUST be generated in FIPS 140-2 Level 3 compliant, evaluated/certified cryptographic module. Key pairs MUST be generated on the device and MUST NOT leave the device except for authorized and documented backups.

In addition, the Root CA utilizes multi-person control; see Section 5.2.2.

For the DocuSign CA, Subscriber keys MUST be generated by the DocuSign Service, and Private Keys MUST be stored in a FIPS 140-2 Level 3 compliant, evaluated/certified cryptographic module. Subscriber key pairs MUST NOT be duplicated to other DocuSign signature engines. There MAY be more than one key pair per subscriber.

6.1.2 Private Key Delivery to Certificate Subject

For non-DocuSign CAs, no stipulation.

For the DocuSign CA, the Private Key SHALL NOT be provided to the Subscriber (see Section 1.4).

6.1.3 Public Key Delivery to Certificate Issuer

A Certificate Subject's Public Key and identity SHALL be delivered securely to the CA in certification request (see Section 3.2).

6.1.4 CA Public Key Delivery to Relying Parties

For any CA governed by this CP, including the DocuSign CA, CA Public Keys SHALL be delivered to the Relying Party.

For the DocuSign CA, CA Public Keys SHALL be delivered to the Relying Party as part of the digitally signed document, if the Relying Party elects to download the document from the DocuSign service. Otherwise, the DocuSign service utilizes CA Public Keys to facilitate signature validation.

6.1.5 Key Sizes

For any CA governed by this CP, including the DocuSign CA, Keys MUST be 2048 bits or longer.

6.1.6 Public Key Parameters Generation and Quality Checking

See PKCS #1 for key generation requirements.

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

See Section 7.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

For any CA governed by this CP, including the DocuSign CA, the relevant standard for cryptographic modules SHALL be FIPS PUB 140-2, Security Requirements for Cryptographic Modules.

6.2.2 Private Key Multi-Person Control

For any CA governed by this CP, including the DocuSign CA, all access to Root CA Private Keys MUST be under multi-person control; see Section 5.2.2.

For the DocuSign CA, there is no stipulation for Sub-CAs or Subscriber Private Keys.

6.2.3 Private Key Escrow

No stipulation.

6.2.4 Private Key Backup

For any CA governed by this CP, including the DocuSign CA, CA Private Keys SHALL be backed up under multi-person control, as required in Section 5.2.2. No more than a single copy of the Private Key SHALL be stored at the CA's location (i.e., only the operational and backup key MAY be stored at the CA's location). Additional copies MAY exist off-site provided that accountability for them is maintained. This does not preclude the ability of the operator of a CA to explain in the CPS and get explicit approval for a secure high-availability high-throughput system, which parallelizes the operation among several machines.

6.2.5 Private Key Archival

No stipulation.

6.2.6 Private Key Transfer into or from a Cryptographic Module

For any CA governed by this CP, including the DocuSign CA, Root CA Private Keys SHALL never leave the cryptographic module, except for during secure and authorized backups.

For any CA governed by this CP, including the DocuSign CA, Sub-CA and Subscriber Private Keys SHALL never leave the cryptographic module.

6.2.7 Private Key Storage on Cryptographic Module

For any CA governed by this CP, including the DocuSign CA, Private keys SHALL be encrypted when not in use.

6.2.8 Method of Activating Private Keys

For any CA governed by this CP, including the DocuSign CA, Activation of the Root CA Private Key SHALL evoke multi-person control, as specified in Section 5.2.2.

For any CA governed by this CP, including the DocuSign CA, Sub-CAs SHALL be online and used when a request is provided to the Sub-CA.

For the DocuSign CA, Subscriber Private Keys SHALL be activated by the Subscriber through the DocuSign Service.

For non-DocuSign CAs, no stipulation for Subscriber Private Keys.

6.2.9 Methods of Deactivating Private Keys

For any CA governed by this CP, including the DocuSign CA, Root CA Private Keys SHALL be deactivated and the media holding the Root CA Private Key SHALL be stored in a secure container (see Section 5.1.6). This action requires multi-person control, as specified in Section 5.2.2. The Root CA Private Key media SHALL NOT be left unattended when not in use.

For any CA governed by this CP, including the DocuSign CA, Sub-CA Private Keys SHALL be deactivated when not in use.

For any CA governed by this CP, including the DocuSign CA, Subscriber Private Keys SHALL be deactivated when not in use.

6.2.10 Method of Destroying Private Key

No stipulation.

6.2.11 Cryptographic Module Rating

For any CA governed by this CP, including the DocuSign CA, the module rating SHALL be Level 3.

6.3 Other Aspects of Key Management

6.3.1 Public Key Archival

For any CA governed by this CP, including the DocuSign CA, Public Keys SHALL be archived as part of the Digital Certificate archival.

6.3.2 Certificate Operational Periods/Key Usage Periods

Root CA certificate lifetimes SHALL be limited to 45 years or less.

For any CA governed by this CP, including the DocuSign CA, Sub-CAs certificates SHALL be limited to 10 years or less.

For any CA governed by this CP, including the DocuSign CA, Subscriber certificates SHALL be limited to 3 years or less, not including renewal times.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

For any CA governed by this CP, including the DocuSign CA, activation data generation and installation for CA Private Keys SHALL use methods that protect the activation data to the extent necessary to prevent the loss, theft, modification, unauthorized disclosure, or unauthorized use of such Private Keys.

For the DocuSign CA, Subscriber Private Keys SHALL be activated via the processes and conditions outlined in Section 1.4.

6.4.2 Activation Data Protection

For any CA governed by this CP, including the DocuSign CA, activation data to invoke Private Keys SHALL be protected from disclosure by a combination of cryptographic and physical access control mechanisms.

6.4.3 Other Aspects of Activation Data

For any CA governed by this CP, including the DocuSign CA, before the Root CA Private Key activation data MAY be entered, the media storing the Root CA's Private Key MUST be retrieved from the locked container as part of a DocuSign PMA approved Root CA ceremony.

No stipulation for Sub-CAs or Subscriber Digital Certificates.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

For any CA governed by this CP, including the DocuSign CA, the computer security functions listed below are required. These functions MAY be provided by the operating system, or through a combination of operating system, software, and physical safeguards. The CA and its ancillary parts SHALL include the following functionality:

- Require authenticated logins;
- Provide a security audit capability;
- Restrict access control to Trusted Roles;
- Enforce separation of Trusted Roles;
- Require identification and authentication;
- Require use of cryptography for session communications and database security;

6.5.2 Computer Security Rating

No Stipulation.

6.6 Life-Cycle Security Controls

6.6.1 System Development Controls

For any CA governed by this CP, including the DocuSign CA, the System Development Controls for the CA are as follows:

- For commercial off-the-shelf software, the software SHALL be designed and developed under a formal, documented development methodology.
- For hardware and software developed specifically for a particular CA, the applicant SHALL demonstrate that security requirements were achieved through a combination of software verification & validation, structure.
- Where open source software has been utilized, the software SHALL demonstrate that security requirements were achieved through software verification & validation and structured development/life-cycle management.
- The CA software SHALL be dedicated to performing one task: the CA. There SHALL be no other applications; hardware devices, network connections, or component software installed which are not part of the CA operation.
- Proper care SHALL be taken to prevent malicious software from being loaded onto the CA equipment.
- Hardware and software updates SHALL be purchased or developed in the same manner as original equipment, and be installed by trusted and trained personnel in a defined manner.
- Any code returned to open source community does not disclose security relevant information.

6.6.2 Security Management Controls

For any CA governed by this CP, including the DocuSign CA, the configuration of the CA system as well as any modifications and upgrades SHALL be documented and controlled. There SHALL be a mechanism for detecting unauthorized modification to the CA software or configuration. A formal configuration management methodology SHALL be used for installation and ongoing maintenance of the CA system.

6.6.3 Life Cycle Security Ratings

No stipulation.

6.7 Network Security Controls

For any CA governed by this CP, including the DocuSign CA, CAs SHALL be protected to prevent unauthorized access, tampering, and denial-of-service. Communications of sensitive information to and from CAs SHALL be protected using point-to-point encryption for confidentiality and digital signatures for non-repudiation and authentication.

Root CAs SHOULD be offline.

6.8 Time Stamping

For the DocuSign CA, times asserted in Digital Certificates SHALL be accurate to within three minutes of the DocuSign Service clock. Electronic or manual procedures MAY be used to maintain system time. Clock adjustments are auditable events (See Section 5.4.1).

There are no stipulations regarding an external trusted time source.

7 Certificate, CRL, SCVP, and OCSP Profiles Format

7.1 Certificate Profile

The fields listed in the tables below SHALL be the only ones populated in Digital Certificates issued by DocuSign CAs.

7.1.1 Root CA Certificate Profile

Field	Value or Value Constraint
Version:	3 (0x2)
Serial Number:	This field contains the serial number of the certificate.
Signature Algorithm:	sha256WithRSAEncryption
Issuer:	CN=DocuSign Inc Root CA
Validity Not Before:	Jan 4 00:18:35 2014 GMT
Validity Not After:	Jan 4 00:28:33 2044 GMT
Subject:	CN=DocuSign Inc Root CA
Public Key Algorithm:	rsaEncryption
RSA Public Key:	Public key is provided in certificate.
X509v3 Key Usage:	Digital Signature, Certificate Sign, CRL Sign
X509v3 Basic Constraints:	critical CA:TRUE
X509v3 Subject Key Identifier:	Subject Key ID is provided in this field.
Microsoft CA Renewal Version (1.3.6.1.4.1.311.21.1)	The value for this field is in the certificate. It is for internal purposes and has no meaning outside of DocuSign.
Signature Algorithm: sha256WithRSAEncryption	Certificate signature is provided in this field.

7.1.2 Sub-CA Certificate Profile

Field	Value or Value Constraint
Version:	3 (0x2)
Serial Number:	This field contains the serial number of the certificate.
Signature Algorithm:	sha256WithRSAEncryption
Issuer:	CN=DocuSign Inc Root CA
Validity Not Before: Not After :	Fields provide validity period for the sub-CA cert.
Subject:	Field contains the subject name of the certificate: C, O, OU, CN
Public Key Algorithm:	rsaEncryption
RSA Public Key:	The Public Key is provided in this field.
Microsoft CA Renewal Version (1.3.6.1.4.1.311.21.1)	The value for this field is in the certificate. It is for internal purposes and has no meaning outside of DocuSign.
X509v3 Subject Key Identifier:	Subject Key ID is provided in this field.
Microsoft szOID_ENROLL_CERTTYPE_EXTENSION	The value for this field is in the certificate. It is for internal purposes and has no meaning outside of DocuSign.
X509v3 Key Usage:	Key usage is provided in this field.
X509v3 Basic Constraints:	critical CA:TRUE
X509v3 Authority Key Identifier:	Authority Key ID is provided in this field.
X509v3 CRL Distribution Points:	The link to the CRL distribution point is provided in this field.
Authority Information Access:	A path to the certificate of the issuing CA is provided in this field.
Signature Algorithm: sha256WithRSAEncryption	Certificate signature is provided in this field.

7.1.3 DocuSign Subscriber Certificate Profile

Field	Value or Value Constraint
Version:	3 (0x2)
Serial Number:	This field contains the serial number of the certificate.
Signature Algorithm:	sha256WithRSAEncryption
Issuer:	Field contains the issuer name of the certificate: C, O, OU, CN
Validity Not Before: Not After:	Fields provide validity period for the subscriber certificates.
Subject:	Field contains the subject name of the certificate: C, O, OU, CN
RSA Public Key:	The Public Key is provided in this field.
X509v3 Key Usage:	Key usage is provided in this field.
X509v3 Extended Key Usage:	Extended key usage is provided in this field.
X509v3 Subject Key Identifier:	Subject Key ID is provided in this field.
X509v3 Authority Key Identifier:	Authority Key ID is provided in this field.
X509v3 CRL Distribution Points:	The link to the CRL distribution point is provided in this field.
Authority Information Access:	A path to the certificate of the issuing CA is provided in this field.
X509v3 Certificate Policies:	Policy OID and URL link to CP and CPS are provided in this field.
Signature Algorithm: sha256WithRSAEncryption	Certificate signature is provided in this field.

7.2 CRL Profile

7.2.1 DocuSign Root CRL Profile

Field	Value or Value Constraint
Version	2 (0x1)
Signature Algorithm:	sha256WithRSAEncryption
Issuer:	/CN=DocuSign Inc Root CA
Last Update:	This field specifies the date and time of the last update of the CRL.
Next Update:	This field specifies the latest date and time that the next CRL will be published.
CRL extensions:	
X509v3 Authority Key Identifier:	Non-critical field that provides the Authority Key ID.
Microsoft CERTSRV_CA_VERSION (1.3.6.1.4.1.311.21.1):	Non-critical field. It is for internal purposes and has no meaning outside of DocuSign.
X509v3 CRL Number:	Non-critical as per RFC 5280.
Microsoft CRL_NEXT_PUBLISH (1.3.6.1.4.1.311.21.4):	Non-critical field. It is for internal purposes and has no meaning outside of DocuSign.
Revoked Certificates	Revoked are listed in this field.
Signature Algorithm: sha256WithRSAEncryption	The CRL is signed. Signature provided in this field.

7.2.2 DocuSign Sub-CA CRL Profile

Field	Value or Value Constraint
Version	2 (0x1)
Signature Algorithm:	sha256WithRSAEncryption
Issuer:	Issuer of the CRL is listed in this field: C, O, OU, CN
Last Update:	This field specifies the date and time of the last update of the CRL.
Next Update:	This field specifies the latest date and time that the next CRL will be published.
Revoked Certificates	Revoked are listed in this field.
CRL extensions:	
X509v3 Authority Key Identifier:	Non-critical field that provides the Authority Key ID.
X509v3 CRL Number:	Non-critical as per RFC 5280.
Signature Algorithm: sha256WithRSAEncryption	The CRL is signed. Signature provided in this field.

7.3 OCSP Profile

No stipulation.

7.4 SCVP Profile

No stipulation.

8 Compliance Audit and Other Assessments

8.1 Frequency of Audit or Assessments

Any CA governed by this CP, including the DocuSign CA, SHALL be subject to a compliance audit at least once per year.

8.2 Identity and Qualifications of Assessor

Any CA governed by this CP, including the DocuSign CA the DocuSign PMA SHALL identify the compliance auditor for the CA. The auditor MUST demonstrate competence in the field of compliance audits.

8.3 Assessor's Relationship to Assessed Entity

Any CA governed by this CP, including the DocuSign CA, the compliance auditor either SHALL be a private firm, that is independent from the entity being audited, or it SHALL be sufficiently organizationally separated from that entity to provide an unbiased, independent evaluation.

The DocuSign PMA SHALL determine whether a compliance auditor meets this requirement.

8.4 Topics Covered By Assessment

The compliance audit of the CA SHALL verify that the CA is implementing all provisions of a CP approved by the DocuSign PMA.

8.5 Actions Taken As A Result of Deficiency

Any discrepancies between how the CA is designed to or is being operated or maintained and the requirements of this CP will result in the compliance auditor documenting the discrepancy.

8.6 Communication of Results

Upon completion, the audit compliance report will be returned to the DocuSign PMA. For any CA governed by this CP, including the DocuSign CA, the report SHALL be treated as company confidential. The report SHALL identify the versions of the CP used in the assessment.

9 Other Business and Legal Matters

This chapter specifies requirements on general business and legal matters.

9.1 Fees

9.1.1 Certificate Issuance/Renewal Fees

Any CA governed by this CP, including the DocuSign CA, MAY charge fees to for the issuance or renewal of Certificates.

9.1.2 Certificate Access Fees

Any CA governed by this CP, including the DocuSign CA, MAY charge fees for access of Certificates.

9.1.3 Revocation or Status Information Access Fee

Any CA governed by this CP, including the DocuSign CA, SHALL NOT charge fees for access to revocation or status information.

9.1.4 Fees for other Services

Any CA governed by this CP, including the DocuSign CA, MAY charge fees for other services.

9.1.5 Refund Policy

Any CA governed by this CP, including the DocuSign CA, MAY develop a refund policy.

9.2 Financial Responsibility

9.2.1 Insurance Coverage

Relying Parties and Subscribers are encouraged to maintain a commercially reasonable level of insurance coverage for errors and omissions, either through an errors and omissions insurance program with an insurance carrier or a self-insured retention.

For the DocuSign CA, DocuSign maintains such errors and omissions insurance coverage.

9.2.2 Other Assets

Any CA operating under the governance of this CP shall have sufficient financial resources to maintain their operations and perform their duties, and they must be reasonably able to bear the risk of liability to Subscribers and Relying Parties.

9.2.3 Insurance/warranty Coverage for End-Entities

No stipulations.

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

The following records of Subscribers and Relying Parties, subject to Section 9.3.2, SHALL be kept confidential and private ("Confidential/Private Information"):

- CA application records, whether approved or disapproved,
- Certificate Application records,
- Private keys held by the CAs, and information needed to utilize such Private Keys,
- Transactional records (both full records and the audit trail of transactions),

- Audit trail records created or retained by the CA or a Customer,
- Audit reports created by the CA or a Customer (to the extent such reports are maintained), or their respective auditors (whether internal or public),
- Contingency planning and disaster recovery plans, and
- Security measures controlling the operations of CA hardware and software and the administration of Certificate services and designated enrollment services.

9.3.2 Information Not Within the Scope of Confidential Information

Certificates, Certificate revocation and other status information, CA repositories and information contained within them SHALL NOT be considered Confidential/Private Information. Information not expressly deemed Confidential/Private Information under Section 9.3.1 SHALL be considered neither confidential nor private.

This section is subject to applicable privacy laws.

9.3.3 Responsibility to Protect Confidential Information

Any CA governed by this CP SHALL secure confidential information from unauthorized access by third parties.

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

Any CA governed by this CP SHALL develop and publish a Privacy Plan or Privacy Policy, which SHALL be made available to CA participants such as Relying Parties, Subscribers, etc.

9.4.2 Information Treated as Private

Any CA governed by this CP SHALL treat as private any information about Subscribers that is not publicly available through the content of the issued certificate, certificate directory and online CRLs.

9.4.3 Information Not Deemed Private

Any CA governed by this CP SHALL NOT treat as private any information made public within a certificate.

9.4.4 Responsibility to Protect Private Information

Recipients of private information shall secure it from unauthorized access and disclosure to third parties and shall comply with all applicable local privacy laws in their jurisdiction.

9.4.5 Notice and Consent to use Private Information

Unless otherwise stated in this CP, the applicable Privacy Policy or by agreement, private information SHALL NOT be used without the consent of the party to whom that information applies.

This section is subject to applicable privacy laws.

9.4.6 Disclosure Pursuant to Judicial/Administrative Process

Any CA governed by this CP shall be entitled to disclose Confidential/Private Information if, in good faith, DocuSign believes that:

- Disclosure is necessary in response to subpoenas and search warrants.
- Disclosure is necessary in response to judicial, administrative, or other legal process during the discovery process in a civil or administrative action, such as subpoenas, interrogatories, requests for admission, and requests for production of documents.

This section is subject to applicable privacy laws.

9.4.7 Other Information Disclosure Circumstances

Any CA governed by this CP, including the DocuSign CA, Privacy Plans or Privacy Policies shall contain provisions relating to the disclosure of Confidential/Private Information to the person disclosing it to DocuSign. This section is subject to applicable privacy laws.

9.5 Intellectual Property Rights

DocuSign owns and reserves all intellectual property rights associated with the products developed by DocuSign to operate the DocuSign CAs, including but not limited to, its databases, web sites, the DocuSign service, DocuSign Digital Certificates and any other publication whatsoever originating from DocuSign, including this CP.

Subscribers and Relying Parties of these services have no intellectual property rights to the elements that support such services. The Distinguished names of all CAs of the DocuSign CA remain the sole property of DocuSign, which enforces these rights.

9.6 Representations and Warranties

9.6.1 PMA

Any CA governed by this CP SHALL form and maintain a PMA (Policy Management Authority)..

9.6.2 Generally Applicable Representations and Warranties

See 9.6.3.

9.6.3 CA Representations and Warranties

Any CA governed by this CP SHALL be in charge of:

- Validation and publication of this CP, and the respective CA's CPS;
- Compliance of issued certificates as per this CP, and the respective CA's CPS;
- Adherence to the security principles for all the components of the CAs and their subsequent controls.

9.6.4 RA Representations and Warranties

See above.

9.6.5 Certificate Subject Representations and Warranties

9.6.6 Relying Parties Representations and Warranties

Relying Parties using certificates from any CA governed by this CP SHALL:

- Verify and adhere to by the usage for which the certificate has been issued;
- Verify the revocation status of the certificate;
- Verify and adhere by the obligations defined in this CP and in the Relying Party Agreement.

9.6.7 Subscriber Representation and Warranties

Subscribers using certificates from any CA governed by this CP SHALL:

- Communicate correct and up-to-date information;
- Protect the access to the Subscriber Private Key, along with any credentials that allow for use of it;
- Use an issued certificate(s) for authorized and legal purposes, consistent with this CPS;

- Be an end-user Subscriber and not a CA, and must not use the Private Key corresponding to any Public Key listed in the Certificate for purposes of digitally signing any Certificate (or any other format of certified Public Key) or CRL, as a CA or otherwise; and
- Verify and adhere by the obligations defined in this CP and in the Subscriber Agreement.

9.6.8 Representations and Warranties of Other Participants

Not applicable.

9.7 Disclaimers of Warranties

To the extent permitted by applicable law, Subscriber Agreements and Relying Party Agreements shall disclaim DocuSign's possible warranties, including any warranty of merchantability or fitness for a particular purpose.

9.8 Limitations of Liability

9.8.1 PMA

For non-DocuSign CAs, no stipulation.

For the DocuSign CA, the remainder of Section 9.9.1 applies

DocuSign shall not be liable for non-authorized or non-compliant usage of the certificate(s), the associated Private Keys, the revocation status information or any other hardware or software provided.

DocuSign shall not be liable for any damage resulting from errors or inaccuracies of information contained in the certificates, when these errors or inaccuracies are a direct result of erroneous information provided by the Subscriber or Relying Party.

To the extent permitted by applicable law, the liability of DocuSign toward a Subscriber or a Relying Party is limited according to what is stated in this CP.

Under no circumstances will DocuSign be liable for:

- Any loss of profits.
- Any loss of data.
- Any indirect, consequential or punitive damages arising from or in connection with the use, delivery, license, and performance or non-performance of certificates or digital signatures.
- Any transactions or services offered or within the framework of this CP.
- Any other damages except for those due to reliance on the verified information in a certificate, except for information featured on free, test or demo certificates.
- Any liability incurred in any case if the error in such verified information is the result of fraud or willful misconduct of the Subscriber or Relying Party.

In any case, whatever originating facts and prejudices and their aggregate amounts, DocuSign's total aggregate liability of any kind is limited to five hundred dollars (\$500.00 USD). The aggregate liability provided shall be the same regardless of the number of digital signatures, transactions, or claims related to a Digital Certificate.

9.8.2 Other Participants.

Not Applicable.

9.9 Indemnities

9.9.1 PMA

For non-DocuSign CAs, no stipulation.

For the DocuSign CA, the remainder of Section 9.8.1 applies

To the extent permitted by applicable law, the Subscriber agrees to indemnify and hold DocuSign harmless from any acts or omissions resulting in liability, any loss or damage, and any suits and expenses of any kind, including reasonable attorney's fees that DocuSign may incur as a result of failure to:

- Protect Subscriber's Private Key
- Use a trustworthy system as required
- Take precautions necessary to prevent the compromise, loss, disclosure, modification, or unauthorized use of the Subscriber's Private Key
- Attend to the integrity of the DocuSign Root.

9.9.2 Other Participants

Not applicable.

9.10 Term and Termination

9.10.1 Term

9.10.1.1 CP Term

For any CA governed by this CP, including the DocuSign CA, this CP/CPS is effective as soon as it is published in the DocuSign Repository and remains in force until the expiration of the last certificate is issued under it.

9.10.1.2 Other Agreements

9.10.2 Termination

9.10.2.1 CP Termination

For any CA governed by this CP, including the DocuSign CA, this CP/CPS shall remain in force until notice of termination is communicated by DocuSign on its website or Repository or until it is replaced by a new version.

For the DocuSign CA, on termination of this CP/CPS, DocuSign CA participants are still bound by the conditions of this CP/CPS for all certificates issued during the validity period, until the expiration of the last certificate.

9.10.2.2 Other Agreements

9.10.3 Effect of Termination and Survival

9.10.3.1 CP

Notified changes are appropriately marked by an indicated version. Following publications, changes become applicable 30 days thereafter.

9.10.3.2 Other Agreements

9.11 Individual Notices and Communications With participants

For any CA governed by this CP, including the DocuSign CA, unless otherwise agreed upon by the relevant parties, all notices and other communications to be provided, delivered or sent in compliance with the current CP/CPS should be written and sent with means providing reasonable confidence of origin and reception.

9.12 Amendments

9.12.1 Procedure for Amendment

9.12.1.1 CP

9.12.1.2 CPS and Participant Agreements.

The DocuSign Policy Management Authority (PMA) may make amendments to this CP. Amendments shall either be in the form of a document containing an amended form of the CP or an update. Amended versions or updates shall be linked to the DocuSign Repository.

Updates supersede any designated or conflicting provisions of the referenced version of the CPS. The PMA shall determine whether changes to the CP require a change in the Certificate Policy.

9.12.2 Notification Mechanism and Period

DocuSign and the PMA reserves the right to amend the CP/CPS without notification for amendments that are not material, including without limitation, editorial or typographic corrections of errors, changes to URLs, and changes to contact information. The PMA's decision to designate amendments as material or non-material shall be within the PMA's sole discretion.

Proposed amendments to the CPS will be published for comments in the DocuSign Repository located at <http://www.docusign.com/certificates> with an indication of the proposed effective date.

When a new version of the CP/CPS is published, all Subscribers and Relying Parties of the DocuSign CA are informed of the nature, the time and the date of change, through publication on the DocuSign web site.

At the end of the comments period, the PMA can decide to publish the new CP/CPS, restart the amendment process with a new version or withdraw the proposed version.

Unless otherwise stated, the new version of the CP/CPS will take effect fourteen (14) working days after its publication and will remain in effect until a new version takes effect.

9.12.3 Circumstances Under Which OID Must Be Changed

If the PMA determines that a change is necessary in the object identifier corresponding to a Certificate policy, the amendment shall contain new object identifiers for the Certificate policies corresponding to each Class of Certificate. Otherwise, amendments shall not require a change in Certificate policy object identifier.

9.13 Dispute Resolution Provisions

To the extent permitted by applicable law, Subscriber Agreements and Relying Party Agreements shall contain a dispute resolution clause.

9.14 Governing Law

This CP will be interpreted, construed, and enforced in all respects in accordance with the local laws of the State of Washington, U.S.A., without reference to the its choice of law rules to the contrary. This choice of law is made to ensure uniform interpretations

of this CP, regardless of the place of residence or place of use of the DocuSign CA or other products and services and regardless of the venue, country and legal entity offering and selling DocuSign CA.

9.15 Compliance with Applicable Law

This CP is subject to applicable laws of the United States. Export of certain types of software used in the DocuSign CA may require the approval of appropriate public or private authorities. DocuSign, Subscribers and Relying Parties agree to conform to applicable export laws.

9.16 Miscellaneous Provisions

9.16.1 Document Incorporated into CP

9.16.2 Entire agreement

Not applicable.

9.16.3 Assignment

This CP shall be binding upon the successors, executors, heirs, representatives, administrators, and assigns, whether express, implied, or apparent, of the parties that this CP/CPS applies to. The rights and obligations detailed in this CP 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 this CP articles on termination or cessation of operations, and provided that such assignment does not affect a notation of any other debts or obligations the assigning party owes to other parties at the time of such assignment.

9.16.4 Severability

If any provision of this CP, including limitation of liability clauses, is found to be invalid or unenforceable, the remainder of the CP shall be interpreted in such a manner as to represent the original intentions of the parties.

9.16.5 Waiver

Not applicable.

9.16.6 Attorneys' Fees

Not applicable.

9.16.7 Force Majeure

To the extent permitted by applicable law, Subscriber Agreements and Relying Party Agreements shall include a force majeure clause protecting DocuSign.

9.17 Other Provisions

Not applicable.