CPS (Certification Practice Statement)

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 CPS was authored in support of the DocuSign Express Digital Signature service, commercially available starting in early 2014.

TABLE OF CONTENTS

1 Introduction

1.1 Overview

The DocuSign® CPS (Certification Practice Statement) defines the policies, procedures, and requirements that DocuSign conforms to (see Section 1.3) when issuing and managing Digital Certificates. This CPS 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 Certification Practice Statement. The OID (Object Identifier) "1.3.6.1.4.1.42482.1.1.1.1.0" is included in certificates to indicate that they are issued in accordance with this CPS.

1.3 PKI Participants

1.3.1 Policy Management Authority

The DocuSign PMA (Policy Management Authority) approves the CPS 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:

- CP (Certificate Policy)
- SA (Subscriber Agreements)
- RPA (Relying Party Agreements)
- PMA bylaws
- ToU (Terms of Use)

1.3.2 Certification Authority

The DocuSign CA (Certification Authority) is the collection of technology and procedures that issues Digital Certificates using the processes and policies outlined within this DocuSign CPS. The 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 any 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 DocuSign Service on behalf of 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 CA managed Digital Certificates can only be used for the following purposes:

- The Root CA only issues 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.
- Subordinate CAs 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.
- Subscriber certificates are 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:

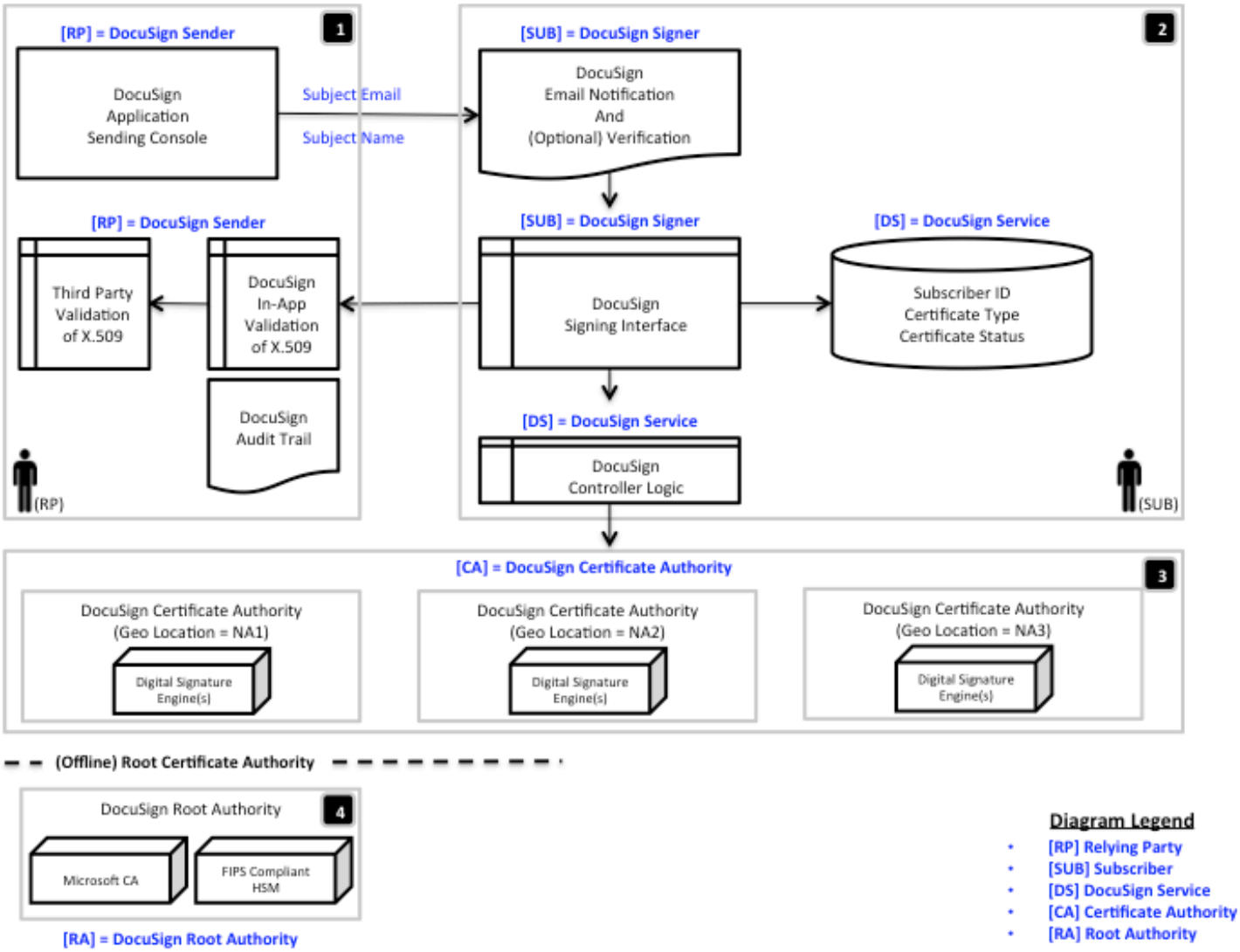

Figure 1 - The DocuSign Express Digital Signature Service

- 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. These 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:
    - An always-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.
  - 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 CPS.
  - 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 accessed 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 key. 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,
        - A tamper-evident 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 is responsible for all aspects of this CPS and approval of all related agreements and amendments.

1.5.2 Contact Person

All communications regarding this CPS should 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 is the entity that determines whether a particular CA conforms to this CPS 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 approves the CPS and any amendments according to the PMA's bylaws. The DocuSign PMA determines whether an amendment to this CPS 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

DocuSign publishes all CA certificates, certificate status information for all certificates, CP, CPS, SA, RPA, and references to TOU (Terms of Use) in online repositories. Repositories will 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

DocuSign Root CA generated CRLs are 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 will be made available no later than one business day after they are generated.

Sub-CA certificates are published within one business day of issuance.

Sub-CA generated CRLs are produced at a frequency no less than every 7 days.

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

Changes to documentation pertaining to the DocuSign Service or any DocuSign CA are published within one business day of approval by the DocuSign PMA.

2.4 Access Controls on Repositories

No stipulation.

3 Identification and Authentication

3.1 Naming

3.1.1 Types of Names

The DocuSign CA issues non-null subject names that are conformant with RFC 5280. Subject Alternative names are not utilized. The following forms are supported:

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

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

3.1.2 Meaningfulness

It is assumed that since the Relying Party specifies the Subscriber subject name and email address, that the subject name and email are meaningful to the Relying Party and 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

CA names will be unique across the whole DocuSign Service.

No stipulation for Subscriber names.

3.1.6 Recognition, Authentication, and Role of Trademarks

The DocuSign CA Operator will revoke any Digital Certificate containing a Subject Name that a court of competent jurisdiction has determined infringes on the trademark of another. This revocation will take place within 48 hours of notification from the DocuSign PMA.

For the DocuSign CA, CA, RA, and Subscriber Digital Certificates all include the string "DocuSign".

The Relying Party Agreement requires that Relying Parties not request subject names for Subscribers that infringe upon the Intellectual Property Rights of others. CAs and RAs will not ensure that the Subscriber has Intellectual Property Rights in the name appearing in the certificate application.

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

The DocuSign CAs generate their own keys and will prove to the issuing CA that they possess the Private Key that corresponds to the Public Key in the certification request via manual validation. The DocuSign Sub-CA with a newly issued certificate will produce a CRL, and the Root CA operator will ensure that the CRL is signed using the appropriate Private Key. PKCS#10 standard certificate requests are utilized.

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

The DocuSign CAs only issue Digital Certificates or generate status information in support of the DocuSign Service. All other uses of DocuSign CA Digital Certificates are expressly prohibited.

Relying Parties can only request Digital Certificates for Subscribers via the DocuSign Service. No other services or mechanisms are provided for Relying Parties to request Digital Certificates. 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

The DocuSign Root CA operator will validate and authenticate all Sub-CAs' requests for renewal. The multi-party controlled procedures and PMA approval for CA renew or re-key are the same those for the original certificates.

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

No stipulation.

3.4 Identification and Authentication for Revocation Request

No DocuSign Sub-CA certificates will be revoked without explicit approval from the DocuSign PMA.

The DocuSign Sub-CA operator will manually process requests for revocation of DocuSign Subscriber Digital Certificates.

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, are the only entities from which certificate applications are accepted for additional Sub-CA Digital Certificates. Furthermore, all sub-CA certificate issuance requires explicit PMA approval.

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

The Root CA operator only issues certificates at the request of the PMA. The Root CA operator validates that the use of the issued certificates in the DocuSign service are consistent with the request of the PMA.

Sub-CAs will 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.

A Relying Party provides 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

The DocuSign CAs and RAs, as part of the DocuSign service, verify and authenticate each Certificate Applicant, as described in Sections 1.4 and 3.2.

4.2.2 Approval or Rejection of Certificate Applications

Sub-CA certificate applications are approved or rejected based on outcome of the procedures in Section 4.1.

The DocuSign Service approves 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

Sub-CA certificate applications are always processed in the timeline specified by the PMA.

4.3 Certificate Issuance

4.3.1 RA Actions During Certificate Issuance

See Section 1.4.

4.3.2 CA Actions During Certificate Issuance

The CA will ensure that the public and Private Keys are bound to the correct Certificate Applicant's name, as specified by the Relying Party, and generate a properly formed Digital Certificate.

Issuance:

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

After issuance:

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

4.3.3 Notification to Certificate Subject of Certificate Issuance

The DocuSign Service notifies the certificate subject when a certificate is being issued on their behalf. This happens as part of the signing flow; see Section 1.4.

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

The PMA authorizes issuance of all DocuSign CA certificates, and is notified upon completion of that activity.

No stipulation is made for Subscriber certificates.

4.5 Key Pair and Certificate Usage

4.5.1 Certificate Subject Private Key and Certificate Usage

DocuSign protects all Private Keys from unauthorized use via the DocuSign Service and administrative controls on the DocuSign CAs. Disclosure to third parties is protected against by use of HSMs and the fundamental design principle of not allowing Private Keys to leave HSMs except in the case of secured backups. See Section 6.

No stipulation beyond those in Section 1.4.

4.5.2 Relying Party Public Key and Certificate Usage

Relying parties are instructed, via the Relying Party agreement, to ensure that the Public Key and associated Digital Certificate are used only for appropriate purposes as identified in certificate extensions (See Section 7).

No stipulation for certificate usage beyond that in Section 1.4.

4.6 Certificate Renewal

4.6.1 Circumstance for Certificate Renewal

DocuSign CAs will renew certificates prior to expiration to maintain continuity. An overlap period is always used to ensure continuity.

Digital Certificates issued by DocuSign CAs are never renewed after expiration.

4.6.2 Who May Request Renewal

A recognized DocuSign technical representative will submit Sub-CA Digital Certificate renewal requests, which are approved by the PMA prior issuance. Sub-CA renewal will be a multi-person procedure as specified in Section 5.2.2 and will require 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

DocuSign CAs will not re-key Digital Certificates.

4.7.1 Circumstance for Certificate Re-key

DocuSign CAs will not re-key Digital Certificates.

4.7.2 Who May Request Certification of a New Public Key

No stipulation.

4.7.3 Processing Certificate Re-keying Requests

No stipulation.

4.7.4 Notification of New Certificate Issuance to Certificate Subject

No stipulation.

4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate

No stipulation.

4.7.6 Publication of the Re-keyed Certificate by the CA

No stipulation.

4.7.7 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 the DocuSign CA, a Digital Certificate will only be revoked when explicitly ordered to do so by the PMA.

4.9.2 Who Can Request Revocation

Any Digital Certificate issued by the DocuSign CA can only be revoked upon request from the DocuSign PMA. 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.

4.9.3 Procedure for Revocation Request

For the DocuSign CA, Digital Certificates will be revoked, and included in a CRL, upon receipt of authorization to do so by the PMA.

4.9.4 Revocation Request Grace Period

For the DocuSign CA, the revocation request grace period is 5 business days.

4.9.5 Time within which CA Must Process the Revocation Request

For the DocuSign CA, the revocation request will be processed within 5 business days.

4.9.6 Revocation Checking Requirements for Relying Parties

Relying parties should always check that certificates have not been revoked before relying on signature.

4.9.7 CRL Issuance Frequency

For the DocuSign CA, CRLs are 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

Certificates will never be suspended.

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 the DocuSign CA, the status of Digital Certificates is made available in a CRL, published to the DocuSign 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 the DocuSign CA, subscriptions 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

The location and construction of the facility that will house CA equipment and operations is in accordance with that afforded the most sensitive business and financial information. CA operations are 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

The physical security requirements pertaining to the DocuSign CAs includes:

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

When not in use:

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

The DocuSign Root CA is always deactivated after use. The deactivation process disables and powers down the CA and HSM, separates key activation materials into three parts such that all three parts are required for activation, and entrusts each of the three sets key activation materials to distinct parties. The key activation material resists tampering by way of tamper evident storage containers that are inventoried each time the Root CA is activated. The tamper evident containers are physically secured by the owner of that key activation material. No key activation material owner is ever granted access to another set of key activation material. The three sets of key activation materials only come together when authorized by the PMA and only in a formal scripted and archived ceremony.

The DocuSign Sub-CAs, since they are active when in operation, require different physical security controls. If the facility where an active Sub-CA resides is not continuously attended, the last person to depart sign-outs from that facility indicating 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 Sub-CA equipment occurs each time the facility is to be left unattended. At a minimum, the check verifies 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”);
- 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 Sub-CA's Private Key is physically moved from one location to another, then:

- The DocuSign PMA has provided authorization for that move.
- The HSM is deactivated and its activation materials are moved by separate means and by separate individuals.
- The HSM is protected from destruction, unauthorized disclosure, and unauthorized modification.

5.1.3 Power and Air Conditioning

The facility that houses the CA equipment is supplied with power and air conditioning sufficient to create a reliable operating environment.

5.1.4 Water Exposures

Facilities that house CAs are 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

Facilities that house CAs are constructed and equipped, and procedures are implemented, to prevent and extinguish fires or other damaging exposure to flame or smoke.

5.1.6 Media Storage

When not in operation, the cryptographic modules storing the Root CA Private Key are secured as described in section 5.1.2.

When not in operation, the cryptographic modules storing the Sub-CA Private Key are stored in a secure room in encrypted form.

5.1.7 Waste Disposal

CAs operators have 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 the Root CA, system backups, sufficient to recover from system failure, are made on a periodic schedule. Backups are 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 is stored at an offsite location (separate from the Root CA equipment). The backup is stored at a site with physical and procedural controls commensurate to that of the operational Root CA system.

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

For DocuSign CAs, the following are the trusted Roles:

- 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;
- Key Activation Material owners: (Root CA only) use key activation materials during PMA authorized ceremonies; secure key activation materials when Root CA is not active.
- 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 the DocuSign Root CA, multi-person control is utilized for all uses of the Root CA Private Key.

For the creation and initial use of the Root CA, including the generation of the key pair, a formal ceremony was required. Participating in the ceremony are three distinct roles. No one person can act in more than one role. The Administrator administers the Root CA and HSM, and owns media and passwords to utilize the Private Key. A Key Activation Material owner generates and later holds a portion of the keys used to initialize and startup the HSM, as well as shut it down. Another Key Activation Material owner creates and later holds a separate portion of the initialization keys, used to initialize the HSM.

For normal use of the Root CA, this multi-party control is accomplished by leaving the Root CA powered off and inactive when not in use. A formal ceremony is required to power it on; and at the end of each ceremony, it is powered off. The Administrator and Key Activation Material owners are required for each ceremony.

If the Root CA needed to be restored from backup, again the same three parties are needed.

When not in use, media needed to perform all steps listed above are stored in secure containers where only that role has access.

No stipulation for Sub-CAs.

5.2.3 Identification and Authentication for Each Role

For the DocuSign CA, a person occupying a trusted role is authenticated before being permitted to perform any action for that role or identity.

5.2.4 Roles Requiring Separation of Duties

For activities pertaining to the DocuSign CAs, Administrators and Auditors are not the same person.

5.3 Personnel Controls

5.3.1 Qualifications and Experience Requirements

For the DocuSign CAs, personnel engaged in the PKI are suitably qualified and experienced.

5.3.2 Background Check Procedures

For the DocuSign CAs, vetting processes used for trusted personnel are owned and maintained by DocuSign HR.

5.3.3 Training Requirements

For the DocuSign CAs, CA Operators are appropriately trained. Topics include the operation of the CA software and hardware, operational and security procedures, and the stipulations of this CPS and local guidance.

5.3.4 Retraining Frequency and Requirements

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 the DocuSign CAs, if an unauthorized action takes place then appropriate action will 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 the DocuSign CAs, contractor personnel employed to perform functions pertaining to the CA meet the personnel requirements set forth in this CPS.

5.3.8 Documentation Supplied to Personnel

For the DocuSign CAs, documentation sufficient to define duties and procedures for each role is provided to the personnel filling that role.

5.4 Audit Logging Procedures

5.4.1 Types of Events Recorded

For the DocuSign CA, security auditing capabilities of the underlying CA equipment operating system are enabled during installation and operation. The following events are recorded:

For the Root CA:

- Root CA software admin activity;
- Root CA Signer Private Key generation;
- Root CA Digital certificate issuance;
- Sub-CA Digital certificate issuance;
- Sub-CA Digital certificate revocation request;
- Sub-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 Root CA equipment, Key Activation Materials, Key Activation Material owners, or any secure container used to support Root CA security.

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

For each auditable event, the record includes:

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

Audit logs will be generated automatically and periodically backed up.

5.4.2 Frequency of Processing Log

For the DocuSign Offline Root CA audit logs are reviewed every time the Root CA is brought online.

For Online Sub-CAs, audit logs are reviewed periodically.

Action taken, as a result of these reviews, is documented.

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

5.4.3 Retention Period for Audit Log

The information generated on the CA equipment is kept on the CA equipment, or on a secure server that retrieves audit log information from the CA. Audit logs are available for one year (See Section 5.5)

5.4.4 Protection of Audit Log

For the DocuSign Root CA, logs are stored within the offline Root CA. These are reviewed at each Ceremony to ensure no activity occurred since the last Ceremony. Only the administrator (SA) of the Root CA has access to these logs and only during a formal ceremony.

For the DocuSign Sub-CAs, logs are generated in the CA by the HSM for all key usage, and by the DocuSign service for events leading up to key usage.

5.4.5 Audit Log Backup Procedures

For the Root CA, logs are backed up at each ceremony. Multi-party control, as described in section 5.2.2, is required for all access to these backups. One backup is securely stored at the same location as the Root CA, another backup copy is stored at an off-site location.

For the Sub-CAs, audit logs are pulled from HSM equipment and stored within the DocuSign Service along with other DocuSign Service logs.. Multiple copies of these logs are maintained in multiple, geo-dispersed locations where strict ISO certified security controls are in place.

5.4.6 Audit Collection System (Internal vs. External)

Automated audit processes will 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

The CA systems and their components are routinely assessed for vulnerabilities and known weaknesses.

5.5 Records Archive

5.5.1 Types of Events Archived

For the DocuSign Offline Root CA, copies of logs are maintained as described in section 5.4.5. This archival contains all logged content as described in 5.4.1.

For DocuSign Sub-CAs, the events described in 5.4.1 are recorded and copies are maintained as described in 5.4.5. Because of the continuous availability of these logs and the nature of the DocuSign server, there is no need for additional archival. As with the recorded events, these copies will be detailed enough to establish the validity of a signature and of the operation of the PKI in accordance with the CPS.

5.5.2 Retention Period for Archive

For DocuSign CAs, archive data will 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 is be required by law.

5.5.3 Protection of Archive

For the DocuSign CA, archive data will be protected to ensure there is no unauthorized disclosure or modification. Archive media will be stored in a safe, secure storage facility separate from the CA itself.

5.5.4 Archive Backup Procedures

For the DocuSign CA, the archive facility will support backups.

5.5.5 Requirements for Time-Stamping of Records

For the DocuSign CA, archive data will 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

DocuSign PMA or designated representative are granted timely access to archive information when requested.

5.6 Key Changeover

For the DocuSign CA, DocuSign certificates are never re-keyed (see Section 4.7).

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

For the DocuSign CA, in the event of suspected compromise of a CA, it will be investigated to determine the nature and the degree of damage. If the CA is 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 will be issued.

Revoked CA Digital Certificates in Relying Party trust stores (Operating Systems, Browsers, Applications, etc.) will need to 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

When computing resources, software, and data are corrupted backups will be utilized as needed and as possible to restore.

5.7.3 CA Private Key Compromise Procedures

For the DocuSign CA, compromised CA Private Keys will be revoked. Compromised CA Private Keys are never used for any reason. CAs with compromised Private Keys will generate new key pairs and will be issued new certificates. This issuance will require the authorization of the PMA as with any CA certificate issuance. 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

In the case of a disaster in which the CA equipment is damaged and inoperative:

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

5.8 CA and RA Termination

In the event a DocuSign CA terminates, or ceases operation, the CA will 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 the DocuSign CA, CA keys are generated in FIPS 140-2 Level 3 compliant, evaluated/certified cryptographic modules. Key pairs remain on the device and do not leave the device except for authorized and documented backups.

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

For the DocuSign CA, Subscriber keys are generated and stored in a FIPS 140-2 Level 3 compliant, evaluated/certified cryptographic module. Subscriber key pairs are not duplicated or backed up. The DocuSign service is such that more than one key pair and certificate per subscriber could exist.

6.1.2 Private Key Delivery to Certificate Subject

For DocuSign CAs, Private Keys are never provided to the Subscriber (see Section 1.4).

6.1.3 Public Key Delivery to Certificate Issuer

For Sub-CAs, the Certificate Subject's Public key is delivered to the Root CA via manual means.

For the Offline Root CA Certificate and Subscriber Certificates, the Certificate Subject's Public Key is generated within the same FIPS compliant device as its issuing CA.

6.1.4 CA Public Key Delivery to Relying Parties

For the DocuSign CA, CA Public Keys are 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 makes the CA Public Keys available to facilitate signature validation.

6.1.5 Key Sizes

For DocuSign issued certificates, all keys are 2048 bits, see section 7 for specifics.

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

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

6.2.2 Private Key Multi-Person Control

For the DocuSign CA, all access to Root CA Private Keys utilizes multi-person control; see Sections 5.2.1 and 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 the DocuSign Root CA, Private Keys are backed up under multi-person control, as required in Sections 5.2.1 and 5.2.2. No more than a single copy of the Private Key is stored at the CA's location (i.e., only the operational and backup key are stored at the CA's location). Additional copies are moved off-site and accountability for them is maintained.

For DocuSign CAs and Subscriber Certificates, no Private Keys are backed up.

6.2.5 Private Key Archival

No stipulation.

6.2.6 Private Key Transfer into or from a Cryptographic Module

DocuSign Root CA Private Keys never leave the cryptographic module, except for during secure and authorized backups.

DocuSign Sub-CAs and Subscriber Private Keys never leave the cryptographic module.

6.2.7 Private Key Storage on Cryptographic Module

DocuSign CA Private Keys are stored on the HSM Signing Engine and are encrypted when not in use.

6.2.8 Method of Activating Private Keys

For the DocuSign Root CA, activation of the Root CA Private Key always utilizes multi-person control, as specified in Sections 5.2.1 and 5.2.2.

DocuSign Sub-CAs are online and used when a request is provided to the Sub-CA.

Subscriber Private Keys are activated by the DocuSign service on behalf of the Subscriber and their authenticated interaction with the DocuSign Service.

6.2.9 Methods of Deactivating Private Keys

Root CA Private Keys are stored in a FIPS 140-2 level 3 certified HSM. When not in use these keys are deactivated by powering off this HSM. The media holding the Root CA Private Key is stored in a secure container (see Section 5.1.6). This action requires multi-person control, as specified in Section 5.2.2.

DocuSign Sub-CA Private Keys are available during issuance and revocation. The DocuSign Service controls their use, but they remain active within the HSM Signing Engine.

Subscriber Private Keys are available during document signing. The DocuSign Service controls their use, but they remain active within the HSM Signing Engine.

For DocuSign Sub-CA Private Keys and Subscriber Private Keys, the Keys are maintained within the same HSM Signing Engine device and they remain active during normal operation. When needed, removing its activation key disables the HSM Signing Engine, and that also deactivates all keys maintained within.

6.2.10 Method of Destroying Private Key

No stipulation.

6.2.11 Cryptographic Module Rating

Level 3.

6.3 Other Aspects of Key Management

6.3.1 Public Key Archival

For the DocuSign CA, Public Keys are archived along with Digital Certificates. For CAs this is done in the repository. For the Sub-CA's and Subscribers Public Keys are stored along with Digital Certificates in documents as part of the DocuSign Service document archival.

6.3.2 Certificate Operational Periods/Key Usage Periods

For the Root CA certificate, validity is limited to 45 years or less.

For the Sub-CAs certificate, validity is limited to 10 years or less.

For the Subscriber certificates, validity is limited to 3 years or less, not including renewal times.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

For DocuSign Root CA Private Keys, activation data generation and installation happens only within a formally scripted and recorded Ceremony. See sections 5.2.1 and 5.2.2 for details.

For the DocuSign Sub-CA, CA Private Keys and Subscriber Private Key activation data generation and installation occurs entirely within the HSM Signing Engine. These Private Keys are activated via the processes and conditions outlined in Section 1.4.

6.4.2 Activation Data Protection

For the DocuSign Root CA, activation data to invoke Private Keys is protected from disclosure by a combination of cryptographic and physical access control mechanisms. See sections 5.2.1 and 5.2.2.

For DocuSign sub-CA and subscriber certificates, activation data to invoke Private Keys is protected by the technical controls associated with the DocuSign Service and physical controls associated with the location of the HSM Signing Engines.

6.4.3 Other Aspects of Activation Data

Before the DocuSign Root CA Private Key activation data is entered, the media storing the Root CA's Private Key are retrieved from the locked container as part of a DocuSign PMA approved Root CA ceremony. See Sections 5.2.1 and 5.2.2.

No stipulation for Sub-CAs or Subscriber Digital Certificates.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

The DocuSign CAs and its ancillary parts contained within the DocuSign Service address the following security technical requirements by means of functions provided by operating systems, or through a combination of operating system, software, and physical safeguards:

- 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

The System Development Controls for the DocuSign CA and DocuSign Service are as follows:

- For commercial off-the-shelf software, the software will be designed and developed under a formal, documented development methodology.
- For hardware and software developed specifically for a particular CA, the applicant will demonstrate that security requirements were achieved through a combination of software verification & validation, structure.
- Where open source software has been utilized, the software will demonstrate that security requirements were achieved through software verification & validation and structured development/life-cycle management.
- Proper care is taken to prevent malicious software from being loaded onto the CA equipment.
- Hardware and software updates will 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

The configuration of DocuSign CAs as well as any modifications and upgrades are documented and controlled. A formal change management methodology is used for installation and ongoing maintenance of DocuSign CAs and the DocuSign Service.

Because the Root CA is offline, tamper evidence controls coupled with the separation of ownership and custody of key activation materials provide a mechanism for detecting any unauthorized modification to the Root CA software or configuration.

6.6.3 Life Cycle Security Ratings

No stipulation.

6.7 Network Security Controls

The DocuSign Root CA is offline. It is never connected to any public or private network other than the one that connects the CA to the HSM during PMA authorized ceremonies.

DocuSign Sub-CAs are protected to prevent unauthorized access, tampering, and denial-of-service by virtue of controls associated with the DocuSign Service. Communications of sensitive information to and from CAs are protected using point-to-point encryption and strong authentication.

6.8 Time Stamping

Times asserted in Subscriber Digital Certificates will be accurate to within three minutes of the DocuSign Service system clock.

For the DocuSign Root CA, since it is offline, manual means are used to ensure system time is maintained. This manual step is part of each ceremony.

For DocuSign Sub-CAs, the Network Time Protocol (NTP) is used to ensure system time is maintained.

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 are 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

The DocuSign CAs and the DocuSign Service supporting them are audited against the CP and this CPS at least once per year.

8.2 Identity and Qualifications of Assessor

The auditor will demonstrate competence in the field of compliance audits. The DocuSign PMA identifies the compliance auditor.

8.3 Assessor's Relationship to Assessed Entity

The compliance auditor is an independent 3rd party as determined by the DocuSign PMA.

The DocuSign PMA determines whether a compliance auditor meets this relationship requirement.

8.4 Topics Covered By Assessment

The compliance audit of the CA verifies that the CA is implementing all provisions of a CP and CPS 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 the CP or this CPS 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. The report is treated as company confidential. The report identifies the version of the CP and CPS 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

The DocuSign CA may charge fees to for the issuance or renewal of Certificates.

9.1.2 Certificate Access Fees

The DocuSign CA does not charge fees for access of Certificates.

9.1.3 Revocation or Status Information Access Fee

The DocuSign CA does not charge fees for access to revocation or status information.

9.1.4 Fees for other Services

The DocuSign CA may charge fees for other services.

9.1.5 Refund Policy

The DocuSign CA does maintain a refund policy, in association with the DocuSign Service.

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

The DocuSign CA has sufficient financial resources to maintain operations and perform duties, and can reasonably 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

Within the DocuSign CA, the following records of Subscribers and Relying Parties, subject to Section 9.3.2, are kept confidential and ("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

Within the DocuSign CA, Certificates, Certificate revocation and other status information, CA repositories, and information contained within are not considered to be Confidential/Private Information. Information not expressly deemed Confidential/Private Information under Section 9.3.1 is considered neither confidential nor private.

This section is subject to applicable privacy laws.

9.3.3 Responsibility to Protect Confidential Information

The DocuSign CA secures confidential information from unauthorized access by third parties.

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

The DocuSign CA develops and publishes a Privacy Plan or Privacy Policy, which made available to CA participants such as Relying Parties, Subscribers, etc. This Privacy Policy can be found at: http://www.docusign.com/company/privacy-policy

9.4.2 Information Treated as Private

The DocuSign CA 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

The DocuSign CA does not treat as private any information made public within a certificate.

9.4.4 Responsibility to Protect Private Information

Recipients of private information secure it from unauthorized access and disclosure to third parties and 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 is not 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

The DocuSign CA is 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

For the DocuSign CA, Privacy Plans or Privacy Policies 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

The DocuSign CA maintains a PMA (Policy Management Authority)..

9.6.2 Generally Applicable Representations and Warranties

See 9.6.3.

9.6.3 CA Representations and Warranties

The DocuSign CA is 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 the DocuSign CA are instructed to:

- 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 the DocuSign CA are instructed to:

- 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 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 9.8.1 applies

DocuSign will 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 will 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 is 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 9.9.1 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 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 the DocuSign CA, this CP/CPS remains 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 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 CPS. Amendments will either be in the form of a document containing an amended form of the CPS or an update. Amended versions or updates will be linked to the DocuSign Repository.

Updates supersede any designated or conflicting provisions of the referenced version of the CPS. The PMA determines whether changes to the CPS 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 is 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 will contain new object identifiers for the Certificate policies corresponding to each Class of Certificate. Otherwise, amendments will 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 will 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 CPS is 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 CPS, including limitation of liability clauses, is found to be invalid or unenforceable, the remainder of the CPS is 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 include a force majeure clause protecting DocuSign.

9.17 Other Provisions

Not applicable.