DocuSign

Cloud Signing Service CP/CPS (Certificate Policy/Practice Statement)

November 2021

DocuSign, Inc.
Version 1.0
20211122

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.0.9	April 13, 2021	JN	Initial version, published to the DocuSign Repository in February 2021. This initial version of the DocuSign CP/CPS was authored in support of the DocuSign Cloud Signing Digital Signature functionality, due for commercial release in mid 2021.
V1.0	May 20, 2021	JN, EF, PA	Updated version with input from the DS-IL Product Development team.
V.1.1	June 30th, 2021	JN,DP	Updated version with final input from Legal, ready for sign-of by DocuSign Policy Management Authority
V1.2	January 28th, 2022	JN	Updated version to reflect the certificate revocation process.
V1.3	April 4th 2022	JN	Updated version to reflect Root CA signing of an issuing CA issuing Digital Seals and inclusion of correct Signer Object Identifiers (OIDs).

1 Introduction 9
1.1 Overview 9
1.2 Document Name and Identification 9
1.3 PKI Participants 9
1.3.1 Policy Management Authority 9
1.3.2 Certification Authority 9
1.3.3 Registration Authority 10
1.3.4 Subscriber 10
1.3.5 Relying Party 10
1.3.6 Certificate Applicant 10
1.3.7 Other Participants 10
1.4 Certificate Usage 10
1.5 Policy Administration 15
1.5.1 Organization Administering the Policy 15
1.5.2 Contact Person 15
1.5.3 Person Determining CP/CPS Suitability for the Policy 15
1.5.4 CP/CPS Approval Procedures 15
1.6 Definitions and Acronyms 15

2 Publication and Repository Responsibilities 17
2.1 Repositories 17
2.2 Publication of certification information 17
2.3 Time or Frequency of Publication 17
2.4 Access Controls on Repositories 18

3 Identification and Authentication 18
3.1 Naming 18
3.1.1 Types of Names 18
3.1.2 Meaningfulness 19
3.1.3 Anonymity or Pseudonymity of Certificate Subjects 19
3.1.4 Rules for Interpreting Various Name Forms 19
3.1.5 Uniqueness of Names 19
3.1.6 Recognition, Authentication, and Role of Trademarks 19
3.2 Initial Identity Validation 19
3.2.1 Method to Prove Possession of Private Key 19
3.2.2 Authentication of Organization Identity 19
3.2.3 Authentication of Subject Identity 20
3.2.4 Non-verified Certificate Subject Information 20
3.2.5 Validation of Authority 20
3.2.6 Criteria for Interoperation 20

3.3 Identification and Authentication for Re-key Requests 20
3.3.1 Identification and Authentication of Re-Key and Renewal Requests 20
3.3.2 Identification and Authentication of Re-Key and Renewal After Revocation 20
3.4 Identification and Authentication for Revocation Request 20

4 Certificate Life-Cycle 20
4.1 Certificate Application 21
4.1.1 Who Can Submit a Certificate Application 21
4.1.2 Enrollment Process and Responsibilities 21
4.2 Certificate Application Processing 21
4.2.1 Performing Identification and Authentication Functions 21
4.2.2 Approval or Rejection of Certificate Applications 21
4.2.3 Time to Process Certificate Applications 21
4.3 Certificate Issuance 21
4.3.1 RA Actions During Certificate Issuance 21
4.3.2 CA Actions During Certificate Issuance 22
4.3.3 Notification to Certificate Subject of Certificate Issuance 22
4.4 Certificate Acceptance 22
4.4.1 Conduct Constituting Certificate Acceptance 22
4.4.2 Publication of the Certificate by the CA 22
4.4.3 Notification of Certificate Issuance by the CA to Other Entities 22
4.5 Key Pair and Certificate Usage 22
4.5.1 Certificate Subject Private Key and Certificate Usage 22
4.5.2 Relying Party Public Key and Certificate Usage 22
4.6 Certificate Renewal 23
4.6.1 Circumstance for Certificate Renewal 23
4.6.2 Who May Request Renewal 23
4.6.3 Processing Certificate Renewal Requests 23
4.6.4 Notification of New Certificate Issuance to Certificate Subject 23
4.6.5 Conduct Constituting Acceptance of a Renewal Certificate 23
4.6.6 Publication of the Renewal Certificate by the CA 23
4.6.7 Notification of Certificate Issuance by the CA to Other Entities 23
4.7 Certificate Re-Key 23
4.7.1 Circumstance for Certificate Re-key 23
4.7.2 Who May Request Certification of a New Public Key 23
4.7.3 Circumstance for Certificate Re-key 24
4.7.4 Who May Request Certification of a New Public Key 24
4.7.5 Processing Certificate Re-keying Requests 24
4.7.6 Notification of New Certificate Issuance to Certificate Subject 24
4.7.7 Conduct Constituting Acceptance of a Re-keyed Certificate 24
4.7.8 Publication of the Re-keyed Certificate by the CA 24

4.7.9 Notification of Certificate Issuance by the CA to Other Entities 24
4.8 Modification 24
4.8.1 Circumstance for Certificate Modification 24
4.8.2 Who May Request Certificate Modification 24
4.8.3 Processing Certificate Modification Requests 24
4.8.4 Notification of New Certificate Issuance to Certificate Subject 24
4.8.5 Conduct Constituting Acceptance of Modified Certificate 24
4.8.6 Publication of the Modified Certificate by the CA 24
4.8.7 Notification of Certificate Issuance by the CA to Other Entities 25
4.9 Certificate Revocation and Suspension 25
4.9.1 Circumstances for Revocation 25
4.9.2 Who Can Request Revocation 25
4.9.3 Procedure for Revocation Request 25
4.9.4 Revocation Request Grace Period 25
4.9.5 Time within which CA Must Process the Revocation Request 25
4.9.6 Revocation Checking Requirements for Relying Parties 25
4.9.7 CRL Issuance Frequency 25
4.9.8 Maximum Latency for CRLs 25
4.9.9 On-line Revocation/Status Checking Availability 25
4.9.10 On-line Revocation Checking Requirements 26
4.9.11 Other Forms of Revocation Advertisements Available 26
4.9.12 Special Requirements Re Key Compromise 26
4.10 Certificate Status Services 26
4.10.1 Operational Characteristics 26
4.10.2 Service Availability 26
4.10.3 Optional Features 26
4.11 End of Subscription 26
4.12 Key Escrow and Recovery 26
4.12.1 Key Escrow and Recovery Policy and Practices 26
4.12.2 Session Key Encapsulation and Recovery Policy and Practices 26

5 Management, Operational, and Physical Controls 26
5.1 Physical Controls 26
5.1.1 Site Location and Construction 26
5.1.2 Physical Access 27
5.1.3 Power and Air Conditioning 27
5.1.4 Water Exposures 27
5.1.5 Fire Prevention and Protection 27
5.1.6 Media Storage 27
5.1.7 Waste Disposal 27
5.2 Procedural Controls 28

5.2.1 Trusted Roles 28
5.2.2 Identification and Authentication for Each Role 28
5.2.3 Roles Requiring Separation of Duties 28
5.3 Personnel Controls 28
5.3.1 Qualifications and Experience Requirements 28
5.3.2 Background Check Procedures 28
5.3.3 Training Requirements 28
5.3.4 Retraining Frequency and Requirements 28
5.3.5 Job Rotation Frequency and Sequence 29
5.3.6 Sanctions for Unauthorized Actions 29
5.3.7 Independent Contractor Requirements 29
5.3.8 Documentation Supplied to Personnel 29
5.4 Audit Logging Procedures 29
5.4.1 Types of Events Recorded 29
5.4.2 Frequency of Processing Log 29
5.4.3 Retention Period for Audit Log 29
5.4.4 Protection of Audit Log 29
5.4.5 Audit Log Backup Procedures 29
5.4.6 Audit Collection System (Internal vs. External) 29
5.4.7 Notification to Event-Causing Subject 30
5.4.8 Vulnerability Assessments 30
5.5 Records Archive 30
5.5.1 Types of Events Archived 30
5.5.2 Retention Period for Archive 30
5.5.3 Protection of Archive 30
5.5.4 Archive Backup Procedures 30
5.5.5 Requirements for Time-Stamping of Records 30
5.5.6 Archive Collection System (Internal or External) 30
5.5.7 Procedures to Obtain and Verify Archive Information 30
5.6 Key Changeover 30
5.7 Compromise and Disaster Recovery 30
5.7.1 Incident and Compromise Handling Procedures 30
5.7.2 Computing Resources, Software, and/or Data Are Corrupted 31
5.7.3 CA Private Key Compromise Procedures 31
5.7.4 Business Continuity Capabilities After a Disaster 31
5.8 CA and RA Termination 31

6 Technical Security Controls 31

6.1 Key Pair Generation and Installation 31
6.1.1 Key Pair Generation 31
6.1.2 Private Key Delivery to Certificate Subject 31

6.1.3 Public Key Delivery to Certificate Issuer 31
6.1.4 CA Public Key Delivery to Relying Parties 32
6.1.5 Key Sizes 32
6.1.6 Public Key Parameters Generation and Quality Checking 32
6.1.7 Key Usage Purposes (as per X.509v3 key usage field) 32
6.2 Private Key Protection and Cryptographic Module Engineering Controls 32
6.2.1 Cryptographic Module Standards and Controls 32
6.2.2 Private Key Multi-Person Control 32
6.2.3 Private Key Escrow 32
6.2.4 Private Key Backup 32
6.2.5 Private Key Archival 32
6.2.6 Private Key Transfer into or from a Cryptographic Module 32
6.2.7 Private Key Storage on Cryptographic Module 32
6.2.8 Method of Activating Private Keys 33
6.2.9 Methods of Deactivating Private Keys 33
6.2.10 Method of Destroying Private Key 33
6.2.11 Cryptographic Module Rating 33
6.3 Other Aspects of Key Management 33
6.3.1 Public Key Archival 33
6.3.2 Certificate Operational Periods/Key Usage Periods 33
6.4 Activation Data 33
6.4.1 Activation Data Generation and Installation 33
6.4.2 Activation Data Protection 33
6.4.3 Other Aspects of Activation Data 34
6.5 Computer Security Controls 34
6.5.1 Specific Computer Security Technical Requirements 34
6.5.2 Computer Security Rating 34
6.6 Life-Cycle Security Controls 34
6.6.1 System Development Controls 34
6.6.2 Security Management Controls 34
6.6.3 Life Cycle Security Ratings 35
6.7 Network Security Controls 35
6.8 Time Stamping 35

7 Certificate Profiles Format 35
7.1 Certificate Profile 35
7.1.1 Root CA Certificate Profile 35
7.1.2 Sub-CA Certificate Profile 36
7.1.3 DocuSign Subscriber Certificate Profile 37
7.2 CRL Profile 38
7.2.1 DocuSign Root CRL Profile 39

7.2.2 DocuSign Sub-CA CRL Profile 39
SubCA CRL publication 40

8 Compliance Audit and Other Assessments 40
8.1 Frequency of Audit or Assessments 40
8.2 Identity and Qualifications of Assessor 40
8.3 Assessor's Relationship to Assessed Entity 40
8.4 Topics Covered By Assessment 40
8.5 Actions Taken As A Result of Deficiency 40
8.6 Communication of Results 40

9 Other Business and Legal Matters 40
9.1 Fees 41
9.1.1 Certificate Issuance/Renewal Fees 41
9.1.2 Certificate Access Fees 41
9.1.3 Revocation or Status Information Access Fee 41
9.1.4 Fees for other Services 41
9.1.5 Refund Policy 41
9.2 Financial Responsibility 41
9.2.1 Insurance Coverage 41
9.2.2 Other Assets 41
9.2.3 Insurance/warranty Coverage for End-Entities 41
9.3 Confidentiality of Business Information 41
9.3.1 Scope of Confidential Information 41
9.3.2 Information Not Within the Scope of Confidential Information 42
9.3.3 Responsibility to Protect Confidential Information 42
9.4 Privacy of Personal Information 42
9.4.1 Privacy Plan 42
9.4.2 Information Treated as Private 42
9.4.3 Information Not Deemed Private 42
9.4.4 Responsibility to Protect Private Information 42
9.4.5 Notice and Consent to use Private Information 42
9.4.6 Disclosure Pursuant to Judicial/Administrative Process 42
9.4.7 Other Information Disclosure Circumstances 43
9.5 Intellectual Property Rights 43
9.6 Representations and Warranties 43
9.6.1 PMA 43
9.6.2 Generally Applicable Representations and Warranties 43
9.6.3 CA Representations and Warranties 43
9.6.4 RA Representations and Warranties 43
9.6.5 Certificate Subject Representations and Warranties 43
9.6.6 Relying Parties Representations and Warranties 44

9.6.7 Subscriber Representation and Warranties 44
9.6.8 Representations and Warranties of Other Participants 44
9.7 Disclaimers of Warranties 44
9.8 Limitations of Liability 44
9.8.1 PMA 44
9.8.2 Other Participants. 45
9.9 Indemnities 45
9.9.1 PMA 45
9.9.2 Other Participants 45
9.10 Term and Termination 45
9.10.1 Term 45
9.10.1.1 CP/CPS Term 45
9.10.1.2 Other Agreements 45
9.10.2 Termination 46
9.10.2.1 CP/CPS Termination 46
9.10.2.2 Other Agreements 46
9.10.3 Effect of Termination and Survival 46
9.10.3.1 CP/CPS 46
9.10.3.2 Other Agreements 46
9.11 Individual Notices and Communications With participants 46
9.12 Amendments 46
9.12.1 Procedure for Amendment 46
9.12.1.1 CP/CPS 46
9.12.1.2 CP/CPS and Participant Agreements. 46
9.12.2 Notification Mechanism and Period 46
9.12.3 Circumstances Under Which OID Must Be Changed 47
9.13 Dispute Resolution Provisions 47
9.14 Governing Law 47
9.15 Compliance with Applicable Law 47
9.16 Miscellaneous Provisions 47
9.16.1 Document Incorporated into CP/CPS 47
9.16.2 Entire agreement 47
9.16.3 Assignment 47
9.16.4 Severability 48
9.16.5 Waiver 48
9.16.6 Attorneys' Fees 48
9.16.7 Force Majeure 48
9.17 Other Provisions 48

1 Introduction

1.1 Overview

The DocuSign® CP/CPS (Certificate Policy/Practice Statement) defines the policies, procedures, and requirements that DocuSign requires participants (see Section 1.3) to comply with when issuing and managing Digital Certificates. This CP/CPS is under the control of 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 Cloud Signing Certificate Policy. The OID (Object Identifier) "1.3.6.1.4.1.42482.2.1.1.4" is included in subscriber certificates to indicate that they are issued in accordance with this CP/CPS.

1.3 PKI Participants

1.3.1 Policy Management Authority

The DocuSign PMA (Policy Management Authority) approves the CP/CPS and any changes to it. The PMA comprises 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/CPS.

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:

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

The PMA Charter can be consulted on request.

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/CPS. 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 . There are two pathways to certificate issuance;

- Responding to an email containing a url requesting a signature, and;
- Single-Sign on where the certificate subject's identity is contained in corporate directory

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 and email address appear in the Digital Certificates' Subject Distinguished Name field, and who uses the DocuSign Cloud Signing Service in accordance with any current DocuSign Subscriber Agreement or any published Terms of Use governing the DocuSign Cloud Signing 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 Cloud Signing Service. The Relying Party uses the Digital Certificate created by the DocuSign Cloud Signing Service to validate the digital signature applied by the Subscriber, and who uses the DocuSign Cloud Signing Service in accordance with any current DocuSign Relying Party Agreement. In this signing scheme, the Sender of the document to be signed is the Relying Party, and the Subscriber is the receiver of the email with the url to the DocuSign

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.

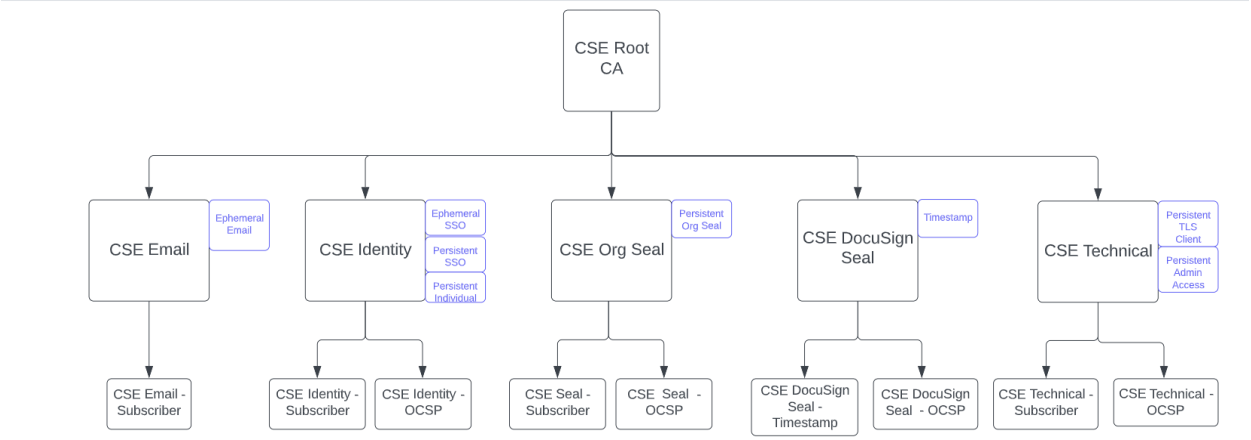
1.3.7 Other Participants

This Root Certificate Authority[1] sits at the apex of a tree of trust under which a number of issuing Certificate Authorities process requests for, and manage the lifecycle of, a number of certificate and participant types including;

[1] The software is based on DocuSign's Core Signing Engine (software) and hardware suite, with key generation taking place on Qualified Signature Creation Devices (QSCDs)

- Ephemeral certificates (with a validity period of 12 minutes) issued to, and designed to facilitate, digital signatures triggered by urls send to possessors of a given email address;
- Persistent certificates (with a validity period of one year=365 days) issued to individuals whose identity data resides in a corporate directory. These certificates are for internal corporate use only and are designed to facilitate, amongst other purposes, single-sign-on (SSO) within the organization in question;
- Persistent certificates issued to North America based Notaries - the issuance process in this case is based on a rigorous process of identity verification prior to certificate issuance - these certificates have a validity period of two years;
- Seal Certificates issued to authorized officers acting on behalf of organizations

The current hierarchy of the structure is as follows;



This CP/CPS is intended to cover the Root and Issuing Certificate Authorities across the complete hierarchy.

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 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 are expressly prohibited.
- Any Subscriber certificate SHALL only be used in the manner described in the remainder of this section.

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

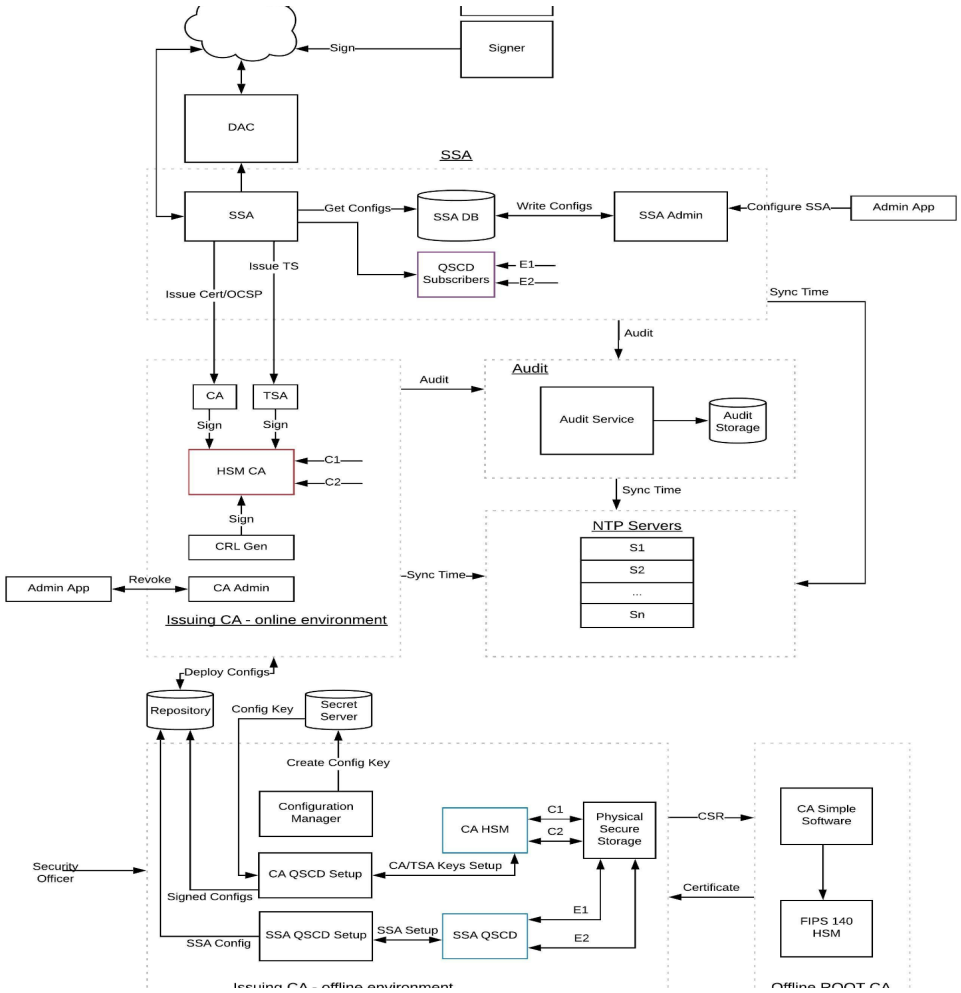


Figure 1 - The DocuSign Cloud Signing Service Digital Signature Service

- Relying Party [RP]
  - Relying Parties determine the trust required for digital signing transactions managed by the DocuSign Cloud Signing Service. The DocuSign Cloud Signing Service executes against that determination.
  - Relying Parties are commonly referred to as “Senders” within the DocuSign Cloud Signing Service.
  - Relying parties use "local methods" to pre-establish the “locally determined” identity of the Subscribers , 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 interpersonal communications (including emails, phone calls, etc.),
    - Personal connections, and
    - Other means.

- Relying parties require the Subscriber to digitally sign documents within the DocuSign Cloud Signing Service. Relying Parties engage Subscribers by inserting into the DocuSign Cloud Signing 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 Cloud Signing 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 Cloud Signing Audit Server 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 Parties should expect the following from the DocuSign Cloud Signing 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 Cloud Signing Service on behalf of the Subscriber).

- Subscriber (SUB)
  - For the DocuSign Cloud Signing Service Digital Signature functionality, Subscribers are required by the Relying Party to digitally sign a document within the DocuSign Cloud Signing Service.
  - Subscribers can receive requests for signing either via email or membership of a directory held by a third-party organization and accessed via an an authorization server by the Relying Party
  - Subscribers are not required to obtain a signing Digital Certificate prior to transacting with the Relying Party . The DocuSign Cloud Signing 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 Cloud Signing 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

- DocuSign Cloud Signing Service [DS]
  - The Service controls access to the DocuSign Cloud Signing Service Digital Signature functionality.
  - The Service controls access to the ability to use supported Digital Certificate Types, including the DocuSign Cloud Signing Service certificate, for supported digital signature operations, which are described by this CP/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 Cloud Signing Service Digital Signature functionality within the DocuSign Cloud Signing 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 Cloud Signing Service 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.
    - Completed and digitally signed documents, which can be exported from the DocuSign Cloud Signing Service. These documents are digitally signed by the Subscriber as per the requirements of the Relying Party, and include the Root, Sub-CA and Subscriber Digital Certificates.
    - High-availability Subordinate Certificate Authorities:
      - 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 Signing Engine .
    - An Root Certificate Authority:
      - The Root CA resides in a secure location, as described within this CP/CPS.

        - The Root CA is generated using Certification Authority software and the Root CA keys are generated and stored in a secure environment.
    - The Service maintains a secure infrastructure that contains information required to manage the transaction, including:
        - A Certificate Type, to distinguish the unique CA being asked to provide the Digital Certificate for a given digital signature transaction.
    - The Service controls access to the Certificate Authority, including:
        - The Signing Engines which power the Sub-CAs,
        - The cryptographic operations that run on the Signing Platform, and
    - The Audit Server maintains logs of activity related to the transaction.
    - The Service will produce evidence of all completed transactions:
        - Documents, digitally signed by the DocuSign Cloud Signing Service, are tamper evident,
        - Documents, digitally signed by the Subscriber, provide identity assurance and compliance with Relying Party requirement,
        - Documents, embedded with a Subscriber's Digital Certificate, contain reliable information about the DocuSign Cloud Signing Service and the Subscriber,
        - An Audit Trail containing standard transaction detail in the DocuSign Cloud Signing Service, and
        - A tamper-evident Certificate of Completion containing additional warranty stipulations and transaction detail.
- DocuSign Certificate Authority [CA]
    - The DocuSign Cloud Signing 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/CPS and CP/CPS.
- DocuSign Root Certificate Authority [CA]
    - The DocuSign Cloud Signing 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/CPS and CP/CPS.
    - The DocuSign Root CA was created using a documented Key Ceremony, based on public key infrastructure (PKI) best practices and policies.

1.5 Policy Administration

1.5.1 Organization Administering the Policy

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

1.5.2 Contact Person

All communications regarding this CP/CPS 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/CPS Suitability for the Policy

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

1.5.4 CP/CPS Approval Procedures

The DocuSign PMA SHALL approve the CP/CPS and any amendments according to the PMA's bylaws. The DocuSign PMA determines whether an amendment to this CP/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/CPS (Certificate Policy)" means a document that establishes the requirements for how a CA is to be governed, managed, and operated.

"CP/CPS (Certification Practice Statement)" means a document that articulates specific procedures and practices that adhere to the CP/CPS-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" (Certificate Revocation List) / "OCSP" (Online Certificate Status Protocol) of the Subscriber. For this DocuSign Cloud Signing Service Digital Signature functionality, utilizes CRLs or OCSP to determine DocuSign's certificate status information relied upon to validate the digital signature generated on behalf

"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 Cloud Signing 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 keys and provides cryptographic processing.

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

"Repository" means a publicly available collection of 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.

"Secure Container" means a physical room, a strongbox, a tamper-evident envelope, or password-protected PFX file .

"Signing Engine" refers to the infrastructure and components used for the purpose of digitally signing documents. In the case of the DocuSign Cloud Signing Service, the Signing Engine device is a CA, a key manager and associated HSMs that will generate, store and manage Subscriber Private Keys 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 Cloud Signing Service certificates (see Section 1.4) are embedded in the signed document by the DocuSign Cloud Signing 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/CPS, DocuSign SHALL generate CRLs produced at a frequency of no less than once every 12 months. If a CA has been compromised, DocuSign SHALL generate a new CRL within five business days of 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/CPS, Sub-CA certificates SHALL be published within one business day of issuance.

For any CA governed by this CP/CPS, Sub-CA generated CRLs SHALL be produced at a frequency no less than every 7 days. Enforcement is achieved through revocation mechanisms and shall be compliant with IETF 5280.

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

For any CA governed by this CP/CPS, 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 Cloud Signing 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/CPS, 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:
  - cn=DocuSign Inc Root CA
- Subordinate CA:
  - cn=DocuSign NA# CA#, where # is an integer,
  - o=DocuSign, Inc.
  - c=US
- Subscriber (email):
  - cn=[name provided by RP]
  - email=[email address provided by RP]
- Subscriber (SSO):
  - cn=[name provided by RP]
  - email=[email address provided by IDP]
  - o=name of Organization acting as the Identity Provider (IDP)

When the naming element is DirectoryString (i.e., O=) 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/CPS, 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/CPS, CA names SHALL be unique across the whole DocuSign Cloud Signing Service.

No stipulation for Subscriber names.

3.1.6 Recognition, Authentication, and Role of Trademarks

For any CA governed by this CP/CPS, 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/CPS, 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/CPS, the 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 Cloud Signing Service on behalf of the Subscriber, at the behest of the Relying Party (see Section 1.4).

3.2.2 Authentication of Organization Identity

For certificates issued on the basis of membership of a corporate directory (SSO workflow) authentication of the organizational identity shall form part of the process. A defined procedure shall be established to achieve this verification mechanism. The organization attribute in SSO based Subscriber certificates is taken from the name established during the onboarding process of that organization.

3.2.3 Authentication of Subject Identity

For email certificates the level of identity verification shall be restricted to the subject responding to messages and links contained in email sent to the subject’s email address.

For SSO based certificates, the subject identity shall form part of the organizational verification process.

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/CPS, the CAs SHALL only issue Digital Certificates or generate status information in support of the DocuSign Cloud Signing 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 Cloud Signing Service. All other uses of a DocuSign Digital Certificate, including the DocuSign Cloud Signing Service 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/CPS, 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 as those for the original certificate.

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/CPS, DocuSign may revoke the Sub-CA.

For any CA governed by this CP/CPS, 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 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 Cloud Signing Service. The DocuSign Cloud Signing 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 non-DocuSign CAs, no stipulations at this time.

For the DocuSign CA, Sub-CAs SHALL only issue certificates as part of the DocuSign Cloud Signing 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 Cloud Signing Service.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

For any CA governed by this CP/CPS, CAs or RAs (which could be Relying Parties or IDPs) SHALL verify and authenticate each Certificate Applicant (including signing requests from operators of issuing/subCAs), 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/CPS, the Sub-CA certificate applications SHALL be approved or rejected based on the outcome of the procedures in Section 4.1.

For the DocuSign CA, the DocuSign Cloud Signing 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/CPS, 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/CPS, 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/CPS, 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.
- Sub-CAs SHALL issue Subscriber certificates within Signing Engines. Key generation, key management, certificate requests, and certificate issuance MUST all occur within the Signing Engines.

After Issuance:

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

4.3.3 Notification to Certificate Subject of Certificate Issuance

For any CA governed by this CP/CPS, the service will notify the certificate subject that 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 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/CPS, 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/CPS, 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

No stipulation.

4.6.1 Circumstance for Certificate Renewal

For any CA governed by this CP/CPS, 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

No stipulation.

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

No stipulation.

4.7.1 Circumstance for Certificate Re-key

No stipulation.

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

No stipulation.

4.7.3 Circumstance for Certificate Re-key

No stipulation.

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 to 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/CPS, 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 comprise 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/CPS, any Digital Certificate issued can be revoked. 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.

4.9.3 Procedure for Revocation Request

For any CA governed by this CP/CPS, 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). A separate document describes the revocation procedure in detail and is available on request.

4.9.4 Revocation Request Grace Period

For any CA governed by this CP/CPS, 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/CPS, 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/CPS, 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.

4.10 Certificate Status Services

4.10.1 Operational Characteristics

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

- The CA MUST provide manual or electronic monitoring for unauthorized intrusion;
- The CA MUST ensure that a Windows access log is maintained;
- The CA MUST ensure that only 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. Activation data SHALL either be memorized, or recorded and stored in a secure container and SHALL NOT be stored with the cryptographic module.

If the facility is not continuously attended, a security check of the facility housing the CA equipment SHALL occur to 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 HSM containing a CA's Private Key is physically moved from one location to another (i.e., not during normal activation), then the HSM MUST be protected from destruction, unauthorized disclosure, and unauthorized modification.

5.1.3 Power and Air Conditioning

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

5.1.7 Waste Disposal

For any CA governed by this CP/CPS, 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 .

5.2 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/CPS, the people selected to fill these roles MUST be ordinarily 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 Number of Persons Required Per Task

For any CA governed by this CP/CPS, Root CA Private Key actions MAY be performed by a CA Operator. Actions include:

- Generation of CA keys;

- Access to CA Private Key;

No stipulation for Sub-CAs.

5.2.2 Identification and Authentication for Each Role

The roles and responsibilities of CA Personnel shall be defined in accordance with ETSI 419-401 and 319-411-2 and shall include but be restricted to the roles defined in section 5.2.3

5.2.3 Roles Requiring Separation of Duties

For any CA governed by this CP/CPS, 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 operators prior to performing any Root CA Private Key actions

5.3 Personnel Controls

5.3.1 Qualifications and Experience Requirements

For any CA governed by this CP/CPS, personnel engaged in the PKI SHALL be suitably qualified and experienced. Background checking and credential verification SHALL take place.

5.3.2 Background Check Procedures

A vetting process is used for personnel engaged in trusted roles.

5.3.3 Training Requirements

Training SHALL take place for all personnel as appropriate.

5.3.4 Retraining Frequency and Requirements

No stipulation.

5.3.5 Job Rotation Frequency and Sequence

No stipulation.

5.3.6 Sanctions for Unauthorized Actions

For any CA governed by this CP/CPS, appropriate action SHALL be taken to ensure disciplinary or other appropriate action is taken if an unauthorized action takes place. 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/CPS, contractor personnel employed to perform functions pertaining to the CA SHALL meet the personnel requirements set forth in this CP/CPS.

5.3.8 Documentation Supplied to Personnel

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

5.4 Audit Logging Procedures

The PKI incorporates an audit server which records all key events and which is configured according to a detailed policy governing elements such as event types recorded, frequency of processing and retention periods. Additional IT functions apply to the audit server service in terms of backup procedures, equipment installation, notification, vulnerability assessments, archiving, retention, protection and time stamping. This is not a publicly available document and may be available on request to parties with a legitimate interest.

5.4.1 Types of Events Recorded

As per the above statement.

5.4.2 Frequency of Processing Log

As per the above statement.

5.4.3 Retention Period for Audit Log

As per the above statement.

5.4.4 Protection of Audit Log

As per the above statement.

5.4.5 Audit Log Backup Procedures

As per the above statement.

5.4.6 Audit Collection System (Internal vs. External)

As per the above statement.

5.4.7 Notification to Event-Causing Subject

As per the above statement.

5.4.8 Vulnerability Assessments

As per the above statement.

5.5 Records Archive

Records are archived in accordance with DocuSign policies and applicable legislation where relevant.

5.5.1 Types of Events Archived

No stipulation.

5.5.2 Retention Period for Archive

No stipulation.

5.5.3 Protection of Archive

No stipulation.

5.5.4 Archive Backup Procedures

No stipulation..

5.5.5 Requirements for Time-Stamping of Records

No stipulation.

5.5.6 Archive Collection System (Internal or External)

No stipulation.

5.5.7 Procedures to Obtain and Verify Archive Information

No stipulation .

5.6 Key Changeover

For any CA governed by this CP/CPS, Root CA keys MAY be re-keyed (see Section 4.7). Sub-CAs MAY be re-keyed (Section 4.7) if the Root CA reconfirms the identity of the Sub-CA, which the Root CA either accepts or rejects.

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/CPS, including the DocuSign CA, the CA SHALL be investigated in order 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 MUST be issued.

Revoked CA Digital Certificates in Relying Party trust stores (Operating Systems, Browsers, Applications, etc.) should be replaced by the Relying Party with the 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

No stipulation.

5.7.3 CA Private Key Compromise Procedures

For any CA governed by this CP/CPS, compromised CA Private Keys should be revoked. 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/CPS, 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/CPS, in the event a CA terminates, or ceases operation, the CA MUST destroy its Signing Engine, which contains the CA's Private Key. Termination procedures will follow procedures laid down in ETSI 319 410 v2.3.0 and ETSI 319 411-2.

6 Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

For any CA governed by this CP/CPS, CA keys MUST be generated in the Signing Engine and the CA Private Keys MUST NOT leave the Signing Engine.

Subscriber Keys MUST be generated by the DocuSign Cloud Signing Service, and Private Keys MUST be stored in a Signing Engine. 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 any CA governed by this CP/CPS, 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/CPS, 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 Cloud Signing Service. (Note that in this workflow, the Relying Party is the sender of the document to be signed). Otherwise, the DocuSign Cloud Signing Service utilizes CA Public Keys to facilitate signature validation.

6.1.5 Key Sizes

For any CA governed by this CP/CPS, Keys MUST be 3072 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/CPS, the relevant standard for cryptographic modules SHALL be certified to either Common Criteria EAL4+ certified or FIPS PUB 140-2.

6.2.2 Private Key Multi-Person Control

For any CA governed by this CP/CPS, Root CA Private Keys must be under dual-access control.

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

No stipulation.

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/CPS, Root CA Private Keys SHALL never leave the cryptographic module of the Signing Engine.

For any CA governed by this CP/CPS, Sub-CA and Subscriber Private Keys SHALL never leave the cryptographic module of the Signing Engine.

6.2.7 Private Key Storage on Cryptographic Module

For any CA governed by this CP/CPS, Private keys SHALL be encrypted when not in use.

6.2.8 Method of Activating Private Keys

For any CA governed by this CP/CPS, activation of the Root CA Private Key MAY be under single-person control.

For any CA governed by this CP/CPS, 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 Cloud Signing 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/CPS, 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).

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

For any CA governed by this CP/CPS, 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

No stipulation.

6.3 Other Aspects of Key Management

6.3.1 Public Key Archival

No stipulation.

6.3.2 Certificate Operational Periods/Key Usage Periods

Root CA certificate lifetimes SHALL be limited to 20 years or less.

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

For any CA governed by this CP/CPS, 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/CPS, 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/CPS, 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/CPS, 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 by a CA Operator.

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/CPS, 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;
- 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/CPS, 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 and validation as well as structure development lifecycle management.
- Where open source software has been utilized, the software SHALL demonstrate that security requirements were achieved through software verification and validation as well as structure development lifecycle management.
- 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 the open source community does not disclose security relevant information.

6.6.2 Security Management Controls

No stipulation.

6.6.3 Life Cycle Security Ratings

No stipulation.

6.7 Network Security Controls

For any CA governed by this CP/CPS, 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 Cloud Signing 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 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

Attribute	Sub-Attribute	Value
Subject		
Common Name	DocuSign Inc Root CA	
Organization	DocuSign Inc.	
OrganizationUnit	DocuSign Compliance	
Country	US	
Public Key	RSA3072	
Key usage	Sign CRL, Sign Certificate Digital Signature Offline CRL Signing	
Authority Key Identifier	Random	
Subject Key Identifier	Random (as above)	
BasicConstraints	None	

7.1.2 Sub-CA Certificate Profile

Attribute	Sub-Attribute	Value	Compliance
Subject	common name	DocuSign Cloud Signing CA-US-Email DocuSign Cloud Signing CA-US-SSO	Support as input an addition to CSR
Public Key		RSA3072	
Key usage		Sign CRL, Sign Certificate	
ExtendedKeyUsage			
Authority Key Identifier		TBD by Root CA	
Subject Key Identifier		Random	
CDP		TBD by Root CA	
AIA		TBD by Root CA	
BasicConstraints		0	

7.1.3 DocuSign Subscriber Certificate Profile

Email-based:

Attribute	Sub-Attribute	Value
Subject	Subscriber email address	

Common Name	DocuSign Cloud Signing CA-US-Email	Support as input an addition to CSR
Public Key	RSA2048	
Key usage	Document Signing Acrobat Authentic Documents	
Authority Key Identifier	TBD by SubCA	
Subject Key Identifier	Random	
CDP	TBD by SubCA	
AIA	TBD by SubCA	

SSO-based:

Attribute	**Sub-Attribute**	**Value**
Subject	Subscriber Common Name as per IdP	
Common Name	DocuSign Cloud Signing CA-US1-SSO	Support as input an addition to CSR
Public Key	RSA2048	
Key usage	Document Signing Acrobat Authentic Documents	
Authority Key Identifier	TBD by Root CA	
Subject Key Identifier	Random	

CDP	TBD by SubCA	
AIA	TBD by SubCA	

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.
X509v3 CRL Number:	Non-critical as per RFC 5280.
Revoked Certificates	Revoked certificates 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 certificates 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.

SubCA CRL publication

1. CRLs are published every 12 hours and expire within one week.
2. CRL should not include expired certificates.

8 Compliance Audit and Other Assessments

8.1 Frequency of Audit or Assessments

No stipulation.

8.2 Identity and Qualifications of Assessor

No stipulation.

8.3 Assessor's Relationship to Assessed Entity

No stipulation.

8.4 Topics Covered By Assessment

No stipulation.

8.5 Actions Taken As A Result of Deficiency

No stipulation.

8.6 Communication of Results

No stipulation.

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/CPS MAY charge fees for the issuance or renewal of Certificates.

9.1.2 Certificate Access Fees

Any CA governed by this CP/CPS MAY charge fees for access to Certificates.

9.1.3 Revocation or Status Information Access Fee

Any CA governed by this CP/CPS SHALL NOT charge fees for access to revocation or status information.

9.1.4 Fees for other Services

Any CA governed by this CP/CPS MAY charge fees for other services.

9.1.5 Refund Policy

Any CA governed by this CP/CPS 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/CPS 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"):

- 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 or private.

This section is subject to applicable privacy laws.

9.3.3 Responsibility to Protect Confidential Information

Any CA governed by this CP/CPS 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/CPS 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/CPS 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/CPS 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/CPS, 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/CPS 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 processes 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/CPS, 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 Cloud Signing Service, DocuSign Digital Certificates and any other publication whatsoever originating from DocuSign, including this CP/CPS.

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/CPS 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/CPS SHALL be in charge of:

- Validation and publication of this CP/CPS, and the respective CA's CP/CPS;
- Compliance of issued certificates as per this CP/CPS, and the respective CA's CP/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/CPS SHALL:

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

9.6.7 Subscriber Representation and Warranties

Subscribers using certificates from any CA governed by this CP/CPS 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 CP/CPS;
- Only use these certificates and keys for document signing;
- Verify and adhere to the obligations defined in this CP/CPS 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 9.8.1 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/CPS.

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/CPS.
- 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 9.9.1 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/CPS Term

For any CA governed by this CP/CPS, 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/CPS Termination

For any CA governed by this CP/CPS, 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 Modification

9.10.3.1 CP/CPS

Notified changes are appropriately marked by an indicated version. Following publications, changes become applicable 15 days thereafter.

9.10.3.2 **Other Agreements**

9.11 Individual Notices and Communications With participants

For any CA governed by this CP/CPS, 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/CPS

9.12.1.2 CP/CPS and Participant Agreements.

The DocuSign Policy Management Authority (PMA) may make amendments to this CP/CPS. Amendments shall either be in the form of a document containing an amended form of the CP/CPS 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 CP/CPS. The PMA shall determine whether changes to the CP/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 shall be within the PMA's sole discretion.

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

9.16.2 Entire agreement

Not applicable.

9.16.3 Assignment

This CP/CPS 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/CPS are assignable by the parties, by operation of law (including as a result of merger or a transfer of a controlling interest in voting securities) or otherwise, provided such assignment is undertaken consistent with this CP/CPS 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/CPS, including limitation of liability clauses, is found to be invalid or unenforceable, the remainder of the CP/CPS shall be interpreted in such a manner as to represent the original intentions of the parties.

9.16.5 Waiver

No provision of this CP shall be modified, waived or discharged unless the modification, waiver or discharge is agreed to in writing. No waiver by DocuSign of any breach of, or of compliance with, any condition or provision of this CP by any Subscriber or Relying Party shall be considered a waiver of any other condition or provision or of the same condition or provision at another time.

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.