DocuSign Certificate Policy for Cross-Certification with TSCP Bridge

DocuSign®

DocuSigned by:

Michael Yatsko

737376E78772458...

Version	2.6	**Pages**	104
Status	☐ Draft	☒ Final	
Author		DocuSign Inc.	

Diffusion List	☒ External	☒ Internal
	Public	Public

History				
Date	Version	Author	Information affected	Verified by
26/09/2018	0.1	DocuSign	Creation of document	EM
06/11/2018	0.2	DocuSign	Review by MY	MY
03/12/2018	0.3	DocuSign	Integration of comments	EM
21/12/2018	1.0	DocuSign	Creation of version 1.0	
01/02/2019	1.1	DocuSign	Integration of comments from TSCP	
11/02/2019	1.2	DocuSign	Integration of comments from TSCP	
11/02/2019	1.3	DocuSign	Creation of the clean version	
08/04/2019	1.4	DocuSign	Integration of comments from DocuSign TSCP Root CA audit	MY
13/08/2019	1.5	DocuSign	Modification of the CP because of the fact that only DocuSign France hosts the CA (dedicated one and dedicated ones for some Customers). CA and Subscriber Certificate profile has been modified in accordance too.	
25/10/2019	1.6	DocuSign	Modification due to review and CPS writing and adding modification due to version 10.0 of TSCP CP (remote access for CA)	
18/12/2019	1.7	DocuSign	Integration of comments from TSCP	

08/01/2020	1.8	DocuSign	Integration of remote access to the CA under conditions allowed by the Federal Bridge.	
15/01/2020	1.9	DocuSign	Integration of review of CA profile and CRL profile and comments from TSCP.	
29/01/2020	2.0	DocuSign	Clean version after review with TSCP auditors.	
10/07/2020	2.1	DocuSign	Add the Seal certificate template and management.	
22/07/2020	2.2	DocuSign	Add OID for Device.	
23/07/2020	2.3	DocuSign	Modification of Device Certificate profile to introduce an additional OU in the DN of Subject	
29/07/2020	2.4	DocuSign	Integration of TSCP comments.	
31/07/2020	2.5	DocuSign	Modification of dedicated CA template for Customer to include optional choice to have the OID policy for Device if Customer wants to have Device Certificate in addition to physical person Certificate.	
17/08/2020	2.6	DocuSign	Modification of EKU for Device Certificate.	

SUMMARY

1 INTRODUCTION

TSCP is the Transglobal Secure Collaboration Program. TSCP operates a PKI Bridge Certificate Authority (CA) and Trust Framework that is cross-certified with the Federal Bridge CA.

DocuSign decided to cross certify with the TSCP Bridge by creating a Root CA (RCA) and dedicated Certification Authority (CA) to support each Customer of DocuSign desiring to join the TSCP Trust Framework. These CAs can only issue subscriber certificate for signature usage.

This Certificate Policy (CP) defines multiple assurance levels for use by DocuSign to facilitate operation within the TSCP Trust Framework. The level of assurance refers to the strength of the binding between the public key and the individual or device whose subject name is cited in the certificate, the mechanisms used to control the use of the private key, and the security provided by the PKI itself.

The RCA enables interoperability among Customers and those within the extended TSCP Trust Framework in a peer-to-peer fashion.

The RCA issues certificates only to CAs designated by DocuSign for sole purpose of issuing certificates to its Customers. The RCA may also issue certificates to individuals who operate the TBCA. The RCA certificates issued to cross-certified CAs act as a conduit of trust. Only the RCA is cross-certified with TSCP CA (TBCA).

Any use of or reference to this CP outside the purview of DocuSign is completely at the using party's risk. An Entity shall not assert the CP OIDs in any certificates not issued by CA signed by RCA, except in the policyMappings extension establishing an equivalency between a DocuSign OID and an OID of TSCP.

This CP is consistent with the Internet Engineering Task Force (IETF) Public Key Infrastructure X.509 (IETF PKIX) RFC 3647, Certificate Policy and Certification Practices Framework.

The terms and provisions of this CP shall be interpreted under and governed by applicable law (see section 9.14).

1.1 OVERVIEW

1.1.1 CERTIFICATE POLICY (CP)

CA cross-certificate and Subscriber certificates contain one or more registered certificate policy object identifiers (OID), which may be used by a Relying Party to decide whether a certificate is trusted for a particular purpose. The OID corresponds to a specific level of assurance established by this Certificate Policy (CP) which shall be available to Relying Parties.

Each certificate issued by the RCA and CA will assert the appropriate level of assurance in the certificate Policies extension as decided by DocuSign.

1.1.2 RELATIONSHIP BETWEEN THE CP & CPS

A CP states what assurance can be placed in a certificate issued by the CA and RCA. The Certification Practice Statement (CPS) states how the CA and RCA establishes that assurance. A CPS shall be more detailed than the CP with which it aligns.

1.1.3 RELATIONSHIP BETWEEN THE TBCA CP AND THIS CP

DocuSign maps this CP to one of the levels of assurance in the TSCP CP (see section 1.2).

The relationship between this CP and the TSCP CP is asserted in RCA certificates issued by the TBCA in the policyMappings extension.

1.1.4 SCOPE

This CP governs RCA and CA and Subscriber certificates and associated key pairs and cross-certification operation. Subscriber certificates are limited to only one type as described in section 10. Customer issues subscriber certificates from the CA and manages Subscriber's key pair hosted in a Digital Signature Appliance (DSA) which is stored on the premises of the Customer facility.

1.1.5 INTERACTION WITH PKIS EXTERNAL TO DOCUSIGN, INC.

Only the RCA is cross-certified to the TBCA. The CAs are all subordinate to the RCA.

1.2 DOCUMENT IDENTIFICATION

There are 2 levels of assurance in this Certificate Policy, which are defined in subsequent sections. These level of assurance has a dedicated Object Identifier (OID), to be asserted in certificates issued by the CA and RCA.

RCA asserts this OIDs in policyMappings extensions of certificates issued to the TBCA. These policy OIDs are a sub-assignment of DocuSign Inc.'s Private Enterprise Number (PEN) registered in the IANA PEN Registry (1.3.6.1.4.1.42482). The PEN sub-assignment is allocated to TBCA policy OID as follows:

- Subscriber: Physical person: 1.3.6.1.4.1.42482.2.1.1.1.
- Subscriber: Device: 1.3.6.1.4.1.42482.2.1.1.3.

This OID is mapped to TSCP's OID as follow:

- 1.3.6.1.4.1.42482.2.1.1.1.: 1.3.6.1.4.1.38099.1.1.1.1 used to identify id-Medium.
- 1.3.6.1.4.1.42482.2.1.1.1.: 1.3.6.1.4.1.38099.1.1.1.2 used to identify MediumHardware.
- 1.3.6.1.4.1.42482.2.1.1.3.: 1.3.6.1.4.1.38099.1.1.1.13 used to identify MediumHardwareDevice.

1.3 PKI ENTITIES

The following are roles relevant to the administration and operation of the RCA and CA.

1.3.1 PKI AUTHORITIES

1.3.1.1 DOCUSIGN POLICY MANAGEMENT AUTHORITY (DS PMA)

The DocuSign PMA (DS PMA) owns this CP and represents the interest of DocuSign, Inc. The DS PMA is responsible for:

- Approving the Certificate Policy and all associated CPSs.
- Approving the technical part of the contract defined with Customers related to the implementation of the present CP by Customer.
- Managing relation and cross-certification with TSCP bridge.
- Notifying the TSCP PMA of any change to the infrastructure that has the potential to affect the TSCP Bridge operational environment at least two weeks and a day prior to implementation. All new artifacts (CA certificates, CRL DP, AIA and/or SIA URLs, etc.) produced as a result of the change shall be provided to the TSCP PMA within

24 hours following implementation. The notice period will begin to run upon written acknowledgement of the TSCP PMA.

- Approves RCA and CA creation, renewal and revocation.
- Define audit guide used to conduct internal audit on all PKI entities (RCA, CA, RA, Trusted Agent…).
- Approves cryptographic specification (algorithms used for signature, encryption, authentication, hash functions and key length, operational lifetime) for the PKI systems and any related change according a survey made on international standards and TSCP requirements.
- Defines procedures for Subscriber keys and certificates management that Customers shall apply.
- Approves Customer's RPS.
- Approves compliance between security practice documents and related policies (for instance CPS/CP and procedures/CP).
- Approves final annual internal audit report of all the PKI's components.
- Manage external audit of Customers and all PKI entities.
- Guarantees the validity and the integrity of the PKI's published information.
- Ensures that a proper process to manage security incidents within PKI components is in place.
- Arbitrates disputes relating to the PKI services and the use of certificates.

A complete description of DS PMA roles and responsibilities is provided in the DS Policy Management Authority Charter [DS PMA CHARTER].

1.3.1.2 DOCUSIGN OPERATIONS AUTHORITY (DS OA)

The DocuSign Operations Authority (DS OA) is the organization that operates and maintains the PKI entities, posting RCA and CA certificates and Certificate Revocation Lists (CRLs) into the DocuSign Repository, and ensuring the continued availability of the repository to all users. The Operational Authority acts upon approval of the DS PMA.

1.3.1.3 DOCUSIGN OPERATIONAL AUTHORITY ADMINISTRATOR (DS OAA)

The Administrator is the individual(s) within the DS Operational Authority who has principal responsibility for overseeing the proper operation of the PKI entities, including the Repository and who appoints individuals to the positions of Operational Authority Officers. The administrator approves the issuance of certificates to the other trusted roles operating the RCA and CAs. DS OAA is selected by and reports to the DS PMA.

As Customer is part of the DS OA, Customer will have also Administrator (Customer OAA) for overseeing the proper operation delegated to the Customer. These particulars Administrators are selected and approved by DS OAA and report to DS OAA.

1.3.1.4 DOCUSIGN OPERATIONAL AUTHORITY OFFICERS (DS OAO)

These officers are the individuals within the Operational Authority, selected by the Administrator, who operate the PKI entities and the Repository including executing the DS PMA direction to take actions to affect interoperability. The roles include Operational Authority Officer, Auditor, and Operator, all described in Section 5.2.1 of this CP.

As Customer is part of the DS OA, Customer will have also OAO (Customer OAO) for operating the proper operation delegated to the Customer. These particulars OAO are selected and approved by Customer OAA and report to Customer OAA.

1.3.1.5 DOCUSIGN PRINCIPAL CERTIFICATION AUTHORITY (PCA)

The DS Root CA, as PCA, will only be cross-certified with the TSCP Bridge CA.

1.3.1.6 DOCUSIGN ROOT CERTIFICATION AUTHORITY (DS RCA)

A Root CA (RCA) is a CA which is characterized by having itself as the issuer (i.e., it is self-signed). RCA can't be revoked in the normal manner (i.e. being included in an Authority Revocation List), and, when used as a Trust Anchor, must be transmitted or made available to any Relying Parties according to secure mechanisms outlined in section 6.1.4.

DocuSign is the Root CA for this CP. DS RCA is used to:

- Be cross-certified with TSCP only as a PCA.
- Issue CA certificates for DS CA only as in this CP. DocuSign shall ensure that no CA under its PKI shall have more than one trust path to the FBCA (regardless of path validation results).
- Revoke CA certificates.
- Generate logs for RCA operation.

DS Root CA will only be cross-certified with TSCP bridge CA. DS Root CA is not signed by any others CAs.

1.3.1.7 INTERMEDIATE CERTIFICATION AUTHORITY (ICA)

An Intermediate CA is a CA that is not a Root CA and whose primary function is to issue certificates to other CAs.

DS does not support Intermediate CAs.

1.3.1.8 DOCUSIGN CERTIFICATION AUTHORITY (DS CA)

A Signing CA is a CA whose primary function is to issue Certificates to Subscriber and CRL. A Signing CA does not issue Certificates to other CAs and cannot be a PCA. For each Customer, DS the Customer chooses one of the following:

- DocuSign Generates a CA dedicated to one Customer hosted and managed by DocuSign according rules and procedures defined by DS PMA;
- Uses the Dedicated CA of DocuSign.

DocuSign is in any case owner of all CAs for this CP. A DS CA is used to:

- Be signed only by the DS RCA.
- Issue Subscriber certificates and CRL.
- Revoke Subscriber certificates.
- Manage Subscriber's key pair centrally.
- Generate logs for CA operation.

CA can only manage Subscriber's Certificate and key pair only for Subscriber covered by Customer agreement established with DS.

In the present CP there 2 categories of CA:

- Generic CA: this CA is singed in the name of DocuSign and a Customer has its Subscriber issued Certificate by a CA containing only DocuSign info in the issuer DN of Subscriber Certificate. This CA is signed by the RCA.
- Customer dedicated CA: this type of CA are dedicated to only one Customer and a Customer has its Subscriber issued Certificate by a CA containing the Legal name of the Customer's entity in the CN value in the issuer DN of Subscriber Certificate. This CA is signed by the RCA.

1.3.1.9 CERTIFICATE STATUS AUTHORITY (CSA)

A CSA is an authority that provides status of certificates or certification paths. A CSA can be:

- Online Certificate Status Protocol (OCSP) Responders that provide revocation status of certificates
- Simple Certificate Validation Protocol (SCVP) Servers that validate certifications paths or provide revocation status checking services.

DocuSign and its Customers do not support this service.

1.3.2 REGISTRATION AUTHORITY (RA)

RA designates DocuSign that collects and verifies Subscriber identity and information for inclusion in the Subscriber’s public key certificate. The requirements for RAs in Entity PKIs are set forth elsewhere in this document. DS defines all procedures and rules and log type to have to manage RA operation.

DocuSign delegates some RA operation to Customer.

Procedures to manage Subscriber’s Certificate and key pairs are performed by Trusted Agent and specific Customer’s roles approved by DS PMA. A Customer is responsible to establish and maintain a list of all Trusted Agent and Customer’s roles that are allowed to manage Subscribers. A Trusted Agent can be employed by entities different from the Customer. In this case, legal entity which employs Trusted Agent shall have a contract to cover all aspect of Customer RPS delegated to the Trusted Agent. In this case, the contract shall be approved by the DS PMA before a Trusted Agent can perform identity verification services.

The Customer RPS shall give details on how RA and Trusted Agent are organized and performs their operation to manage Subscriber’s Certificate and key pair.

A Customer operates some RA services according to the Customer RPS and its associated procedures approved by DS PMA. A Customer can’t start operating RA operation without prior approval of the DS PMA and having signed an agreement with DS.

1.3.3 CARD MANAGEMENT SYSTEM (CMS)

The Card Management System is responsible for managing smart card token content.

DocuSign and its Customers do not support this service.

1.3.4 SUBSCRIBERS

In the case of this CP, a Subscriber is a natural person to whom a certificate and associated key pair is issued or a Device to seal documents in the name of a Customer. Subscribers are individuals with a contractual relationship with the Customer and enrolled by the Customer or Device under control of Customer. Where certificates are issued to devices, the entity must have a human sponsor who is responsible for carrying out Subscriber duties.

Customers shall maintain their Subscribers certificates in their repositories and associated key pair shall remain in the HSM provided by DocuSign. Subscribers, as the term is used in this CP, does not include or refer to CAs. However, the term “Subscriber” as used in this document refers only to those who request certificates for uses other than signing and issuing certificates or certificate status information.

1.3.5 AFFILIATED ORGANIZATIONS

In this CP, Subscriber certificates are always issued in conjunction with an organization that has a relationship with the Subscriber; this is termed affiliation. The organization affiliation will be indicated in the certificate in the field "O" of the subject

DN. Affiliated organizations, also referred to as Customers in this CP, are responsible for verifying the affiliation at the time of certificate application and requesting revocation of the certificate if the affiliation is no longer valid. For the present CP, only the Customer name will appear in the certificate issued to the Subscriber.

1.3.6 RELYING PARTIES

A Relying Party uses a Subscriber's certificate to verify the integrity of a digitally signed document and relies on the validity of the binding of the Subscriber's identity and affiliated organization to a Public Key. The Relying Party is responsible for deciding whether or how to check the validity of the certificate by checking the appropriate certificate status information. A Relying Party may use information in the certificate (such as certificate policy identifiers) to determine the suitability of the certificate for a particular use.

This CP makes no assumptions or limitations regarding the identity of Relying Parties and its relationship with Subscribers, CA, RCA, Customer and TSCP organization entities.

1.3.7 OTHER PARTICIPANTS

1.3.7.1 TSCP INC. (TSCP)

TSCP, Inc. is a nonprofit 501(c)(6), tax-exempt trade association incorporated in the State of Delaware and is led by its Chief Executive Officer. TSCP, Inc. is ultimately accountable for its PKI bridging services.

DS Root CA is cross-certified with TSCP bridge CA.

1.3.7.2 CUSTOMER

Customer is a Legal Entity different from DocuSign that has an agreement with DocuSign Inc to issue certificate to subscriber under this CP.

Customer is considered a delegated Registration Authority as some operations of RA are performed by the Customer. Therefore, there is dedicated RPS for each Customer.

The Customer designates entities that act as Trusted Agent. In the contract between Customer and DocuSign all Customer's obligations are included to cover operation made by Customer to implement some CP and CPS operation.

The DocuSign TSCP's service is fully audited by the PMA. When Trusted Agents are used, only a sample of Trusted Agents may be audited by the PMA (refer to section 8 below).

1.3.7.3 TRUSTED AGENT

A Trusted Agent is the entity that collects and verifies each Subscriber's identity and information on behalf of an RA. Information shall be verified in accordance with section 3.2 and communicated to the RA in a secure manner.

Trusted Agents are under contract with Customers. Trusted Agents are selected and designated by a Customer OAA according rules approved by DS OAA.

1.3.7.4 ADDITIONAL PARTICIPANTS

The Root CA and CA and more generally PKI authorities operating under this CP will require the services of other security, community, and application authorities, such as compliance auditors and attribute authorities. The CPS shall identify the parties responsible for providing such services, and the mechanisms used to support these services.

1.4 CERTIFICATE USAGE

1.4.1 APPROPRIATE CERTIFICATE USES

The sensitivity of the information processed or protected using certificates issued by CA will vary significantly. Relying Parties must evaluate the environment and the associated threats and vulnerabilities and determine the level of risk they are willing to accept based on the sensitivity or significance of the information. This evaluation is done by each Relying Party for its application and is not controlled by this CP.

To provide sufficient granularity, this CP specifies security requirements at one level of assurance. The following table provides a brief description of the appropriate uses for certificates at the selected level of assurance defined in this CP. These descriptions are intended as guidance and are not binding.

Assurance Level	Appropriate Certificate Uses
id-MediumHardware	This level is relevant to environments where threats to data are high or the consequences of the failure of security services are high. This may include very high value transactions or high levels of fraud risk.

1.4.2 PROHIBITED CERTIFICATE USES

No stipulation.

1.5 POLICY ADMINISTRATION

1.5.1 ORGANIZATION ADMINISTERING THE DOCUMENT

The DS PMA is responsible for all aspects of this CP.

1.5.2 CONTACT PERSON

Questions regarding this CP shall be directed to PMA, who can be reached at DS-PMA@docusign.com.

1.5.3 PERSON DETERMINING CERTIFICATION PRACTICES STATEMENT SUITABILITY FOR THE POLICY

The Certification Practices Statement (CPS) must conform to the corresponding Certificate Policy. The DS OAA is responsible for approving CPS and asserting whether the CPS conforms to this CP. The DS PMA shall commission an analysis to determine whether the CPSs (RCA CPS and all Customer's RPS) conform to this CP. The DS OAA shall receive a report and make the ultimate decision concerning the adequacy of the CPS. In each case, the determination of suitability shall also be based on an independent compliance auditor's results and recommendations. The compliance analysis shall be from a firm, which is independent from the entity being audited.

See Section 8 for further details.

1.5.4 CPS APPROVAL PROCEDURES

1.5.4.1 RCA CPS APPROVAL PROCEDURES

The CPSs shall provide (whether written or through the completion of a template) more detailed information than this CP. The CPSs shall specify how this CP shall be implemented to ensure compliance with the provisions of this CP.

DS OAA creates the RCA CPS and the generic Customer RPS template. Customer OAA completes the Customer RPS based on the CPS template provided by DS OAA. DS OAA control the content of the Customer RPS provided by Customer OAA. RCA CPS describes RCA, CA and RA practice. Customer RPS describes delegated RA, Trusted Agent and Subscriber key pair management practice.

The DS OAA shall prepare and submit the RCA CPS and each Customer RPS to the DS PMA for approval. If rejected, the identified discrepancies shall be resolved, and the CPS shall be resubmitted to the DS PMA.

The DS PMA shall commission RCA CPS compliance analysis prior to authorizing the DS OA to issue and manage RCA and CA Certificates asserting this CP.

1.5.4.2 CUSTOMER RPS APPROVAL PROCEDURES

The DS PMA shall commission for each Customer, a Customer RPS compliance analysis prior to authorizing the DS OA to issue and manage Subscriber Certificates asserting this CP. Subscriber certificates can only be issued by DS OA based on a Customer needs using either DocuSign Generic CA or Customer dedicated CA.

The Customer OAA shall transmit the Customers CPS, written to the format of the Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework [RFC 3647], to DS OAA for approval.

The following information shall accompany the CPS request:

- Customer’s RPS signed by the Customer OAA and DSF OAA.
- Signed Subscriber’s naming document (refer below in same section).
- Audit report from DS PMA about Customer RPS implementation that is applied to cover the present CP requirements.
- Any other requested information or documents asked from DS PMA in order to audit and control CPS request against the present CP requirements.

The following information shall be contained in the Subscriber naming document:

- Type of identity to set in the subscriber certificate (refer to section **Error! Reference source not found.** above).
- Legal name of the Customer to be used in the Subscriber certificate.
- CRL profile to be generated by the CA.
- Identity of the CA to be used to sign the subscriber certificate.
- Validity period of the Subscriber certificate.
- Cryptographic information of the subscriber certificate.
- Subscriber Certificate content.
- Customer OAA information:
  - The full name, including surname and given name(s).
  - The full legal name of Customer.
  - Professional phone number and email.
  - A reference to its national ID and the type of ID used to authenticate the person.
- DS OAO information:
  - The full name, including surname and given name(s).
  - The full legal name of DS Administrator company.
  - Professional phone number and email.
  - A reference to its national ID and the type of ID used to authenticate the person.
- DS OAA information:
  - The full name, including surname and given name(s).
  - The full legal name of DS Administrator company.
  - Professional phone number and email.
  - A reference to its national ID and the type of ID used to authenticate the person.

The Subscriber naming document shall be signed digitally by the 3 persons with means as described in CPS.DS PMA shall store copy of all ID used in signed document above. Subscriber naming document is part of the Customer RPS.

The DS PMA either determines that the Customer RPS meets the CP requirements or that the Customer RPS is not able to address remaining issues. When Customer RPS doesn't meet the CP requirement, then Customer shall be required to modify its practice to address the discrepancy.

If Customer is not able or not willing to address remaining discrepancies, then DS PMA ends the process and Subscriber certificate cannot be delivered. If Customer RPS fulfills the CP requirement, then Subscriber certificates can be issued.

The DS PMA shall be responsible for approving or rejecting the Customer RPS. In the case where the Customer CPS is compliant with this CP, the DS PMA approves the Customer RPS and continue the evaluation process. In the case where the Customer RPS is rejected, the DS PMA will ask the Customer to re-submit the Customer RPS with all required information.

After completion of a successful CPS analysis, the Customer's practice shall be audited by DS PMA as defined in section 8 below.

If Customer wants a dedicated CA to issue subscriber certificates, the Customer authorized representative shall submit the contract signed to use the DocuSign service cross-certified with the TSCP Bridge to PMA Chair indicating clearly this choice.

In any case, Customer authorized representative shall submit the contract signed to use the DocuSign service cross-certified with the TSCP Bridge to PMA Chair before to be authorized to issue Subscriber Certificate.

The DS PMA reviews the audit report of the Customer. The DS PMA either determines that the Customer meets the compliance audit requirements or that the Customer is not able to address remaining issues. When Customer doesn't meet the compliance audit requirement, then Customer shall be required to modify its practice to address any discrepancy.

If Customer is not able or not willing to address remaining discrepancies, then DS PMA ends the process and Subscriber certificate cannot be delivered to Customer. If the Customer's audit results in a report that demonstrates compliance with the CP requirements, Subscriber certificates can be issued,

1.5.5 WAIVERS

Waivers shall not be issued. Instead, CP and/or CPS changes shall be made or remediation activities shall be scheduled and implemented.

1.6 DEFINITIONS AND ACRONYMS

See Sections 14 and 15 of the CP.

2 PUBLICATION & REPOSITORY RESPONSIBILITIES

2.1 REPOSITORIES

DocuSign and its Customer shall operate multiple repositories to support all PKI operations. These repositories are used to hold information needed by an internal user of the PKI and by external users to support interoperation with other organizational PKI domains. These repositories shall contain the information necessary to support interoperation such as CA certificates, CRL files, and information on organizational policy (such as this Certificate Policy document itself).

2.1.1 REPOSITORY OBLIGATIONS

CAs may use a variety of mechanisms for posting information into a Repository as required by this CP. These mechanisms at a minimum shall include:

- Web Server System accessible through the Hypertext Transport Protocol (HTTP),
- Availability of the information as required by the certificate information posting and retrieval stipulations of this CP, and
- Access control and communication mechanisms when needed to protect repository information as described in later sections.

Optionally, an X.500 Directory Server System may also function as a Repository to complement a Web Server System. In such cases, the Repository shall be accessible through the Lightweight Directory Access Protocol (LDAP) and meet the availability and access control requirements as stated above.

In cases where a CA has multiple Repositories, the following rule shall apply to Repository references within certificates:

- All HTTP URI shall appear before LDAP URI

2.2 PUBLICATION OF CERTIFICATION INFORMATION

2.2.1 PUBLICATION OF CERTIFICATES AND CERTIFICATE STATUS

CA, RCA and Subscribers certificates shall only contain valid Uniform Resource Identifiers (URIs) that are accessible by relying parties.

DocuSign publishes RCA certificate, cross-certificate issued to or by RCA and CRL produced by RCA.

DocuSign shall publish all CA certificates issued by or to the RCA and all CRLs issued by the CA.

The PKI Repositories containing Certificates and CRL shall be deployed so as to provide high levels of reliability (24/24h & 7/7d at a rate of 99% availability or better).

2.2.2 PUBLICATION OF CA INFORMATION

DocuSign shall publish information concerning the RCA necessary to support use and operation of the service provided by the CP. The CP shall be publicly available on the DocuSign website (see https://www.docusign.com/trust/compliance/public-certificates).

Even if CP shall be published electronically by DocuSign, applicable RCA and Customers CPSs must be kept confidential (not published) by DocuSign and Customers.

2.2.3 INTEROPERABILITY

Where certificates and CRLs are published in directories, standards-based schemas for directory objects and attributes shall be implemented. Certificates and CRLs shall be published to an externally facing HTTP location to foster interoperability with external relying parties.

Where certificates and CRLs are published in directories, standards-based schemas for directory objects and attributes shall be implemented and shall be consistent with the Repository Profile.

See Section 11 for more details.

2.3 FREQUENCY OF PUBLICATION

This CP and any subsequent changes shall be made publicly available within thirty days of approval. Certificates and certificate status information shall be published as specified in sections 4.4.2, 4.9.7, 4.9.8, 4.9.9, and 4.9.10.

2.4 ACCESS CONTROLS ON REPOSITORIES

DocuSign and Customer shall protect any repository information not intended for public dissemination or modification.

Certificate status information (CRL) in DocuSign repository shall be publicly available through the Internet.

Direct and/or remote access to information in DocuSign repositories shall be determined by the PMA and controlled by DS OAA.

At a minimum, DocuSign repositories shall make RCA certificates, cross-certificate and CRLs issued by RCA, and CA certificates and CRLs issued by CA available to Relying Parties on the Internet,

Subscriber certificates that contain the UUID in the subject alternative name extension shall not be distributed via publicly accessible repositories (e.g., LDAP, HTTP).

3 IDENTIFICATION & AUTHENTICATION

3.1 NAMING

3.1.1 TYPES OF NAMES

The RCA and CA shall only generate and sign certificates that contain a non-null subject and issuer Distinguished Name (DN).

Certificates shall indicate that the Subscriber is associated with an Affiliated Organization by including the name of the Affiliated Organization in the distinguished name as an organization “O”.

All the exact content of DN for issuer and subject field of each type of certificate is described in section 10 below. Profile of certificate described in section 10 are the sole authorized to be issued under this CP.

3.1.2 NEED FOR NAMES TO BE MEANINGFUL

The certificates issued pursuant to this CP are meaningful and the names that appear in the certificates shall be understood and used by Relying Parties (humans). Names used in the certificates must identify the legal person which owns the CA and RCA in a meaningful way.

The identity (name) set in the Subscriber certificate is the built using at least one of first name and last name as written in official ID of the Subscriber or a pseudonym (see section 3.1.3). Subscriber identity is always set in field “CN” of the subject in certificate.

When DNs are used, the directory information tree must accurately reflect organizational structures.

A key pair can be linked with only a unique DN for each RCA, CA and Subscriber certificate.

Name space shall be limited as specified in Section 7.1.5.

3.1.3 ANONYMITY OR PSEUDONYMITY OF CERTIFICATE

RCA and CA certificates shall not contain anonymous or pseudonymous identities.

DNs in certificates issued to subscriber may contain a pseudonym to meet local privacy regulations as long as name space uniqueness requirements are met and as long as such name is unique and traceable to the actual entity. Trusted agent shall record the link between the real name of the subscriber as written in official ID and the pseudonym used for the subscriber in the certificate.

3.1.4 RULES FOR INTERPRETING VARIOUS NAME FORMS

Rules for interpreting name forms shall be contained in the applicable certificate profile (see section 10 and 3.1.1, 3.12 and 3.1.3). The DS PMA shall be the authority responsible for RCA and CA name space control. Customer shall be responsible for the authority responsible for Subscriber name space control.

Relying parties shall use the subject name contained in the certificate (refer to section 3.1.1) to identify the RCA, CA and Subscriber.

The CN field is not guaranteed to be unique for Subscriber.

3.1.5 UNIQUENESS OF NAMES

The DNs contained in the certificate of RCA and CA (refer to section 3.1.1 above) shall be unique in the RCA trust domain. The PMA controls that the RCA cross-certificate and the CA certificates are unique, by controlling the DN used in the RCA cross-certificate and the CA certificates and approving the RCA cross-certificate and CA certificate creation. The same CN shall not be given to two or more distinct CAs, cross-certificates, or RCAs representing distinct entities. Name (subject DN) uniqueness must be enforced by the Customer for the name space for subscriber certificates. Two distinct subscribers may have the same CN, but shall always have unique DNs.

Name uniqueness is not violated when multiple certificates are issued to the same entity.

Practice Note: Relying party applications may assume a one-to-one relationship between a certificate and a distinguished name / subject alternative name. However, such applications may not be interoperable with PKIs that issue multiple certificates to the same entity thereby creating a one-to-many relationship if only the distinguished name and/or subject alternative names are verified by the Relying Party application.

The applicable CPS shall specify how name (DN) uniqueness will be ensured, including in circumstances where a Person or device has the same name (CN) as a Person or device who has been issued a certificate in the past. This includes circumstances where a Person or device has left the organization at the time the next Person or device applies for a certificate thereby guaranteeing uniqueness of names over time.

3.1.6 RECOGNITION, AUTHENTICATION, AND ROLE OF TRADEMARKS

No stipulations.

3.1.7 NAME CLAIM DISPUTE RESOLUTION

The DS PMA and Customer will not knowingly use trademarks in names unless the Subscriber, Customer or DocuSign has the rights to use that name.

The DS PMA shall resolve or cause to be resolved any name collision brought to its attention in RCA and CA certificates.

The Customer shall resolve or cause to be resolved any name collision brought to its attention in Subscriber certificate that may affect interoperability. For that case, Customer can request advice from DS PMA to help to resolve the problem.

3.2 INITIAL IDENTITY VALIDATION

3.2.1 METHOD TO PROVE POSSESSION OF PRIVATE KEY

3.2.1.1 RCA AND CA

In the case where a key is generated by the RCA or CA either (1) directly on the party's hardware or software token; or (2) in a key generator that benignly transfers the key to the party's token, then proof or possession is not required.

In all cases where the party named in a certificate generates its own keys that party shall be required to prove possession of the private key that corresponds to the public key in the certificate request.

Practice Note: For signature keys, this may be done by the entity using its private key to sign a value and providing that value to the RCA. The RCA shall then validate the signature using the party's public key. The DS PMA may allow other mechanisms that are at least as secure as those cited here.

3.2.1.2 SUBSCRIBER

In the case where a key is generated by the CA either (1) directly on the party's hardware or software token; or (2) in a key generator that benignly transfers the key to the party's token, then proof or possession is not required. As subscriber's key pair never leave the CA equipment, then proof of possession is not required.

3.2.2 AUTHENTICATION OF ORGANIZATION IDENTITY

Requests for RCA and CA and Subscriber certificates in the name of an Affiliated Organization shall include the organization name, address, and documentation of the existence of the organization.

The DS PMA for RCA, DS OAO for CA and Trusted Agent for subscriber as applicable, shall verify the information provided, the authenticity of the requesting representative, and the representative's authorization to act in the name of the organization.

3.2.3 AUTHENTICATION OF PHYSICAL PERSON IDENTITY

Successful authentication binds together the process documentation, public key, applicant identity information, and applicant.

3.2.3.1 INITIAL IDENTITY PROOFING OF HUMAN SUBSCRIBERS

Identity proofing shall be performed in-person before a Trusted Agent for Subscriber, or an entity certified by a Government Entity as being authorized to confirm identities.

Identity proofing of Customer OAA shall be performed by DS OA (DS OAA or DS OAO) for CA according rules set in RCA CPS. The Customer OAA shall present suitable identity source documents as describe below in same section. Presentation of document can be done either by video of in face to face meeting. DS OA records same information as for Subscriber as described below in same section.

The applicant shall present suitable identity source documents. Suitable identity source documents vary according to level of assurance as follows:

1) One unexpired National Government-issued or REAL ID Act issued Picture ID, or
2) Two Non-Federal Government IDs, one of which shall be a photo ID.

The CA, and/or associated Customers shall ensure that the applicant's identity information is verified in accordance with the process established by the applicable CPS.

Process information shall depend upon the certificate level of assurance and shall be addressed in CPS. The documentation and authentication requirements vary depending upon the level of assurance. The Trusted Agent for Subscriber, as applicable, shall record the process information set forth below for issuance of each certificate:

- The identity of the person performing the identification;
- A signed declaration by that person that he or she verified the identity of the applicant as required using the format set forth at 28 U.S.C. 1746 (declaration under penalty of perjury) or comparable procedure under local law. The signature on the declaration may be either a handwritten or digital signature using a certificate that is of equal or higher level of assurance as the credential being issued;
- If in-person or supervised remote (see below requirements for remote) identity proofing is done, unique identifying number(s), issuance date of ID and type of ID from the ID(s) of the applicant, or a facsimile of the ID(s), except where capturing such information violates local law, in which case, the DS PMA will consider and approve other comparable procedures for collecting identity evidence.
    - The minimum requirements associated with supervised remote identity proofing are described in NIST SP 800-63A, Digital Identity Guidelines: Enrollment and Identity Proofing, Section 5.3.3. If Customer uses this method, then Customer shall be trained and use procedures and means compliant with NIST requirement. The compliancy to NIST requirements shall be approved by an external auditor (distinct from DocuSign). DocuSign will test the solution and verify that Customer implements what external auditor has approved as compliant to NIST.
- The date and time of the verification; and
- A declaration of identity signed by the applicant using a handwritten signature or appropriate digital signature (see Practice Note) and performed in the presence of the person performing the identity authentication, using the format set forth at 28 U.S.C. 1746 (declaration under penalty of perjury) or comparable procedure under local law.

Practice Note: In those cases in which the individual is in possession of a valid digital signature credential of equal or higher level of assurance or the signature certificate is generated immediately upon authentication of the applicant's identity, the applicant may sign the declaration of identity and certificate of acceptance using the digital credential. In the latter case, if the applicant fails to sign the declaration of identity then the certificate must be revoked.

3.2.3.2 HUMAN SUBSCRIBER IDENTITY PROOFING VIA ANTECEDENT RELATIONSHIP

The following requirements shall apply when human subscriber identity is verified using antecedent relationship with the sponsoring organisation:

1. The applicant shall personally appear before a verifier (usually a Trusted Agent);
2. The applicant and the verifier shall have an established working (*An example of "established working relationship" is the person is employed by the sponsoring organization. Another example of "established working relationship" is the person is consultant to the sponsoring organization or is employed by a contractor of the sponsoring organization*) relationship with the sponsoring organisation. The relationship shall be sufficient to enable the verifier to, with a high degree of certainty, verify that the applicant is the same person that was identity proofed. An example to meet this requirement is when the applicant and Trusted Agents are employed by the same company and the company badge forms the basis for the applicant authentication;
3. The applicant shall present a valid sponsoring organisation-issued photo ID. This photo ID shall have been issued on the basis of previously performed in-person identity proofing using one valid National Government-issued Picture ID, or two valid non-National Government IDs, one of which shall be a recent photo ID (e.g., Driver's License);

4. The verifier shall record the following:
    a. His/her own identity;
    b. Unique identifying number from the Identifier (ID) of the verifier;
    c. Unique identifying number from the applicant's sponsoring organization issued photo ID;
    d. Date and time of the identity verification; and
    e. Date and time of sponsoring organisation-issued photo ID, if applicable.
5. The verifier shall sign a declaration that he or she verified the identity of the applicant as required by the applicable certificate policy which may be met by establishing how the applicant is known to the verifier as required by this certificate policy; and
6. The applicant shall sign a declaration of identity using a handwritten signature or appropriate digital signature. This declaration shall be signed in the presence of the verifier.

3.2.3.3 HUMAN SUBSCRIBER RE-PROOFING FOLLOWING LOSS, DAMAGE, OR KEY COMPROMISE

If human subscriber credentials containing the private keys associated with the public key certificates are lost, damaged, or stolen, the subscriber may be issued new certificates according to the re-proofing provisions in this Section.

The re-proofing provisions are the same as those followed for the initial identity proofing (Section 3.2.3.1 or Section 3.2.3.2) with the following modifications:

- The validity period of the certificates issued using this process shall not exceed the identity-reproofing requirements in Section 3.3.1.
- Only one National Government-Issued Photo ID or non-National Government issued Photo ID (e.g., Driver's License, Passport) is required.
- As applicable, match a good fingerprint or other adequate biometric from the subscriber with the biometric stored in an authoritative trusted database. This database shall be protected as stipulated in Section 4.3 of this CP.

Practice Note: As biometric authentication accuracy degrades with the time elapsed since initial collection, Entity PKIs may desire to update biometric(s) after a match has been made.

3.2.3.4 IDENTITY PROOFING HUMAN SUBSCRIBERS FOR ROLE-BASED CERTIFICATES

Not applicable.

3.2.3.5 AUTHENTICATION OF DEVICES

Computing and communications devices (routers, firewalls, servers, etc.) may be named as certificate subjects. In such cases, the device must have a human sponsor. The sponsor is responsible for providing the following registration information:

- Equipment identification (e.g., serial number) or service name (e.g., DNS name)
- Equipment public keys
- Equipment authorizations and attributes (if any are to be included in the certificate)
- Contact information to enable the CA or RA to communicate with the sponsor when required

Aircraft, aircraft components, and aircraft on-board systems may be named as certificate subjects. In such cases, all of the requirements above apply and the sponsor shall also provide the following additional registration information:

- Relevant Aircraft National Registration Paperwork

These certificates shall be issued only to devices under the issuing entity's control (i.e., require registration and validation that meets all issuing agency's requirements, as well as requiring re-validation prior to being re-issued).

Practice Note: An entity can issue to organizations not controlled or related to the entities organization i.e. a different company.

In the case a human sponsor is changed, the new sponsor shall review the status of each device under his/her sponsorship to ensure it is still authorized to receive certificates. The CPS shall describe procedures to ensure that certificate accountability is maintained.

The registration information shall be verified to an assurance level commensurate with the certificate assurance level being requested. Acceptable methods for performing this authentication and integrity checking include, but are not limited to:

- Verification of digitally signed messages sent from the sponsor (using certificates of equivalent or greater assurance than that being requested).
- In person or supervised remote registration by the sponsor, with the identity of the sponsor confirmed in accordance with the requirements of Section 3.2.3.1.

3.2.4 NON-VERIFIED SUBSCRIBER INFORMATION

Information that is not verified shall not be included in certificates.

3.2.5 VALIDATION OF AUTHORITY

For cross-certification, the DS PMA shall validate the requestor's authorization to act in the name of the organization.

Approval from the DS PMA for RCA and CA certificate shall be obtained prior to issuing such certificate. In the case of the Customer dedicated CA certificates, certificate issuance by the RCA shall be based on DS PMA Approval for CA Certificate content (CN of CA).

Certificates that contain explicit or implicit organizational affiliation shall be issued only after ascertaining the applicant has the authorization to act on behalf of the organization in the asserted capacity.

Prior to issuing Subscriber certificates, the Trusted Agent shall verify that the Subscriber is authorized to have a certificate in the name of the affiliated organization.

3.2.6 CRITERIA FOR INTEROPERATION

DS PMA shall control that RCA is only cross-certified with TSCP bridge. CA are not authorized to be cross-certified or signed by another CA of DocuSign or external to DocuSign. CA are only authorized to be signed by RCA of DocuSign.

The DS PMA shall determine the criteria to certify a CA by RCA. Such methodology shall include the following verifications:

- DS CP to Customer RPS mapping has completed and found the Customer RPS correctly implements the DS CP.
- Customer has successfully passed a compliance audit (see section 8 of the DS CP).
- Verification that Certificate Profiles and Certificates are compliant with the DS CP.
- Verification that Certificate Status (e.g. CRL) are compliant with the DS CP.
- Verification that CA certificates and CRL are published and available for Relying Parties.

Under no circumstance shall any certificate have more than one intentional trust path to the TSCP bridge, irrespective of extension processing.

NOTE: Multiple trust paths created as a result of Certificate renewal or CA rekey do not violate the single trust path requirement.

3.3 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS

3.3.1 IDENTIFICATION AND AUTHENTICATION FOR ROUTINE RE-KEY

CA shall be authenticated through use of a private key and corresponding valid certificate or one of the initial identity proofing processes described in Section 3.2.3.1 and 3.2.3.2.

If it has been more than three years since a CA was identified as required in Section 3.2, identity shall be re-established through the initial identity proofing process.

Subscribers shall be authenticated through the use of the current signature key or one of the initial identity proofing processes describe in Section 3.2.3.1 and 3.2.3.2. If it has been more than nine years since the Subscriber was identified as required in Section 3.2, identity shall be re-established through the initial identity proofing process.

When current private key and corresponding valid certificate is used for identification and authentication purposes, the life of the new certificate shall not exceed beyond the initial identity-proofing times specified in the paragraphs above and the assurance level of the new certificate shall not exceed the assurance level of the certificate being used for identification and authentication purposes.

3.3.2 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY AFTER REVOCATION

After a certificate has been revoked, other than during a renewal, update, or to replace a lost/stolen/damaged credential, the Subscriber is required to go through the initial registration processes described in Section 3.2.3 to obtain a new certificate unless the Subscriber can be authenticated with a non-revoked certificate of equal or higher assurance issued from the same CA.

3.4 IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST

Revocation requests must be authenticated. Requests to revoke a certificate may be authenticated using that certificate's public key, regardless of whether or not the associated private key has been compromised.

4 CERTIFICATE LIFE-CYCLE

4.1 CERTIFICATE APPLICATION

Sections 4.1, 4.2, 4.3 and 4.4 specify the requirements for an initial application for certificate issuance. Sections 4.6, 4.7 and 4.8 specify the requirements for certificate renewal. Subscriber here covers both individual and device.

Certificates and corresponding private keys must be managed safely at their initial creation through their full life-cycle.

With the present CP, DS PMA establishes and publishes its criteria and procedures describing how Customer and Subscribers may apply for certificate(s).

4.1.1 SUBMISSION OF CERTIFICATE APPLICATION

4.1.1.1 RCA

DS OAA creates the RCA request (RCA naming document) and transmit to DS PMA for approval.

4.1.1.2 CROSS-CERTIFICATE

DocuSign signs the MOA with TSCP before to be cross-certified with TSCP.

DS OAO generates the RCA's CSR with the format described in section 10. DS PMA fills and transmits the certificate application form to the TPMA to perform the certification of the RCA by the TBCA.

TPMA shall transmit the CSR of the TBCA to DS PMA.

DS PMA transmits the CSR of TBCA to DS OAO to prepare the naming document to issue a cross-certificate by RCA to TBCA.

4.1.1.3 CA: DOCUSIGN GENERIC CA

DS OAA creates the CA request (CA naming document) and transmits it to DS PMA for approval.

4.1.1.4 CA: CUSTOMER DEDICATED CA

DS PMA transmits the contract to DS OAO. DS OAO prepares the CA certificate request (CA naming document).

4.1.1.5 SUBSCRIBER

A Trusted Agent acting on behalf of the Subscriber shall submit a Certificate application to the CA. Trusted Agent shall use the electronic application form approved by RA with the technical tools approved by RA.

4.1.2 ENROLLMENT PROCESS AND RESPONSIBILITIES

All communications among PKI authorities materially supporting the certificate application and issuance process shall be authenticated and protected from modification.

4.1.2.1 RCA

RCA certificates must be authorized by the DS PMA prior to issuance. The issuance process shall include documenting the following information to be contained in the RCA certificate request (naming document):

- Identity to set in the RCA certificate (refer to section **Error! Reference source not found.** above).
- Validity period of the RCA certificate.
- Cryptographic information of the RCA certificate.
- RCA Certificate content (refer to section 10).
- CRL information to be produced with the RCA Certificate generation.
- DocuSign Inc. as the legal Entity which owns RCA.
- DS OAO information:
    - The full name, including surname and given name(s) of the representative.
    - The full name and legal status of the authorized representative's Employer.
    - Professional phone number and email of the authorized representative.
    - A reference to its national ID and the type of ID used to authenticate the person.
- DS OAA information:
    - The full name, including surname and given name(s) of the representative.
    - The full name and legal status of the authorized representative's Employer.
    - Professional phone number and email of the authorized representative.

  - A reference to its national ID and the type of ID used to authenticate the person.

DS PMA shall store copy of Authorized representative's ID. The RCA certificate request shall be signed digitally by the DS OAO with means as described in CPS.

In parallel the DS OAO shall transmit the RCA CPS, written to the format of the Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework [RFC 3647], for approval. RCA key pair and certificate can't be generated without prior having the RCA CPS and RCA key ceremony script approved by DS PMA. RCA CPS shall be signed by DS OAA.

4.1.2.2 CROSS-CERTIFICATE

DS OAA applying for cross-certification with TSCP is responsible for providing accurate information in its certificate applications requested by TSCP. Application form to be filled for cross-certificate issued by TBCA is given by TSCP.

Cross-certificate issued by RCA must be authorized by the DS PMA prior to issuance. The issuance process shall include documenting the following information to be contained in the RCA cross-certificate request (naming document):

- Identity to set in the cross-certificate (refer to section 10).
- Legal name of TSCP.
- TBCA's CSR associated with the generated key pair (refer to section 10).
- Identity of the RCA to be used to sign the cross-certificate.
- Validity period of the cross-certificate.
- Cryptographic information of the CA certificate.
- Cross-certificate content.
- DS OAO information:
  - The full name, including surname and given name(s).
  - The full legal name of Customer.
  - Professional phone number and email.
  - A reference to its national ID and the type of ID used to authenticate the person.
- DS OAA information:
  - The full name, including surname and given name(s).
  - The full legal name of DS Administrator company.
  - Professional phone number and email.
  - A reference to its national ID and the type of ID used to authenticate the person.

The CA certificate request shall be signed digitally by the DS OAO persons with means as described in CPS.

4.1.2.3 CA: DOCUSIGN GENERIC CA

CA certificates shall be authorized by the DS PMA prior to issuance. The issuance process shall include documenting the following information to be contained in the CA certificate request (naming document):

- Identity to set in the CA certificate (refer to section **Error! Reference source not found.** above).
- Identity of the RCA to be used to sign the CA certificate.
- Validity period of the CA certificate.
- Cryptographic information of the CA certificate.
- CA Certificate content (refer to section 10).
- DocuSign Inc. as the legal Entity which owns CA.
- DS OAO information:
  - The full name, including surname and given name(s) of the representative.
  - The full name and legal status of the authorized representative's Employer.
  - Professional phone number and email of the authorized representative.
  - A reference to its national ID and the type of ID used to authenticate the person.
- DS OAA information:
  - The full name, including surname and given name(s) of the representative.

  - The full name and legal status of the authorized representative's Employer.
  - Professional phone number and email of the authorized representative.
  - A reference to its national ID and the type of ID used to authenticate the person.

DS PMA shall store copy of Authorized representative's ID. The CA certificate request shall be signed digitally by the DS OAO as described in CPS.

In parallel the DS OAO shall transmit the RCA CPS, written to the format of the Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework [RFC 3647], for approval. RCA key pair and certificate shall not be generated having the RCA CPS and RCA key ceremony script prior approval by DS PMA. RCA CPS shall be signed by DS OAA.

4.1.2.4 CA: CUSTOMER DEDICATED CA

CA certificates shall be be authorized by the DS PMA prior to issuance. The issuance process shall include documenting the following information to be contained in the CA certificate request (naming document):

- Identity to set in the CA certificate (refer to section **Error! Reference source not found.** above).
- Legal name of the Customer.
- Identity of the RCA to be used to sign the CA certificate.
- Validity period of the CA certificate.
- Cryptographic information of the CA certificate.
- CA Certificate content.
- Customer OAA information:
  - The full name, including surname and given name(s).
  - The full legal name of Customer.
  - Professional phone number and email.
  - A reference to its national ID and the type of ID used to authenticate the person.
- DS OAO Administrator information:
  - The full name, including surname and given name(s).
  - The full legal name of DS Administrator company.
  - Professional phone number and email.
  - A reference to its national ID and the type of ID used to authenticate the person.
- DS OAA information:
  - The full name, including surname and given name(s).
  - The full legal name of DS Administrator company.
  - Professional phone number and email.
  - A reference to its national ID and the type of ID used to authenticate the person.

The CA certificate request shall be signed digitally by the Customer OAA and DS OAO persons as described in CPS. Customer RPS.

DS PMA shall store copy of all ID used in signed document above.

4.1.2.5 SUBSCRIBER

Subscriber certificate application shall contain the following information:

- Name of the affiliated organization to be set in the subscriber certificate (refer to section 3.2.2).
- Email and mobile phone number of the subscriber.
- Date and time of the request.
- All required information to construct the Subscriber's identity (name) to be set in the Certificate as described in section 3.1.
- Subscriber's ID information from its official ID for method described in section 3.2.3.1 or requested ID information in case of method described in section 3.2.3.2 used to authenticate the Subscriber.

- Subscriber agreement which includes the Subscriber's obligation (see section 9.6.3) to protect the private key and only use the certificate and private key for authorized purposes and the personal data management (privacy policy, see section 9.4).
- For Device only, information requested in section 3.2.3.5.
- The date and time of the verification.

This application form shall be signed in the presence of the Trusted Agent. Application form shall be digitally signed by the Trusted agent and by Subscriber using digital signature system as described in CPS.

4.2 CERTIFICATE APPLICATION PROCESSING

Information in certificate applications must be verified as accurate by the approver before certificates are issued. The applicable CPS shall specify procedures to verify information in certificate applications.

4.2.1 PERFORMING IDENTIFICATION AND AUTHENTICATION FUNCTIONS

4.2.1.1 RCA

Requests are submitted by DS OAO to DS OAA prior to issuance using means and process described in CPS and approved by PMA. It is the responsibility of the DS OAA to authenticate the DS OAO as described in section 3.2 above, and to verify that the information in RCA Certificate request is accurate for the RCA.

4.2.1.2 CROSS-CERTIFICATE

Requests are submitted by TPMA trusted contact to DS OAA prior to issuance using means and process described in CPS and approved by PMA. It is the responsibility of the DS OAA to authenticate the TPMA trusted contact as described in section 3.2 above, and to verify that the information in cross-certificate request is accurate for the cross-certificate to be issued by RCA.

4.2.1.3 CA: DOCUSIGN GENERIC CA

Using means and process described in CPS, requests shall be submitted by DS OAO to DS OAA prior to issuance and approved by PMA. It is the responsibility of the DS OAA to authenticate the DS OAO as described in section 3.2 above, and to verify that the information in CA Certificate request is accurate for the CA.

4.2.1.4 CA: CUSTOMER DEDICATED CA

A Contract is submitted by Customer OAA to DS OAA prior to issuance. It is the responsibility of the DS OAA to authenticate the Customer OAA as described in section 3.2 above, and to verify that the information in contract is accurate for the CA.

CA request is then submitted by DS OAO to DS OAA prior to issuance. It is the responsibility of the DS OAA to authenticate the DS OAO as described in section 3.2 above, and to verify that the information in request is accurate for the CA.

4.2.1.5 SUBSCRIBER

It is the responsibility of the Trusted Agent to verify that the information in Certificate request is accurate and to authenticate and verify subscriber identity to be set in certificate (see sections 3.2 and 3.3). It is also responsibility of Trusted Agent to verify the link between subscriber and affiliated organization to be set in the certificate.

4.2.2 APPROVAL OR REJECTION OF CERTIFICATE APPLICATIONS

4.2.2.1 RCA

Once a completed RCA certificate request has been submitted to the DS PMA, the DS PMA studies it. DS PMA can't take decision based on an incomplete RCA certificate request. All required information listed in section 4.1.2 above shall be given to the DS PMA. The DS PMA shall evaluate the completeness of the submitted request. The DS PMA shall commission a CPS compliance analysis prior to authorizing the DS OA to issue and manage RCA Certificates asserting this CP.

In the case where the RCA certificate request is complete and compliant with this CP statement, the DS PMA approves the RCA certificate creation.

In the case where the RCA certificate request is rejected, the PMA will ask to re-submit a new RCA certificate request.

4.2.2.2 CROSS-CERTIFICATE

Once a completed cross-certificate request has been submitted to the DS PMA, the DS PMA studies it. DS PMA can't take decision based on an incomplete cross-certificate request. All required information listed in section 4.1.2 above shall be given to the DS PMA. The DS PMA shall evaluate the completeness of the submitted request.

In the case where the cross-certificate request is complete and compliant with this CP statement, the DS PMA approves the cross-certificate creation.

In the case where the cross-certificate request is rejected, the PMA will ask to re-submit a new cross-certificate request.

4.2.2.3 CA: DOCUSIGN GENERIC CA

Once a completed CA certificate request has been submitted to the DS PMA, the DS PMA reviews it. DS PMA shall not make decision based on an incomplete CA certificate request. All required information listed in section 4.1.2 above shall be given to the DS PMA. The DS PMA shall evaluate the completeness of the submitted request. The DS PMA shall commission a CPS compliance analysis prior to authorizing the DS OA to issue and manage CA Certificates asserting this CP.

In the case where the CA certificate request is complete and compliant with this CP, the DS PMA shall make a decision on approval of the CA certificate creation.

In the case where the CA certificate request is rejected, the PMA shall ask the Customer to submit a new CA certificate request.

4.2.2.4 CA: CUSTOMER DEDICATED CA

CA certificate can't be issued before Customer RPS has been successfully audited by DS PMA.

Once a completed CA certificate request has been submitted to the DS PMA, the DS PMA studies it. DS PMA can't take decision based on an incomplete CA certificate request. All required information listed in section 4.1.2 above shall be given to the PMA. The PMA shall evaluate the completeness of the submitted request.

In the case where the CA certificate request is complete and compliant with this CP, the DS PMA approves the CA certificate creation.

In the case where the CA certificate request is rejected, the PMA shall ask the Customer to submit a new CA certificate request.

CA signed by RCA can only issue type of Subscriber Certificate that are approved by DS PMA (see section 1.5.4).

4.2.2.5 SUBSCRIBER

The Trusted agent shall be responsible for approving or rejecting Subscriber certificate applications.

4.2.3 TIME TO PROCESS CERTIFICATE APPLICATIONS

Individual Identity shall be confirmed by Trusted Agent no more than 30 days before initial certificate issuance.

4.3 CERTIFICATE ISSUANCE

Upon receiving a request for a certificate, the CA or RA shall respond in accordance with the requirements set forth in this CP and corresponding CPS.

The certificate request may contain an already built ("to-be-signed") certificate. This certificate will not be signed until the process set forth in this CP and the corresponding CPS has been met.

While the Subscriber may do most of the data entry, it is still the responsibility of the CA and RA (Trusted Agent) to verify that the information is correct and accurate. This may be accomplished through a system approach linking trusted databases containing personnel information, other equivalent authenticated mechanisms, or through personal contact with the Subscriber’s sponsoring organization. If databases are trusted to confirm Subscriber information, then these databases must be protected from unauthorized modification to a level commensurate with the level of assurance of the certificate being sought.

Specifically, the databases shall be protected using physical security, personnel controls, cryptographic security controls, computer security controls, and network security controls specified for the RA elsewhere in this CP.

When information is obtained through one or more data sources, the Customer operating the CA shall ensure there is an auditable chain of custody.

4.3.1 CA ACTIONS DURING CERTIFICATE ISSUANCE

The CA and RCA shall verify the source of a certificate request before issuance. RCA, CA and subscriber certificates and cross-certificate shall be checked to ensure that all fields and extensions are properly populated. After generation, verification, and acceptance the RCA, CA and subscriber certificates and cross-certificate shall be posted in the repository system as specified in this CP and CPSs.

4.3.2 NOTIFICATION TO SUBSCRIBER OF CERTIFICATE ISSUANCE

The Customer shall notify Subscribers of successful Certificate issuance in accordance with procedures set forth in the applicable Customer RPS.

The RCA shall notify the DS PMA for RCA and CA certificate of successful Certificate issuance in accordance with procedures set forth in the applicable RCA CPS.

When Customer has a dedicated CA, the RCA shall notify the Customer for CA certificate, of successful Certificate issuance in accordance with procedures set forth in the applicable RCA CPS and contract signed with Customer.

The DS PMA shall notify TSCP for cross-certificate of successful cross-certificate issuance in accordance with procedures set forth in the applicable RCA CPS and MOA signed with TSCP.

4.4 CERTIFICATE ACCEPTANCE

4.4.1 CONDUCT CONSTITUTING CERTIFICATE ACCEPTANCE

4.4.1.1 RCA

The DS PMA accepts the RCA certificate when the DS OAA representative that witnesses the RCA key ceremony signs the RCA certificate issuance attestation.

Once the RCA certificate has been accepted, the RCA may start signing certificate and CRL.

4.4.1.2 CROSS-CERTIFICATE

The DS PMA accepts the cross-certificate issued by RCA when the DS OAA representative that witnesses the cross-certificate key ceremony signs the cross-certificate certificate issuance attestation.

Once the cross-certificate has been accepted, the DS PMA may transmit the cross-certificate to TPMA. TPMA accept the cross-certificate according rules set in MOA.

4.4.1.3 CA: DOCUSIGN GENERIC CA

The DS PMA accepts the CA certificate when the DS OAA representative that witnesses the CA key ceremony signs the CA certificate issuance attestation.

Once the CA certificate has been accepted, the CA may start signing certificate and CRL.

4.4.1.4 CA: CUSTOMER DEDICATED CA

The DS PMA accepts the CA certificate when the DS OAA representative that witnesses the CA certificate generation signs the CA certificate issuance attestation. When the Customer does not attend the key ceremony, the Customer shall control the CA certificate content before its use and advise the DS PMA if there is a mistake in the CA certificate content. In case of mistake that is described in section 4.9.1, then Customer shall request CA revocation to the DS PMA. If CA certificate is good, then Customer transmits its acceptance to DS PMA according contract and CPS.

Once the CA certificate acceptance has been received by the DS PMA, the CA may start to sign certificates and CRLs.

4.4.1.5 SUBSCRIBER

Before a Subscriber can make effective use of its private key, a Trusted Agent shall convey to the Subscriber its responsibilities as defined in Section 9.6.3 (see section 4.1.2).

For subscriber, first use of the certificate constitutes acceptance of the issued certificate. If the Subscriber finds mistake in the Certificate, then subscriber shall proceed to a revocation request.

4.4.2 PUBLICATION OF THE CERTIFICATE BY THE CA

As specified in 2.2.1, all RCA and CA certificates shall be published in Repositories.

This CP makes no stipulation regarding publication of Subscriber certificates.

4.4.3 NOTIFICATION OF CERTIFICATE ISSUANCE BY THE CA TO OTHER ENTITIES

Notification of Certificate issuance is provided by publishing RCA and CA certificates (refer to section 2.2 above).

For Customer, notification of CA Certificate issuance is provided according to the contractual obligations established with DocuSign.

For TSCP, notification of CA and RCA and cross-certificate is provided according to the contractual obligations established with MOA.

The TPMA shall be notified at least two weeks and a day prior to the issuance of a new CA certificate or issuance of CA certificates external to the Entity's PKI domain. The notice period will begin to run upon written acknowledgement of the TPMA. In addition, all new artifacts (CA certificates, CRL DP, AIA and/or SIA URLs, etc.) produced as a result of the CA certfiicate issuance shall be provided to the TPMA and FPKIPA within 24 hours following issuance.

4.5 KEY PAIR AND CERTIFICATE USAGE

4.5.1 SUBSCRIBER PRIVATE KEY AND CERTIFICATE USAGE

Subscribers shall protect their private keys from access by other parties.

Subscribers, RCA and CAs shall use their private key as specified through certificate extensions, including the key usage, extended key usage extensions, and certificate policies in the associated certificate.

4.5.2 RELYING PARTY PUBLIC KEY AND CERTIFICATE USAGE

Relying parties shall accept public key certificates and associated public keys for the purposes intended as constrained by the extensions (such as key usage, extended key usage, certificate policies, etc.) in the certificates.

4.6 CERTIFICATE RENEWAL

Certificate renewal consists of issuing a new certificate with a new validity period and serial number while retaining all other information in the original certificate including the public key. Frequent renewal of certificates may assist in reducing the size of CRLs. After certificate renewal, the old certificate may or may not be revoked, but must not be further re-keyed, renewed, or modified.

This practice is not allowed for RCA and Subscriber (physical person and Device). In case a new certificate is created, a new key pair shall be created.

While this practice is allowed for CA and cross-certificate, it is discouraged for the CA and must be submitted to the DS PMA for approval.

4.6.1 CIRCUMSTANCE FOR CERTIFICATE RENEWAL

A certificate may be renewed if the private key has not reached the end of its validity period, has not been revoked or compromised, and the CA name and attributes are unchanged.

Certificates may also be renewed when the RCA that issued the certificates is re-keyed.

The validity period of the certificate and private key must meet the requirements specified in Section 5.6.

4.6.2 WHO MAY REQUEST RENEWAL

For CAs and cross-certificate where renewal is supported, such requests shall only be accepted by DS PMA (see section 4.1 and 4.2). Same rules as section 4.1 applies.

4.6.3 PROCESSING CERTIFICATE RENEWAL REQUESTS

For the DocuSign Generic CA, certificate renewal shall be approved by the DS PMA., In the case of a Customer dedicated CA, it also requires an active contract which does not expire prior to the new period of the renewed certificate.

For the cross-certificate, certificate renewal shall be approved by the DS PMA and requires an active MOA with TSCP which does not expire prior to the new period of the renewed certificate.

Certificate requests shall be processed according to the requirements in Section 3.3.1. For renewal, however, the keys may not change.

4.6.4 NOTIFICATION OF NEW CERTIFICATE ISSUANCE TO SUBSCRIBER

See Section 4.3.2.

4.6.5 CONDUCT CONSTITUTING ACCEPTANCE OF A RENEWAL CERTIFICATE

See Section 4.4.1.

4.6.6 PUBLICATION OF THE RENEWAL CERTIFICATE BY THE CA

See Section 4.4.2.

4.6.7 NOTIFICATION OF CERTIFICATE ISSUANCE BY THE CA TO OTHER ENTITIES

See Section 4.4.3.

4.7 CERTIFICATE RE-KEY

Re-keying a certificate consists of creating new certificates with a new and different private key (and serial number) and corresponding new and different public key, while retaining the remaining contents of the old certificate that describe the subject. The new certificate may be assigned a different validity period, key identifiers, specify a different CRL distribution point, and/or be signed with a different key. Re-key of a certificate does not require a change to the subject Distinguished Name or subject Alternative Name(s) and does not violate the requirement for name uniqueness.

After certificate rekey, the old certificate may or may not be revoked, but must not be further re-keyed, renewed, or modified.

4.7.1 CIRCUMSTANCE FOR CERTIFICATE RE-KEY

A CA may issue a new certificate to the Subscriber when the Subscriber has generated a new key pair and is entitled to a certificate.

A RCA may issue a new certificate or cross-certificate when the CA has generated a new key pair and is entitled to a certificate.

CAs and Trusted Agent may initiate re-key of a Subscriber's certificates without a corresponding request from the Subscriber.

4.7.2 WHO MAY REQUEST CERTIFICATION OF A NEW PUBLIC KEY

For RCA, only the DS PMA can make this request (see section 4.1).

For CA, only Customer or DocuSign can make this request (see section 4.1).

For Subscriber, only the Subscriber can make this request (see section 4.1).

For Device certificates, only the PKI sponsors can make this request.

For cross-certificate, only DS PMA and TSCP can make this request (see section 4.1).

4.7.3 PROCESSING CERTIFICATE RE-KEYING REQUESTS

For the CA, certificate rekey shall be approved by the DS PMA and requires an active contract with Customer, when CA is a Customer dedicated CA only, which does not expire prior to the new period of the renewed certificate.

For the cross-certificate, certificate rekey shall be approved by the DS PMA and requires an active MOA with TSCP which does not expire prior to the new period of the renewed certificate.

In all cases, identity proofing shall be processed as defined in Section 3.3.1 before performing re-key. For Subscriber only the certificate may be automatically re-keyed by the CA based on an electronically authenticated request from the Subscriber as per Section 3.3.1.

4.7.4 NOTIFICATION OF NEW CERTIFICATE ISSUANCE TO SUBSCRIBER

See Section 4.3.2.

4.7.5 CONDUCT CONSTITUTING ACCEPTANCE OF A RE-KEYED CERTIFICATE

See Section 4.4.1.

4.7.6 PUBLICATION OF THE RE-KEYED CERTIFICATE BY THE CA

See Section 4.4.2.

4.7.7 NOTIFICATION OF CERTIFICATE ISSUANCE BY THE CA TO OTHER ENTITIES

See Section 4.4.3.

4.8 CERTIFICATE MODIFICATION

Certificate modification consists of creating new certificates with subject information (e.g., a name or email address) that differs from the old certificate. For example, a CA may perform certificate modification for a Subscriber whose characteristics have changed (e.g., has just received a medical degree). The new certificate may have the same or different subject public key. After certificate modification, the old certificate may or may not be revoked, but must not be further re-keyed, renewed, or modified.

4.8.1 CIRCUMSTANCE FOR CERTIFICATE MODIFICATION

RCA may perform a certificate modification process in support of cases where one or more of the CA’s or cross CA names has changed. Such circumstances included, but are not limited to name change from marriage, post nominal change, and email address change.

CA and cross CA must be entitled to continue with its existing certificate before certificate modification is performed.

This practice is not allowed for Subscriber (physical person and Device). In case a new certificate is created, a new key pair shall be created.

4.8.2 WHO MAY REQUEST MODIFICATION

For CAs and cross-certificate where Modification is supported, such requests shall only be accepted by DS PMA (see section 4.1 and 4.2). Same rules as section 4.1 applies.

4.8.3 PROCESSING CERTIFICATE MODIFICATION REQUESTS

For the CA, certificate renewal shall be approved by the DS PMA and, when CA is a Customer dedicated CA, requires an active contract with Customer, which does not expire prior to the new period of the renewed certificate.

For the cross-certificate, certificate renewal shall be approved by the DS PMA and requires an active MOA with TSCP which does not expire prior to the new period of the renewed certificate.

Certificate requests shall be processed according to the requirements in Section 3.3.1. For renewal, however, the keys may not change.

4.8.4 NOTIFICATION OF NEW CERTIFICATE ISSUANCE TO SUBSCRIBER

See Section 4.3.2.

4.8.5 CONDUCT CONSTITUTING ACCEPTANCE OF A MODIFIED CERTIFICATE

See Section 4.4.1.

4.8.6 PUBLICATION OF THE MODIFIED CERTIFICATE BY THE CA

See Section 4.4.2.

4.8.7 NOTIFICATION OF CERTIFICATE ISSUANCE BY THE CA TO OTHER ENTITIES

See Section 4.4.3.

4.9 CERTIFICATE REVOCATION AND SUSPENSION

Revocation requests must be authenticated. Requests to revoke a certificate may be authenticated using that certificate's associated private key, regardless of whether or not the private key has been compromised.

For RCA and CAs, the TPMA shall be notified by DS PMA at least two weeks and one day prior to the revocation of a CA or RCA certificate, whenever possible. The notice period will begin to run upon written acknowledgement by the TPMA. For emergency revocation, CAs shall follow the notification procedures in Section 5.7.

4.9.1 CIRCUMSTANCES FOR REVOCATION

Whenever any of the below circumstances occur, the associated certificate shall be revoked and placed on the CRL. Revoked certificates shall be included on all new publications of the certificate status information until the certificates expire.

4.9.1.1 CROSS-CERTIFICATE

For the TBCA cross-certificate issued by RCA and RCA cross-certificate issued by TBCA, a certificate shall be revoked when the binding between the subject and the subject's public key defined within a certificate is no longer considered valid.

The circumstances under which certificates issued by the RCA will be revoked include:

- When the TPMA requests to DS PMA for a TBCA cross-certificate issued by RCA to be revoked. This will be the normal mechanism for revocation in cases where the TPMA determines that DocuSign or Customer(s) does not meet the policy requirements or applicable MOA.
- DS PMA may request revocation of cross-certificate for convenience. DS PMA shall request revocation if it cannot meet its obligations within this CP and/or TSCP CP or the obligations corresponding to any "pass-through" policy OIDs asserted in its Cross-Certificate and/or MOA.
- When the DS Operational personnel determine that an emergency has occurred that may impact the integrity of the certificates issued by the RCA (e.g. key compromise, severe violation threatening to cross-certified parties). Under such circumstances, the following individuals may authorize immediate certificate revocation:
    - Chair of DS PMA, or
    - Other personnel as designated by the Chair of DS PMA.

The DS PMA shall meet as soon as practicable to review the emergency revocation.

4.9.1.2 CA

The circumstances under which certificates issued by a RCAs shall be revoked include:

- The Customer or DS PMA requests revocation.
- The affiliation with an organization asserted in the DN is no longer valid. RCAs shall ensure in their agreements with Customer organizations that the Organization be required to notify the RCA of any changes to the Customer legal name.
- The affiliation with an organization can no longer be confirmed (e.g. Customer terminates relationship with DocuSign).
- Content in a certificate is no longer valid (e.g. name, role, or privilege change).
- Customer and Customer roles, set in DocuSign CPS or Customer RPS can be shown to have violated the stipulations of its respective contract or this CP.
- CA Private key is compromised or suspected of compromise

4.9.1.3 SUBSCRIBER

The circumstances under which certificates issued by CAs shall be revoked include:

- The Subscriber, Customer authorized roles or DS PMA requests revocation.

- The affiliation with an affiliated organization asserted in the DN is no longer valid. Customer shall ensure in their agreements with Subscriber that the Customer and Subscriber be required to notify the Customer of any changes to the Subscriber affiliated organization.
- The affiliation with an organization can no longer be confirmed (e.g. Subscriber terminates relationship with Customer).
- Content in a certificate is no longer valid (e.g. name, role, or privilege change)
- Subscriber or Customer roles can be shown to have violated the stipulations of its respective Subscriber Agreement or this CP.
- Private key is compromised or suspected of compromise

4.9.2 WHO CAN REQUEST REVOCATION

4.9.2.1 CROSS-CERTIFICATE

A cross-certificate may be revoked upon direction of the DS PMA or upon an authenticated request by a designated official of the TSCP (such official or officials shall be identified in the MOA as authorized to make such a request).

The RCA is permitted to revoke the certificates they issue at the DS PMA sole discretion.

4.9.2.2 CA

RCAs shall accept revocation requests as followed:

- From DS PMA.
- From designated officials of Customer in the contract for certificates limited to those asserting an affiliation with their organization.

The RCA is permitted to revoke the certificates they issue at the DS PMA sole discretion.

4.9.2.3 SUBSCRIBER

CAs shall accept revocation requests as followed:

- From Subscriber for its certificates.
- From PKI Sponsor for Device certificate.
- From Trusted Agent.
- From designated officials of Affiliated Organizations for certificates limited to those asserting an affiliation with their organization.
- Authorized roles and person as described in Customer RPS.

The CA is permitted to revoke the certificates they issue at the DS PMA’s sole discretion.

4.9.3 PROCEDURE FOR REVOCATION REQUEST

A revocation request shall identify the certificate to be revoked, explain the reason for revocation, and allow the request to be authenticated (digitally or manually signed). Upon receipt, the revocation request shall be authenticated, and the corresponding certificate shall be revoked.

For the cross-certificate and CA, the RCA shall authenticate the request and seek approval to revoke from the DS PMA. DS PMA approval is not necessary under emergency circumstances as defined in Section 4.9.1. Cross-certificate and CA certificate are revoked in DS OA premises according procedure set in RCA CPS.

For CA issuing subscriber certificate:

- If a Subscriber leaves an organization, then all Subscriber Certificates shall be revoked immediately for the reason of 'key compromise.'
- If a Subscriber's token is lost or stolen, then all Subscriber Certificates associated with that token shall be revoked immediately for the reason of 'key compromise.'
- When a certificate (e.g. PIV, CAC, etc.) is revoked for the reason of key compromise, the derivative certificates (i.e., certificates issued on the basis of the compromised certificate) shall also be revoked. If it is determined that a private key used to authorize the issuance of one or more certificates may have been compromised, all certificates directly or indirectly authorized by that private key since the date of the actual or suspected compromise shall be revoked or shall be verified as appropriately issued.

Practice Note: This requirement pertains to credentials directly derived from an end entity certificate where the derived certificate is issued to the same Subscriber or device (e.g. FIPS 201-2 derived credentials).

Customer RPS details revocation process for Subscriber certificate.

4.9.4 REVOCATION REQUEST GRACE PERIOD

The revocation request grace period is the time available to the responsible party within which the responsible party must make a revocation request after reasons for revocation have been identified.

This CP does not allow a revocation grace period. Responsible parties must request revocation as soon as they identify the need for revocation.

4.9.5 TIME WITHIN WHICH CA MUST PROCESS THE REVOCATION REQUEST

For the RCA all revocation requests shall be processed within 24 hours of receipt of request.

CAs will revoke certificates before the next CRL is published, except when the request is validated within two hours of CRL issuance. Revocation requests validated within two hours of CRL issuance shall be processed before the following CRL is published.

4.9.6 REVOCATION CHECKING REQUIREMENT FOR RELYING PARTIES

Although the CRL issued by the RCA has a validity period of 30 days, the Relying Party shall check for a refreshed CRL every 24 hours to obtain the latest cross-certificate revocations reported.

In any case, use of revoked certificates could have damaging or catastrophic consequences in certain cases. The matter of how often new revocation data should be obtained and whether to rely upon a certificate whose revocation status is temporarily unavailable is a determination to be made by the Relying Party, considering the risk, responsibility, and consequences for using a certificate whose revocation status cannot be guaranteed.

4.9.7 CRL ISSUANCE FREQUENCY

CAs shall issue CRL, even when no changes have occurred. CRL issuance encompasses designating a CRL for activation, creation and publication to replace the previous CRL.

For the RCA and CAs, the interval between CRLs shall not exceed the following:

Type of Issuance	Scope	CRL Issuance Frequency

Routine	RCAs that do not issue end entity certificates except administration of the CA itself certificates	30 days
	All other CAs	24 Hours
Emergency	CA Key Compromise	18 hours
	All other Key Compromise	18 hours

DS PMA is required to notify the TSCP upon Emergency CRL issuance for RCA or CA Key Compromise according to the requirements in the MTFSA (MOA) between the TSCP and DocuSign Inc.

4.9.8 MAXIMUM LATENCY FOR CRLS

CRLs shall be published within 4 hours of generation. Furthermore, each CRL shall be published no later than the time specified in the nextUpdate field of the previously issued CRL for same scope.

CAs and RCA shall coordinate with Repositories to reduce the latency between the moment the CA and RCA desires the CRL to be published and the moment the CRL is available to Relying Parties within the applicable Repositories.

The maximum latency between the moment a revocation request is validated and the moment the revocation information is published and available to Relying Parties shall be no greater than 24 hours.

4.9.9 ON-LINE REVOCATION/STATUS CHECKING AVAILABILITY

Not applicable.

4.9.10 ON-LINE REVOCATION CHECKING REQUIREMENTS

Not applicable.

4.9.11 OTHER FORMS OF REVOCATION ADVERTISEMENTS AVAILABLE

A CA or RCA may also use other methods to publicize the certificates it has revoked. Any alternative method must meet the following requirements:

- The alternative method must be described in the CA’s or RCA’s approved CPS.
- The alternative method must provide authentication and integrity services commensurate with the assurance level of the certificate being verified.
- The alternative method must meet the issuance and latency requirements for CRLs stated in Sections 4.9.7 and 4.9.8.

A CA or RCA is not required to check for such forms of advertisements.

Not applicable for the present CP.

4.9.12 SPECIAL REQUIREMENTS RELATED TO KEY COMPROMISE

See Section 4.9.7.

4.9.13 CIRCUMSTANCES FOR SUSPENSION

Not applicable.

4.9.14 WHO CAN REQUEST SUSPENSION

Not applicable.

4.9.15 LIMITS ON SUSPENSION PERIOD

Not applicable.

4.10 CERTIFICATE STATUS SERVICES

Not applicable.

4.10.1 OPERATIONAL CHARACTERISTICS

Not applicable.

4.10.2 SERVICE AVAILABILITY

Not applicable.

4.10.3 OPTIONAL FEATURES

Not applicable.

4.11 END OF SUBSCRIPTION

Certificates that have expired prior to or upon end of subscription are not required to be revoked. Unexpired CA certificates shall always be revoked at the end of subscription with the Customer.

4.12 KEY ESCROW AND RECOVERY

Not applicable.

4.12.1 KEY ESCROW AND RECOVERY POLICY AND PRACTICES

Not applicable.

4.12.2 SESSION KEY ENCAPSULATION AND RECOVERY POLICY AND PRACTICES

Not applicable.

5 FACILITY, MANAGEMENT AND OPERATIONAL CONTROLS

5.1 PHYSICAL CONTROLS

5.1.1 SITE LOCATION & CONSTRUCTION

The location and construction of the facility housing CA and RCA (See Section 1.3.3) equipment shall be consistent with facilities used to house high value, sensitive information. The site location and construction, when combined with other physical security protection mechanisms such as guards, high security locks, and intrusion sensors, shall provide robust protection against unauthorized access to CA and RCA equipment and records.

5.1.2 PHYSICAL ACCESS

5.1.2.1 PHYSICAL ACCESS FOR CA AND RCA EQUIPMENT

CA and RCA equipment, including remote workstations used to administer the CAs, shall always be protected from unauthorized access. The security mechanisms shall be commensurate with the level of threat in the equipment environment.

The physical security requirements pertaining to CAs are:

- Ensure no unauthorized access to the hardware is permitted
- Ensure all removable media and paper containing sensitive plain-text information is stored in secure containers
- Ensure manual or electronic monitoring for unauthorized intrusion at all times
- Ensure an access log is maintained and inspected periodically
- Require two person physical access control to both the cryptographic module and computer systemsEnsure security of remote access
- Provide at least three layers of physical access boundaries (e.g. perimeter, building, PKI room)

Removable cryptographic modules shall be deactivated prior to storage. When not in use, cryptographic modules, activation information used to access or enable cryptographic modules, and other sensitive CA equipment shall be placed in secure containers when not in use. Activation data shall either be memorized, or recorded and stored in a manner commensurate with the security afforded the cryptographic module, and shall not be stored with the cryptographic module.

A security check of the facility housing the CA and RCA equipment shall occur if the facility is to be left unattended. At a minimum, the check shall verify the following:

- The equipment is in a state appropriate to the current mode of operation (e.g., that cryptographic modules are in place when “open”, and secured when “closed”);
- Off-line RCA equipment is shut down or HSMs are deactivated and securely stored;
- 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.

A person or group of persons shall be made explicitly responsible for making such checks. When a group of persons is responsible, a log identifying the person performing a check at each instance shall be maintained. If the facility is not continuously attended, the last person to depart shall initial a sign-out sheet that indicates the date and time and assert that all necessary physical protection mechanisms are in place and activated.

5.1.2.2 PHYSICAL ACCESS FOR RA EQUIPMENT

RA equipment shall be protected from unauthorized access while the cryptographic module is installed and activated. The RA shall implement physical access controls to reduce the risk of equipment tampering even when the cryptographic module is not installed and activated. These security mechanisms shall be commensurate with the level of threat in the RA equipment environment.

5.1.2.3 PHYSICAL ACCESS FOR CSS EQUIPMENT

Not applicable.

5.1.2.4 PHYSICAL ACCESS FOR CMS EQUIPMENT

Not applicable.

5.1.3 POWER AND AIR CONDITIONING

CAs shall have backup capability sufficient to automatically lock out input, finish any pending actions, and record the state of the equipment before lack of power or air conditioning causes a shutdown. Repositories shall be provided with Uninterrupted Power sufficient for a minimum of six hours operation in the absence of commercial power.

5.1.4 WATER EXPOSURES

CA equipment shall be installed such that it is not in danger of exposure to water (e.g., on tables or elevated floors). Water exposure from fire prevention and protection measures (e.g. sprinkler systems) are excluded from this requirement.

5.1.5 FIRE PREVENTION AND PROTECTION

CA equipment shall be installed such that it is not in danger of exposure to fire (e.g., no inflammable thing stored in cage and not closed to possible explosive location). CA equipment are protected by fire prevention and protection measures (e.g. sprinkler systems for example).

5.1.6 MEDIA STORAGE

CA media shall be stored so as to protect it from accidental damage (water, fire, electromagnetic) and unauthorized physical access.

5.1.7 WASTE DISPOSAL

Sensitive media and documentation that are no longer needed for operations shall be destroyed in a secure manner. For example, sensitive paper documentation shall be shredded, burned, or otherwise rendered unrecoverable.

5.1.8 OFF-SITE BACKUP

CAs and RCA shall create full system backups sufficient to recover full PKI services from a system failure on a periodic schedule. Backups are to be performed and stored off-site not less than once every seven days. At least one full backup copy shall be stored at an off-site location separate from the CA and RCA equipment. Only the latest full backup need be retained.

The backup shall be stored at a site with physical and procedural controls commensurate to that of the operational CA and RCA.

5.2 PROCEDURAL CONTROLS

5.2.1 TRUSTED ROLES

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

The requirements of this policy are defined in terms of four roles. (Note: the information derives from the Certificate Issuing and Management Components (CIMC) Protection Profile.)

1. Administrator – authorized to install, configure, and maintain the CA; establish and maintain user accounts; configure profiles and audit parameters; and generate component keys.
2. Officer – authorized to request or approve certificates or certificate revocations.
3. Auditor – authorized to maintain audit logs.
4. Operator – authorized to perform system backup and recovery.

The following subsections provide a detailed description of the responsibilities for these primary trusted roles and secondary trusted roles.

5.2.1.1 ADMINISTRATOR

The administrator role is responsible for:

- Installation, configuration, and maintenance of the CA;
- Establishing and maintaining CA system accounts;
- Configuring certificate profiles or templates and audit parameters, and;
- Generating and backing up CA keys.

Administrators shall not issue certificates to subscribers.

5.2.1.2 OFFICER

The officer role is responsible for issuing certificates, that is:

- Registering new subscribers and requesting the issuance of certificates;
- Verifying the identity of subscribers and accuracy of information included in certificates;
- Approving and executing the issuance of certificates, and;
- Requesting, approving and executing the revocation of certificates.

5.2.1.3 AUDITOR

The auditor role is responsible for:

- Reviewing, maintaining, and archiving audit logs;
- Performing or overseeing internal compliance audits to ensure that the CA is operating in accordance with its CPS;

5.2.1.4 OPERATOR

The operator role is responsible for the routine operation of the CA equipment and operations such as system backups and recovery or changing recording media.

5.2.1.5 REGISTRATION AUTHORITY

An RA's responsibilities are:

- Verifying identity, pursuant to section 3.2;
- Entering Subscriber information, and verifying correctness;
- Securely communicating requests to and responses from the CA;
- Receiving and distributing Subscriber certificates.

The RA role is highly dependent on public key infrastructure implementations and local requirements. The responsibilities and controls for RAs shall be explicitly described in the CPS of CA.

5.2.1.6 CSS ROLES

Not applicable.

5.2.1.7 5.2.1.7 CMS ROLES

Not applicable.

5.2.2 NUMBER OF PERSONS REQUIRED PER TASK

Two or more persons are required for the following tasks:

- CA and RCA key generation;
- CA and RCA signing key activation;
- CA and RCA private key backup.

Where multiparty control for logical access is required, at least one of the participants shall be an Administrator. All participants must serve in a trusted role as defined in Section 5.2.1. Multiparty control for logical access shall not be achieved using personnel that serve in the Auditor Trusted Role.

5.2.3 IDENTIFICATION AND AUTHENTICATION FOR EACH ROLE

An individual in a trusted role shall identify and authenticate him/herself before being permitted to perform any actions set forth above for that role or identity.

5.2.4 ROLES REQUIRING SEPARATION OF DUTIES

Role separation, when required as set forth below, may be enforced either by the CA and RCA equipment, or procedurally, or by both means.

The CA, RCA and RA software and hardware shall identify and authenticate its users and shall ensure that no user identity can assume both an Administrator and an Officer role, assume both the Administrator and Auditor roles, and assume both the Auditor and Officer roles.

Requirements for the separation of roles, and limitations on use of procedural mechanisms to implement role separation, are as follows:

- Individual personnel shall be specifically designated to the four roles defined in Section 5.2.1 above
- Individuals who assume an Auditor role shall not assume any other role

  - *Practice Note: Persons in auditor role may perform backups limited to the audit logs and archive without being categorized as being in an operator trusted role.*
- Individuals who assume an Officer role shall not assume an Auditor or Administrator role.
- No individual in a trusted role shall have more than one identity.

5.3 PERSONNEL CONTROLS

5.3.1 BACKGROUND, QUALIFICATIONS, EXPERIENCE, & SECURITY CLEARANCE REQUIREMENTS

DocuSign and Customer shall identify the set of individuals assigned to primary and secondary trusted roles, who are responsible and accountable for the operation of each CA, RCA, and RA in that Entity.

All persons filling trusted roles shall be selected on the basis of loyalty, trustworthiness, and integrity and shall be subject to a background investigation. Personnel appointed to trusted roles shall:

- Have successfully completed an appropriate training program;
- Have demonstrated the ability to perform their duties;
- Be trustworthy;
- Have no other duties that would interfere or conflict with their duties for the trusted role;
- Have not been previously relieved of duties for reasons of negligence or nonperformance of duties;
- Have not been denied a security clearance, or had a security clearance revoked for cause;
- Have not been convicted of a felony offense; and
- Be appointed in writing by an approving authority.

In circumstances where satisfactory evidence of the above cannot be confirmed, an active clearance equal to or higher than U.S. Secret issued by a NATO member nation or major non-NATO ally as defined by the International Traffic in Arms Regulation (ITAR) – 22 CFR 120.32 may be used as an alternative.

Each person filling a trusted role must also satisfy at least one of the following:

- The person shall be a citizen of the country where the CA is located; or
- For PKIs operated on behalf of multinational governmental organizations, the person shall be a citizen of one of the member countries; or
- For PKIs located within the European Union, the person shall be a citizen of one of the member States of the European Union; or
- The person shall have a security clearance equivalent to U.S. Secret or higher issued by a NATO member nation or major non-NATO ally as defined by the International Traffic in Arms Regulation (ITAR) – 22 CFR 120.32; or
- For RA Administrator, Trusted Agents, and personnel appointed to the trusted roles for the RCA, in addition to the above, the person may be a citizen of the country where the function is located.

5.3.2 BACKGROUND CHECK PROCEDURES

Trusted Role Personnel (primary and secondary) shall, at a minimum, pass a background investigation covering the following areas:

- Employment;
- Education;
- Place of residence;
- Law Enforcement; and

- References.

The period of investigation must cover at least the last five years for each area, excepting the residence check which must cover at least the last three years and the employment check may be limited to the period of time the individual has been in the work-force. Regardless of the date of award, the highest educational degree shall be verified.

Adjudication of the background investigation shall be performed by a competent adjudication authority using a process consistent with Executive Order 12968 August 1995 or later, or an equivalent level of investigation and adjudication.

If a formal clearance or other check is the basis for background check, the background refresh shall be in accordance with the corresponding formal clearance or other check. Otherwise, the background check shall be refreshed every ten years.

Background check procedures shall be described in the CPS.

Background check results shall not be released except as required in Section 9.3 and 9.4.

In circumstances where an interim clearance used to satisfy background check requirements is later found unfavorable, all certificates issued while the person had a trusted role shall be re-evaluated and possibly revoked at the discretion of the CA and RCA.

5.3.3 TRAINING REQUIREMENTS

All trusted roles shall receive comprehensive training in all operational duties they are expected to perform. Training shall cover the following:

- Security principles and mechanisms applicable to the trusted role
- All PKI software versions in use by the trusted role
- All duties the trusted role is expected to perform
- Disaster recovery and business continuity procedures

Documentation shall be maintained identifying all personnel who received training and the level of training completed. Where competence was demonstrated in lieu of training, supporting documentation shall be maintained.

5.3.4 RETRAINING FREQUENCY AND REQUIREMENTS

Individuals in trusted roles shall be aware of changes in the PKI operation. Any significant change to the operations shall have a training (awareness) plan, and the execution of such plan shall be documented. Examples of such changes are CA software or hardware upgrade, changes in automated security systems, and relocation of equipment.

Documentation shall be maintained identifying all personnel who received training and the level of training completed.

5.3.5 JOB ROTATION FREQUENCY AND SEQUENCE

No stipulation.

5.3.6 SANCTIONS FOR UNAUTHORIZED ACTIONS

The DS PMA shall take appropriate actions where personnel have performed actions not authorized in this CP.

The Customer shall take appropriate actions where personnel have performed actions not authorized in this CP.

5.3.7 INDEPENDENT CONTRACTOR REQUIREMENTS

Contractor personnel employed to perform trusted role functions shall meet the personnel requirements set forth in Section 5.3 as applicable.

5.3.8 DOCUMENTATION SUPPLIED TO PERSONNEL

For the RCA and CAs, documentation sufficient to define duties and procedures for each trusted role shall be provided to the personnel filling that role. The documentation and procedures shall include the applicable portions of the CP and CPS, relevant policies or contracts, and manuals as applicable.

5.4 AUDIT LOGGING PROCEDURES

Audit log files shall be generated for all events relating to the security of the CAs, RCA and RAs. For CAs operated in a virtual machine environment (VME, For purposes of this policy, the definition of a virtual machine environment does not include cloud-based solutions (e.g., platform-as-a-server) or container type solutions (e.g., Docker), which are not permitted for any CA cross-certified with TSCP.), audit logs shall be generated for all applicable events on both the virtual machine (VM) and isolation kernel. (i.e., hypervisor).

Where possible, the security audit logs shall be automatically collected. Where this is not possible, a logbook, paper form, or other physical mechanism shall be used. All security audit logs, both electronic and non-electronic, shall be retained and made available during compliance audits and per Section 5.5.2.

5.4.1 TYPES OF EVENTS RECORDED

All security auditing capabilities of the CA, RCA, RA operating system and CA, RCA, RA applications required by this CP shall be enabled. As a result, most of the events identified in the table shall be automatically recorded. Where events cannot be automatically recorded, the CA and RCA shall implement manual procedures to satisfy this requirement.

At a minimum, each audit record shall include the following (either recorded automatically or manually for each auditable event):

- The type of event,
- The date and time the event occurred,
- A success or failure indicator, where appropriate
- The identity of the entity and/or operator that caused the event
- A message from any source received by the CA and RCA requesting an action related to the operational state of the CA and RCA is an auditable event.

The following events shall be audited:

Auditable Event	CA	RCA	RA
SECURITY AUDIT			
Any changes to the Audit parameters, e.g., audit frequency, type of event audited	X	X	X
Any attempt to delete or modify the Audit logs	X	X	X
Obtaining a third-party time-stamp	X	X	X
IDENTIFICATION AND AUTHENTICATION			
Successful and unsuccessful attempts to assume a role	X	X	X
The value of maximum authentication attempts is changed	X	X	X
The number of unsuccessful authentication attempts exceeds the maximum authentication attempts during user login	X	X	X
A person or device unlocks an account that has been locked as a result of unsuccessful authentication attempts	X	X	X
An person or device changes the type of authenticator, e.g., from password to biometrics	X	X	X
LOCAL DATA ENTRY			
All security-relevant data that is entered in the system	X	X	X
REMOTE DATA ENTRY			
All security-relevant messages that are received by the system	X	X	X
DATA EXPORT AND OUTPUT			
All successful and unsuccessful requests for sensitive and security-relevant information	X	X	X
KEY GENERATION			
Whenever the CA generates a key. (Not mandatory for single session or one-time use symmetric keys)	X	X	X
Subscriber key pair generation on Customer side	N/A	N/A	X
PRIVATE KEY LOAD AND STORAGE			
The loading of Component private keys	X	X	N/A
All access to certificate subject private keys retained within the CA for key recovery purposes	X	X	N/A
TRUSTED PUBLIC KEY ENTRY, DELETION AND STORAGE			
All changes to the trusted public keys, including additions and deletions	X	X	X
SECRET KEY STORAGE			
The manual entry of secret keys used for authentication	X	X	X
PRIVATE AND SECRET KEY EXPORT			
The export of private and secret keys (keys used for a single session or message are excluded)	X	X	N/A
CERTIFICATE REGISTRATION			
All certificate requests	X	X	X
CERTIFICATE REVOCATION			
All certificate revocation requests	X	X	X
CERTIFICATE STATUS CHANGE APPROVAL			
The approval or rejection of a certificate status change request	X	X	X
CONFIGURATION			
Any security-relevant changes to the configuration of the component	X	X	X
ACCOUNT ADMINISTRATION			
Roles and users are added or deleted	X	X	X
The access control privileges of a user account or a role are modified	X	X	X
CERTIFICATE PROFILE MANAGEMENT			
All changes to certificate profiles	X	X	N/A
CERTIFICATE STATUS SERVER MANAGEMENT			
All changes to CSS profile (e.g. OCSP profile)	N/A	N/A	N/A
REVOCATION PROFILE MANAGEMENT			

All changes to the revocation profile	X	X	N/A
CERTIFICATE REVOCATION LIST PROFILE MANAGEMENT			
All changes to the certificate revocation list profile	X	X	N/A
MISCELLANEOUS			
Appointment of an individual to a Trusted Role	X	X	X
Designation of personnel for multiparty control	X	X	X
Installation of the Operating System	X	X	X
Installation of PKI Application	X	X	X
Installing hardware cryptographic modules	X	X	X
Removing hardware cryptographic modules	X	X	X
Destruction of cryptographic modules	X	X	X
System Startup	X	X	X
Logon Attempts to PKI Applications	X	X	X
Receipt of Hardware/Software	X	X	X
Attempts to set passwords	X	X	X
Attempts to modify passwords	X	X	X
Backing up internal database	X	X	N/A
Restoring internal database	X	X	N/A
File manipulation (e.g., creation, renaming, moving)	X	X	N/A
Posting of any material to a repository	X	X	N/A
Access to CA internal database	X	X	N/A
All certificate compromise notification requests	X	X	X
Loading tokens with certificates	X	X	X
Shipment of Tokens	X	X	X
Zeroizing tokens	X	X	X
Re-key of the Component	X	X	X
Configuration changes:	X	X	X
• Hardware	X	X	N/A
• Software	X	X	X
• Operating System	X	X	X
• Patches	X	X	N/A
• Security Profiles	X	X	X
PHYSICAL ACCESS / SITE SECURITY			
Personnel Access to room housing component	X	X	N/A
Access to the Component	X	X	N/A
Known or suspected violations of physical security	X	X	X
ANOMALIES			
Software Error conditions	X	X	X
Software check integrity failures	X	X	X
Receipt of improper messages	X	X	X
Misrouted messages	X	X	X
Network attacks (suspected or confirmed)	X	X	X
Equipment failure	X	X	N/A
Electrical power outages	X	X	N/A
Uninterruptible Power Supply (UPS) failure	X	X	N/A
Obvious and significant network service or access failures	X	X	N/A
Violations of Certificate Policy	X	X	X
Violations of Certification Practice Statement	X	X	X
Resetting Operating System clock	X	X	X

5.4.2 LOG PROCESSING FREQUENCY

Audit logs shall be reviewed at least every month, except for RCA where the review shall be performed the longer between each month and when the system is activated.

Such reviews involve verifying that the log has not been tampered with, and then briefly inspecting log entries, with a more thorough investigation of any alerts or irregularities in the log. Examples of irregularities include discontinuities in the logs and loss of audit data.

A statistically significant set of security audit data generated by CA, RCA, RA since the last review shall be examined (where the confidence intervals for each category of security audit data are determined by the security ramifications of the category and the availability of tools to perform such a review), as well as a reasonable search for any evidence of malicious activity. Actions taken as a result of these reviews shall be documented.

An auditor trusted role shall explain all significant events in an audit log summary.

5.4.3 RETENTION PERIOD FOR AUDIT LOGS

Audit logs shall be retained on-site for the longer of when it is reviewed and 60 days. For CA and RCA the individual who removes audit logs, either directly or through supervision, shall be an auditor trusted role. For RA, the individual who removes audit logs shall be a system administrator who is not an RA.

5.4.4 PROTECTION OF AUDIT LOG

CA, RCA, RA system configuration and procedures must be implemented together to ensure that:

- Only personnel assigned to Trusted Roles have read access to the logs;
- Only authorized people may archive audit logs; and,
- Audit logs are not modified.

The person performing audit log archive need not have modify access, but procedures must be implemented to protect archived data from destruction prior to the end of the audit log retention period (note that deletion requires modification access).

The off-site storage location for audit logs shall be a safe, secure location separate from the location where the data was generated.

Practice Note: If a system over-writes audit logs after a given time, the audit log is not considered deleted or destroyed if the audit log has been backed up and archived.

5.4.5 AUDIT LOG BACKUP PROCEDURES

Audit logs and audit summaries shall be backed up at least monthly, except for RCA where the backup shall be performed the longer between monthly and when the system is activated. With sufficient system redundancy in place, backups for the RCA shall be performed at least every three months if an operation with RCA has been from the last backup.

A copy of the audit log shall be sent off-site on a monthly basis.

5.4.6 AUDIT COLLECTION SYSTEM (INTERNAL VS. EXTERNAL)

The audit log collection system may or may not be external to the CA, RCA, or RA system. Automated audit processes shall be invoked at system (or application) startup and cease only at system (or application) shutdown. Should it become apparent that an automated audit system has failed, and the integrity of the system or confidentiality of the information protected by the system is at risk, then the CA and RCA shall determine whether to suspend its operation until the problem is remediated.

5.4.7 NOTIFICATION TO EVENT-CAUSING SUBJECT

This CP imposes no requirement to provide notice that an event was audited to the individual, organization, device, or application that caused the event.

5.4.8 VULNERABILITY ASSESSMENTS

See Section 5.4.2.

5.5 RECORDS ARCHIVAL

CA, RCA and RA archive records shall be sufficiently detailed as to verify that the PKI was properly operated as well as verify the validity of any certificate (including those revoked or expired) issued by the CA and RCA.

5.5.1 TYPES OF RECORDS ARCHIVED

At a minimum, the following data shall be recorded for archive in accordance with each assurance level:

Data To Be Archived	CA	RCA	RA
Certificate Policy	X	X	X
Certification Practice Statement	X	X	X
Contractual obligations	X	X	X
Other agreements concerning operations of the CA	X	X	X
System and equipment configuration	X	X	N/A
Modifications and updates to system or configuration	X	X	N/A
Certificate requests	X	X	N/A
Revocation requests	X	X	N/A
Subscriber identity Authentication data as per Section 3.2.3	X	X	X
Documentation of receipt and acceptance of certificates (if applicable)	X	X	X
Signed Subscriber Agreements	X	X	X
Documentation of receipt of tokens	X	X	X
All certificates issued or published	X	X	N/A
Record of Component Re-key	X	X	X
All CRLs issued and/or published	X	X	N/A
All Audit Logs	X	X	X
Other data or applications to verify archive contents	X	X	X
Documentation required by compliance auditors	X	X	X
Compliance Auditor reports	X	X	X

5.5.2 ARCHIVE RETENTION PERIOD

Archive data and the applications required to process it shall be retained for the longer of 10 years and 6 months and the applicable record retention laws in the CAs chosen jurisdiction. Where the retention period is longer than 10 years and 6 months the applicable CP shall state the retention period. The maximum duration shall be 17 years for RCA and CA.

If the original media cannot retain the data for the required period, a mechanism to transfer the archived data to new media shall be defined by the archive site.

5.5.3 ARCHIVE PROTECTION

No unauthorized user shall be permitted to write to or delete the archive. For CA and RCA only the auditor trusted role shall be permitted. For RA, someone other than an RA role shall be permitted.

The contents of the archive shall not be released except as determined by the DS PMA for PKI components or as required by law.

Records of individual transactions may be released upon request of any subscribers involved in the transaction or their legally recognized agents.

Archive media shall be stored in a safe, secure storage facility separate from the PKI (CA, RCA, RA) with physical and procedural security controls equivalent or better than those of the PKI (CA, RCA, RA).

5.5.4 ARCHIVE BACKUP PROCEDURES

The CPS or a referenced document shall describe how the records are backed up and how the archive backups are managed.

5.5.5 REQUIREMENTS FOR RECORD TIME-STAMPING

CA and RCA archive records shall be automatically (not for CA as it is off-line) time-stamped as they are created. The CPS shall describe how system clocks used for time-stamping are maintained in synchrony with an authoritative time standard.

5.5.6 ARCHIVE COLLECTION SYSTEM (INTERNAL OR EXTERNAL)

No stipulation.

5.5.7 PROCEDURES TO OBTAIN AND VERIFY ARCHIVE INFORMATION

Procedures detailing how to create, verify, package, transmit, and store archive information shall be defined in the applicable CPS. The contents of the archive shall not be released except in accordance with Sections 9.3 and 9.4.

5.6 KEY CHANGEOVER

To minimize risk from compromise of a RCA and CA’s private signing key, that key may be changed often; from that time on, only the new key will be used for certificate signing purposes. The older, but still valid, public key will be available to verify old signatures until all of the certificates signed using the associated private key have also expired. If the old private key is used to sign CRLs that cover certificates signed with that key, then the old key must be retained and protected.

The following table provides the maximum life times for Certificates and associated Private Keys:

Certificate Type	2048 Bit Keys		4096 Bit Keys	
	Private Key	Certificate	Private Key	Certificate
Root CA	20 years	20 years	20 years	20 years
CA	10 years	10 years	10 years	10 years (*)
Cross Certificate	10 years	10 years	10 years	10 years (*)
Subscriber	3 years	3 years	3 years	3 years

(*): For purposes of determining key usage lifetime, it will commence on activation of the key pair.

Practice Note: Maximum life times are also limited to the duration of acceptance for a cryptographic algorithm.

A CA cannot generate a Certificate for a Subscriber whose validity period would be longer than the CA Certificate validity period. The CA key pair shall be changed prior to the end of the validity period of the CA certificate in time to ensure that no certificate issued by the CA asserts a validity period that extends beyond the validity period of the CA certificate.

Practice Note: CA software may automatically shorten the validity period of a Subscriber certificate such that it will not extend beyond the CAs certificate validity period.

A RCA cannot generate a Certificate for a CA or cross-certificate whose validity period would be longer than the RCA Certificate validity period. The RCA key pair shall be changed prior to the end of the validity period of the RCA certificate in time to ensure that no certificate issued by the RCA asserts a validity period that extends beyond the validity period of the RCA certificate.

CAs shall describe their key changeover procedures in the applicable CPS. Key changeover procedures will establish key rollover certificates where a certificate containing the old public key will be signed by the new private key, and a certificate containing the new public key will be signed by the old private key.

After a CA or RCA performs a Key Changeover, the CA or RCA may continue to issue CRLs with the old key until all certificates signed with that key have expired. As an alternative, after all certificates signed with that old key have been revoked, the CA or RCA may issue a final long-term CRL using the old key, with a nextUpdate time passed the validity period of all issued certificates. This final CRL shall be available for all relying parties until the validity period of all issued certificates has passed. Once the last CRL has been issued, the old private signing key of the CA or RCA may be destroyed.

5.7 COMPROMISE AND DISASTER RECOVERY

5.7.1 INCIDENT AND COMPROMISE HANDLING PROCEDURES

If a CA or RCA detects a potential penetration it shall perform an investigation to determine the nature and extent of damage. If a CA or RCA key is suspected of compromise, the procedures in Section 5.7.3 shall be followed. Otherwise, the damage shall be assessed to determine if the remediation required will be to rebuild the impacted servers, revoke a set of certificates, and/or declare a CA or RCA key compromise.

The DS PMA shall be notified if any of the following incidents occur:

- suspected or detected compromise of the RCA or CA systems;
- physical or electronic attempts to penetrate RCA or CA systems;
- denial of service attacks on RCA or CA components;
- any incident preventing the RCA or CA from issuing a CRL within 24 hours of the time specified in the next update field of its currently valid CRL.

This will allow member entities to protect their interests as Relying Parties.

DS OA shall reestablish operational capabilities as quickly as possible in accordance with procedures set forth in the CPS for RCA and CA.

DS PMA shall provide notice to the TSCP (TPMA) of the following;

- suspected or detected compromise of an RCA or CA system;
- physical or electronic attempts to penetrate the RCA or CA system or systems;
- denial of service attacks on RCA or CA components;
- any incident preventing the Entity CA from issuing a CRL within 24 hours of the time specified in the next update field of its currently valid CRL.

In the event of an incident as described above, the DS PMA shall notify the TSCP (TPMA) within 24 hours of incident discovery, along with preliminary remediation analysis. Within 10 business days of incident resolution, the Entity shall post a notice on its public web page identifying the incident and provide notification to the TPMA. The public notice shall include the following:

- Which RCA or CA components were affected by the incident;
- The RCA’s or CA's interpretation of the incident;
- Who is impacted by the incident;
- When the incident was discovered;
- A complete list of all certificates that were either issued erroneously or not compliant with the CP/CPS as a result of the incident; and
- A statement that the incident has been fully remediated.

The notification provided directly to the TSCP (TPMA) shall also include detailed measures taken to remediate the incident.

5.7.2 COMPUTING RESOURCES, SOFTWARE, AND/OR DATA ARE CORRUPTED

When CA or RCA computing resources, software, and/or data are corrupted, the CA or RCA shall respond as follows:

- If the CA or RCA signature keys are not destroyed, CA or RCA operation shall be re-established, giving priority to the ability to generate certificate status information;
- Before returning to operation, ensure that the system’s integrity has been restored;
- If a CA or RCA cannot issue a CRL prior to the time specified in the next update field of its currently valid CRL, then all CAs that have been issued Certificates by the CA or RCA shall be securely notified immediately.
- If the ability to revoke Certificates is damaged, the CA or RCA shall re-establish revocation capabilities as quickly as possible in accordance with procedures set forth in the applicable CPS.
- If the RCA’s or CA’s revocation capability cannot be recovered in a reasonable timeframe, the CA or RCA shall determine whether the request revocation of its Certificate(s). Root CA shall determine whether to notify all Subscribers that use the CA as a trust anchor to no longer trust the Root CA as a trust anchor.

In the event of an incident as described above, the DS PMA shall post a notice on its web page identifying the incident and provide notification to the TPMA. See Section 5.7.1 for contents of the notice.

5.7.3 PRIVATE KEY COMPROMISE PROCEDURES

If a CA or RCA signature key is compromised or lost (such that compromise or loss is possible even though not certain):

- The DS PMA shall securely notify the TPMA and all cross-certified entities so that entities may issue CRLs revoking any cross-certificates issued to the compromised CA or RCA;
- A new CA or RCA key pair shall be generated by the CA or RCA in accordance with procedures set forth in the applicable CPS; and
- New CA or RCA certificates shall be issued to Entities in accordance with this CP.
- If RCA distributes its key in a self-signed certificate (e.g. Root CA), the new self-signed certificate shall be distributed as specified in Section 6.1.4.;
- The TPMA or DS PMA governing body shall also investigate what caused the compromise or loss, and what measures shall be taken to preclude recurrence.

If a RA signature key is compromised or lost (such that compromise or loss is possible even though not certain):

- The RA certificate shall be revoked immediately;
- A new RA key pair shall be generated according to the applicable CPS;

- A new RA certificate shall be requested according to the applicable CPS;
- All certificate requests approved by the RA since the data of the suspected compromise shall be reviewed to identify inappropriate certificate lifecycle actions which were a result of the compromise;
- For actions that are identified as inappropriate or for which it is uncertain whether an action was appropriate or not, the resulting active certificates shall be revoked and the subjects shall be notified of both the inappropriate action(s) and revocation event(s). The Entity CA shall post a notice on its web page describing the compromise. See Section 5.7.1 for contents of the notice.

5.7.4 BUSINESS CONTINUITY CAPABILITIES AFTER A DISASTER

In the case of a disaster whereby all of a CA's or RCA's installations are physically damaged and all copies of the CA or RCA Signing Key are destroyed as a result, the CA or RCA shall follow the requirements for key compromise as defined in Section 5.7.3.

5.8 CA, RCA & RA TERMINATION

In the event that an CA or RCA terminates operation, the DS PMA shall:

- Whenever possible, provide notice to the TPMA at least two weeks and a day, which notice period will begin to run upon written acknowledgement of the TPMA, prior to termination of any CA or RCA. For emergency termination, RCAs shall follow the notification procedures in Section 5.7.
- If it is a cross-certified RCA, request revocation on a date certain of all cross-certificates issued to the DocuSign.
- The CA, RCA, and RA shall archive all audit logs and records prior to termination.
- The CA, RCA, and RA shall destroy all of its private keys upon termination.
- The CA, RCA, and RA shall transfer all archive records to DS PMA.
- If a Root CA is terminated, the Customer shall use secure means to notify the Subscribers to delete all trust anchors representing the terminated CA Technical Security Controls.

6 TECHNICAL SECURITY CONTROLS

6.1 KEY PAIR GENERATION AND INSTALLATION

6.1.1 KEY PAIR GENERATION

Cryptographic keying material shall be generated in FIPS 140 or EAL4+ Common Criteria validated cryptographic modules according to the following minimum requirements:

Entity Role / Certificate Profile	FIPS 140-2 Level or EAL4+	Hardware or Software	Key Storage Restricted to the Module on which the Key Was Generated
RCA	EAL 4+ enhanced	Hardware	Yes for usage but there is backup of RCA private key (see section 6.2.4.1).
CA	EAL 4+ enhanced	Hardware	Yes for usage but there is backup of CA private key (see section 6.2.4.2).
Subscriber	Level 3	Hardware	Yes

Random numbers shall be generated within FIPS 140 Level 3 validated hardware cryptographic modules for Subscriber.

When Private Keys are not generated on the cryptographic module to be used, originally generated Private Keys shall be destroyed after they have been transferred to the replacement cryptographic module. This does not prohibit a key generating module from being repurposed.

For CA and RCA, key pair generation shall create a verifiable audit trail that the security requirements for procedures were followed. The documentation of the procedure must be detailed enough to show that appropriate role separation was used. Multiparty control requirements in Section 5.2.2 apply.

An independent third party shall validate the execution of the key generation.

Practice Note: This may be through witnessing key generation directly or by examining the signed and documented record of the key generation.

6.1.2 PRIVATE KEY DELIVERY TO SUBSCRIBER

CAs and RCA shall generate their own Key Pair and therefore do not need Private Key delivery.

RAs generate keys on behalf of the Subscriber and the private key is not delivered to the Subscriber. Private keys of Subscriber are stored in the hardware cryptographic modules (HSM) used by a Customer to centrally generate, store, use and destroy all Subscriber key pairs.

The following requirements must be met:

- RAs which generate a private signing key for a Subscriber shall securely deliver access to the private key to the Subscriber.
- The generation shall be performed in such a way as to avoid compromising the private key and associated activation data of the Subscriber (see section 6.4) and avoid non-required signature operation. The private key shall be protected with the associated activation data of the subscriber (see section 6.4).
- The Subscriber shall acknowledge generation of the private key(s) by activating it.
- Generation shall be accomplished in a way that ensures that the correct private key and activation data are provided and associated to the correct Subscribers.

6.1.3 PUBLIC KEY DELIVERY TO CERTIFICATE ISSUER

Key pairs are generated by CA in a way to guarantee the public key and the Subscriber's identity are securely bound by the CA for certificate issuance. The delivery mechanism shall bind the Subscriber's verified identity to the public key. If cryptography is used to achieve this binding, it must be at least as strong as the CA keys used to sign the certificate.

6.1.4 CA PUBLIC KEY DELIVERY TO RELYING PARTIES

When a CA or RCA updates its signature key pair, the CA or RCA shall distribute the new public key in a secure fashion.

The new public key may be distributed in a self-signed certificate, in a key rollover certificate, or in a new CA (e.g., cross-) certificate obtained from the issuer(s) of the current CA certificate(s).

Self-signed certificates shall be conveyed to relying parties in a secure fashion to preclude substitution attacks. Acceptable methods for self-signed certificate delivery include:

- The CA loading a self-signed certificate onto tokens delivered to Relying Parties via secure mechanisms;
- Secure distribution of self-signed certificates through secure out-of-band mechanisms;

- Comparison of the hash of the self-signed certificate against a hash value made available via authenticated out-of-band sources (note that hashes posted in-band along with the certificate are not acceptable as an authentication mechanism); and
- Loading certificates from web sites secured with a currently valid certificate of equal or greater assurance level than the certificate being downloaded. The web site certificate shall not be issued by a CA subordinated to the self-signed CA.

Key rollover certificates are signed with the CA's current private key, so secure distribution is not required.

Practice Note: To ensure the availability of the new public key, the key rollover certificates should be distributed using repositories.

CA Certificates that are signed by another CA's current private key are protected, so secure distribution is not required.

6.1.5 KEY SIZES

If the security of a particular algorithm becomes compromised, the DS PMA may require CAs or RCA to revoke affected certificates (Subscriber or CA), according to the terms of the applicable Customer contract.

All certificates, CRL and cryptographic network protocols (e.g. TLS) materially relied on or issued by the PKI shall use the following key sizes and algorithms:

Cryptographic Function	Expires 1/1/2011 - 12/31/2030	Expires after 12/31/2030
Signing (per FIPS 186-3)	2048 bit RSA Or 224 bit prime field or 233 bit binary field ECDSA	3072 bit RSA Or 256 bit prime field or 283 bit binary field ECDSA
Asymmetric Encryption (Per PKCS1 for RSA and per 800 - 56A for ECDH)	2048 bit RSA Or 224 bit prime field or 233 bit binary field ECDH	3072 bit RSA Or 256 bit prime field or 283 bit binary field ECDH
Symmetric Encryption	3 Key TDES or AES	AES

The hashing algorithm used for certificates and CRL shall meet the following minimum requirements:

Scope	Issued 1/1/2011 - 12/31/2030	Issued after 12/31/2030
RCA, CA and Subscriber Certificates	SHA-224 or SHA-256	SHA-256
CRL issued by CA and RCA	SHA-224 or SHA-256	SHA-256

CRLs shall use the same or better signature algorithm, key size, and hash algorithm used for the certificate that is being validated.

6.1.6 PUBLIC KEY PARAMETERS GENERATION AND QUALITY CHECKING

RSA keys and prime numbers shall be generated and tested in accordance with FIPS 186-3.

ECDSA and ECDH keys shall be generated in accordance with FIPS 186-3. Curves in FIPS 186-3 shall be used.

6.1.7 KEY USAGE PURPOSES (AS PER X.509 V3 KEY USAGE FIELD)

The use of a specific key for RCA, CA and Subscriber are determined by the keyUsage and Extended key usage (only for Subscriber) extension in the X.509 Certificate. The Certificate Profiles in section **Error! Reference source not found.** below specify the allowable values for this extension for different types of Certificates defined under this CP. Extended key usage OIDs shall be consistent with the key usage bits set. Subscriber Certificate is only used for digital signature operation and not for authentication (TLS) or encryption.

Public keys that are bound into certificates shall not be certified for use in encrypting.

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. The DS PMA may determine that other comparable and equivalent validation, certification, or verification international standards are sufficient (like EAL4+ enhanced qualification).

Cryptographic modules shall be validated to the FIPS 140-2 level identified in Section 6.1.1 or higher. Additionally, the DS PMA reserves the right to review technical documentation associated with any cryptographic modules under consideration for use by RCA and CAs.

6.2.1.1 CUSTODIAL SUBSCRIBER KEY STORES

Custodial Subscriber Key Stores hold keys for a number of Subscriber certificates in one location.

When a collection of private keys for Subscriber certificates are held in a single location, there is a higher risk associated with compromise of that cryptographic module than that of a single Subscriber. Cryptographic modules for Custodial Subscriber Key Stores shall be no less than FIPS 140-2 Level 2 (Hardware). In addition, authentication to the Cryptographic Device in order to activate the private key associated with a given certificate shall require authentication commensurate with the assurance level of the certificate.

6.2.2 PRIVATE KEY MULTI-PERSON CONTROL

Use of a RCA and a CA private signing key shall require action by multiple persons as set forth in Section 5.2.2 of this CP.

6.2.3 PRIVATE KEY ESCROW

Under no circumstances shall a RCA, CA and Subscriber private key be escrowed by any PKI component or third party.

6.2.4 PRIVATE KEY BACKUP

6.2.4.1 BACKUP CA PRIVATE SIGNATURE KEY

RCA and CA private signature keys shall be backed up under multi-person control, as specified in Section 5.2.2.

A copy of the RCA and CA private signature key shall be stored at or near the CA and RCA location and off site.

Procedures for key backup shall be defined in the applicable CPS.

All copies of the RCA and CA private signature key shall be accounted for and protected in the same manner as the original.

6.2.4.2 BACKUP OF SUBSCRIBER PRIVATE SIGNATURE KEY

Subscriber private signature keys may not be copied.

Subscriber private signature keys may be copied in another identical Cryptographic modules for Custodial Subscriber Key Stores, but must be held in the Subscriber's control. Storage and usage of the Subscriber private key copy must ensure security controls consistent with the protection provided by the Subscriber's cryptographic module. Backed up subscriber private signature keys shall not be stored in plain text form outside the cryptographic module.

CPS gives details about the mechanism for the copy of subscriber private key. Subscriber private key can be copied from a Cryptographic modules for Custodial Subscriber Key Stores to another for redundancy. Subscriber key are still protected and usable with same subscriber activation data.

6.2.4.3 BACKUP OF DEVICE PRIVATE KEYS

Backed up Subscriber key management keys, used by Cryptographic modules for Custodial Subscriber Key Stores, shall not be stored in plain text form outside the cryptographic module. Storage must ensure security controls consistent with the protection provided by the Subscriber's cryptographic module.

6.2.4.4 BACKUP OF SUBSCRIBER KEY MANAGEMENT PRIVATE KEYS

Subscriber private signature keys may not be copied.

Device private keys may be backed up or copied, but must be held under the control of the device's human sponsor or other authorized administrator. Backed up device private keys shall not be stored in plaintext form outside the cryptographic module. Storage must ensure security controls consistent with the protection provided by the device's cryptographic module.

6.2.5 PRIVATE KEY ARCHIVAL

RCA, CA and Subscriber private keys shall not be archived.

6.2.6 PRIVATE KEY TRANSFER INTO OR FROM A CRYPTOGRAPHIC MODULE

CA and RCA private keys may be exported from the cryptographic module in accordance with key backup procedures as described in Section 6.2.4.

At no time shall a CA or RCA private key exist in plain text outside the cryptographic module.

Private or symmetric keys used to encrypt other private keys for transport must be protected from disclosure

6.2.7 PRIVATE KEY STORAGE ON CRYPTOGRAPHIC MODULE

The cryptographic module may store Private Keys in any form as long as the keys are not accessible without an authentication mechanism that is in compliance with the FIPS 140-2 rating of the cryptographic module. The cryptographic module storing the key shall be at least as strong as that required in Section 6.1.1.

6.2.8 METHOD OF ACTIVATING PRIVATE KEY

The Subscriber must be authenticated to the cryptographic module before the activation of any private key(s). Acceptable means of authentication include but are not limited to passphrases, PINs or biometrics. Entry of activation data shall be protected from disclosure (i.e., the data should not be displayed while it is entered).

6.2.9 METHOD OF DEACTIVATING PRIVATE KEY

Cryptographic modules that have been activated shall not be available to unauthorized access. After use, the cryptographic module shall be deactivated, e.g., via a manual logout procedure, or automatically after a period of inactivity as defined in the applicable CPS.

CA and RCA Hardware cryptographic modules shall be removed and stored in a secure container when not in use.

6.2.10 METHOD OF DESTROYING PRIVATE KEY

Private signature keys shall be destroyed when they are no longer needed or when the certificates to which they correspond expire or are revoked. For software cryptographic modules, this can be accomplished by overwriting the data. For hardware cryptographic modules, this will likely be accomplished by executing a “zeroize” command. For CA, RA and RCA private signature keys, the keys shall be destroyed by individuals in Trusted Roles.

Physical destruction of hardware is not generally required.

6.2.11 CRYPTOGRAPHIC MODULE RATING

See Section 6.2.1.

6.3 OTHER ASPECTS OF KEY PAIR MANAGEMENT

6.3.1 PUBLIC KEY ARCHIVAL

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

6.3.2 CERTIFICATE OPERATIONAL PERIODS/KEY USAGE PERIODS

See Section 5.6.

6.4 ACTIVATION DATA

6.4.1 ACTIVATION DATA GENERATION AND INSTALLATION

The activation data used to unlock private keys, in conjunction with any other access control, shall have an appropriate level of strength for the keys or data to be protected and shall meet the applicable security policy requirements of the cryptographic module used to store the keys.

A Subscriber may select its own activation data. For RCA and CAs, activation data shall either be biometric data or satisfy the policy enforced at/by the cryptographic module. If the activation data must be transmitted, it shall be via an appropriately protected channel, and distinct in time and place from the associated cryptographic module.

6.4.2 ACTIVATION DATA PROTECTION

Data used to unlock private keys shall be protected from disclosure by a combination of cryptographic and physical access control mechanisms. Activation data shall be:

- Memorized;
- biometric in nature; or

- recorded and secured at the level of assurance associated with the activation of the cryptographic module and shall not be stored with the cryptographic module.

The protection mechanisms shall include a facility to temporarily lock the account, or terminate the application, after a predetermined number of failed login attempts and defined in the applicable CPS.

6.4.3 OTHER ASPECTS OF ACTIVATION DATA

CA, RCA and RA shall change activation data whenever the token is re-keyed or returned for maintenance.

6.5 COMPUTER SECURITY CONTROLS

6.5.1 SPECIFIC COMPUTER SECURITY TECHNICAL REQUIREMENTS

CA, RCA and RA shall provide the following computer security functionality through operating system, software, and physical safeguards (in a VME, these functions are applicable to both the VM and hypervisor):

- Require authenticated logins
- Provide Discretionary Access Control
- Provide a security audit capability
- Restrict access control to CA and RCA services and PKI roles
- Enforce separation of duties for PKI roles
- Require identification and authentication of PKI roles and associated identities
- Prohibit object re-use
- Require use of cryptography for session communication and database security
- Require a trusted path for identification and authentication
- Enforce domain integrity boundaries for security critical processes
- Require self-test security related CA and RCA services
- Support recovery from key or system failure
- CAs and RCA shall have a recovery mechanism for keys and the CA and RCA system

When CA and RCA equipment is hosted on evaluated platforms in support of computer security assurance requirements then the system (hardware, software, operating system) shall, when possible, operate in an evaluated configuration. At a minimum, such platforms shall use the same version of the computer operating system as that which received the evaluation rating.

CA and RCA equipment shall be configured with a minimum of the required accounts, network services, and, for RCA equipment only, no remote login.

6.5.2 COMPUTER SECURITY RATING

No stipulations.

6.6 LIFE-CYCLE SECURITY CONTROLS

6.6.1 SYSTEM DEVELOPMENT CONTROLS

The System Development Controls for CA and RCA are as follows:

- For commercial off-the-shelf software, the software shall be designed and developed under a formal, documented development methodology.
- Where open source software has been utilized, the RCA and CA shall demonstrate that security requirements were achieved through software verification & validation and structured development/lifecycle management.
- Procured Hardware and software shall be purchased and shipped in a fashion to reduce the likelihood that any particular component was tampered with (e.g., by ensuring the equipment was randomly selected at time of purchase).
- Custom developed hardware and software shall be developed in a controlled environment and the development process shall be defined and documented.
- Hardware (e.g. HSM, Computers, and Firewalls) must be shipped or delivered via controlled methods that provide a continuous chain of accountability from the purchase location to the operations location.
- The hardware and software, including the VME hypervisor, shall be dedicated to operating and supporting the CA and RCA (i.e., the system and services dedicated to the issuance and management of certificates). There shall be no other applications; hardware devices, network connections, or component software installed which is not part of the PKI operation.
- In a VME, a single hypervisor may support multiple CAs and RCA and their supporting systems, provided all systems have comparable security controls and are dedicated to the support of the CA and RCA.
- In a VME, all VM systems must operate in the same security zone as the CA and RCA.
- Proper care shall be taken to prevent malicious software from being loaded onto the equipment. Software required to perform PKI operations shall be obtained from authorized sources. Hardware and software shall be scanned for malicious code on first use and periodically thereafter.
- 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.

The System Development Controls for RA are as follows:

- Hardware and software shall be scanned for malicious code on first use and periodically thereafter.

6.6.2 SECURITY MANAGEMENT CONTROLS

The configuration of the CA and RCA equipment as well as any modifications and upgrades shall be documented and controlled. There shall be a mechanism for detecting unauthorized modification to the CA and RCA software or configuration. A formal configuration management methodology shall be used for installation and ongoing maintenance of the CA and RCA equipment. The CA and RCA software, when first loaded, shall be verified as being that supplied from the vendor, with no modifications, and be the version intended for use.

6.6.3 LIFE CYCLE SECURITY CONTROLS

No stipulation.

6.7 NETWORK SECURITY CONTROLS

RCAs and their internal PKI repositories shall be offline.

Online CAs and RAs and directories containing CA and CRL publications (or distribution) points shall employ appropriate security controls to protect against denial of service and intrusion. Such measures shall include the use of guards, firewalls, and filtering routers. Networking equipment shall turn off unused network ports and services.

Any network software present shall be necessary to PKI operations.

Any boundary control devices used to protect the network on which PKI equipment is hosted shall deny all but the necessary services to the PKI equipment even if those services are enabled for other devices on the network.

6.8 TIME-STAMPING

All CA and RCA equipment shall regularly synchronize with a time service such as the National Institute of Standards and Technology (NIST) Atomic Clock or the NIST Network Time Protocol (NTP) service.

Time derived from this time service shall be used for establishment of the following times:

- Initial validity time of a Subscriber's Certificate
- Revocation of a Subscriber's Certificate
- Posting of CRL Updates and CRL validity time
- Audit Log Timestamps

Asserted times shall be accurate to within three minutes. Electronic or manual procedures may be used to maintain system time. Clock adjustments are auditable events, see Section 5.4.1. Certificate and CRL Profiles Format

7 CERTIFICATE, CRL, AND OCSP PROFILES

7.1 CERTIFICATE PROFILE

7.1.1 VERSION NUMBERS

Issued certificates for RCA, CA and Subscriber are X.509 v3 Certificates (populate version field with integer "2"). Refer to section 10.

7.1.2 CERTIFICATE EXTENSIONS

Critical private extensions shall be interoperable in their intended community of use. RCA, CA and Subscriber certificates may include any extensions as specified by RFC 5280 in a certificate, but must include those extensions required by this CP. Any optional or additional extensions shall be non-critical and shall not conflict with the certificate and CRL profiles defined in this CP. Section 10 contains the certificate formats for RCA, cross-certificate, CA and Subscriber.

Interoperability testing shall be completed by testing a representative set of end user applications for successful certificate usage.

7.1.3 ALGORITHM OBJECT IDENTIFIERS

Certificates issued by CAs and RCA shall identify the signature algorithm using one of the following OIDs:

- sha256WithRSAEncryption: { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11 }.
- ecdsa-with-SHA224: { iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 1 }.
- ecdsa-with-SHA256: { iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2 (3) 2 }.

Certificates issued by CAs and RCA shall identify the cryptographic algorithm associated with the subject public key using one of the following OIDs:

- RsaEncryption: { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1 }.
- id-ecPublicKey: { iso(1) member-body(2) us(840) ansi-X9-62(10045) idpublicKeyType(2) 1 }.

7.1.4 NAME FORMS

The subject and issuer fields of the certificate shall be populated with an X.500 Distinguished Name. Distinguished names shall be composed of standard attribute types found in RFC 5280.

Section 10 gives the exact name form for issuer and subject set in RCA, CA, cross-certificate and Subscriber certificate and CRL.

When multiple values exist for an attribute in a DN, the DN shall be encoded so that each attribute value is encoded in a separate relative distinguished name.

7.1.5 NAME CONSTRAINTS

There is no name constraint in RCA, CA and Subscriber certificate.

7.1.6 CERTIFICATE POLICY OBJECT IDENTIFIER

Except for Self-Signed Root CA, all CA and Subscriber Certificates issued under this CP shall assert one or more of the certificate policy OIDs listed in Section 1.2. When a CA asserts a policy OID (for both CA certificates and issued end entity certificates), it shall also assert all policy OIDs corresponding to the lower assurance levels defined in this CP. Refer to section 10.

7.1.7 USAGE OF POLICY CONSTRAINTS EXTENSION

Not applicable for RCA, CA and Subscriber certificate.

Only extensions “Policy Mapping” and “Inhibit anyPolicy” (with v skipCcerts shall be set to 0) are used in cross-certificate issued by RCA to TBCA. Refer to section 10.

7.1.8 POLICY QUALIFIERS SYNTAX AND SEMANTICS

Certificates issued under this CP may contain policy qualifiers such as user notice, policy name, and CP and CPS pointers. Refer to section 10.

7.1.9 PROCESSING SEMANTICS FOR THE CRITICAL CERTIFICATE POLICY EXTENSION

Processing semantics for the critical Certificate Policy extension shall conform to X.509 certification path processing rules.

7.2 CRL PROFILE

7.2.1 VERSION NUMBERS

CAs shall issue X.509 version two (v2) CRLs (populate version field with integrate value of ‘1’). Refer to section 10.

7.2.2 CRL ENTRY EXTENSIONS

Critical private extensions shall be interoperable in their intended community of use. Section 10 contains the CRL profiles.

7.3 OCSP PROFILE

Not applicable.

7.3.1 VERSION NUMBER

Not applicable.

7.3.2 OCSP EXTENSIONS

Not applicable.

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

The DS PMA shall have a compliance audit mechanism in place to ensure that the requirements of the TSCP CP, and the DS CP and CPS are being implemented and enforced. DS PMA shall be responsible for ensuring audits are conducted for all PKI functions regardless of how or by whom the PKI components are managed and operated.

8.1 FREQUENCY OF AUDIT OR ASSESSMENTS

CAs, RCA, and RAs shall be subject to a periodic compliance audit at least once per year.

The DS OA has the right to require unscheduled compliance inspections of subordinate CA, RCA, or RA operations to validate that the subordinate entities are operating in accordance with the security practices and procedures described in their respective CPS.

The DS PMA has the right to require unscheduled compliance audits of all entities in the PKI. The DS PMA shall state the reason for any unscheduled compliance audit. This compliance audit allows the DS PMA to authorize or not (regarding the audit results) the CAs and RCA and RA to operate under this CP.

In the context of cross-certification, audits shall be requested as stated in the respective contracts and/or MOA with TSCP.

In the context of Customer, audit shall be requested as stated in the respective contract with Customer. Customer may be audited by TSCP.

8.2 IDENTITY & QUALIFICATIONS OF ASSESSOR

The compliance auditor must demonstrate competence in the field of compliance audits and at the time of the audit, the applicable CP. The compliance auditor must perform such compliance audits as a regular ongoing business activity.

The applicable CPS shall identify the compliance auditor and the required qualifications.

8.3 ASSESSOR’S RELATIONSHIP TO ASSESSED ENTITY

The compliance auditor shall either represent a firm, which is independent from the entity being audited, or it shall be sufficiently organizationally separated from that entity to provide an unbiased, independent evaluation. An example of the latter situation may be an organizational audit department, provided it can demonstrate organizational separation and independence. To further ensure independence and objectivity, the compliance auditor may not have served the entity in developing or maintaining the entity’s PKI Facility, associated IT and network systems, or CPS. The DS PMA shall determine whether a compliance auditor meets this requirement.

In the event an entity chooses to engage compliance auditor services internal to its parent organization, it shall undergo an audit from an external third-party audit firm no less often than every third year.

8.4 TOPICS COVERED BY ASSESSMENT

The purpose of a compliance audit of a PKI shall be to verify that an entity is complying with the requirements of the applicable CP, CPS, and agreement (MTFSA), MOA and contract with TSCP and Customer. The audit shall also include a compliance analysis assessment that the applicable CPS adequately addresses the requirements of the applicable CP.

Practice Note: If the auditor uses statistical sampling, all PKI components, PKI component managers and operators shall be considered in the sample. The samples shall vary on an annual basis.

8.5 ACTIONS TAKEN AS A RESULT OF DEFICIENCY

For RCA and CAs, when the compliance auditor finds a discrepancy between how the CA and RCA is designed or is being operated or maintained, and the requirements of the CP, any applicable MTFSAs, MOA, contracts, or the applicable CPS, the following actions shall be performed:

- The compliance auditor shall document the discrepancy and transmit it to the DS PMA;
- The compliance auditor shall notify the PKI component of the discrepancy;
- The DS PMA shall notify the TPMA without delay and provide a remediation plan
- The DS PMA shall determine what further notifications or actions are necessary to meet the requirements of the Entity CP, CPS, and any relevant MTFSA provisions. The DS PMA shall proceed to make such notifications and take such actions without delay.

Depending upon the nature and severity of the discrepancy, and how quickly it can be corrected, the DS PMA may decide to halt temporarily operation of the CA or RCA, to revoke a Certificate issued by the CA or RCA, or take other actions it deems appropriate. The DS PMA shall develop procedures for making and implementing such determinations.

8.6 COMMUNICATION OF RESULTS

On an annual basis, the DS PMA shall submit a compliance audit package to the TPMA. This package shall be prepared in accordance with the “Compliance Audit Requirements” document and shall include an assertion from the DS PMA that all PKI components have been audited - including any components that may be separately managed and operated. The package shall identify the versions of the CP and CPS used in the assessment.

Additionally, where necessary, the results shall be communicated as set forth in Section 8.5 above.

Practice Note: Components of the PKI may be audited separately. In such cases, the compliance audit package may include multiple audit reports (e.g. one per component) or the audit results may be aggregated by the CA and RCA compliance auditor.

9 OTHER BUSINESS AND LEGAL MATTERS

9.1 FEES

9.1.1 CERTIFICATE ISSUANCE/RENEWAL FEES

DocuSign set reasonable fees for issuance and renewal transactions provided that such fees are in accordance with the terms of the MTFSA and are described in contract with Customer.

9.1.2 CERTIFICATE ACCESS FEES

CAs and RCA shall not charge fees for accessing a certificate (e.g. PKI Repository Access as described in section 2).

9.1.3 REVOCATION OR STATUS INFORMATION ACCESS FEES

CAs shall not charge fees for accessing revocation or status information (e.g. PKI Repository Access as described in section 2).

9.1.4 FEES FOR OTHER SERVICES

See section 9.1.1.

9.1.5 REFUND POLICY

Refund policy is defined in the contract with Customer.

9.2 FINANCIAL RESPONSIBILITY

9.2.1 INSURANCE COVERAGE

DocuSign shall maintain reasonable levels of insurance coverage to address all foreseeable liability obligations to the other Entities as defined in Section 1.3.

9.2.2 OTHER ASSETS

DocuSign shall maintain reasonable and sufficient financial resources to maintain operations and fulfill obligations.

9.2.3 INSURANCE/WARRANTY COVERAGE FOR END-ENTITIES

Described in Customer contract.

9.3 CONFIDENTIALITY OF BUSINESS INFORMATION

All PKI entities shall handle confidential information according to the terms of the applicable MTFSA, MOA and contract between parties and CPS.

Entities shall maintain the confidentiality of confidential business information that is clearly marked or labeled as confidential or by its nature should reasonably be understood to be confidential and shall treat such information with the same degree of care it would for its own most confidential information.

9.4 PRIVACY OF PERSONAL INFORMATION

9.4.1 PRIVACY PLAN

CA, RCA, RA that collect, store, process, or disclose personally identifiable information shall adhere to a written privacy policy that is readily available to Subscribers and subject to applicable law.

9.4.2 INFORMATION TREATED AS PRIVATE

CA, RCA, RA shall protect all subscriber personally identifying information from unauthorized disclosure. The RCA shall also protect personally identifying information for Entity personnel collected to support cross-certification and MTFSA requirements from unauthorized disclosure. The contents of the archives maintained by PKI entities shall not be released except as required by law.

9.4.3 INFORMATION NOT DEEMED PRIVATE

Information included in certificates is not considered private and are not subject to protections outlined in Section 9.4.2.

9.4.4 RESPONSIBILITY TO PROTECT PRIVATE INFORMATION

Private information must be stored securely, and may be released only in accordance with other stipulations in Section 9.4.

9.4.5 NOTICE AND CONSENT TO USE PRIVATE INFORMATION

CA, RCA, and RA are not required to provide any notice or obtain the consent of the Subscriber or Entity personnel in order to release private information in accordance with the stipulations of Section 9.4.

9.4.6 DISCLOSURE PURSUANT TO JUDICIAL/ADMINISTRATIVE PROCESS

CA and RCA shall disclose privacy information in judicial or administrative circumstances according to their privacy policy (See Section 9.4.1).

9.4.7 OTHER INFORMATION DISCLOSURE CIRCUMSTANCES

No stipulation.

9.5 INTELLECTUAL PROPERTY RIGHTS

Entities operating under this CP shall not knowingly violate intellectual property rights held by others.

9.5.1 PROPERTY RIGHTS IN CERTIFICATES AND REVOCATION INFORMATION

CAs and RCA shall retain the property rights to certificates and revocation information they issue.

CAs and RCA grant permission to reproduce its certificates and revocation information they issue on a non-exclusive and royalty-free basis.

9.5.2 PROPERTY RIGHTS IN THE CPS

CP and all corresponding CPS is owned and/or licensed to DocuSign, Inc.

9.5.3 PROPERTY RIGHTS IN NAMES

Certificate applicants retain all rights to their names (e.g. trademarks, corporate name, and personal name).

9.5.4 PROPERTY RIGHTS IN KEYS

The subject of a certificate retains the rights and intellectual property associated with the corresponding private key.

9.6 REPRESENTATIONS & WARRANTIES

Additional representations and warranties of the PKI and contractual partners are contained in contractual agreements between the parties. This includes agreement on responsibility for export compliance.

9.6.1 CA REPRESENTATIONS AND WARRANTIES

9.6.1.1 RCA REPRESENTATIONS AND WARRANTIES

The RCA represents and warrant that to its knowledge:

- All RCA signing keys which pertain to unrevoked certificates are protected, have never been compromised, and are being maintained in a manner consistent with this CP.
- The Customer have been obligated to a Customer agreement which includes Customer representation and warrants. Further, the Customer agreement includes a representation and warranty from the Subscriber that the information 1) they have provided to the CA and 2) that is in their certificate is true and accurate.
- The RCA has an Agreement with Customer for which it presently has unrevoked certificates. The Agreement incorporates the applicable obligations from this CP and assigns them to the Customer.
- The unrevoked certificates issued by the RCA are being used for authorized and legal purposes.
- The RCA PKI repository and CRL are being maintained in a manner consistent with this CP.

9.6.1.2 CA REPRESENTATIONS AND WARRANTIES

The CA represents and warrant that to its knowledge:

- All CA signing keys which pertain to unrevoked certificates are protected, have never been compromised, and are being maintained in a manner consistent with this CP.
- Subscribers, including Customers who are issued a Subscriber certificate, have been obligated to a subscriber agreement which includes Subscriber representation and warrants. Further, the subscriber agreement includes a representation and warranty from the Subscriber that the information 1) they have provided to the CA and 2) that is in their certificate is true and accurate.
- The CA has an Agreement with all Customer for which it presently has unrevoked certificates. The Agreement incorporates the applicable obligations from this CP and assigns them to the Customer.
- The unrevoked certificates issued by the CA are being used for authorized and legal purposes.
- The CA PKI repository and CRL are being maintained in a manner consistent with this CP.

9.6.1.3 CUSTOMER REPRESENTATIONS AND WARRANTIES

The Customer represents and warrant that to its knowledge:

- Make available signed document to the Subscriber.
- Respect and operate the section(s) of the Customer RPS that deals with their duties (this part of RPS has to be transmitted to the corresponding component).
- Protect its information system and guaranty the security of the data transmitted to the RA and CA.
- Protect subscriber identity information and produce subscriber certificate with correct identity as required in CP and Customer RPS.
- Protect personal data of Subscriber according the contract and the local law and the Customer RPS.
- Manage, deliver and protect activation data of the subscriber used to activate the private key of subscriber.

- Notify Subscriber in case of Customer private key has been lost, stolen potentially compromised due to compromise of activation data or other reason.
- Notify DS PMA in case of Customer or Subscriber private key has been lost, stolen potentially compromised due to compromise of activation data or other reason.
- Document their internal procedures to complete the global CPS and its security policy.
- Respect the total of the agreement(s) that binds Customer to DocuSign Inc.
- Defines procedures to manage and use Trusted Agent and Customers roles as defined in Customer RPS.
- In case of being informed that the Subscriber(s) private key has been compromised, ensure that the certificate is not used by the Subscriber or a Relying Party.
- Protect from unauthorized use of the secret to be connected with RA platform.
- Protect from unauthorized use of the subscriber private key, the private key and all activation data managed by Customer according Customer RPS.
- Respect the CP and corresponding Customer RPS.
- Run the Subscriber’s key according procedures defined by DS PMA and referenced in Customer CPS.Alert DS PMA in case of incident due to non-respect of Customer RPS.
- Establishes contract with Customer and external entity when they are different legal entity from it with clear identification of PKI services of the Customer RPS run by the entity and all Customer's and Entity's obligations and warranties according PKI services of the Customer RPS managed.
- Communicate to DS PMA any intention to change any part of the Customer RPS and wait for approval from DS PMA before to proceed to the change and implement it.
- In case of termination of use of the service, transmit all logs and archive as described in the Customer RPS to DS PMA according protocol and means defined with DS PMA.
- Collect and archive all the document managed with RA platform according Customer RPS.
- Let auditor team mandated by DS PMA and TSCP audit and communicate the requested information to them, according to the DS PMA or TSCP intention, control and check (onsite and remotely) the compliance with the present CP and with the components Customer RPS, the contract between DocuSign and the Customer and all procedures and means (physical or IT system) used to complete the Customer RPS.

9.6.2 RA REPRESENTATIONS AND WARRANTIES

The RA represents and warrant that to its knowledge:

- It has complied with the CP and all Customers CPSs in executing its functions.
- Protect all documents of the Customer and personal data.
- Has granted the auditor team engaged and mandated by DS PMA access to its site, communicated any requested information to the auditor as required by the DS PMA, allowed any necessary control and checking (onsite and remotely) by the audit team of the compliance with the present CP and with the components Customer RPSs, the contract between DocuSign and the Customer and all other procedures and means (physical or IT system) used to complete the Customer RPS.

9.6.3 SUBSCRIBER REPRESENTATIONS AND WARRANTIES

Subscriber shall be required to sign a Subscriber Agreement containing the requirements the Subscriber shall meet respecting protection of the private key and use of the certificate before being issued the certificate. Specifically, the Subscriber agreement shall obligate the Subscriber to the following:

- Accurately represent themselves in all communications with the Trusted Agent authorities.
- Provide accurate information of its identity and affiliation information to be set in the Subscriber’s certificate.
- The Subscriber is the sole user of the key corresponding to Subscriber’s certificate(s).

- Protect their private key by protecting their activation data (used to activate its private key) at all times, in accordance with this policy, as stipulated in their certificate acceptance agreements and local procedures.
- Promptly notify the appropriate Trusted Agent in case of change in its affiliation and/or identity.
- Promptly notify the appropriate Trusted Agent upon suspicion of loss or compromise of their activation data. Such notification shall be made directly or indirectly through mechanisms consistent with the issuing Customer's RPS.
- Abide by all the terms, conditions, and restrictions levied on the use of their private keys and certificates.
- Acknowledge that any information contained within a certificate is not considered private.

9.6.4 RELYING PARTY REPRESENTATIONS AND WARRANTIES

Any time a Relying Party uses or otherwise relies on a Certificate, it represents and warrants that it shall:

- Use the Certificate for the purpose for which it was issued as defined in the key usage and enhanced key usage certificate extensions.
- Perform status checks as set forth in section 4.9.6, Revocation Checking Requirements for Relying Parties
- Check each Certificate for validity, using procedures described in the X.509 standard [ISO 9594-8], prior to reliance;
- Establish trust in the CA who issued a Certificate by verifying the Certificate path in accordance with the guidelines set by the X.509 Version 3 Amendment;
- Preserve original signed data, the applications necessary to read and process that data, and the cryptographic applications needed to verify the digital signatures on that data for as long as it may be necessary to verify the signature on that data.

Practice Note: Application upgrades may modify data structures in a manner that invalidates a previously captured and stored digital signature.

9.6.5 REPRESENTATIONS AND WARRANTIES OF AFFILIATED ORGANIZATIONS

Affiliated Organizations shall authorize the affiliation of subscribers with the organization and shall inform the DS PMA of any severance of affiliation with any current subscriber.

9.6.6 REPRESENTATIONS AND WARRANTIES OF OTHER PARTICIPANTS

None.

9.7 DISCLAIMERS OF WARRANTIES

To the extent permitted by applicable law, this CP, and MTFSA, other Customer agreements may contain disclaimers of all warranties.

TO THE EXTENT PERMITTED BY APPLICABLE LAW, DocuSign, INC. DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTIES, OTHER THAN THOSE EXPRESS WARRANTIES CONTAINED IN THIS CP.

EXCEPT FOR THE EXPLICIT REPRESENTATIONS, WARRANTIES, AND CONDITIONS PROVIDED IN THIS CP OR THOSE BETWEEN DOCUSIGN, INC. AND ITS CUSTOMERS UNDER SEPARATE AGREEMENTS: (A) CERTIFICATES ISSUED BY DOCUSIGN, INC. ARE PROVIDED "AS IS", AND DOCUSIGN, INC., ITS EMPLOYEES, OFFICERS, AGENTS, REPRESENTATIVES, AND DIRECTORS DISCLAIM ALL OTHER WARRANTIES, CONDITIONS AND OBLIGATIONS OF EVERY TYPE (INCLUDING, WITHOUT LIMITATION, ANY WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, TITLE, SECURITY, SATISFACTORY QUALITY, OR FITNESS FOR A PARTICULAR PURPOSE, OR ACCURACY AND COMPLETENESS OF INFORMATION PROVIDED), AND FURTHER DISCLAIM ANY AND ALL LIABILITY FOR NEGLIGENCE, FAILURE TO WARN, OR LACK OF REASONABLE CARE AND (B) THE ENTIRE RISK OF THE USE OF ANY DOCUSIGN, INC. CERTIFICATES, ANY SERVICES PROVIDED BY DOCUSIGN, INC., OR THE VALIDATION OF ANY DIGITAL SIGNATURES LIES WITH THE APPLICABLE PARTICIPANT.

9.8 LIMITATIONS OF LIABILITY

Limitation of Liability between DocuSign, Inc. and TSCP shall be defined in MTFSA (MOA) with TSCP.

The liability (and/or limitation thereof) of Subscribers shall be as set forth in the applicable subscriber agreement, subject to the applicable law governing the relationship between the parties.

The liability (and/or limitation thereof) of DocuSign to Customer shall be set forth in the applicable Customer agreements, whether the Customer uses a dedicated Customer CA or DocuSign Generic CA to issue Subscriber Certificates.

The liability (and/or limitation thereof) of Relying Parties may be as set forth in the applicable Relying Party Agreements between the applicable Customer and the Relying Party.

OTHERWISE, TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL DOCUSIGN, INC. BE LIABLE FOR ANY INDIRECT DAMAGES OF ANY KIND, INCLUDING CONSEQUENTIAL, INCIDENTAL, SPECIAL, PUNITIVE, ANY COSTS, EXPENSES, OR LOSS OF PROFITS, OR OTHER DAMAGES WHATSOEVER ARISING OUT OF OR RELATED TO THIS CP, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT SHALL DOCUSIGN, INC. BE LIABLE FOR ANY USAGE OF CERTIFICATE THAT EXCEEDS THE LIMITATIONS OF USAGE STATED UNDER THIS CP OR THAT IS NOT IN COMPLIANCE WITH THIS CP AND ASSOCIATED CPS.

DocuSign, INC. SHALL NOT BE LIABLE FOR ANY DAMAGE ARISING FROM THE COMPROMISE OF A SUBSCRIBER’S PRIVATE KEY OR ANY LOSS OF DATA. THE TOTAL, AGGREGATE LIABILITY OF EACH ENTITY CA ARISING OUT OF OR RELATED TO IMPROPER ACTIONS BY THE ENTITY CA SHALL BE LIMITED TO ONE THOUSAND DOLLARS ($1,000 USD) PER TRANSACTION AND ONE MILLION DOLLARS ($1 MILLION USD) PER INCIDENT.

9.9 INDEMNITIES

9.9.1 INDEMNIFICATION BY CUSTOMER

To the extent permitted by applicable law, Customer agree to indemnify and hold DocuSign, Inc. 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, Inc. may incur as a result of:

- Falsehood or misrepresentation of fact by the other Customer in the applicable contractual agreements.
- Failure by the Customer to disclose a material fact in any applicable contractual agreement, if the misrepresentation or omission was made negligently or with intent to deceive any party.
- Customer’s failure to perform obligations related to its Subscribers Private Keys, to use a Trustworthy System, or to otherwise take the precautions necessary to prevent the compromise, loss, disclosure, modification, or unauthorized use of the Subscriber Private Key, or
- The Customer’s use of a name (including without limitation within a common name, domain name, or e-mail address) that infringes upon the Intellectual Property Rights of a third party.

Any applicable agreement may include additional indemnity obligations.

9.9.2 INDEMNIFICATION BY RELYING PARTY

To the extent permitted by applicable law, and any applicable contractual agreements, Relying Party agrees to indemnify and hold DocuSign, Inc. harmless from any acts or omissions resulting in liability, any loss or damage, and any suits and expenses of any kind including reasonable attorneys’ fees that DocuSign, Inc. may incur as a result of:

- The Relying Party’s failure to perform the obligations of a Relying Party,

- The Relying Party's reliance on a Certificate that is not reasonable under the circumstances,
- The Relying Party's reliance on a "pass-through" certificate policy OID, or
- The Relying Party's failure to check the status of such Certificate to determine if the Certificate is expired or revoked.

Any applicable contractual agreement with DocuSign, Inc. may include additional indemnity obligations.

9.10 TERM AND TERMINATION

9.10.1 TERM

This CP has no specified term.

9.10.2 TERMINATION

Termination of this CP is at the discretion of the DS PMA. This CP survives termination of any MTFSA or other Customer agreement.

This CP may be amended from time to time, and shall remain in force until replaced by a newer version or until terminated. Termination of this CP is at the discretion of the DS PMA. For purposes of clarity, termination of any Memoranda of Agreement or Customer agreement shall not operate as a termination of this CP unless this CP is explicitly terminated by a separate resolution of the DS PMA.

9.10.3 EFFECT OF TERMINATION AND SURVIVAL

The following requirements of this CP remain in effect through the end of the archive period for the last certificate issued: 2.1.1, 2.2, 5.4, 5.5, 6.2-6.4, 6.8, 9.2-9.4, 9.7-9.10, and 9.13-9.16.

9.11 INDIVIDUAL NOTICES & COMMUNICATIONS WITH PARTICIPANTS

Unless otherwise specified in an MTFSA, DS PMA shall use commercially reasonable methods for communications commensurate with the sensitivity of the communication.

For RCA and CAs, any planned change to the infrastructure that has the potential to affect the DS OA operational environment shall be communicated to the TPMA at least two weeks and a day prior to implementation, which notice period will begin to run upon written acknowledgement by the TPMA. All new artifacts (RCA certificate, CA certificates, CRL DP, AIA and/or SIA URLs, etc.) produced as a result of the change must be provided to the TPMA within 24 hours following implementation.

9.12 AMENDMENTS

9.12.1 PROCEDURE FOR AMENDMENT

The DS PMA shall review this CP at least once every year. Corrections, updates, or suggested changes to this CP shall be communicated to every Customer if there is an impact on the Customer RPS.

This CP and amendments to it become effective once approved by the DS PMA, and published into the DocuSign PKI Repository.

Additional reviews may be performed at any time at the discretion of the DS PMA. If the DS PMA wishes to recommend amendments, including modifications and corrections, to the CP or CPS, such amendments shall be circulated to appropriate parties identified by the DS PMA. Comments from such parties will be collected by the DS PMA in a fashion prescribed by the DS PMA.

After collection and incorporation of comments, the DS PMA shall make the necessary amendments. Following approval by the DS PMA, public notification of amendments shall be made.

Notwithstanding the foregoing, if the DS PMA believes that material amendments to the CP are necessary immediately to stop or prevent a breach of the security of DocuSign; DocuSign shall be entitled to make such amendments effective immediately CP upon publication in the Repository for on-line access. DocuSign shall use commercially reasonable efforts to immediately notify cross certified CAs of such changes.

9.12.2 NOTIFICATION MECHANISM AND PERIOD

For the RCA and CA, proposed changes to this CP shall be distributed electronically to DS PMA members and observers in accordance with the DS PMA Charter. The CP approved by the DS PMA shall be published into the DocuSign PKI Repository.

Errors, updates and anticipated changes to the CP and CPS resulting from reviews shall be published online. In addition, changes are communicated to every cross-certified CA via a designated point of contact, including a description of the change.

This CP and all subsequent changes to it shall be made publicly available within seven days of approval.

9.12.3 CIRCUMSTANCES UNDER WHICH OID MUST BE CHANGED

Certificate Policy OIDs shall be changed if the DS PMA determines that a change in the CP reduces the level of assurance provided.

9.13 DISPUTE RESOLUTION PROVISIONS

Provisions for resolving disputes between the DocuSign Inc and contractually linked entities shall be set forth in the applicable agreements between the parties.

Otherwise, any dispute in connection with this CP shall be resolved by binding arbitration in accordance with the rules of the American Arbitration Association in effect at the time of the dispute. The arbitration rules shall be used as follows:

- One or more parties is a non-US Entity: International Rules
- Otherwise: Commercial Rules

The arbitration panel shall consist of one (1) neutral arbitrator if the amount in controversy is less than $10,000, otherwise the panel shall consist of three (3) neutral arbitrators, each an attorney with five (5) or more years of experience in computer and technology law and/or the primary area of law as to which the dispute relates. The arbitrator(s) shall have never been employed (either as an employee or as an independent consultant) by either of the Parties, or any parent, subsidiary or affiliate thereof. The Parties shall have the right to take discovery of the other Party by any or all methods provided in the Federal Rules of Civil Procedure. The arbitrator(s) may upon request exclude from being used in the arbitration proceeding any evidence not made available to the other Party pursuant to a proper discovery request. The arbitrator(s) shall apply federal law of the United States and/or the law of the State of California, and the arbitration proceeding shall be held in California, USA or in such other location as is mutually agreed upon. The cost of the arbitration shall be borne equally by the Parties, unless the arbitrator(s) awards costs and attorneys' fees to the prevailing Party. Notwithstanding the choice of law provision in this Agreement, the Federal Arbitration Act, except as modified herein, shall govern the interpretation and enforcement of this provision. All arbitration proceedings shall be conducted in English. Any claim, dispute and controversy shall be arbitrated on an individual basis and not aggregated with the claims of any third-party class action arbitration is prohibited. The arbitrator(s) shall have no discretion to award punitive damages. Notwithstanding the foregoing dispute resolution procedures, either Party may apply to any court having jurisdiction to (i) enforce the agreement to arbitrate, (ii) seek provisional injunctive relief so as to maintain the status quo until the arbitration award is rendered or the dispute in otherwise resolved, or to otherwise prevent irreparable harm, (iii) avoid the expiration of any applicable limitation period, (iv) preserve a superior position with respect to creditors, or (v) challenge or vacate any final decision or award of the arbitration panel that does not comport with the express provisions of CP.

9.14 GOVERNING LAW

Subject to any limits appearing in applicable law, the federal laws of the United States and/or the laws State of California shall govern the enforceability, construction, interpretation, and validity of this CP, irrespective of contract or other choice of law provisions and without the requirement to establish a commercial nexus in the State of California. This choice of law is made to ensure uniform procedures and interpretation for all RCA and CAs, no matter where they are located.

This governing law provision applies only to this CP. Agreements incorporating the CP by reference may have their own governing law provisions, provided that this Section 9.14 governs the enforceability, construction, interpretation, and validity of the terms of the CP separate and apart from the terms of such other agreements, subject to any limitations appearing in applicable law.

9.15 COMPLIANCE WITH APPLICABLE LAW

This CP is subject to applicable national, state, local and foreign laws, rules, regulations, ordinances, decrees, and orders including, but not limited to, restrictions on exporting or importing software, hardware, or technical information.

9.16 MISCELLANEOUS PROVISIONS

9.16.1 ENTIRE AGREEMENT

No stipulation.

9.16.2 ASSIGNMENT

Except where specified by other contracts, no party may assign or delegate this CP or any of its rights or any of its obligations under this CP, without prior written consent of the other party. Such consent shall not be unreasonably withheld.

9.16.3 SEVERABILITY

Should it be determined by a court of competent jurisdiction that a provision or set of provisions in this CP is incorrect or invalid, the other sections of this CP shall remain in effect.

9.16.4 ENFORCEMENT (ATTORNEY FEES/WAIVER OF RIGHTS)

No waiver of any breach or default or any failure to exercise any right hereunder shall be construed as a waiver of any subsequent breach or default or relinquishment of any future right to exercise such right. The headings in this CP are for convenience only and cannot be used in interpreting this CP.

9.16.5 FORCE MAJEURE

DocuSign Inc. shall not be liable for any failure or delay in its performance under this CP due to causes that are beyond its reasonable control, including, but not limited to, an act of God, act of civil or military authority, fire, epidemic, flood, earthquake, riot, war, failure of equipment, failure of telecommunications lines, lack of Internet access, sabotage, and governmental action.

DOCUSIGN, INC. HAS NO LIABILITY FOR ANY DELAYS, NONDELIVERIES, NONPAYMENTS, MIS-DELIVERIES OR SERVICE INTERRUPTIONS CAUSED BY ANY THIRD-PARTY ACTS OR THE INTERNET INFRASTRUCTURE OR ANY NETWORK EXTERNAL TO DOCUSIGN, INC.

9.17 OTHER PROVISIONS

No stipulation.

10 CERTIFICATE, CRL, AND OCSP PROFILES

There is no OCSP profile.

10.1 RCA TO TBCA CROSS CERTIFICATE

Base Certificate	Value		
Version	2 (=version 3)		
Serial number	Defined by the RCA software		
Issuer	**Attribute type**	**Attribute value**	**Directory String[1]**
	C	US	PrintableString
	O	DocuSign Inc.	UTF8String
	OU	TSCP	UTF8String
	CN	DocuSign Root CA	UTF8String
NotBefore	ZZZZ/MM/DD HH:MM:SS Z (expressed in Expressed in UTCTime) that is the date of key ceremony.		
NotAfter	ZZZZ/MM/DD HH:MM:SS Z (expressed in Expressed in UTCTime) that is the date of key ceremony plus time agreed in the contract with TSCP.		
Subject	**Attribute type**	**Attribute value**	**Directory String[2]**
	C	US	PrintableString
	O	TSCP Inc.	UTF8String
	OU	Content provided by TSCP.	UTF8String
	CN	Content provided by TSCP.	UTF8String

[1] DirectoryString = TeletexString, PrintableString, UniversalString, UTF8String ou BMPString

[2] DirectoryString = TeletexString, PrintableString, UniversalString, UTF8String ou BMPString

Subject Public Key Info	**Key generation (algorithm & OID)**	rsaEncryption {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1 }
	Key size	4096 or 2048 according key submitted by TSCP.
Signature (algorithm & OID)	sha256WithRSAEncryption iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}	

Extensions	Criticality (True/False)	Value
Authority Key Identifier	**FALSE**	
keyIdentifier		Completed with the value of the fingerprint of Root CA SKI
Subject Key Identifier	**FALSE**	
Methods of generating key ID		Defined by RCA Software (SHA1 160bits of the TBCA public key)
Key Usage	**TRUE**	
keyCertSign		Set
cRLSign		Set
Certificate Policies	**FALSE**	
policyIdentifier		1.3.6.1.4.1.42482.2.1.1.1
policyQualifier-cps		https://www.docusign.com/trust/compliance/public-certificates
Policy Mapping	**FALSE**	
Policy Mapping		[{1.3.6.1.4.1.42482.2.1.1.1} {1.3.6.1.4.1.38099.1.1.1.2 }], [{1.3.6.1.4.1.42482.2.1.1.3} {1.3.6.1.4.1.38099.1.1.1.13}],
Basic Constraint	**TRUE**	
cA		True
pathLenConstraint		None
Authority Information Access	**FALSE**	
caIssuers		http://crt.dsf.docusign.net/DocuSignRootCA.p7c
CRL Distribution Points	**FALSE**	
distributionPoint		URI: http://crl.dsf.docusign.net/DocuSignRootCA.crl
Inhibit anyPolicy	**FALSE**	
skipCerts		0

10.2 RCA: SELF-SIGNED ROOT CERTIFICATE / TRUST ANCHOR

Base Certificate	Value		
Version	2 (=version 3)		
Serial number	Defined by the RCA software		
Issuer	**Attribute type**	**Attribute value**	**Directory String[3]**
	C	US	PrintableString
	O	DocuSign Inc.	UTF8String
	OU	TSCP	UTF8String
	CN	DocuSign Root CA	UTF8String
NotBefore	ZZZZ/MM/DD HH:MM:SS Z (expressed in Expressed in UTCTime) that is the date of key ceremony.		
NotAfter	ZZZZ/MM/DD HH:MM:SS Z (expressed in Expressed in UTCTime) that is the date of key ceremony plus 20 years.		
Subject	**Attribute type**	**Attribute value**	**Directory String[4]**
	C	US	PrintableString
	O	DocuSign Inc.	UTF8String
	OU	TSCP	UTF8String
	CN	DocuSign Root CA	UTF8String
Subject Public Key Info	**Key generation (algorithm & OID)**	rsaEncryption {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1 }	
	Key size	4096	
Signature (algorithm & OID)	sha256WithRSAEncryption iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}		

Extensions	Criticality (True/False)	Value
Subject Key Identifier	**FALSE**	
Methods of generating key ID		Defined by RCA Software (SHA1 160bits of the RCA public key)
Key Usage	**TRUE**	
keyCertSign		Set

[3] DirectoryString = TeletexString, PrintableString, UniversalString, UTF8String ou BMPString

[4] DirectoryString = TeletexString, PrintableString, UniversalString, UTF8String ou BMPString

Extensions	**Criticality (True/False)**	**Value**
cRLSign		Set
Digital Signature		Set
nonRepudiation		Set
Basic Constraint	**TRUE**	
cA		True
pathLenConstraint		None

10.3 CA: POLICY CA OR ISSUING CA CERTIFICATE

10.3.1CA: DOCUSIGN GENERIC CA

Base Certificate	**Value**		
Version	2 (=version 3)		
Serial number	Defined by the RCA software		
Issuer	**Attribute type**	**Attribute value**	**Directory String**[5]
	C	US	PrintableString
	O	DocuSign Inc.	UTF8String
	OU	TSCP	UTF8String
	CN	DocuSign Root CA	UTF8String
NotBefore	ZZZZ/MM/DD HH:MM:SS Z (expressed in Expressed in UTCTime) that is the date of key ceremony.		
NotAfter	ZZZZ/MM/DD HH:MM:SS Z (expressed in Expressed in UTCTime) that is the date of key ceremony plus 10 years.		
Subject	**Attribute type**	**Attribute value**	**Directory String**[6]
	C	US	PrintableString
	O	DocuSign Inc.	UTF8String
	OU	TSCP	UTF8String

[5] DirectoryString = TeletexString, PrintableString, UniversalString, UTF8String ou BMPString

[6] DirectoryString = TeletexString, PrintableString, UniversalString, UTF8String ou BMPString

	CN	DocuSign CA for TSCP G<X where is an incremental integer starting from 1 for first CA>	UTF8String
Subject Public Key Info	**Key generation (algorithm & OID)**	rsaEncryption {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1 }	
	Key size	2048	
Signature (algorithm & OID)	sha256WithRSAEncryption iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}		

Extensions	**Criticality (True/False)**	**Value**
Authority Key Identifier	**FALSE**	
keyIdentifier		Defined by RCA Software (SHA1 160bits of the RCA public key)
Subject Key Identifier	**FALSE**	
Methods of generating key ID		Octet String (same as in PKCS-10 request from the CA)
Key Usage	**TRUE**	
keyCertSign		Set
cRLSign		Set
Digital Signature		Set
nonRepudiation		Set
Basic Constraint	**TRUE**	
cA		True
pathLenConstraint		0
Certificate Policies	**FALSE**	
policyIdentifier		1.3.6.1.4.1.42482.2.1.1.1
policyQualifier-cps		https://www.docusign.com/trust/compliance/public-certificates
policyIdentifier		1.3.6.1.4.1.42482.2.1.1.3
policyQualifier-cps		https://www.docusign.com/trust/compliance/public-certificates
CRL Distribution Points	**FALSE**	
distributionPoint		URI: http://crl.dsf.docusign.net/DocuSignRootCA.crl
Authority Information Access	**FALSE**	
caIssuers		http://crt.dsf.docusign.net/DocuSignRootCA.p7c

10.3.2 CA: CUSTOMER DEDICATED CA

Base Certificate	**Value**		
Version	2 (=version 3)		
Serial number	Defined by the RCA software		
Issuer	**Attribute type**	**Attribute value**	**Directory String**[7]
	C	US	PrintableString
	O	DocuSign Inc.	UTF8String
	OU	TSCP	UTF8String
	CN	DocuSign Root CA	UTF8String
NotBefore	ZZZZ/MM/DD HH:MM:SS Z (expressed in Expressed in UTCTime) that is the date of key ceremony.		
NotAfter	ZZZZ/MM/DD HH:MM:SS Z (expressed in Expressed in UTCTime) that is the date of key ceremony plus 10 years.		
Subject	**Attribute type**	**Attribute value**	**Directory String**[8]
	C	US	PrintableString
	O	DocuSign Inc.	UTF8String
	OU	TSCP	UTF8String
	CN	<Legal name of the Customer's entity> G<X where is an incremental integer starting from 1 for first CA>	UTF8String
Subject Public Key Info	**Key generation (algorithm & OID)**	rsaEncryption {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1 }	
	Key size	2048	
Signature (algorithm & OID)	sha256WithRSAEncryption iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}		

Extensions	**Criticality (True/False)**	**Value**
Authority Key Identifier	**FALSE**	
keyIdentifier		Defined by RCA Software (SHA1 160bits of the RCA public key)

[7] DirectoryString = TeletexString, PrintableString, UniversalString, UTF8String ou BMPString

[8] DirectoryString = TeletexString, PrintableString, UniversalString, UTF8String ou BMPString

Extensions	**Criticality (True/False)**	**Value**
Subject Key Identifier	**FALSE**	
Methods of generating key ID		Octet String (same as in PKCS-10 request from the CA)
Key Usage	**TRUE**	
keyCertSign		Set
cRLSign		Set
Digital Signature		Set
nonRepudiation		Set
Basic Constraint	**TRUE**	
cA		True
pathLenConstraint		0
Certificate Policies	**FALSE**	
policyIdentifier		1.3.6.1.4.1.42482.2.1.1.1
policyQualifier-cps		https://www.docusign.com/trust/compliance/public-certificates
policyIdentifier (present only if customer wants Device Certificate)		1.3.6.1.4.1.42482.2.1.1.3
policyQualifier-cps (present only if customer wants Device Certificate)		https://www.docusign.com/trust/compliance/public-certificates
CRL Distribution Points	**FALSE**	
distributionPoint		URI: http://crl.dsf.docusign.net/DocuSignRootCA.crl
Authority Information Access	**FALSE**	
caIssuers		http://crt.dsf.docusign.net/DocuSignRootCA.p7c

10.4 SUBSCRIBER: HUMAN SUBSCRIBER SIGNATURE CERTIFICATE

10.4.1 SUBSCRIBER: DOCUSIGN GENERIC CA: PHYSICAL PERSON

Base Certificate Fields	**Value**
Version	2 (=version 3)

Serial number	Defined by the software		
Issuer	**Attribute type**	**Attribute value**	**Directory String**[9]
	C	US	PrintableString
	O	DocuSign Inc.	UTF8String
	OU	TSCP	UTF8String
	CN	DocuSign CA for TSCP G<X where is an incremental integer starting from 1 for first CA>	UTF8String
NotBefore	YYYY/MM/DD HH:MM:SS Z that is the date of certificate generation.		
NotAfter	YYYY/MM/DD HH:MM:SS Z that is the date of certificate generation plus 3 years.		
Subject	**Attribute type**	**Attribute value**	**Directory String**[10]
	C	Country code on 2 character ISO 3166-1. Country where the legal entity of the Customer using the DSA box is officially registered	PrintableString
	O	<to be completed with name of the Customer configured by CA >	UTF8String
	E	<email of the Subscriber as registerer by Trusted Agent and provided by RA >	IA5String
	CN	<name and first name of the Subscriber as registerer by Trusted Agent and provided by RA >	UTF8String
Subject Public Key Info	**Key generation (algorithm & OID)**	rsaEncryption {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1 }	
	Key size	2048	
Signature (algorithm & OID)	sha256WithRSAEncryption iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}		

Extensions	**Criticality (True/False)**	**Value**
Authority Key Identifier	**FALSE**	
keyIdentifier		Value of the CA Subject Key Identifier
Subject Key Identifier	**FALSE**	
Methods of generating key ID		Defined by DSA box (SHA1 160bits of the subject public key)
Key Usage	**TRUE**	
Digital Signature		Set
nonRepudiation		Set
Extended Key Usage	**FALSE**	
1.3.6.1.4.1.311.10.3.12 (Microsoft document signing)		Set
1.2.840.113583.1.1.5 (Adobe Certified Document Service)		Set

[9] DirectoryString = TeletexString, PrintableString, UniversalString, UTF8String ou BMPString

[10] DirectoryString = TeletexString, PrintableString, UniversalString, UTF8String ou BMPString

Extensions	Criticality (True/False)	Value
Subject Alternative Name	**FALSE**	
Rfc822Name		=<UserCertMail>
Certificate Policies	**FALSE**	
policyIdentifier		1.3.6.1.4.1.42482.2.1.1.1
policyQualifier-cps		https://www.docusign.com/trust/compliance/public-certificates
CRL Distribution Points	**FALSE**	
distributionPoint		URI: http://crl.dsf.docusign.net/DocuSignCAforTSCPGX.crl
Authority Information Access	**FALSE**	
caIssuers		http://crt.dsf.docusign.net/DocuSignCAforTSCPGX.p7c

10.4.2 SUBSCRIBER: DOCUSIGN GENERIC CA: DEVICE SEAL

Base Certificate Fields	Value		
Version	2 (=version 3)		
Serial number	Defined by the software		
Issuer	**Attribute type**	**Attribute value**	**Directory String**[11]
	C	US	PrintableString
	O	DocuSign Inc.	UTF8String
	OU	TSCP	UTF8String
	CN	DocuSign CA for TSCP G<X where is an incremental integer starting from 1 for first CA>	UTF8String
NotBefore	YYYY/MM/DD HH:MM:SS Z that is the date of certificate generation.		
NotAfter	YYYY/MM/DD HH:MM:SS Z that is the date of certificate generation plus 3 years.		
Subject	**Attribute type**	**Attribute value**	**Directory String**[12]
	C	Country code on 2 character ISO 3166-1. Country where the legal entity of the Customer using the DSA box is officially registered	PrintableString
	O	<to be completed with name of the Customer configured by CA >	UTF8String
	OU	Device Seal Certificate	UTF8String

[11] DirectoryString = TeletexString, PrintableString, UniversalString, UTF8String ou BMPString

[12] DirectoryString = TeletexString, PrintableString, UniversalString, UTF8String ou BMPString

	OU	<information to clearly identify application or process comming from the common name information from AD>	UTF8String
	E	<generic email used for device provided by DSA>	IA5String
	CN	<IP Address of DSA Box>	UTF8String
Subject Public Key Info	**Key generation (algorithm & OID)**	rsaEncryption {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1 }	
	Key size	2048	
Signature (algorithm & OID)	sha256WithRSAEncryption iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}		

Extensions	**Criticality (True/False)**	**Value**
Authority Key Identifier	**FALSE**	
keyIdentifier		Value of the CA Subject Key Identifier
Subject Key Identifier	**FALSE**	
Methods of generating key ID		Defined by DSA box (SHA1 160bits of the subject public key)
Key Usage	**TRUE**	
Digital Signature		Set
Extended Key Usage	**FALSE**	
1.3.6.1.4.1.311.10.3.12 (Microsoft document signing)		Set
1.2.840.113583.1.1.5 (Adobe Certified Document Service)		Set
Subject Alternative Name	**FALSE**	
IP Address		=IP of DSA Box
Certificate Policies	**FALSE**	
policyIdentifier		1.3.6.1.4.1.42482.2.1.1.3
policyQualifier-cps		https://www.docusign.com/trust/compliance/public-certificates
CRL Distribution Points	**FALSE**	
distributionPoint		URI: http://crl.dsf.docusign.net/DocuSignCAforTSCPGX.crl
Authority Information Access	**FALSE**	
caIssuers		http://crt.dsf.docusign.net/DocuSignCAforTSCPGX.p7c

10.4.3 SUBSCRIBER: CUSTOMER DEDICATED CA: PHYSICAL PERSON

Base Certificate Fields	**Value**		
Version	2 (=version 3)		
Serial number	Defined by the software		
Issuer	**Attribute type**	**Attribute value**	**Directory String**[13]
	C	US	PrintableString
	O	DocuSign Inc.	UTF8String
	OU	TSCP	UTF8String
	CN	<Legal name of the Customer's entity> G<X where is an incremental integer starting from 1 for first CA>	UTF8String
NotBefore	YYYY/MM/DD HH:MM:SS Z that is the date of certificate generation.		
NotAfter	YYYY/MM/DD HH:MM:SS Z that is the date of certificate generation plus 3 years.		
Subject	**Attribute type**	**Attribute value**	**Directory String**[14]
	C	Country code on 2 character ISO 3166-1. Country where the legal entity of the Customer using the DSA box is officially registered	PrintableString
	O	<Legal name of the Customer's entity configured by CA>	UTF8String
	E	<Email of the Subscriber as registerer by Trusted Agent and provided by RA>	IA5String
	CN	<Name and first Name of the Subscriber as registerer by Trusted Agent and provided by RA >	UTF8String
Subject Public Key Info	**Key generation (algorithm & OID)**	rsaEncryption {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1 }	
	Key size	2048	
Signature (algorithm & OID)	sha256WithRSAEncryption iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}		

Extensions	**Criticality (True/False)**	**Value**
Authority Key Identifier	**FALSE**	
keyIdentifier		Value of the CA Subject Key Identifier
Subject Key Identifier	**FALSE**	
Methods of generating key ID		Defined by DSA box (SHA1 160bits of the subject public key)
Key Usage	**TRUE**	
Digital Signature		Set
nonRepudiation		Set
Extended Key Usage	**FALSE**	

[13] DirectoryString = TeletexString, PrintableString, UniversalString, UTF8String ou BMPString

[14] DirectoryString = TeletexString, PrintableString, UniversalString, UTF8String ou BMPString

Extensions	Criticality (True/False)	Value
1.3.6.1.4.1.311.10.3.12 (Microsoft document signing)		Set
1.2.840.113583.1.1.5 (Adobe Certified Document Service)		Set
Subject Alternative Name	**FALSE**	
Rfc822Name		=<UserCertMail>
Certificate Policies	**FALSE**	
policyIdentifier		1.3.6.1.4.1.42482.2.1.1.1
policyQualifier-cps		https://www.docusign.com/trust/compliance/public-certificates
CRL Distribution Points	**FALSE**	
distributionPoint		URI: http://crl.dsf.docusign.net/<CN of CA Customer>.crl
Authority Information Access	**FALSE**	
caIssuers		URI: http://crt.dsf.docusign.net/<CN of CA Customer>.p7

10.4.4 SUBSCRIBER: CUSTOMER DEDICATED CA: DEVICE SEAL

Base Certificate Fields	Value		
Version	2 (=version 3)		
Serial number	Defined by the software		
Issuer	**Attribute type**	**Attribute value**	**Directory String**[15]
	C	US	PrintableString
	O	DocuSign Inc.	UTF8String
	OU	TSCP	UTF8String
	CN	<Legal name of the Customer's entity> G<X where is an incremental integer starting from 1 for first CA>	UTF8String
NotBefore	YYYY/MM/DD HH:MM:SS Z that is the date of certificate generation.		
NotAfter	YYYY/MM/DD HH:MM:SS Z that is the date of certificate generation plus 3 years.		
Subject	**Attribute type**	**Attribute value**	**Directory String**[16]
	C	Country code on 2 character ISO 3166-1. Country where the legal entity of the Customer using the DSA box is officially registered	PrintableString

[15] DirectoryString = TeletexString, PrintableString, UniversalString, UTF8String ou BMPString

[16] DirectoryString = TeletexString, PrintableString, UniversalString, UTF8String ou BMPString

	O	<Legal name of the Customer's entity configured by CA>	UTF8String
	OU	Device Seal Certificate	UTF8String
	OU	<information to clearly identify application or process comming the common name information from AD>	UTF8String
	E	<generic email used for device provided by DSA>	IA5String
	CN	<IP Address of DSA Box>	UTF8String
Subject Public Key Info	**Key generation (algorithm & OID)**	rsaEncryption {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1 }	
	Key size	2048	
Signature (algorithm & OID)	sha256WithRSAEncryption iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}		

Extensions	**Criticality (True/False)**	**Value**
Authority Key Identifier	**FALSE**	
keyIdentifier		Value of the CA Subject Key Identifier
Subject Key Identifier	**FALSE**	
Methods of generating key ID		Defined by DSA box (SHA1 160bits of the subject public key)
Key Usage	**TRUE**	
Digital Signature		Set
Extended Key Usage	**FALSE**	
1.3.6.1.4.1.311.10.3.12 (Microsoft document signing)		Set
1.2.840.113583.1.1.5 (Adobe Certified Document Service)		Set
Subject Alternative Name	**FALSE**	
IP Address		=IP of DSA Box
Certificate Policies	**FALSE**	
policyIdentifier		1.3.6.1.4.1.42482.2.1.1.3
policyQualifier-cps		https://www.docusign.com/trust/compliance/public-certificates
CRL Distribution Points	**FALSE**	
distributionPoint		URI: http://crl.dsf.docusign.net/<CN of CA Customer>.crl
Authority Information Access	**FALSE**	
caIssuers		URI: http://crt.dsf.docusign.net/<CN of CA Customer>.p7

10.5 PKCS 10 REQUEST FORMAT

CA, RCA and TBCA shall provide a CSR with the following requirements:

Field	Value
Version	V1 (0)
Subject Distinguished Name	Value approved by DS PMA and to be set in field "Subsject" with same coding in the associated certificate to be produced using the CSR.
Subject Public Key Information	RSA key modulus of the CA, RCA or TBCA
Subject's Signature	sha256WithRSAEncryption iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}

Extension	Criticality (True/False)	Value
Subject Key Identifier	**FALSE**	Defined by Software used to generate the CSR (SHA1 160bits of the subject public key)

The format of the CSR is in base 64.

10.6 RCA CRL: FULL CRL PROFILE

CRLs will be created, with the following template, and the validity dates and CRLNumbers detailed after the template in the table "Validity dates and CRL Numbers".

CRL Fields	Value
Version	1 (=version 2)

Issuer	C = US
	O = DocuSign Inc.
	OU = TSCP
	CN = DocuSign Root CA

ThisUpdate	YYYY/MM/DD 12:00:00 Z (date shall be taken from the table below)
NextUpdate	YYYY/MM/DD 12:00:00 Z (date is defined in table below "Validity dates and CRL Numbers")
Signature (algorithm & OID)	sha256WithRSAEncryption iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}
Revoked certificates list	Completed by RCA with serial number of CA or TBCA revoked non-expired certificate.

CRL Extensions	Criticality (True/False)	Value
Authority Key Identifier	**FALSE**	
keyIdentifier		Defined by issuer RCA (in its Subject Key Identifier)
CRL Number	**FALSE**	
crlNumber		Monotonically increasing sequence number

CRL Entry Extensions	Criticality (True/False)	Value
No CRL entry extension allowed	**N/A**	N/A

10.7 CA CRL: FULL CRL PROFILE

CA creates CRLs every day, with the following template, and the validity dates and CRLNumbers detailed after the template in the table “Validity dates and CRL Numbers”.

CRL Fields	Value
Version	1 (=version 2)

Issuer	C = US (PrintableString)
	O = DocuSign Inc. (UTF8String)
	(*) OU = TSCP (UTF8String)
	(*) CN = <CN of CA as defined in section 10.3.1 and 10.3.2 above> (UTF8String)

ThisUpdate	YYYY/MM/DD HH:MM:SS Z that is the date of certificate generation.
NextUpdate	YYYY/MM/DD HH:MM:SS Z that is the date of certificate generation plus 7 days.
Signature (algorithm & OID)	sha256WithRSAEncryption iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}
Revoked certificates list	Completed by CA with serial number of Subscriber revoked non-expired certificate.

(*): shall be encoded like in CA certificate

CRL Extensions	Criticality (True/False)	Value
Authority Key Identifier	**FALSE**	
keyIdentifier		Defined by issuer CA (in its Subject Key Identifier)
CRL Number	**FALSE**	
crlNumber		Monotonically increasing sequence number

CRL Entry Extensions	Criticality (True/False)	Value
No CRL entry extension allowed	**N/A**	N/A

11 PKI REPOSITORY PROFILES

This section defines the interoperability profile for a PKI Repository as defined in Section 2.

11.1 PROTOCOL

A PKI Repository shall implement the HTTP protocol for accessing Certificates and CRL. Implementing the LDAPv3 protocol is optional.

11.2 AUTHENTICATION

No authentication shall be used to read Certificate and CRL. For X.500 Directory Server System, a 'none' authentication shall be sufficient.

11.3 NAMING

For X.500 Directory Server System:

- CA Certificates shall be stored in the entry that appears in the Certificate subject name.
- The issuedByThisCA element of crossCertificatePair shall contain the Certificate(s) issued by a CA whose name the entry represents.
- CRLs shall be stored in the Directory in the entry that appears in the CRL issuer name.

11.4 OBJECT CLASS

For X.500 Directory Server System:

- Entries that describe CAs shall be defined by organizationUnit or organizationalRole structural object class. These entries shall also be a member of pkiCA cpCPS auxiliary object classes.
- Entries that describe individuals (human entities) shall be defined by the inetOrgPerson class, which inherits from other classes: person, and organizationalPerson.

These entries shall also be a member of pkiUser auxiliary object class.

11.5 ATTRIBUTES

For X.500 Directory Server System:

- CA entries shall be populated with the caCertificate, crossCertificatePair, certificateRevocationList, cpCPS attributes, as applicable.
- User entries may be populated with userCertificate attribute containing encryption certificate. Signature certificate need not be published to the PKI Repository.

12 SMARTCARD PROFILES

Not applicable.

13 BIBLIOGRAPHY

The following documents were used in part to develop this CP:

ABADSG: Digital Signature Guidelines, 1996-08-01. http://www.abanet.org/scitech/ec/isc/dsgfree.html

AUDIT: FPKI Compliance Audit Requirements. http://www.idmanagement.gov/documents/fpki-compliance-audit-requirements

CIMC: Certificate Issuing and Management Components Family of Protection Profiles, version 1.0, October 31, 2001.

FIPS 140-2: Security Requirements for Cryptographic Modules May 25, 2001. http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

FIPS 186-2: Digital Signature Standard, January 27, 2000. http://csrc.nist.gov/publications/fips/fips186-2/fips186-2-change1.pdf

FIPS 201: Personal Identity Verification (PIV) of Federal Employees and Contractors. http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf and http://csrc.nist.gov/publications/drafts/fips201-2/Draft_NIST-FIPS-201-2.pdf

FOIACT: 5 U.S.C. 552, Freedom of Information Act. http://www4.law.cornell.edu/uscode/5/552.html

FPKI-E: Federal PKI Version 1 Technical Specifications: Part E-X.509 Certificate and CRL Extensions Profile, 7 July 1997

FPKI-Prof: Federal PKI X.509 Certificate and CRL Extensions Profile ISO9594-8 Information Technology-Open Systems Interconnection-The Directory: Authentication Framework, 1997.

ITMRA: 40 U.S.C. 1452, Information Technology Management Reform Act of 1996. http://www4.law.cornell.edu/uscode/40/1452.html

NAG69C: Information System Security Policy and Certification Practice Statement for Certification Authorities, rev C, November 1999.

NIST SP 800-73: Interfaces for Personal Identity Verification (4 Parts) http://csrc.nist.gov/publications/PubsSPs.html

NIST SP 800-76: Biometric Data Specification for Personal Identity Verification. http://csrc.nist.gov/publications/nistpubs/800-76-1/SP800-76-1_012407.pdf

NIST SP 800-78: Cryptographic Algorithms and Key Sizes for Personal Identification Verification (PIV). http://csrc.nist.gov/publications/nistpubs/800-78-2/sp800-78-2.pdf

NSD42: National Policy for the Security of National Security Telecom and Information Systems, 5 Jul 1990. http://snyside.sunnyside.com/cpsr/privacy/computer_security/nsd_42.txt (redacted version)

NS4005: NSTISSI 4005, Safeguarding COMSEC Facilities and Material, August 1997.

NS4009: NSTISSI 4009, National Information Systems Security Glossary, January 1999.

PIV-I Profile: X.509 Certificate and Certificate Revocation List (CRL) Extensions Profile for Personal Identity Verification Interoperable (PIV-I) Cards, Date: April 23 2010, Reference Link: http://www.idmanagement.gov/documents/piv-i-x509-certificate-and-certificaterevocation-list-crl-extensions-profile

PKCS#12: Personal Information Exchange Syntax Standard, April 1997. ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-12/pkcs-12v1.pdf

RFC 2510: Certificate Management Protocol, Adams and Farrell, March 1999.

RFC 3647: Certificate Policy and Certification Practices Framework, Chokhani and Ford, Sabett, Merrill, and Wu, November 2003.

14 ACRONYNS AND ABBREVIATIONS

- AID: Application Identifier
- CA: Certification Authority
- CARL: Certificate Authority Revocation List

- CMS: Card Management System
- COMSEC: Communications Security
- CP: Certificate Policy
- CPS: Certification Practice Statement
- CRL: Certificate Revocation List
- CSOR: Computer Security Object Registry
- CSS: Certificate Status Server
- DN: Distinguished Name
- DSA: Digital Signature Algorithm
- DSS: Digital Signature Standard
- ERC: Enhanced Reliability Check
- FAR: Federal Acquisition Regulations
- FBCA: Federal Bridge Certification Authority
- FPKIMA: Federal Public Key Infrastructure Management Authority
- FED-STD: Federal Standard
- FIPS PUB: (US) Federal Information Processing Standard Publication
- FPKI: Federal Public Key Infrastructure
- FPKI-E: Federal PKI Version 1 Technical Specifications: Part E – X.509 Certificate and CRL Extensions Profile
- FPKISC: Federal PKI Steering Committee
- FPKIPA: Federal PKI Policy Authority
- GPEA: Government Paperwork Elimination Act of 1998
- GSA: General Services Administration
- HTTP: HyperText Transfer Protocol
- HSM: Hardware Security Module
- IETF: Internet Engineering Task Force
- ISO: International Organization for Standardization
- ISSO: Information Systems Security Officer
- ITU: International Telecommunications Union
- ITU-T: International Telecommunications Union – Telecommunications Sector
- ITU-TSS: International Telecommunications Union – Telecommunications System Sector
- LDAP: Lightweight Directory Access Protocol
- MOU: Memorandum of Understanding
- NIST: National Institute of Standards and Technology
- NSA: National Security Agency
- NSTISSI: National Security Telecommunications and Information Systems Security Instruction
- OCSP: Online Certificate Status Protocol
- OID: Object Identifier
- MTFSA: Master Trust Framework Service Agreement
- PCA: Principal CA
- PIN: Personal Identification Number
- PIV-I: Personal Identity Verification – Interoperable
- PKCS: Public Key Certificate Standard
- PKI: Public Key Infrastructure
- PKIX: Public Key Infrastructure X.509
- RA: Registration Authority
- RFC: Request For Comments
- RPS: Registration Practice Statement
- RSA: Rivest-Shamir-Adleman (encryption algorithm)

- SCA: Subordinate CA
- SHA-1: Secure Hash Algorithm, Version 1
- S/MIME: Secure Multipurpose Internet Mail Extension
- SSL: Secure Sockets Layer
- TSDM: Trusted Software Development Methodology
- UPN: User Principal Name
- UPS: Uninterrupted Power Supply
- URL: Uniform Resource Locator
- U.S.C.: United States Code
- UUID: Universally Unique Identifier (defined by RFC 4122)
- VME: Virtual Machine Environment

15 GLOSSARY

Access: Ability to make use of any information system (IS) resource. [NS4009]

Access Control: Process of granting access to information system resources only to authorized users, programs, processes, or other systems. [NS4009]

Accreditation: Formal declaration by a Designated Approving Authority that an Information System is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk. [NS4009]

Activation Data: Private data, other than keys, that are required to access cryptographic modules (i.e., unlock private keys for signing or decryption events).

Affiliated Organization: Organizations that authorize affiliation with Subscribers of PIV-I certificates.

Applicant: The subscriber is sometimes also called an "applicant" after applying to a certification authority for a certificate, but before the certificate issuance procedure is completed. [ABADSG footnote 32]

Archive: Long-term, physically separate storage.

Attribute Authority: An entity, recognized by the FPKIPA or comparable Entity body as having the authority to verify the association of attributes to an identity.

Audit: Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures. [NS4009]

Audit Data: Chronological record of system activities to enable the reconstruction and examination of the sequence of events and changes in an event. [NS4009, "audit trail"]

Authenticate: To confirm the identity of an entity when that identity is presented.

Authentication: Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information. [NS4009]

Backup: Copy of files and programs made to facilitate recovery if necessary. [NS4009]

Binding: Process of associating two related elements of information. [NS4009]

Biometric: A physical or behavioral characteristic of a human being.

Certificate: A digital representation of information which at least (1) identifies the certification authority issuing it, (2) names or identifies its subscriber, (3) contains the subscriber's public key, (4) identifies its operational period, and (5) is digitally signed by the certification authority issuing it. [ABADSG]. As used in this CP, the term “Certificate” refers to certificates that expressly reference the OID of this CP in the “Certificate Policies” field of an X.509 v.3 certificate.

Certification Authority (CA): An authority trusted by one or more users to issue and manage X.509 Public Key Certificates and CARLs or CRLs.

Certification Authority Revocation List (CARL): A signed, time-stamped list of serial numbers of CA public key certificates, including cross-certificates that have been revoked.

CA Facility: The collection of equipment, personnel, procedures and structures that are used by a Certification Authority to perform certificate issuance and revocation.

Certificate: A digital representation of information which at least (1) identifies the certification authority issuing it, (2) names or identifies its Subscriber, (3) contains the Subscriber’s public key, (4) identifies its operational period, and (5) is digitally signed by the certification authority issuing it. [ABADSG]

Certificate Management Authority (CMA): A Certification Authority or a Registration Authority.

Certification Authority Software: Key Management and cryptographic software used to manage certificates issued to subscribers.

Certificate Policy (CP): A Certificate Policy is a specialized form of administrative policy tuned to electronic transactions performed during certificate management. A Certificate Policy addresses all aspects associated with the generation, production, distribution, accounting, compromise recovery and administration of digital certificates. Indirectly, a certificate policy can also govern the transactions conducted using a communications system protected by a certificatebased security system. By controlling critical certificate extensions, such policies and associated enforcement technology can support provision of the security services required by particular applications.

Certification Practice Statement (CPS): A statement of the practices that a CA employs in issuing, suspending, revoking and renewing certificates and providing access to them, in accordance with specific requirements (i.e., requirements specified in this CP, or requirements specified in a contract for services).

Certificate-Related Information: Information, such as a subscriber's postal address, that is not included in a certificate. May be used by a CA managing certificates.

Certificate Revocation List (CRL): A list maintained by a Certification Authority of the certificates which it has issued that are revoked prior to their stated expiration date.

Certificate Status Authority: A trusted entity that provides on-line verification to a Relying Party of a subject certificate's trustworthiness, and may also provide additional attribute information for the subject certificate. Same as CSS (Certificate Status Server).

Client (application): A system entity, usually a computer process acting on behalf of a human user that makes use of a service provided by a server.

Common Criteria: A set of internationally accepted semantic tools and constructs for describing the security needs of customers and the security attributes of products.

Compromise: Disclosure of information to unauthorized persons, or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred. [NS4009]

Computer Security Objects Registry (CSOR): Computer Security Objects Registry operated by the National Institute of Standards and Technology.

Confidentiality: Assurance that information is not disclosed to unauthorized entities or processes. [NS4009]

Cross-Certificate: A certificate used to establish a trust relationship between two Certification Authorities.

Cryptographic Module: The set of hardware, software, firmware, or some combination thereof that implements cryptographic logic or processes, including cryptographic algorithms, and is contained within the cryptographic boundary of the module. [FIPS1401]

Cryptoperiod: Time span during which each key setting remains in effect. [NS4009]

Data Integrity: Assurance that the data are unchanged from creation to reception.

Digital Signature: The result of a transformation of a message by means of a cryptographic system using keys such that a Relying Party can determine: (1) whether the transformation was created using the private key that corresponds to the public key in the signer’s digital certificate; and (2) whether the message has been altered since the transformation was made.

Dual Use Certificate: A certificate that is intended for use with both digital signature and data encryption services.

Duration: A field within a certificate which is composed of two subfields; “date of issue” and “date of next issue”.

E-commerce: The use of network technology (especially the internet) to buy or sell goods and services.

Encrypted Network: A network that is protected from outside access by NSA approved high-grade (Type I) cryptography. Examples are SIPRNET and TOP SECRET networks.

Encryption Certificate: A certificate containing a public key that is used to encrypt electronic messages, files, documents, or data transmissions, or to establish or exchange a session key for these same purposes.

End-entity: Relying Parties and Subscribers.

Entity: For the purposes of this document, “Entity” refers to an organization, corporation, community of interest, or government agency with operational control of a CA.

Entity CA: A CA that acts on behalf of an Entity, and is under the operational control of an Entity. The Entity may be an organization, corporation, or community of interest. For the Federal Government, an Entity may be any department, subordinate element of a department, or independent organizational entity that is statutorily or constitutionally recognized as being part of the Federal Government.

FBCA Management Authority (FPKIMA): The Federal Public Key Infrastructure Management Authority is the organization selected by the Federal Public Key Infrastructure Policy Authority to be responsible for operating the Federal Bridge Certification Authority.

Federal Public Key Infrastructure Policy Authority (FPKIPA): The FPKIPA is a federal government body responsible for setting, implementing, and administering policy decisions regarding inter Entity PKI interoperability that uses the FBCA.

Firewall: Gateway that limits access between networks in accordance with local security policy. [NS4009]

High Assurance Guard (HAG): Hypervisor An enclave boundary protection device that controls access between a local area network that an enterprise system has a requirement to protect, and an external network that is outside the control of the enterprise system, with a high degree of assurance.

Hypervisor: Computer software, firmware or hardware that creates and runs virtual machines. A hypervisor uses native execution to share and manage hardware, allowing for multiple environments which are isolated from one another, yet exist on the same physical machine. Also known as an isolation kernel or a virtual machine monitor.

Information System Security Officer (ISSO): Person responsible to the designated approving authority for ensuring the security of an information system throughout its lifecycle, from design through disposal. [NS4009]

Inside threat: An entity with authorized access that has the potential to harm an information system through destruction, disclosure, modification of data, and/or denial of service.

Integrity: Protection against unauthorized modification or destruction of information. [NS4009]. A state in which information has remained unaltered from the point it was produced by a source, during transmission, storage, and eventual receipt by the destination.

Intellectual Property: Useful artistic, technical, and/or industrial information, knowledge or ideas that convey ownership and control of tangible or virtual usage and/or representation.

Intermediate CA: A CA that is subordinate to another CA, and has a CA subordinate to itself.

Key Escrow: A deposit of the private key of a subscriber and other pertinent information pursuant to an escrow agreement or similar contract binding upon the subscriber, the terms of which require one or more agents to hold the subscriber's private key for the benefit of the subscriber, an employer, or other party, upon provisions set forth in the agreement. [adapted from ABADSG, "Commercial key escrow service"]

Key Exchange: The process of exchanging public keys in order to establish secure communications.

Key Generation Material: Random numbers, pseudo-random numbers, and cryptographic parameters used in generating cryptographic keys.

Key Pair: Two mathematically related keys having the properties that (1) one key can be used to encrypt a message that can only be decrypted using the other key, and (ii) even knowing one key, it is computationally infeasible to discover the other key.

Key Recovery Policy (KRP): A key recovery policy is a specialized form of administrative policy that ensures the protection and recovery of key management private keys (i.e., decryption keys) held in escrow. A key recovery policy addresses all aspects associated with the storage and recovery of key management certificates.

Key Recovery Practice Statement (KRPS): A statement of the practices that a key recovery system employs in protecting and recovering key management private keys, in accordance with the specific requirements specified in the relevant KRP.

Local Registration Authority (LRA): A Registration Authority with responsibility for a local community.

Memorandum of Understanding (MOU): Agreement between the FPKIPA and an Entity allowing interoperability between the Entity Principal CA and the FBCA.

Mission Support Information: Information that is important to the support of deployed and contingency forces.

Mutual Authentication: Occurs when parties at both ends of a communication activity authenticate each other (see authentication).

Naming Authority: An organizational entity responsible for assigning distinguished names (DNs) and for assuring that each DN is meaningful and unique within its domain.

National Security System: Any telecommunications or information system operated by the United States Government, the function, operation, or use of which involves intelligence activities; involves cryptologic activities related to national security;

involves command and control of military forces; involves equipment that is an integral part of a weapon or weapons system; or is critical to the direct fulfillment of military or intelligence missions, but does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications). [ITMRA]

Non-Repudiation: Assurance that the sender is provided with proof of delivery and that the recipient is provided with proof of the sender's identity so that neither can later deny having processed the data. [NS4009] Technical non-repudiation refers to the assurance a Relying Party has that if a public key is used to validate a digital signature, that signature had to have been made by the corresponding private signature key. Legal non-repudiation refers to how well possession or control of the private signature key can be established.

Object Identifier (OID): A specialized formatted number that is registered with an internationally recognized standards organization. The unique alphanumeric/numeric identifier registered under the ISO registration standard to reference a specific object or object class. In the federal government PKI they are used to uniquely identify each of the seven policies and cryptographic algorithms supported.

Out-of-Band: Communication between parties utilizing a means or method that differs from the current method of communication (e.g., one party uses U.S. Postal Service mail to communicate with another party where current communication is occurring online).

Outside Threat: An unauthorized entity from outside the domain perimeter that has the potential to harm an Information System through destruction, disclosure, modification of data, and/or denial of service.

Physically Isolated Network: A network that is not connected to entities or systems outside a physically controlled space.

PKI Sponsor: Fills the role of a Subscriber for non-human system components that are named as public key certificate subjects, and is responsible for meeting the obligations of Subscribers as defined throughout this CP.

Policy Management Authority (PMA): The individual or group that is responsible for the creation and maintenance of Certificate Policies and Certification Practice Statements, and for ensuring that all Entity PKI components (e.g., CAs, CSSs, CMSs, and RAs) are audited and operated in compliance with the entity PKI CP. The PMA evaluates non-domain policies for acceptance within the domain, and generally oversees and manages the PKI certificate policies. For the FBCA, the PMA is the FPKIPA.

Principal CA: The Principal CA is a CA designated by an Entity to interoperate with the FBCA. An Entity may designate multiple Principal CAs to interoperate with the FBCA.

Privacy: Restricting access to subscriber or Relying Party information in accordance with Federal law and Entity policy.

Private Key: (1) The key of a signature key pair used to create a digital signature. (2) The key of an encryption key pair that is used to decrypt confidential information. In both cases, this key must be kept secret.

Public Key: (1) The key of a signature key pair used to validate a digital signature. (2) The key of an encryption key pair that is used to encrypt confidential information. In both cases, this key is made publicly available normally in the form of a digital certificate.

Public Key Infrastructure (PKI): A set of policies, processes, server platforms, software and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, and revoke public key certificates.

Registration Authority (RA): An entity that is responsible for identification and authentication of certificate subjects, but that does not sign or issue certificates (i.e., a Registration Authority is delegated certain tasks on behalf of an authorized CA).

Re-key (a certificate): To change the value of a cryptographic key that is being used in a cryptographic system application; this normally entails issuing a new certificate on the new public key.

Relying Party: A person or Entity who has received information that includes a certificate and a digital signature verifiable with reference to a public key listed in the certificate, and is in a position to rely on them.

Renew (a certificate): The act or process of extending the validity of the data binding asserted by a public key certificate by issuing a new certificate.

Repository: A database containing information and data relating to certificates as specified in this CP; may also be referred to as a directory.

Responsible Individual: A trustworthy person designated by a sponsoring organization to authenticate individual applicants seeking certificates on the basis of their affiliation with the sponsor.

Revoke a Certificate: To prematurely end the operational period of a certificate effective at a specific date and time.

Risk: An expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular harmful result.

Risk Tolerance: The level of risk an entity is willing to assume in order to achieve a potential desired result.

Root CA: In a hierarchical PKI, the CA whose public key serves as the most trusted datum (i.e., the beginning of trust paths) for a security domain.

Server: A system entity that provides a service in response to requests from clients.

Signature Certificate: A public key certificate that contains a public key intended for verifying digital signatures rather than encrypting data or performing any other cryptographic functions.

Subordinate CA: In a hierarchical PKI, a CA whose certificate signature key is certified by another CA, and whose activities are constrained by that other CA. (See superior CA).

Subscriber: A Subscriber is an entity that (1) is the subject named or identified in a certificate issued to that entity, (2) holds a private key that corresponds to the public key listed in the certificate, and (3) does not itself issue certificates to another party. This includes, but is not limited to, an individual or network device.

Superior CA: In a hierarchical PKI, a CA who has certified the certificate signature key of another CA, and who constrains the activities of that CA. (See subordinate CA).

System Equipment Configuration: A comprehensive accounting of all system hardware and software types and settings.

System High: The highest security level supported by an information system. [NS4009]

Technical non-repudiation: The contribution public key mechanisms to the provision of technical evidence supporting a non-repudiation security service.

Threat: Any circumstance or event with the potential to cause harm to an information system in the form of destruction, disclosure, adverse modification of data, and/or denial of service. [NS4009]

Trust List: Collection of trusted certificates used by Relying Parties to authenticate other certificates.

Trusted Agent: Entity authorized to act as a representative of an Entity in confirming Subscriber identification during the registration process. Trusted Agents do not have automated interfaces with Certification Authorities.

Trusted Certificate: A certificate that is trusted by the Relying Party on the basis of secure and authenticated delivery. The public keys included in trusted certificates are used to start certification paths. Also known as a "trust anchor".

Trusted Timestamp: A digitally signed assertion by a trusted authority that a specific digital object existed at a particular time.

Trustworthy System: Computer hardware, software and procedures that: (1) are reasonably secure from intrusion and misuse; (2) provide a reasonable level of availability, reliability, and correct operation; (3) are reasonably suited to performing their intended functions; and (4) adhere to generally accepted security procedures.

Two-Person Control: Continuous surveillance and control of positive control material at all times by a minimum of two authorized individuals, each capable of detecting incorrect and/or unauthorized procedures with respect to the task being performed and each familiar with established security and safety requirements. [NS4009]

Update (a certificate): The act or process by which data items bound in an existing public key certificate, especially authorizations granted to the subject, are changed by issuing a new certificate.

Virtual Machine Environment: An emulation of a computer system (in this case, a CA) that provides the functionality of a physical machine and a platform-independent environment. It consists of a host (virtual machine) and isolation kernel (hypervisor) and provides functionality needed to execute entire operating systems. At this time, allowed VMEs are limited to Hypervisor type virtual environments. Other technology, such as Docker Containers, is not permitted.

Zeroize: A method of erasing electronically stored data by altering the contents of the data storage so as to prevent the recovery of the data. [FIPS1401].