DocuSign Certificate Policy for External CA

Version	1.1	**Pages**	75
Status	☐ Draft	☒ Final	
Author		DocuSign Inc.	

Diffusion List	☒ External	☒ Internal
	Public	Public

History				
Date	Version	Author	Information affected	Verified by
20/09/2019	0.1	DocuSign	Creation of document	EM
21/10/2019	0.2	DocuSign	Comments of document	DF
22/10/2019	0.3	DocuSign	Integration of comments	EM
13/01/2020	1.0	DocuSign	Creation of version 1.0	EM
10/03/2020	1.1	DocuSign	Creation of version 1.1 with correct check box “FINAL”.	

SUMMARY

1 INTRODUCTION

DocuSign (DS) decided to create a trusted domain by creating a Root CA (RCA) and dedicated Certification Authority (CA) to support each Customer of DocuSign desiring to manage Subscriber Certificate with a DocuSign box on premise to sign document. These CAs can only issue subscriber certificate for signature usage.

The RCA enables interoperability among Customers and relying party who accepts the RCA and the present CP level.

The RCA issues certificates only to CAs designated by DocuSign for sole purposes of Customer.

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 and Subscriber certificates contain one 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 SCOPE

This CP governs RCA and CA and Subscriber certificates. Subscriber certificates are limited to only one type as described in section 10. Customer issues subscriber certificates from the CA hosted in a Digital Signature Appliance (DSA) which is stored on the premises of the Customer facility. There is only one generic CA for all Customers.

1.2 DOCUMENT IDENTIFICATION

There is one level of assurance in this Certificate Policy, which is defined in subsequent sections. This level of assurance has an Object Identifier (OID), to be asserted in certificates issued by the CA and RCA.

The policy OIDs is 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 policy OID as follows: 1.3.6.1.4.1.42482.2.1.1.2.

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.
- 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.
- Defines procedures for Subscriber keys and certificates management that Customers shall apply.
- Approves Customer's CPS.
- Approves compliance between security practice documents and related policies (for instance CPS/CP and procedures/CP).
- Approves final annual internal audit report of 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 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:

- Issue CA certificates for DS CA only as in this CP.
- Revoke CA certificates.
- Generate logs for RCA operation.

DS Root CA is not signed by any others type of internal or external CAs.

1.3.1.4 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.

DocuSign is 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.

1.3.2 REGISTRATION AUTHORITY (RA)

RA designates Customer 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.

Procedures to manage Subscriber's Certificate and key pairs are performed by Trusted Agent and Customer internal repository of Customer data, recorded by Trusted Agent, approved by Customer. A Customer is responsible to establish and maintain a list of all Trusted Agent and internal repository that are allowed to manage Subscribers and Subscriber data. 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 CPS delegated to the Trusted Agent.

The Customer CPS 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 CPS 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 SUBSCRIBERS

In the case of this CP, a Subscriber is a natural person to whom a certificate and associated key pair is issued. This CP does not provide for issuance of certificates to devices. Subscribers are individuals with a contractual relationship with the Customer and enrolled by the Customer. Customers shall maintain their Subscribers' certificate in their repositories and associated key pair in the DSA box 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.

1.3.4 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.

1.3.5 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 and Customer.

1.3.6 OTHER PARTICIPANTS

1.3.6.1 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 as a Registration Authority. Customer is responsible to hosts the dedicated DSA box it will have according rules and procedures defines by PMA. Therefore, there is dedicated CPS for each Customer detailing some section of CP implemented by 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.

When a Customer wants to use the DocuSign External trusted domain service is controlled by the PMA (refer to section 8 below).

1.3.6.2 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, or legal entity of Trusted Agent, are under contract with Customers.

1.4 CERTIFICATE USAGE

1.4.1 APPROPRIATE CERTIFICATE USES

The sensitivity of the information processed or protected using Certificates issued by CA is under sole decision of Customer.

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 protected by the key pair and Certificate managed according the present CP. This evaluation is done by each Customer and Relying Party for its application and is not controlled by this CP and DocuSign.

Technically Certificate and associated private key usage are defined by the present CP for CA and Subscriber.

1.4.2 PROHIBITED CERTIFICATE USES

No other uses than the ones stated in section 1.4.1 above are covered by this CP.

DocuSign is not responsible for any other use than the ones stated in this CP.

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 PMA is responsible for approving CPS and asserting whether the CPS conforms to this CP.

See Section 8 for further details.

1.5.4 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.

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

The DS shall prepare and submit the DOCUSIGN CPS and each Customer CPS 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 DOCUSIGN CPS compliance analysis, made by PMA, prior to authorizing the DS OA to issue and manage RCA and CA Certificates asserting this CP.

The DS PMA shall commission for each Customer a Customer CPS compliance analysis, made by PMA, prior to authorizing the DS OA to issue and manage Subscriber Certificates asserting this CP.

The Customer 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 for approval.

The following information shall accompany the Customer request:

- Customer's CPS.
- Signed Subscriber's naming document (refer below in same section).
- 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 Contact 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.
- DocuSign Contact 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 electronically by the 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 CPS.

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

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

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

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 one or 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).

2.2 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 publicly by relying parties.

DocuSign publishes RCA certificate and CRL produced by RCA.

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

See Section 10 for more details.

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).

Customer shall have at least an internal repository to publish Subscriber Certificate. Customer decides which kind of Relying Party can have access to all or part of this repository.

2.2.2 PUBLICATION OF CA INFORMATION

DocuSign shall publish the CP 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.

See Section 10 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.

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

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, Customer name, 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 RCA and CA 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 internal repository of the Customer. Trusted Agent is responsible to collect identity of the Subscriber and store it in Customer's repository.

Subscriber identity is always set in field "CN" of the subject in certificate.

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

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 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 be able to make 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.

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 and the CA certificates are unique, by controlling the DN used in the RCA and the CA certificates and approving the RCA and CA certificate creation. The same CN shall not be given to two or more distinct CAs 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 thanks the to email set in the DN of Subscriber.

Customer is responsible to guaranty the uniqueness of DN for Subscriber registered by its Trusted Agent.

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

3.1.6 RECOGNITION, AUTHENTICATION, AND ROLE OF TRADEMARKS

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.

3.1.7 NAME CLAIM DISPUTE RESOLUTION

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 advise to 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

RCA and CA key pairs shall be generated, stored, activated, used, and destroyed by the DS OA in a way that demonstrates to the PMA that DocuSign owns the private key corresponding to the public key contained in its RCA and CA certificate.

3.2.1.2 SUBSCRIBER

Customer is responsible to generate the Subscriber's key pair in the DSA box in a secured manner in order to guaranty that nobody can use key on behalf of the Subscriber. Subscriber's key can only be used by DSA box to sign a CSR and transmit it to CA to have a Subscriber Certificate.

For Subscriber Certificates, proof of ownership of the private key corresponding to the Subscriber Certificate used for signing purposes is provided by the technical and organizational resources defined in the consent protocol (request Subscriber to enter its activation data for use of key pair at the beginning and after each certain time frame that not exceeds 15 minutes) used and applied as part of the DSA box when the key is used.

3.2.2 AUTHENTICATION OF ORGANIZATION IDENTITY

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

Request for Subscriber Certificate is always associated to the Customer name organization identity.

The DS PMA, shall verify the information provided, the authenticity of the requesting representative, and the representative's authorization to act in the name of the organization for RCA and CA certificate.

The RA legal entity, Customer, is authenticated by DS OA during contractual phase with RA. The DS OA shall verify the existence and authenticity of the claimed legal name to be used in the Subscriber Certificate for the field "O". DS OA uses information retrieved from official database documentation (Qualified Independent Information Source, Qualified Government Information Source, Qualified Government Tax Information Sources), that confirms the existence of the organization. That database documentation contains trusted information that is filled by the trusted source that registers the legal company. DS OA verifies also that the Customer Contact is empowered by Customer to act on behalf of the Customer to use DS service covered by the present CP with the legal name of the Customer. DocuSign OA shall check that the legal person is not known by an authoritative source to be in a status that would prevent it from acting as that legal person or contained in a black list.

Customer is responsible to define which kind of natural person (employee of Customer, contractor of Customer …) can be issued a Subscriber Certificate.

Trusted Agent is responsible to control that only the authorized natural persons are issued Subscriber Certificate.

3.2.3 AUTHENTICATION OF PHYSICAL PERSON IDENTITY

3.2.3.1 INITIAL IDENTITY PROOFING OF HUMAN SUBSCRIBERS

Identity proofing of Customer Contact shall be performed by DocuSign under rules approved by PMA (during the sales process). DS OA is in charge of collecting the identity and contact information of Customer Contact using rules approved by PMA.

The RA is responsible for collecting and storing the required information to provide evidence of the Subscriber identity set in the Certificate and information used by Subscriber to sign (email and name). Subscriber identity verification rules are left to the discretion of the RA, which is in charge of managing the Subscriber.

The enrollment of a Subscriber prior to issuing a Subscriber Certificate is performed directly by the RA and Trusted Agent. Customer shall ensure that its registration process guaranties the following:

- Ensure the applicant (natural person who will be issued a Subscriber Certificate) is aware of the terms and conditions related to the use of the Certificate and associated private key and associated activation data (refer to section 9.6.3).
- Ensure the applicant is aware of recommended security precautions related to the activation data.
- Collect the relevant identity data required for identity proofing and verification.
- The applicant can be assumed to be in possession of evidence either; one unexpired National Government-issued or REAL ID Act issued Picture ID or two Non-Federal Government IDs, one of which shall be a photo ID, in which the application for the electronic identity means is being made and representing the claimed identity.
- The evidence of applicant can be assumed to be genuine, or to exist according to an authoritative source and the evidence appears to be valid.
- Natural person corresponds to the criteria defined by Customer to be authorized to be issued a Subscriber Certificate (refer to section 3.2.2 above).

After having authenticated the Subscriber, RA shall fill the Customer repository with the collected Subscriber's information and authorized the Subscriber in the Customer repository to be issued a Certificate.

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

If Subscriber's 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 provision is made using the Customer repository with Subscriber status. If Subscriber is contained in the Customer repository then Certificate is re-issued using a new key pair and same information containing in the Customer Repository.

3.2.4 NON-VERIFIED SUBSCRIBER INFORMATION

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

3.2.5 VALIDATION OF AUTHORITY

Approval from the DS PMA for RCA and CA certificate shall be obtained prior to issuing such certificate. 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 and CA are not signed by another CA of DocuSign or external to DocuSign. CA are only authorized to be signed by RCA of DocuSign.

This CP represents one level of trust. Customer is responsible to communicate the RCA certificate to Relying Party who accepts this level of trust for their needs. DS PMA takes care to ensure, controlling Customer CPS, that all Customers has same level of security in their practice. By this way Subscriber Certificate shares the same level of trust.

3.3 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS

3.3.1 IDENTIFICATION AND AUTHENTICATION FOR ROUTINE RE-KEY

DS PMA uses the same procedures as defined in section 3.2 to authenticate an RCA and CA certificate request. A new RCA and CA certificate shall use a new key pair.

Trusted Agent shall regularly control that only legitimate natural person, according rules defined in section 3.2, are contained in the Customer repository and still be authorized to be issued Certificate. Trusted Agent shall control that information of Subscriber are still accurate and true. Customer is responsible of the update of Subscriber information in the Customer repository. Any update of Subscriber information shall be authenticated as described in section 3.2 above.

RA is synchronized with Customer repository and controls that Subscriber is still in the Customer repository. If Customer is removed from Customer repository or not anymore authorized to be issued a Certificate, then the DSA box revoke the Subscriber Certificate.

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 by RA.

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.

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

4.1.1.2 CA: DOCUSIGN GENERIC CA

DS OA creates the CA request (CA naming document) and transmit to DS PMA for approval.

4.1.1.3 SUBSCRIBER

RA is in charge to create the technical Subscriber Certificate request.

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 OA 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 electronically by the authorized representative with means as described in CPS/

In parallel the DS OA shall transmit the DOCUSIGN 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 DOCUSIGN CPS and RCA key ceremony script approved by DS PMA. DOCUSIGN CPS shall be signed by DS OA.

4.1.2.2 CA: DOCUSIGN DEDICATED CA

CA 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 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 OA 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 electronically by the authorized representative with means as described in CPS.

In parallel the DS OA shall transmit the DOCUSIGN 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 DOCUSIGN CPS and RCA key ceremony script approved by DS PMA. DOCUSIGN CPS shall be signed by DS OA.

4.1.2.3 SUBSCRIBER

Subscriber certificate request created by RA using Customer repository shall contain the following information:

- Email of the subscriber (refer to section 3.2).
- All required information to construct the Subscriber's identity (name) to be set in the Certificate as described in section 3.1.

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 OA to DS PMA prior to issuance using means and process described in CPS and approved by PMA. It is the responsibility of the DS PMA to authenticate the DS OA 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 CA: DOCUSIGN GENERIC CA

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

4.2.1.3 SUBSCRIBER

It is the responsibility of the Trusted Agent to verify that the information in Customer repository is accurate (see sections 3.2). It is also responsibility of Trusted Agent to verify the link between Subscriber and affiliated organization to be set in the certificate (see sections 3.2).

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 CA: DOCUSIGN GENERIC CA

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 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 statement, the DS PMA approves the CA certificate creation.

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

4.2.2.3 SUBSCRIBER

The Trusted agent shall be responsible for approving or rejecting Subscriber in Customer repository after successful authentication (see section 3.2).

4.2.3 TIME TO PROCESS CERTIFICATE APPLICATIONS

No stipulation.

4.3 CERTIFICATE ISSUANCE

4.3.1 CA ACTIONS DURING CERTIFICATE ISSUANCE

4.3.1.1 RCA

The PMA transmits the RCA certificate request to the DS OA. The OA authenticates the certificate request before issuance. DS OA authenticates all key ceremony attendee (refer to section 3.2 above) using list provided by authorized representative (for witness) and the list of DS OA of PKI trusted role (refer to section 5.2).

The RCA certificate is generated during a key ceremony using a RCA key pair (refer to section 6.1.1.1 below). During the key ceremony, the RCA private key is backed-up (refer to section 6.2.4.1 below). At the end of the key ceremony the RCA private key is deactivated (refer to section 6.2.9.1 below) and destroyed inside the HSM (refer to section 6.2.9.1 below) and only exist on backup format.

4.3.1.2 CA: DOCUSIGN GENERIC CA

The PMA shall transmit the CA certificate request to the DS OA. The OA shall authenticate the CA certificate request prior to the generation of the CA key pair and CSR. Transmission of the certificate request and CSR shall be performed in a

manner which ensures the integrity of the information. DS OA authenticates all key ceremony attendee (refer to section 3.2 above) using list provided by authorized representative (for witness) and the list of OA of PKI trusted role.

The following actions must occur during a CA Key Ceremony, which shall be witnessed by an DOCUSIGN FRANCE PMA witness at least:

- Issuance of CA keys (refer to section 6.1.1.3 below).
- Backup of CA private key (refer to section 6.2.4.3 below).
- Generation of CA CSR (The CSR shall include the CA's public key).
- RCA private key is activated to sign CA certificate (refer to section 6.2.6.1, 6.2.7.1 and 6.2.8.1 below).
- At the end of the key ceremony the CA private key is deactivated (refer to section 6.2.9.3 below), CA key is destroyed inside the HSM (refer to section 6.2.9.2 below) and only exist on backup format (refer to section 6.2.4.2 below).

At the end of the key ceremony the RCA private key is deactivated (refer to section 6.2.9.1 below), RCA key is destroyed inside the HSM (refer to section 6.2.9.1 below) and only exist on backup format (refer to section 6.2.4.1 below).

4.3.1.3 SUBSCRIBER

RA signs and transmits the technical certificate request to the CA containing Subscriber's information (name and email) over a mutual TLS session with CA.

CA authenticates the RA using the TLS client certificate and verifying the signature of certificate request.

CA generates the Subscriber's Subscriber certificate.

CA returns the Subscriber Certificate to RA.

4.3.2 NOTIFICATION TO SUBSCRIBER OF CERTIFICATE ISSUANCE

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

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

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 OA 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 CA: DOCUSIGN GENERIC CA

The DS PMA accepts the CA certificate when the DS OA 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.

4.4.1.3 SUBSCRIBER

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 to Trusted Agent.

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).

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. In case a new certificate is created, a new key pair shall be created.

While this practice is allowed for CA, 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.

For CA, procedure is the same as described in section 3.3, 4.1, 4.2, 4.3 and 4.4.

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.

For RCA, CA and Subscriber procedure is the same as described in section 3.3, 4.1, 4.2, 4.3 and 4.4.

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, an 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.

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

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

This practice is not allowed for Subscriber. In case a new certificate is created, a new key pair shall be created.

For CA, procedure is the same as described in section 3.3, 4.1, 4.2, 4.3 and 4.4.

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 Customer shall be notified by DS PMA at least 3 months prior to the revocation of a CA or RCA certificate, whenever possible. The notice period will begin to run upon written acknowledgement by the Customer.

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 CA: DOCUSIGN GENERIC CA

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

- DS PMA requests revocation.
- 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).
- CA Private key is compromised or suspected of compromise.

4.9.1.2 SUBSCRIBER

The circumstances under which certificates issued by an 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 CA: DOCUSIGN GENERIC CA

DS OA shall accept revocation requests as followed:

- From DS PMA.

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

4.9.2.2 SUBSCRIBER

RAs shall accept revocation requests as followed:

- From Subscriber for its certificates.
- 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 CPS.

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

4.9.3 PROCEDURE FOR REVOCATION REQUEST

4.9.3.1 CA: DOCUSIGN GENERIC CA

Revocation of the CA certificate requires also revocation of all Subscriber certificates CA has issued. The revocation of an CA certificate requires the authorization of 2 distinct individuals acting as permanent members of the PMA.

CA revocation request is transmitted to the DS OA by the PMA. The DS OA authenticates the CA revocation request during a face to face meeting. DS OA authenticates all key ceremony attendee (refer to section 3.2 above) using list provided by authorized representative (for witness) and the list of DS OA of PKI trusted role.

The operation is video-recorded and performed according to a key ceremony script.

RCA key pair, according which has to be used for the revocation operation, is undertaken and witnessed in a physically secure environment (refer to section 5.1 above) by personnel in trusted roles (refer to section 5.2 above) under at least dual supervision. Private Key activation data are distributed to activation data holders that are trusted employees.

RCA key pair is carried out within a hardware security module (refer to section 6.2 and below). Witnesses are persons other than the operational personnel. RCA private key is activated to sign CRL (refer to section 6.2.6.1, 6.2.7.1 and 6.2.8.1 below).

At the end of the key ceremony the RCA private key is deactivated (refer to section 6.2.9.1 below), RCA key is destroyed inside the HSM (refer to section 6.2.9.1 below) and only exist on backup format (refer to section 6.2.4.1 below).

The current RCA issued CRL is replaced by the new one in the PS.

DS PMA can decide in this particular case to also destroy the CA private key backup and CA key in HSM hosted by DS OA after all Subscriber certificate issued by CA has been revoked.

4.9.3.2 SUBSCRIBER

Revocation requests are authenticated by the RA.

The revocation request is stored in the RA's logs.

The RA authenticates the revocation request it receives (refer to section 3.4 above).

The RA transmits the signed revocation request to the CA over mutual TLS session.

The CA authenticates the RA and makes sure the request was issued by an RA authorized by the CA.

The CA revokes the certificate by including the certificate's serial number in the next CRL to be issued by the Sub-CA if the certificate is not expired.

The reason code set in CRL is always "unspecified".

RA shall inform the Subscriber about the new status of the certificate.

4.9.4 REVOCATION REQUEST GRACE PERIOD

The revocation request grace period for CA 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 revocation shall be processed as quickly as possible not to exceed 10 business days.

This CP does not allow a revocation grace period for Subscriber. 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

The DS PMA shall process a revocation request as soon as possible after receiving the revocation request, not to exceed 10 business days.

The CA shall process a revocation request as soon as practical after receiving, authenticated and approving the revocation request. The maximum delay to revoke a certificate is 24 hours.

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

RCA issues CRL every year.

CA issues a CRL every 24 hours but CRL.

CRL publication service availability is 24 out of 24 hours and 7 out of 7 days.

4.9.8 MAXIMUM LATENCY FOR CRLS

CA issues CRL every 24 hours but CRL is valid for 7 days.

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

Not applicable.

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 Subscriber certificates shall always be revoked at the end of subscription with the Customer.

The contract between Customer and DocuSign deals with end of relationship.

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 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 systems
- Require in-person access (no 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 DSA box is installed and activated. The RA shall implement physical access controls to reduce the risk of equipment tampering even when the DSA box is not installed and activated. These security mechanisms shall be commensurate with the level of threat in the RA equipment environment.

The physical security mechanisms for RA equipment (Customer repository, DSA box, DSA box activation data and DSA box backup) at minimum shall be in place to:

- Ensure monitoring, either manually or electronically, of unauthorized intrusion at all times.
- Ensure no unauthorized access to the hardware and activation data and back up of DSA box is permitted.
- Ensure all removable media and paper containing sensitive plain-text information is stored in secure location.
- Any non-authorized individual entering secure areas shall always be under oversight by a trusted role.
- Ensure an access log is maintained and inspected periodically.
- Provide at least 2 layers of increasing security such as perimeter, building, and operational room.

- Ensure that DSA box activation data and DSA box backup are stored in a protected location (safe for example) and under dual control in way requiring 2 persons to restore a DSA box with activation data and back up file.
- Require trusted roles physical access controls.

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

No stipulation.

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 a month. 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 RA, CA and RCA is weakened. The functions performed in these roles form the basis of trust for all uses of the RA, 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.

Customer is responsible to define and documented trusted roles and associated operation. Customer shall define trusted to manage RA and Trusted Agent shall be formally appointed by senior manager.

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.

Customer should appoint and define role to make at least a separation between personal in charge of RA services (Trusted Agent) and personal in charge of RA software to proceed the following operation; configuration, installation, backup, maintain and recovery. DSA box configuration and backup shall require 2 distinct persons in trusted roles. Customer repository shall be under control of trusted roles approved by Customer.

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 RA, CA and RCA equipment, or procedurally, or by both means.

Segregation of duties is defined in CPS and may be enforced using PKI equipment, procedures or both. PKI component employees are individually appointed to trusted roles for operations defined in section 5.2.1 and 5.2.2 above.

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.

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;
- Current place of residence;
- Law Enforcement; and
- References.

The period of investigation must cover at least the last five years for each area. Regardless of the date of award, the highest educational degree shall be verified.

Adjudication of the background investigation shall be performed according local law of the country where person live.

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.

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 RA, 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

Audit log files are generated by DS OA and PMA for all events related to security and PKI services.

Audit log files are generated for all events related to security and PKI services. Where possible, 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. Each event related to certificate life cycle is logged in such a way that it can be attributed to the person that performed it.

Logging will include the following topics:

- Physical facility access.
- Trusted roles management.
- Logical access.
- Backup management.
- Log management.
- Data from the authentication process for Subscribers and PKI components.
- Date, time, phone number used, persons spoken to, and end results of verification telephone calls.
- Acceptance and rejection of certificate requests.
- Certificate creation.
- Certificate renewal.
- HSM management.
- Key creation, use and destruction.
- Activation data management.
- Role management.
- IT and network management, as they pertain to the PKI systems.
- PKI documentation management.
- Security management (Successful and unsuccessful PKI system access attempts, PKI and security system actions performed, Security profile changes, System crashes, hardware failures and other anomalies, Firewall and router activities; and entries to and exits from the DS OA facility).

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

- Type of event.
- Trusted date and time the event occurred.
- Result of the event: success or failure where appropriate.
- Identity of the entity and/or operator that caused the event.
- Identity for which the event is addressed.
- Cause of the event.

Customer for its RA activity shall record the following:

- Information used to verify the Subscriber identity.
- Subscriber Certificate.
- DSA box log.
- Customer CPS.
- Person with a Trusted role.
- Access to RA equipment.
- RA IT logs.

5.4.2 LOG PROCESSING FREQUENCY

CA and RA audit logs shall be reviewed regularly (at least every quarter), 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 RA, CA and RCA since the last review shall be examined, as well as a reasonable search for any evidence of malicious activity. Actions taken as a result of these reviews shall be documented.

A DS OA trusted role shall explain all significant events in an audit log summary.

Customer is responsible to review its log regularly especially for Customer repository, to check the accuracy and validity of Subscriber information used by RA and to detect Certificate that has been issued for Subscriber that are not any more authorized to be issued certificate, and use of DSA box and its backup.

5.4.3 RETENTION PERIOD FOR AUDIT LOGS

Records related to PKI operation are held on the site, at least one month, before being archived.

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.

Event logs are protected in such a way that only authorized users can access them.

Events are logged in such a way that they cannot be easily deleted or destroyed (except for transfer to long term media) within the period of time that they are required to be held.

Event logs are protected in such a way so as to remain readable for the duration of their storage period.

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 regularly with a reasonable frequency, except for RCA where the backup shall be performed the longer between monthly and when the system is activated.

Audit logs and audit summaries are backed up via enterprise backup mechanisms, under the control of authorized trusted roles, separated from their component source generation. Audit log backups are protected with the same level of trust defined for the original logs. RCA and CA have offsite backup. It is not mandatory for Customer.

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 Customer or DS PMA 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

For RCA, CA and RA, trusted roles in charge of conducting audit and roles in charge of realizing PKI system operation explain all significant events in an audit log summary. Such reviews involve verifying that the log has not been tampered with, there is no discontinuity or other loss of audit data, and then briefly inspecting all log entries, with a more thorough investigation of any alerts or irregularities in the logs. Actions taken as a result of these reviews are documented.

For vulnerability, the following rules apply for DS OA and Customer:

- Implement detection and prevention controls to protect PKI systems against viruses and malicious software.
- Document and follow a vulnerability correction process that addresses the identification, review, response, and remediation of vulnerabilities.
- Undergo or perform a vulnerability scan on RA interface of Customer repository and interface to communicate with DS OA (external IP address) and CA interface (internal and external IP address).
- Undergo a penetration test on the PKI's systems on; at least an annual basis and after infrastructure or application upgrades or modifications that the PMA determine as significant for CA and on regular basis for Customer for RA.
- Record evidence that each vulnerability scan and penetration test was performed by a person or entity (or collective group thereof) with the skills, tools, proficiency, code of ethics, and independence necessary to provide a reliable vulnerability or penetration test; and
- Track and remediate vulnerabilities according to enterprise cybersecurity policies and risk mitigation methodology.

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 by DS OA for archive:

- CP and CPS: 7 years.
- Contract with Customer: 7 years.
- Technical logs (IT system, physical access …): one year.
- Audit report: 7 years.
- PKI equipment software: 7 years.
- RCA, CA and Subscriber Certificates: 7 years.
- Trusted role record: 7 years.

Customer for its RA activity shall keep the logs during:

- Information used to verify the Subscriber identity: within Subscriber employment period as defined by Customer according local law and at least until Certificate is still valid.
- Subscriber Certificate: until Certificate is still valid years.
- DSA box log: 1 year inside DSA box.
- Customer CPS: until end of service.
- Person with a Trusted role: 5 years.
- Access to RA equipment: 1 year.
- RA IT logs : 1 year.

5.5.2 ARCHIVE RETENTION PERIOD

The minimum retention period for archived data is defined in section 5.5.1 above. The PMA and Customer decide, according the archive owner, to delete or keep all or part of the archives at the end of the retention period of each archive.

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

The archives are created in such a way that they cannot be easily deleted or destroyed within their defined retention period. Archive protection ensures that only authorized people can access them.

Archives are held in a manner that ensures integrity, authenticity and confidentiality of data.

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

Time stamping services for PKI are not mandatory.

The records and log data have a trusted time defined by the PKI. Details are given in section 6.8 below.

5.5.6 ARCHIVE COLLECTION SYSTEM (INTERNAL OR EXTERNAL)

The archive collection system is compliant with security requirements defined in section 5.4.6.

5.5.7 PROCEDURES TO OBTAIN AND VERIFY ARCHIVE INFORMATION

Media storing PKI archive information are verified upon creation. Periodically, statistical samples of archived information are tested to check the continued integrity and readability of the information.

Only authorized trusted roles personnel are allowed to access archives.

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.

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.

A RCA cannot generate a Certificate for a CA 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.

After a CA or RCA performs a Key Changeover, the CA or RCA continue to issue CRLs with the old key until all certificates signed with that key have expired. As soon as a new key pair is generated for the CA, only the new private key is used to sign Subscriber certificates.

The Subscriber private key validity period is defined in compliance with cryptographic security recommendations for key size length. The Subscriber certificate validity period is defined in this CP (refer to section 6). Subscriber shall only use private key to sign document with a non-expired Certificate.

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 Customer as soon as possible after investigation 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 CA from issuing a CRL within 24 hours of the time specified in the next update field of its currently valid CRL.

If a RA component (for Customer) detects a potential hacking attempt or other form of compromise, it performs an investigation in order to determine the nature and the degree of damage. The scope of potential damage is assessed by the Customer in order to determine if the RA needs to be rebuilt, if only some certificates need to be revoked, and/or if the RA has been compromised. In addition, the Customer determines which services are to be maintained and how, in accordance with the Customer business continuity plan. Customer shall alert PMA in case of RA compromission as soon as investigation is ended.

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 (CRL);
- 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 alert impacted Customer. See Section 5.7.1 for contents of the notice.

If RA equipment is damaged or rendered inoperative or corrupted, but technical signature keys, used by RA to communicate with CA, are not destroyed and not corrupted, the operation is re-established as quickly as possible, with priority given to the ability to generate certificate status information. In particular:

- If the RA signature technical keys are not destroyed and not corrupted, RA operation shall be re-established, giving priority to the ability to generate revocation request;
- Before returning to operation, ensure that the system's integrity has been restored;
- If a RA cannot issue a revocation request prior 24H00 after recent revocation request registered by RA, then DS PMA shall be securely notified immediately.
- If the ability to revoke Certificates is damaged, the RA shall re-establish revocation capabilities as quickly as possible in accordance with procedures set forth in the applicable contract with DocuSign.
- If investigation reveals some Subscriber data in the RA repository are corrupted, then RA shall interrupt immediately the Certificate request issuance. RA shall investigate to determine which Subscriber data are corrupted and if they have been used to issue Subscriber's Certificate. If it is case, Customer shall immediately inform DS PMA and proceed to revocation request for all impacted Subscriber Certificate.

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 Customer;
- A new CA or RCA key pair shall be generated by the CA in accordance with procedures set forth in the applicable CPS;
- As 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 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, used to communicate with CA, is compromised or lost (such that compromise or loss is possible even though not certain):

- The RA certificate shall be revoked immediately by CA;
- 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).

5.7.4 BUSINESS CONTINUITY CAPABILITIES AFTER A DISASTER

For DocuSign OA and Customer, the business continuity plan addresses all necessary operations as described in section **Error! Reference source not found.** to 5.7.3 above.

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 Customer at least two months, which notice period will begin to run upon the notice is transmitted to Customer, prior to termination of any CA or RCA. For emergency termination, RCAs shall follow the notification procedures in Section 5.7.
- 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 (self-signed Root CA).

6 TECHNICAL SECURITY CONTROLS

6.1 KEY PAIR GENERATION AND INSTALLATION

6.1.1 KEY PAIR GENERATION

6.1.1.1 RCA

After the DS PMA agrees to the generation of the RCA, a key pair and RCA certificate are generated for the RCA.

The operation of the RCA key pair and RCA certificate generation is video-recorded and performed according to a key ceremony script.

The HSM used for the key ceremony is compliant with requirements defined in section 6.2.1 below.

RCA key pair generation is undertaken and witnessed in a physically secure environment (refer to section 5.1.1. above) by personnel in trusted roles (refer to section 5.2 above) under at least dual supervision. Private Key activation data are distributed to activation data holders that are trusted employees. RCA key generation is carried out within a hardware security module (refer to section 6.2 below). During the key ceremony, the RCA key pair is backed up (refer to section 6.2. below).

The key pair and certificate generation process shall create a verifiable audit trail that the security requirements for procedures were followed. The documentation of the procedure shall be detailed enough to show that appropriate role separation was used. An independent third party shall validate the process.

6.1.1.2 CA: DOCUSIGN GENERIC CA

After the DS PMA agrees to the generation of the CA, a key pair and CSR are generated for the CA.

The operation of the CA key pair and CSR generation is video-recorded and performed according to a key ceremony script. The HSM used for the key ceremony is compliant with requirements defined in section 6.2.1 below.

CA key pair generation is undertaken in a physically secure environment (refer to section 5.1.1 above) by personnel in trusted roles (refer to section 5.2 above) under at least dual supervision. Private Key activation data are distributed to activation data holders that are trusted employees. CA key generation is carried out within a hardware security module (refer to section 6.2 below). During the key ceremony, the CA key pair is backed up (refer to section 6.2. below).

After key ceremony, CA key pair are securely transferred to HSM (refer to section 6.2.6.3 below) in the online environment (refer to section 5.1.1. above).

The key pair and certificate generation process shall create a verifiable audit trail that the security requirements for procedures were followed. The documentation of the procedure shall be detailed enough to show that appropriate role separation was used.

6.1.1.3 : SUSCRIBER

RA shall request generation of the Subscriber signature key pair to the DSA box. The generation is performed using a DSA Box (refer to section 6.2.11 below). The generation shall be performed in such a way as to avoid compromising the private key and associated activation data and avoid non required signature operation. The private key shall be protected with the associated activation data of the Subscriber.

6.1.2 PRIVATE KEY DELIVERY TO SUBSCRIBER

RA generates keys on behalf of the Subscriber and the private key are not delivered to the Subscriber. Private keys of Subscriber are stored in the DSA Box to centrally generates, stores, uses, backup and destroys all Subscriber key pairs.

6.1.3 PUBLIC KEY DELIVERY TO CERTIFICATE ISSUER

6.1.3.1 CA: DOCUSIGN GENERIC CA

CA public keys are securely delivered to the relevant RCA for certificate issuance during key ceremonies (for PKI set-up) or during the registration process (refer to section 4.1 and 4.2 above). The delivery mechanism binds CA checked identities to the public keys to be certified using the Pkcs#10 format.

6.1.3.2 SUBSCRIBER

RA sings a certificate request containing the pubic of Subscriber to be certified by CA and transmits using TLS mutual authentication with CA.

6.1.4 CA PUBLIC KEY DELIVERY TO RELYING PARTIES

Refer to section 2 above for downloading the RCA and CA certificate and section 10 below to use technical URL to download RCA and CA certificate.

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.

RCA, CA and Subscriber keys are generated in accordance with the cryptography tools of the hardware security modules (refer to section 6.2.11 below).

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

Key pairs are generated and stored within an HSM or a token that is certified according to the rating specified in section 6.2.11 below.

6.2.2 PRIVATE KEY MULTI-PERSON CONTROL

6.2.2.1 RCA

The RCA implements technical and procedural mechanisms that require the participation of multiple trusted individual authorizations to perform sensitive RCA cryptographic operations.

6.2.2.2 CA: DOCUSIGN GENERIC CA

The CA implements technical and procedural mechanisms that require the participation of multiple trusted individual authorizations to perform sensitive CA cryptographic operations.

6.2.2.3 SUBSCRIBER

The RA implements technical and procedural mechanisms that require the participation of multiple trusted individual authorizations to perform sensitive DSA Box cryptographic configuration.

Subscriber’s key pair is activated after successful authentication of the Subscriber using its activation data according consent protocol defined in DSA Box.

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 RCA

The RCA private signature keys shall be backed-up under the same multi-person control as the RCA operational signature operation. All back-up copy of the signature key shall be stored in the RCA off-site location (refer to section 5.1.8 above) and the number of back-up copy is controlled by trusted roles.

6.2.4.2 CA: DOCUSIGN GENERIC CA

CA private signature keys shall be backed-up under the same multi-person control as the operational ones. All back-up copy of the signature key shall be stored in the CA off-site location (refer to section 5.1.8 above) and the number of back-up copy is controlled by trusted roles.

6.2.4.3 SUBSCRIBER

Subscriber private signature keys may be copied in another identical DSA Box protected with same secret as the initial one (refer to section 6.2.2 above) for redundancy only. 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. Backup file of the Subscriber key pair shall be stored under dual control.

Subscriber key are still protected and usable with same subscriber activation data.

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

6.2.6.1 RCA

In case of private key transfer, then the RCA key pair is transferred to another Hardware Security Module (HSM) of the same specification as described in section 6.2.1 above, by direct token-to-token copy or via a trusted transfer under N out of M multi-person control (Refer to section 6.2.2 above).

RCA keys are generated, activated and stored in HSMs or in an encrypted format. When they are not stored onto HSMs, RCA private keys are encrypted. An encrypted RCA private key cannot be decrypted without using an HSM with the required trusted role (activation data holder), and must be performed in the presence of multiple persons in trusted roles.

6.2.6.2 CA: DOCUSIGN GENERIC CA

In case of private key transfer, then the CA key pair is transferred to another Hardware Security Module (HSM) of the same specification as described in section 6.2.1 above, by direct token-to-token copy or via a trusted transfer under N out of M multi-person control (Refer to section 6.2.2 above).

CA keys are generated, activated and stored in HSMs or in an encrypted format. When they are not stored onto HSMs, private keys are encrypted. An encrypted private key cannot be decrypted without using an HSM with the required trusted role (activation data holder), and must be performed in the presence of multiple persons in trusted roles.

6.2.6.3 SUBSCRIBER

In case of private key transfer, then the Subscriber key pair is transferred to another DSA Box of the same specification as described in section 6.2.1 above, by direct token-to-token copy or via a trusted transfer under N out of M multi-person control (Refer to section 6.2.2 above).

Subscriber keys are generated, activated and stored in DSA Box or in an encrypted format. When they are not stored onto DSA Boxs, private keys are encrypted. An encrypted private key cannot be decrypted without using an DSA Box with the required trusted role (activation data holder), and must be performed in the presence of multiple persons in trusted roles.

6.2.7 PRIVATE KEY STORAGE ON CRYPTOGRAPHIC MODULE

6.2.7.1 RCA

The HSM may store Private Keys in any form as long as the keys are not accessible without authentication mechanisms that are compliant with the ones mentioned in the security policy attached to the HSM approved use and the present CP section 6.2.

6.2.7.2 CA: DOCUSIGN GENERIC CA

The HSM may store Private Keys in any form as long as the keys are not accessible without authentication mechanisms that are compliant with the ones mentioned in the security policy attached to the HSM approved use and the present CP section 6.2.

6.2.7.3 SUBSCRIBER

The HSM may store Private Keys in any form as long as the keys are not accessible without authentication mechanisms that are compliant with the ones mentioned in the security policy attached to the HSM approved use and the present CP section 6.2.

6.2.8 METHOD OF ACTIVATING PRIVATE KEY

6.2.8.1 RCA

Activation of the RCA's HSM, to sign and/or revoke CA certificates, requires several trusted roles with activation data to activate the RCA private key. Each trusted role is authenticated before activating a RCA private key.

6.2.8.2 CA: DOCUSIGN GENERIC CA

Several trusted roles with activation data are required to realize the initial activation of the HSM that contains the key pair corresponding to the CA certificate. Once the HSM containing the CA key are operational, only the authorized services of the PKI system can use the CA key pair within the HSM.

6.2.8.3 SUBSCRIBER

Subscriber key pair is activated according the DSA Box consent protocol. Consent protocol shall require a technical activation data (password of minimum 8 characters minimum with a standard complexity).

6.2.9 METHOD OF DEACTIVATING PRIVATE KEY

6.2.9.1 RCA

An activated RCA HSM is never left unattended or otherwise available to unauthorized access. After use, the HSMs are deactivated. The HSMs are removed from RCA component and stored in secure locations (refer to section 5.1 above) to

avoid their use without authorization and strongly authenticated roles. After deactivation, the use of the HSM based RCA key pair shall require the presence of the trusted roles with the activation data in order to reactivate said RCA key pair (refer to section **Error! Reference source not found.** above).

6.2.9.2 CA: DOCUSIGN GENERIC CA

HSM that has been activated is never left unattended or otherwise available to unauthorized access.

After use, HSM are deactivated. After deactivation, the use of the HSM based CA key pair shall require the presence of the trusted roles with the activation data in order to reactivate said CA key pair (refer to section **Error! Reference source not found.** above).

The HSM automatically deactivate the HSM if there is an incident.

6.2.9.3 SUBSCRIBER

DSA box that has been activated is never left unattended or otherwise available to unauthorized access.

When a DSA Box is not used anymore, DSA Box is deactivated. Before deactivation of the DSA Box, all Subscriber key pair shall be destroyed requiring the presence of the trusted roles with the activation data.

Subscriber's key pair is used to sign document during a transaction with DSA Box and after each signature, Subscriber key pair is deactivated and requires activation again by Subscriber with activation data of Subscriber to use it again.

6.2.10 METHOD OF DESTROYING PRIVATE KEY

6.2.10.1 RCA

Destroying RCA private key inside an HSM requires destroying the key(s) inside the HSM using the zeroization function of the HSM in a manner that any information cannot be used to recover any part of the private key. All the RCA private key back-ups have to be destroyed in a manner that any information cannot be used to recover any part of the private key. If the functions of HSM are not accessible in order to destroy the key contained inside, then the HSM has to be physically destroyed.

The destruction operation is realized in a physically secure environment (refer to section 5.1 above) by personnel in trusted roles (refer to section 5.2 above) under at least dual control.

6.2.10.2 CA: DOCUSIGN GENERIC CA

Destroying CA private key inside an HSM requires destroying the key(s) inside the HSM using the zeroization function of the HSM in a manner that any information cannot be used to recover any part of the private key. All the CA private key back-ups have to be destroyed in a manner that any information cannot be used to recover any part of the private key. If the functions of HSM are not accessible in order to destroy the key contained inside, then the HSM has to be physically destroyed.

The destruction operation is realized in a physically secure environment (refer to section 5.1 above) by personnel in trusted roles (refer to section 5.2 above) under at least dual control.

6.2.10.3 SUBSCRIBER

Destroying Subscriber private key inside an DSA Box requires destroying the key(s) inside the DSA Box using the zeroization function of the DSA Box in a manner that any information cannot be used to recover any part of the private key. By default it is the RA which request the destruction of Subscriber key pair in the DSA box due to renewal of Certificate or end of issuance of Certificate to Subscriber.

All the Subscriber private key back-ups have to be destroyed in a manner that any information cannot be used to recover any part of the private key. If the functions of DSA Box are not accessible in order to destroy the key contained inside, then the DSA Box has to be physically destroyed.

The destruction operation is realized in a physically secure environment (refer to section 5.1 above) by personnel in trusted roles (refer to section 5.2 above) under at least dual control.

6.2.11 CRYPTOGRAPHIC MODULE RATING

The Hardware Security Module used to generate RCA and CA key pairs is at least approved in accordance with FIPS 140 - 2 Level 3 standard or EAL4+ Common Criteria equivalent. DSA Box may be FIPS certified, but it is not mandatory.

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.

The Certificate validity period is given in section 10.

6.4 ACTIVATION DATA

6.4.1 ACTIVATION DATA GENERATION AND INSTALLATION

6.4.1.1 RCA

RCA activation data used to protect HSM containing RCA private keys are generated during the initial key ceremony. 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.

The DS PMA appointed individuals shall receive their activation data during the key ceremony through a face to face meeting. Creation and distribution of activation data are logged. The activation data are never transmitted by any other means.

6.4.1.2 CA: DOCUSIGN GENERIC CA

CA activation data used to protect HSM containing CA private keys are generated during the initial PKI key ceremony. 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.

The DS PMA, appointed individuals shall receive their activation data during the key ceremony through a face-to-face meeting. Creation and distribution of activation data are logged. The activation data are never transmitted by any other means.

6.4.1.3 SUBSCRIBER

DSA Box activation data used to protect DSA Box containing Subscriber private keys are generated during the initial DSA Box ceremony. The activation data used to protect use of DSA Box and backup of DSA Box and transfer between DSA Box, 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.

The Customer, appointed individuals shall receive their activation data during the DSA Box ceremony through a face-to-face meeting. Creation and distribution of activation data are logged. The activation data are never transmitted by any other means.

This activation data to use Subscriber Key pair is generated either by Subscriber according the Customer security policy for its IT system.

6.4.2 ACTIVATION DATA PROTECTION

6.4.2.1 RCA

Activation data is protected from disclosure by a combination of cryptographic and physical access control mechanisms. Activation data holders are responsible for their accountability and protection.

The DS PMA requires that activation data holder store activation data in a safe for which access is controlled by both the holder and other employees in trusted roles. When they are not used, activation data are always stored in safe (refer to section 5.1 above).

If activation data is written on paper, then the paper has to be stored securely in a safe.

6.4.2.2 CA: DOCUSIGN GENERIC CA

Activation data is protected from disclosure by a combination of cryptographic and physical access control mechanisms. Activation data holders are responsible for their accountability and protection.

The DS PMA, requires that activation data holder store activation data in a safe for which access is controlled by both the holder and other employees in trusted roles. When they are not used, activation data are always stored in safe (refer to section 5.1 above).

If activation data is written on paper, then the paper has to be stored securely in a safe.

6.4.2.3 SUBSCRIBER

Activation data is protected from disclosure by a combination of cryptographic and physical access control mechanisms. Activation data holders are responsible for their accountability and protection.

Customer, requires that activation data holder store activation data in a safe for which access is controlled by both the holder and other employees in trusted roles. When they are not used, activation data are always stored in safe (refer to section 5.1 above).

If activation data is written on paper, then the paper has to be stored securely in a safe.

A Subscriber is responsible for ensuring the protection of his/her activation data according Customer security policy.

6.4.3 OTHER ASPECTS OF ACTIVATION DATA

6.4.3.1 RCA

Activation data are changed in case hardware security modules are returned to manufacturer for maintenance or destroyed. Before sending HSM to the manufacturer for maintenance, all sensitive information contained in the HSM shall be destroyed (refer to section 6.2.10 above).

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

6.4.3.2 CA: DOCUSIGN GENERIC CA

Activation data are changed in case hardware security modules are returned to manufacturer for maintenance or destroyed. Before sending HSM to the manufacturer for maintenance, all sensitive information contained in the HSM shall be destroyed (refer to section 6.2.10 above).

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

6.4.3.3 SUBSCRIBER

Activation data are changed in case hardware security modules are returned to manufacturer for maintenance or destroyed. Before sending DSA Box to the manufacturer for maintenance, all sensitive information contained in the DSA Box shall be destroyed (refer to section 6.2.10 above).

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, RA and RCA services and PKI roles;
- Enforce separation of duties for PKI roles;
- Require identification and authentication of PKI roles and associated identities;
- Require use of authentication for session communication and database security for CA and RA;
- Require a trusted path for identification and authentication;
- Enforce domain integrity boundaries for security critical processes;
- Support recovery from key or system failure;
- CA, RA and RCA shall have a recovery mechanism for keys used by 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.

CA and RA equipment shall be configured with a minimum of the required accounts, network services, and secured remote access to equipment using secured channel (for example VPN) and multiple factors. RCA has no remote login.

The following rules apply for CA and RA:

- Follow a documented procedure for appointing individuals to trusted roles and assigning responsibilities to them on each PKI component.
- Document the responsibilities and tasks assigned to trusted roles and implement “separation of duties” for said trusted roles based on the security-related concerns of the functions to be performed on each PKI component.
- Ensure that only personnel assigned to trusted roles have access to PKI components.
- Ensure that an individual in a trusted role acts only within the scope of said role when performing administrative tasks assigned to that role on the PKI component.
- Require employees and contractors to observe the principle of “least privilege” when accessing, or when configuring access privileges on PKI system (refer to section 5.2 above).
- Require that each individual in a trusted role use a unique credential created by or assigned to that person in order to authenticate to PKI component.
- If an authentication control used by a trusted role is a username and password, then the handling of those authentications shall be performed in accordance with corporate enterprise security policy.
- Require trusted roles to log out from the PKI service of the PKI component and lock workstations when no longer in use.
- Configure workstations with inactivity time-outs that log the user off and lock the workstation after a set time of inactivity without input from the user (PKI components allow a workstation to remain active and unattended if the workstation is otherwise secured and running administrative tasks that would be interrupted by an inactivity time-out or system lock).
- Review regularly all system accounts and deactivate any accounts that are no longer necessary for operations.
- If applicable for a PKI component (means only for a PKI component that uses a different access control system than a certificate for a trusted role) lockout account access to the PKI component after no more than a defined maximum value of failed access attempts, provided that this security measure is supported by the PKI component and does not weaken the security of this authentication control.
- Implement a process that disables all privileged access of an individual to the PKI component within 24 hours upon termination of the individual’s (with trusted role) employment or contracting relationship with the PKI component.
- Enforce strong authentication for administrator access to all PKI components.

Customer shall ensure that DSA Box is configured and used according documentation provided by DocuSign and configuration approved by DocuSign.

6.5.2 COMPUTER SECURITY RATING

DSA Box used by RA is certified FIPS 104 – 2 level 3.

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, RA 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.
- 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, should be dedicated to operating and supporting the CA, RA and RCA (i.e., the system and services dedicated to the issuance and management of certificates). There should be no other applications; hardware devices, network connections, or component software installed which is not part of the PKI operation. If it is not dedicated software and/or hardware, the configuration shall ensure separation between applications and services in a way to avoid compromission.
- 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.
- 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 PKI system as well as any modifications and upgrades shall be documented and controlled. A procedure shall be used for installation and ongoing maintenance of the PKI system. The PKI software shall be verified as being that supplied from the vendor, with no modifications, and be the version intended for use. There shall be a mechanism for detecting unauthorized modification to software or configuration. A configuration management documentation shall be used for installation and ongoing maintenance for the system.

The following rules apply:

- Implement an IT administration system under the control of the OA and Customer that monitors, detects, and reports any security-related configuration change to PKI systems.
- Require trusted role personnel to follow up on alerts of possible critical security events.
- Conduct a human review of application and system logs and ensure that monitoring, logging, alerting, and log-integrity-verification functions are operating properly (refer to section 5.4.8 above)

6.6.3 LIFE CYCLE SECURITY CONTROLS

For the software and hardware that are evaluated, the DS PMA monitors the maintenance scheme requirements to ensure the same level of trust. DS PMA will alert the Customer about the DSA Box certification and required update due to certification maintenance to avoid a Customer using expired certification DSA Box FIPS.

Capacity demands are monitored and projections of future capacity requirements made to ensure that adequate processing power and storage are available.

6.7 NETWORK SECURITY CONTROLS

Key ceremony operations for RCA and CA hosted by DocuSign France; are performed in off-line environment. The key ceremony workstation is never connected to any communication network.

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.

The following rules apply:

- Any boundary control devices used to protect the network on which PKI equipment is hosted shall only authorized the necessary services to the PKI equipment.
- Segment PKI equipment into networks or zones based on their functional, logical, and physical (including location) relationship.
- Maintain and protect PKI components in at least a dedicated zone and make a separation between interfaces accessible from Internet to interfaces accessible by internal needs.
- Implement and configure an administration network distinct from those on public networks to administrate the PKI component.
- Configure each network boundary control (firewall, switch, router, gateway, or other network control device or system) with rules that support only the services, protocols, ports, and communications that the PKI component has identified as necessary to its operations.
- Configure PKI components by removing or disabling all accounts, applications, services, protocols, and ports that are not used in the PKI component's operations and allowing only those that are approved by the PKI component.
- Review configurations of the PKI system on a regular basis to determine whether any changes have violated the PKI component's security policies.
- Grant administration access to PKI components only to persons acting in trusted roles and require their accountability for the PKI component's security.
- Change authentication keys and passwords for any privileged account or service account on a PKI System whenever a person's authorization to administratively access that account on the PKI System is changed or revoked.
- Apply recommended security patches, viewed by the software editor and entity like CERT as mandatory to avoid a concrete and high risk attack on the PKI system, with to PKI systems within six months of the security patch's availability, unless the PKI establishes that the security patch would introduce additional vulnerabilities or instabilities that outweigh the benefits of applying the security patch.

6.8 TIME-STAMPING

All CA and RA 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 or internal trust time source mechanism such as active directory time.

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.

RCA is synchronized during the key ceremony manually by trusted role.

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

Section 10 gives the exacts name form for issuer and subject set in RCA, CA and Subscriber certificate.

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 and CA, 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, 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.

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 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. RCA and CA is audited every year by DS PMA according rules defined by DS PMA. Customer CPS is controlled by DS PMA before Customer can be authorized by DocuSign to use the service covered by the present CP. RCA and CA are onsite audited against the RCA CPS by DS PMA.

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 Customer, audit shall be requested as stated in the respective contract with Customer. Customer may be audited on site by DS PMA in case of breach, suspected or verified, in their practice and/or security issue with the Customer. By default, there is no onsite audit for the Customer.

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.

DS PMA select the auditor. The auditor is either a private firm, which is independent from the entity being audited, or sufficiently organizationally separated from that audited entity to provide an unbiased and independent evaluation.

8.3 ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY

The auditor is either a private firm, which is independent from the entity being audited, or sufficiently organizationally separated from that audited entity to provide an unbiased and independent evaluation.

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 contract with DocuSign and Customer. DS PMA defines the audit methodology and topic to be covered according type of entity to be audited.

Customer CPS controls consists in mainly checking the following points:

- Security of the Customer repository;
- Security of the hosting of the DSA box;
- Management of the DSA box activation data;
- Security of the storage of the DSA Box activation data;
- Security of the storage of the DSA Box backup;
- Security of the IDP used for SAML ticket used as Subscriber activation data;
- DSA box configuration;
- Subscriber certificate template;
- IT security of the environment where Customer repository and DSA box is used;
- Customer organization to implement RA and Trusted Agent roles.

8.5 ACTIONS TAKEN AS A RESULT OF DEFICIENCY

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

- The auditor shall document the discrepancy and transmit it to the DS PMA;

- The auditor shall notify the PKI component of the discrepancy;
- The DS PMA shall determine what further notifications or actions are necessary to meet the requirements of the Entity CP, CPS, and any relevant contractual 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.

For Customer, CPS control is explained in section 1.5.4 above. If an onsite audit is required for the Customer, then DS PMA designate an auditor as described above in section 8. The management of the discrepancy are the same as for the RCA and CA. In case of serious violation of the Customer CPS and/or contract signed by the Customer with DocuSign, the DS PMA may decide to interrupt the service for the Customer. Service will be open again for the customer if and only of Customer fixes the finding. DS PMA communicates the finding the Customer and Customer shall provide an action plan to fix the finding to the DS PMA. All delay are described in contract signed with the Customer.

8.6 COMMUNICATION OF RESULTS

On an annual basis, the auditor shall submit a compliance audit package to DS PMA. This package shall be prepared in accordance with the audit policy of the DS PMA 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.

9 OTHER BUSINESS AND LEGAL MATTERS

9.1 FEES

9.1.1 CERTIFICATE ISSUANCE/RENEWAL FEES

DocuSign set fees for issuance and renewal Certificate that are described in contract with Customer.

9.1.2 CERTIFICATE ACCESS FEES

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

9.1.3 REVOCATION OR STATUS INFORMATION ACCESS FEES

RCA and 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

DS PMA guarantees a special treatment for the following confidential information:

- Records and archive of DS OA.
- Personal identity data.
- RCA and RCA private keys.
- Subscriber certificate request.
- RCA and CA activation data.
- Audit result and reports.
- Business continuity plan.
- Contractual and agreement with Customer.
- Internal facility security policy.
- Production environment security procedures.
- CPS.

The treatment of confidential business information provided by Customer in the context of managing Subscriber key pair, DSA Box activation data and backup and submitting a Certificate request for Subscriber will be in accordance with the terms of the contract entered into between the applicable Customer and DocuSign.

Customer 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 (like Subscriber key pair, DSA Box activation data and backup and technical key used to securely communicate with CA) 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 and RCA that collect, store, process, or disclose personal data of Subscriber and Customer according applicable laws and regulations, specifically the European Data Protection regulation (GDPR), and the present Certification Policy.

Customer manages personal data of Subscriber according applicable laws and regulations applying to such data and the present Certification Policy. Customer is responsible to ensure that Subscriber is aware of the following:

- Subscriber Certificate contains email and identity of Subscriber.
- Subscriber Certificate is kept by DocuSign for 7 years minimum for audit purpose.

- Subscriber can't request modification of data contained in Certificate. Subscriber can only request revocation of Certificate in case of mistake inside it, but all issued Certificate are kept by DocuSign.
- Access to information retained by DocuSign is not authorized as Customer has all Subscriber's data that DocuSign have. DocuSign doesn't collect additional data than the one sent by Customer about subscriber and contained in certificate request (refer to section 4.1 to 4.8 above) and revocation request (refer to section 4.9 above).
- Subscriber can't request deletion of Subscriber data stored by Customer and DocuSign as audit proof (refer to section 5.4 and 5.5 above).
- Subscriber understand that Subscriber's data are collected by DocuSign only to issue Certificate and revoke certificate.
- Customer is responsible of the Subscriber data treatment.

9.4.2 INFORMATION TREATED AS PRIVATE

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

The Subscriber information must be treated as private as well as any information protected under national law of the CA and RA.

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

RCA and CA 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.

Customer is responsible to obtain consent of Subscriber, according the applicable law, to be authorized to treat the Subscriber data for the purpose of the service as described in the present CP.

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).

Customer is compliant with its national law of the entity that owns the RA and has secure procedures to clear access to private data.

9.4.7 OTHER INFORMATION DISCLOSURE CIRCUMSTANCES

The DS PMA obtains consent from Customer to transfer Subscriber data in case of a transfer of activity as described in section **Error! Reference source not found.**.

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.

Customer defines its own property right according the applicable law for Subscriber Certificate.

9.5.2 PROPERTY RIGHTS IN THE CPS

CP and all corresponding RCA CPS and Customer 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

DocuSign retains the rights and intellectual property associated with the RCA and CA private key.

Customer retains the rights and intellectual property associated with the Subscriber 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 DS PMA REPRESENTATIONS AND WARRANTIES

The DS PMA defines the present CP and the corresponding CPS. The DS PMA establishes that PKI components are compliant with the present CP. The processes, procedures and audit framework used to determine compliance are documented within the CPS.

The DS PMA ensures that all requirements on a PKI component, as detailed in the present CP and in the corresponding CPS, are implemented as applicable to deliver and manage certification services.

The DS PMA has the responsibility for compliance with the procedures prescribed in this CP, even when PKI component functionality is undertaken by sub-contractors. PKI components provide all their certification services consistent with their CPS.

The DS PMA has the responsibility to audit the RA and approve RA’s procedures before allows Customer (RA) uses the Service.

9.6.1.2 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 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.
- All incident due to RCA shall be reported to DS PMA.
- The auditor team to control and check the compliance with the present CP and with the components CP/CPS shall be allowed by RCA and RCA shall communicate requested information to them, in accordance with the intentions of the PMA.

9.6.1.3 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.
- Customers who are issued a Subscriber certificate, have been obligated to an agreement which includes Customer, acting as RA, and Subscriber representation and warrants. Further, this agreement includes a representation and warranty from the Customer that the information 1) they have provided to the CA and 2) that is in their certificate is true and accurate.
- The data transmitted by Subscriber to the CA shall not be modified by CA to issue a Subscriber Certificate.
- 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.
- All incident due to CA shall be reported to DS PMA.
- The auditor team to control and check the compliance with the present CP and with the components CP/CPS shall be allowed by CA and CA shall communicate requested information to them, in accordance with the intentions of the PMA.

9.6.1.4 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 CPS that deals with their duties (this part of CPS has to be transmitted to the corresponding component).
- 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 CPS.
- 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 CPS.

- Respect the CP and corresponding Customer CPS.
- 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 CPS.
- Inform Subscriber about usage of key pair and subscriber's data.
- Protect DSA box activation data, backup and technical key in a secured manner as described in Customer CPS.
- Establishes contract with Customer and external entity when they are different legal entity from it with clear identification of PKI services of the Customer CPS run by the entity and all Customer's and Entity's obligations and warranties according PKI services of the customer CPS managed.
- Communicate to DS PMA any intention to change any part of the Customer CPS 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 CPS to DS PMA according protocol and means defined with DS PMA.
- Collect and archive all the document managed with RA platform according Customer CPS.
- 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 CPS, the contract between DocuSign and the Customer and all procedures and means (physical or IT system) used to complete the Customer CPS.

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 its information system and guaranty the security of the data transmitted to the CA.
- Protect subscriber identity information and produce subscriber certificate with correct identity as requested in CP and Customer CPS.
- Maintain up to date the Customer repository used to transmit Subscriber data to DSA Box and CA.
- Request revocation in due delay as soon as revocation reason is applicable.
- Protect personal data of Subscriber according the contract and the local law and the Customer CPS.
- Manage, deliver and protect activation data of the Subscriber used to activate the private key of Subscriber.
- 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 CPSs, the contract between DocuSign and the Customer and all other procedures and means (physical or IT system) used to complete the Customer CPS.

9.6.3 SUBSCRIBER REPRESENTATIONS AND WARRANTIES

Subscriber shall be required to be informed by Customer about 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 CPS.
- 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 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 Customer shall be defined in Customer agreement.

The liability (and/or limitation thereof) of Subscribers shall be as set forth in the applicable subscriber information provided by Customer, 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. to which DS PMA allow to use a dedicated Customer CA or DocuSign Generic CA to issue Subscriber Certificates shall be set forth in the applicable Customer agreements.

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 AS STATED IN THE AGREEMENT WITH CUSTOMER.

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 protect Subscriber Private Key, to use a Trustworthy System, or to otherwise take the precautions necessary to prevent the compromise, loss, disclosure, modification, or unauthorized use of the Subscriber 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 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 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 Customer agreement, 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 Customer shall be communicated to the Customer at least two weeks and a day prior to implementation, which notice period will begin to run upon DS PMA has transmitted the information to Customer. 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 Customer within delay defined in Customer agreement 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 CPS.

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 3 weeks 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 defined in the agreement signed with Customer.

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: 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 String1
	C	US	PrintableString
	O	DocuSign Inc.	UTF8String
	OU	DocuSign External trusted domain	UTF8String
	CN	DocuSign External Root CA GX<where X is an integer starting from 1 and increased of 1 for each new RCA>	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 String2**
	C	US	PrintableString
	O	DocuSign Inc.	UTF8String
	OU	DocuSign External trusted domain	UTF8String
	CN	DocuSign External Root CA GX<where X is an integer starting from 1 and increased of 1 for each new RCA>	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)
Authority Key Identifier		
Methods of generating key ID		Defined by RCA Software (SHA1 160bits of the RCA public key)
Key Usage	**TRUE**	
keyCertSign		Set
cRLSign		Set
Basic Constraint	**TRUE**	

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

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

Extensions	Criticality (True/False)	Value
cA		True
pathLenConstraint		None

10.2 CA: ISSUING CA CERTIFICATE

Base Certificate	Value			
Version	2 (=version 3)			
Serial number	Defined by the RCA software			
Issuer	**Attribute type**	**Attribute value**		**Directory String3**
	C	US		PrintableString
	O	DocuSign Inc.		UTF8String
	OU	DocuSign External trusted domain		UTF8String
	CN	DocuSign External Root CA GX<where X is an integer starting from 1 and increased of 1 for each new RCA>		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 String4**
	C	US		PrintableString
	O	DocuSign Inc.		UTF8String
	OU	DocuSign External trusted domain		UTF8String
	CN	DocuSign External Issuing CA GX<where X is an integer starting from 1 and increased of 1 for each new 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}			

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

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

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
Basic Constraint	**TRUE**	
cA		True
pathLenConstraint		0
Certificate Policies	**FALSE**	
policyIdentifier		“2.5.29.32.0”
policyQualifier-cps		https://www.docusign.com/trust/compliance/public-certificates
CRL Distribution Points	**FALSE**	
distributionPoint		URI: http://crl.dsf.docusign.net/docusignexternalrootcagx.crl (*)

(*): where X is an integer starting from 1 and increased of 1 for each new RCA.

10.3 DEMO CA: ISSUING CA CERTIFICATE FOR TEST PURPOSES ONLY

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	DocuSign External trusted domain	UTF8String

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

	CN	DocuSign External Root CA GX<where X is an integer starting from 1 and increased of 1 for each new 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 String6**
	C	US	PrintableString
	O	DocuSign Inc.	UTF8String
	OU	DocuSign TC DEMO	UTF8String
	CN	FOR TEST PURPOSE ONLY CA GX<where X is an integer starting from 1 and increased of 1 for each new 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**
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
Basic Constraint	**TRUE**	
cA		True
pathLenConstraint		0
Certificate Policies	**FALSE**	
policyIdentifier		“2.5.29.32.0”

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

Extensions	Criticality (True/False)	Value
policyQualifier-cps		https://www.docusign.com/trust/compliance/public-certificates
CRL Distribution Points	**FALSE**	
distributionPoint		URI: http://crl.dsf.docusign.net/docusignexternalrootcagx.crl (*)

(*): where X is an integer starting from 1 and increased of 1 for each new RCA.

10.4 SUBSCRIBER: TEST CERTIFICATE UNDER DEMO CA

There is no specific profile rules for such test except that in the DN of the Subscriber, the following mention shall appear: “FOR TEST PURPOSE ONLY”.

10.5 SUBSCRIBER: HUMAN SUBSCRIBER SIGNATURE CERTIFICATE UNDER ISSUING CA

Base Certificate Fields	Value		
Version	2 (=version 3)		
Serial number	Defined by the software		
Issuer	**Attribute type**	**Attribute value**	**Directory String**[7]
	C	US	PrintableString
	O	DocuSign Inc.	UTF8String
	OU	DocuSign External trusted domain	UTF8String
	CN	DocuSign External Issuing CA GX<where X is an integer starting from 1 and increased of 1 for each new 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**[8]
	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>	UTF8String
	E	<Email of the Subscriber>	IA5String
	CN	<Name and first Name of the Subscriber as registerer by Trusted Agent>	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	

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

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

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
1.3.6.1.5.5.7.3.4 (emailProtection)		Set
Certificate Policies	**FALSE**	
policyIdentifier		1.3.6.1.4.1.42482.2.1.1.2
policyQualifier-cps		https://www.docusign.com/trust/compliance/public-certificates
CRL Distribution Points	**FALSE**	
distributionPoint		URI: http://crl.dsf.docusign.net/docusignexternalissuingcagx.crl (*)

(*) where X is an integer starting from 1 and increased of 1 for each new CA.

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	DN of RCA (*)
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 revoked non-expired certificate.

(*): shall be encoded like in RCA 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

Validity dates and CRL Numbers (based on an 11 months renewal period, and a 1 year CRL duration):

This Update (YYYY/MM/DD)	Next Update (YYYY/MM/DD)	CRL Number
2019/11/26	2020/11/26	1 (0x1)
2020/10/26	2021/10/26	2 (0x2)
2021/09/26	2022/09/26	3 (0x3)
2022/08/26	2023/08/26	4 (0x4)
2023/07/26	2024/07/26	5 (0x5)
2024/06/26	2025/06/26	6 (0x6)
2025/05/26	2026/05/26	7 (0x7)
2026/04/26	2027/04/26	8 (0x8)
2027/03/26	2028/03/26	9 (0x9)
2028/02/26	2029/02/26	10 (0xA)
2029/01/26	2030/01/26	11 (0xB)
2029/12/26	2030/12/26	12 (0xC)
2030/11/26	2031/11/26	13 (0xD)
2031/10/26	2032/10/26	14 (0xE)
2032/09/26	2033/09/26	15 (0xF)
2033/08/26	2034/08/26	16 (0x10)
2034/07/26	2035/07/26	17 (0x11)
2035/06/26	2036/06/26	18 (0x12)

This Update (YYYY/MM/DD)	Next Update (YYYY/MM/DD)	CRL Number
2036/05/26	2037/05/26	19 (0x13)
2037/04/26	2038/04/26	20 (0x14)
2038/03/26	2039/03/26	21 (0x15)
2039/02/26	2039/11/26	22 (0x16)

If new CRL to be issued by RCA has to be created, then the CP will be updated with table above.

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	DN of issuing CA (*)
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