Certificate Policy and Public Certificate Practice Statement

Cloud Signing Personal Signature CA ETSI

DocuSigned by:

Olivier PIN

B1AB707E6A75498...

CLOUD SIGNING PERSONAL SIGNATURE CA ETSI

Version	2.3	**Pages**	84
Status	☐ Draft	☒ Final	
Author	DocuSign France		

Diffusion List	☒ External	☒ Internal DocuSign
	Public	Public

History				
Date	Version	Author	Comments	Verified by
24/10/2013	1.0	EM	Creation of the version 1.0	JYF
21/10/2014	1.1	EM	Integration of renewal certificate rules for Subscriber	JYF
15/02/2016	1.2	EM	Modification following DocuSign acquisition of OpenTrust (now called DocuSign France)	
15/02/2016	1.3	EM	Integration of qualified certificate with SSCD and modification following DocuSign acquisition of OpenTrust (now called DocuSign France)	
31/03/2017	1.4	EM	Move to new standards ETSI EN 319 411	
26/05/2017	1.5	EM	Integration of comments from LSTI.	
16/10/2018	1.6	EM	Update and integration of Austrian driving license to authenticate a Subscriber only in Austria.	
26/10/2018	1.7	EM	Modification to not have TOU signed by Subscriber for LCP level.	
03/06/2019	1.8	EM	Update PMA contact and certificates profiles and CP.	
09/08/2019	1.9	EM	Integration of comments from LSTI.	
08/11/2019	2.0	EM	Integration of comments from	

			LSTI.	
07/10/2020	2.1	EM	Modification of certificate profile to have starting minus one hour, CPS URI to have update URL and LCP certificate as ”Digital signature” instead of “nonRepudiation".	
16/03/2021	2.2	EM	Modification of the extension the KeyUsages to add the value “nonRepudiation" to be compliant with the new ESTI standard 319 412.	
17/03/2021	2.3	EM	Change information contact.	

CONTENTS

1 INTRODUCTION

1.1 Overview

This Certificate Policy (CP) defines the requirements applicable to the life cycle management of subscriber digital certificates delivered by Protect and Sign (Personal signature) service.

The present CP contains also the public information of the Certificate Practice Statement (CPS) but it is named CP.

Subscriber certificates are signed by Subordinate Certification Authorities (Sub-CA) owned by DOCUSIGN FRANCE or a customer of DOCUSIGN FRANCE (according to [PSMP]).

The electronic certificates issued and managed in compliance with this certificate policy, hereafter referred to as “Subscriber certificates,” are delivered to the users (hereafter named Subscriber) of the Protect and Sign (Personal signature) Customers using the Protect and Sign (Personal signature) Service.

The present CP describes the management of Subscriber and CA certificate and key pair.

The CA shall implement the services described in this CP in a non-discriminatory manner within the limits of what current technologies allow.

This CP is based on:

- RFC 3647 « Certificate Policy and Certification Practices Framework » issued by the Internet Engineering Task Force (IETF).
- ETSI documents:
    - [119 312]: “ETSI TS 119 312 V1.3.1 (2019-02): Electronic Signatures and Infrastructures (ESI); Cryptographic Suites”;
    - [319 401]: « ETSI EN 319 401 V2.2.1 (2018-04) Electronic Signatures and Infrastructures (ESI), General Policy Requirements for Trust Service Providers. »;
    - [319 412]:
        - « ETSI EN 319 412-1 1.4.1 (2020-06): Electronic Signatures and Infrastructures (ESI); Certificate Profiles, Part 1: Overview and common data structures. »;
        - « ETSI EN 319 412-2 V2.2.1 (2020-07): Electronic Signatures and Infrastructures (ESI), Certificate Profiles, Part 2: Certificate profile for certificates issued to natural persons »;
        - « ETSI EN 319 412-5 V2.3.1 (2020-04): Electronic Signatures and Infrastructures (ESI), Certificate Profiles, Part 5: QCStatements »;
    - [319 411]:
        - « ETSI EN 319 411-1 V1.2.2 (2018-04) »: « Electronic Signatures and Infrastructures (ESI), Policy and security requirements for Trust Service Providers issuing certificates, Part 1: General requirements »;
        - « ETSI EN 319 411-2 V2.2.2 (2018-04) »: « Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates ».
- [PSMP]: Proof Signature and Management Policy, version 1.6 “DSF_Protect and Sign_Personal Signature_PSGP v 1 6”;
- [PSM SSCD]: “Secure Information Technology Center – Austria, QSCD-CERTIFICATE PURSUANT TO ART. 30 PARA 3 LIT B. EIDAS1, Qualified Signature Creation Device (QSCD), Protect & Sign, version 4.67, QSCD-Certificate issued on: 2019-12-06, Reference number: A-SIT-VIG-19-070” notified in EU list (https://esignature.ec.europa.eu/efda/notification-tool/#/screen/browse/list/QSCD_SSCD).

1.2 Document Name and Identification

Issued under OID numbers are given in the table below:

- CA « Cloud Signing Personal Signature CA »:
  - SBS EU certified (usage unique signature), ETSI 102 042 LCP:
    - 1.3.6.1.4.1.22234.2.8.3.9: This certificate profile will not be anymore issued by the CA after July 2017. CA will still publish the associated CRL. There is no valid certificate under this CA with this profile.
  - Advanced signature with qualified certificate (usage unique de signature), ETSI 101 456 QCP:
    - 1.3.6.1.4.1.22234.2.8.3.7: This certificate profile will not be anymore issued by the CA after July 2017. CA will still publish the associated CRL. There is no valid certificate under this CA with this profile.
  - SBS Qualified (usage unique signature), ETSI EN 319 411-2 QCP-n-qscd:
    - 1.3.6.1.4.1.22234.2.8.3.20: This profile is implemented by the CA and certified ETSI. This profile will no longer be implemented by the CA from 01 October 2019 because the CA will no longer be qualified from 01 October 2019.
- CA “DocuSign Premium Cloud Signing CA – SI1”:
  - SBS Qualified (usage unique signature), ETSI EN 319 411-2 QCP-n-qscd:
    - 1.3.6.1.4.1.22234.2.14.3.31: This profile is implemented by the CA and ETSI certified with the new certificate profile.
- CA “DocuSign Cloud Signing CA – SI1”:
  - SBS EU certified (usage unique signature), ETSI EN 319 411-1 LCP
    - 1.3.6.1.4.1.22234.2.14.3.32: This profile is implemented by the CA and ETSI certified with the new certificate profile.

This CP covers all these OID in one document. When there are dedicated and particular rules that shall be described in a section of the CP, OID is used to identify a sub-section in the CP in order to clearly identify the applied rules for the particular mentioned level.

1.3 PKI Components

DOCUSIGN FRANCE has established a Policy Management Authority (PMA) to manage the PKI components and services. The PKI is composed of the components described hereafter and supports the following services (PKI services):

- Generation of Sub-CA key pair: generates the sub-CA key pairs and associated CSR during key ceremonies.
- Subscriber registration: consist in collecting and verify Subscriber identity and information that will be used to construct certificate requests and/or included in technical certificates.
- Key pair generation for Subscriber: consist in generate key pair for a Subscriber.
- Subscriber certificate generation: generating Subscriber certificates.
- Authentication of Subscriber revocation request (only for emergency cases according the contract signed between DocuSign France and the Customer): consist in collecting information in order to authenticate a revocation request and transmitting a revocation request to the CA.
- Revocation of Subscriber certificates (only for unexpired certificate): when the link between a Subscriber and the public key included in its certificate is considered no longer valid, and then the CA revokes the Subscriber certificate.
- Log trail generation: generates log that are used either for the audit purpose or to be analyzed in order to solve an incident.
- Publication of a CRL: a CRL is issued by CA for Subscriber certificate. This CRL is always empty because there is no revocation service for Subscriber.
- OCSP services: CA delivers OCSP status information for the Subscriber certificate.

- Publication services: publication of Sub-CA certificate and all relevant information related to the use of Sub-CA services and Subscriber certificate.

This CP gives the security requirements applicable to all services while the associated Certification Practice Statement (CPS) will give more details on practices enforced by each components participating in the PKI activities.

Major changes within the TSP or its AE partners are notified to ANSSI.

1.3.1 Policy Management Authority (PMA)

The PMA is the PKI lead authority and is managed by DOCUSIGN FRANCE.

The PMA approves CP and Certification Practice Statement (CPS) used to support the PKI certification services.

The PMA defines the organization of PKI components and services, is in charge of nominating the PKI components and verifying the compliance of the services they deliver with applicable sections of this CP and its corresponding CPS.

PMA main mission at minimum the following:

- Approves PKI services and prices to be delivered by the PKI infrastructure.
- Approves Certificate Policies.
- Approves CA creation and revocation.
- Approves the choice of RCA and ICA used to sign Sub-CA.
- Approves cryptographic specification (algorithms used for signature, encryption, authentication, hash functions and key length, operational lifetime) for the PKI systems and any related change.
- Approves the specifications of cryptographic tokens that generate keys and host subscribers certificates
- Approves PKI applications standards. This will guarantee the required level of interoperability and acceptance by RCA.
- Approves compliance between security practice documents and related policies (for instance CPS/CP).
- Approves final annual internal audit report of all the PKI's components.
- Approves external audit report of RA performed by DocuSign France.
- Manage external audit of RA.
- Approves the Consent Protocol chosen defined with DocuSign France.
- Approves procedures defined by Customer for Subscriber management.
- Guarantees the validity and the integrity of the PKI published information.
- Ensures that a proper process to manage security incidents within the PKI services and PKI components is in place.
- Arbitrates disputes relating to the PKI services and the use of certificates and ensures that the resolution of such disputes is published.

1.3.2 Subordinate Certification Authorities (Sub-CA)

The Sub-CA is owned by DOCUSIGN FRANCE or a Customer and operated by DOCUSIGN FRANCE.

The Sub-CA supports the following PKI services:

- Generation of Sub-CA key pairs.

- Subscriber certificate generation.

- Revocation of Subscriber certificates (according the contract between DocuSign France and Customer)

- Publication of a CRL.

- Log trail generation.

A Sub-CA operates its services according to this CP and the corresponding CPS. A Sub-CA cannot start operation without prior approval of the PMA.

1.3.3 Registration Authority (RA)

RA is owned by Customer and operated by entity designated by Customer.

RA supports the following PKI services:

- Authentication of Subscriber revocation request.
- Subscriber registration.
- Log trail generation.

The RA is designated and authorized by the Sub-CA on a contractual basis. Consequently, the RA documents and implements procedures for the identification of legal entities and private individuals, in accordance with the rules it has defined based on its needs, particularly in the Consent Protocol. Its role is to prove that the requester matches the identity and attributes that will be indicated in the Certificate. These identification procedures vary depending on the level of trust the RA decides to apply to this verification.

RA is responsible to define procedure that address especially section 3, 4, 5, 6, 8 and 9 of the present CP that concerns RA. If the Customer designates a different legal entity different from the Customer, then a contract, or legal document according the link between the Customer and legal Entity designated by Customer, has to be established between Customer and the legal entity designated by the Customer in order to cover the RA services addressed by the designated entity.

Procedures to manage Subscriber, defined by RA, are performed by RA Operator. RA is responsible to establish and maintain a RA Operator list of all RA Operator that are allowed to enroll Subscriber.

The CPS gives details how an RA is organized and performs its operation according to the type of certificate to be delivered to a Subscriber.

An RA operates its services according to this CP and the corresponding CPS. An RA cannot start operation without prior approval of the PMA.

1.3.4 Operational Authority (OA)

The Operational Authority (OA) is the entity that hosts and manages all the software, hardware and HSM used to support PKI services. The OA is the entity which sets up and realizes all operations for the PKI services. The CPS gives details on how each service is provided to each PKI component.

PKI components are operated by:

– DOCUSIGN FRANCE that is the OA for the Sub-CA and PS.

– Customer that is the OA for the RA.

The OA operates its services according to this CP and the corresponding CPS. The OA cannot start operation without prior approval of the PMA.

1.3.5 Publication Service (PS)

PS is owned by DOCUSIGN FRANCE and operated by DOCUSIGN FRANCE.

The Publication Service (PS) is the DOCUSIGN FRANCE repository (refer to chapter 2 below) which provides the following PKI services:

- Publication services (refer to section 2 below).
- Log trail generation.

1.3.6 Subscriber

A Subscriber is a physical person whose identity appears as subject in a Subscriber Certificate and who signs a document using Protect and Sign (Personal Signature) service. Subscriber key pair and certificate generation are linked to the signature operation performed by Subscriber according [PSMP] and customer rules, described in Customer documents, technically implemented in Consent Protocol.

Subscribers abide to this CP and the associated procedures as described in the RA documentation.

1.3.7 Other Participants

1.3.7.1 Customer

Customer is a Legal Entity that establishes a contract with DOCUSIGN FRANCE to use Protect and Sign (Personal signature) service. Customer designates entity that is RA. In the contract between Customer and DOCUSIGN FRANCE all RA obligations are included. Customer defines enrollment rules that RA shall implements, selects the level of trust for Subscriber Certificate and selects and defines the Consent Protocol. Consent Protocol shal request the use of a technical activation data from Subscriber. RA shall be audited according rules defined in section 8 below.

1.3.7.2 Relying Parties

Relying Parties are entities that act in reliance on the validity of the binding of the Subscriber identity to a public key. A Relying Party is responsible for deciding how to check the validity of a Subscriber certificate, at least by checking the appropriate certificate status information (using CRLs and ARLs or OCSP responses) for the Subscriber, Sub-CA, ICA and Root CA certificates. 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.

1.4 Certificate Usage

1.4.1 Appropriate Certificate Use

1.4.1.1 Sub-CA Certificate

A Sub-CA certificate is used to validate Subscriber certificates and CRLs and OCSP certificate it has delivered.

Each Sub-CA private key is allowed to sign the following types of certificates:

- Sub-CA CSR.
- Subscriber certificate.

1.4.1.2 Subscriber

The uses of private key are the following:

- Used to sign electronic document according Consent Protocol (with a technical activation data) and Customer Signature Policy.
- Used to sign CSR (Pkcs#10 format).

The uses of certificate are the following:

- Used to verify electronic signature applied on document using Protect and Sign (Personal signature) service.

1.4.2 Prohibited Certificate Use

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

DocuSign France 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

PMA is responsible for all aspects of this CP and the associated CPS.

1.5.2 Contact Person

PMA is the entity to be contacted for all questions about the present document:

- PMA de DocuSign France.
- https://www.docusign.fr/ (Les informations de contacts sont disponibles sur cette page).
- DocuSign France – 9-15 rue Maurice Mallet - 92131 Issy-les-Moulineaux Cedex – France.

1.5.3 Person Determining CPS Suitability for the Policy

The PMA approves the CPS. The PKI will be audited periodically to verify compliance as per PMA guidelines and standards approved by the PMA. The Audit ensures that the CPS is implemented correctly and is compliant with the CP. Further, the PMA reserves the right to audit the PKI as set in section 8 of this CP.

In any case, determination of compliance shall be based on independent audits.

1.5.4 CPS Approval Procedures

Amendments shall either be in the form of a new CPS (with a sum up of the modifications) or an update notice that contains the modifications and the references in the previous CPS. The creation or modification of the existing CPS is at the discretion of the PMA. A new CPS automatically replaces the previous one and becomes operational as soon as the PMA has approved it. Any new CPS or update to the existing CPS must be compliant with this CP before approval.

1.6 Definitions and Acronyms

1.6.1 Definitions

Term	Definition
Accreditation	Formal declaration by a Designated Approving Authority that an Information System is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk.
Activation Data	Secret data (e.g.: password, PIN code, certificate or OTP) that is used to perform cryptographic operations using a Private Key.
Audit	An independent review and examination of documentation, records and activities to access the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies or procedures.
Authentication	The process whereby one party has presented an identity and claims to be that identity and the second party confirms that this assertion of identity is true.
Authentication data	Particular technical activation data (like for example OTP or authentication certificate) used by Subscriber to be authenticated by Protect and Sign

	(Personal signature) service in order to sign a document according a Consent Protocol.
Authority Revocation List (ARL)	A list of revoked Certification Authority Certificates. Technically, an ARL is a CRL.
Availability	The property of being accessible and upon demand by an authorized entity [ISO/IEC 13335-1:2004]. It means that an electronic data stored using means (hard disk, paper …) can be still readable and have the same meaning after and during its storage.
Certificate	A Certificate is a data structure that is digitally signed by a Certification Authority, and that contains the following pieces of information: ○ The identity of the Certification Authority issuing it. ○ The identity of the certified Subscriber. ○ A Public Key that corresponds to a Private Key under the control of the certified Subscriber. ○ The Operational Period. ○ A serial number. ○ The Certificate format is in accordance with ITU-T Recommendation X.509 version 3.
Certificate Extension	A Certificate may include extension fields to convey additional information about the associated Public Key, the Subscriber, the Certificate Issuer, or elements of the certification process.
Certificate Manufacturing	The process of accepting a Public Key and identifying information from an authorized Subscriber, producing a digital Certificate containing that and other pertinent information, and digitally signing the Certificate.
Certificate Policy (CP)	A named set of rules that indicates the applicability of a Certificate to a particular community and/or class of applications with common security requirements.
Certificate Request	A message sent from a Customer to a Sub-CA in order to apply for a digital Certificate. The Certificate request contains information identifying the Subscriber and sometimes activation data.
Certificate Revocation List (CRL)	A list of revoked Certificates that is created and signed by a CA. A Certificate is added to the list if revoked (e.g., because of suspected key compromise, distinguished name (DN) change) and then removed from it when it reaches the end of the Certificate's validity period. In some cases, the CA may choose to split a CRL into a series of smaller CRLs. When a Subscriber chooses to accept a Certificate the Relying Party Agreement requires that this Relying Party check that the Certificate is not listed on the most recently issued CRL.
Certificate Validity Period	The certificate validity period is the time interval during which the CA warrants that it will maintain information about the status of the certificate. [RFC 3280].
Certification Path (also called trusted path or trusted certification	A chain of multiple certificates needed to validate a certificate containing the required public key. A certificate chain consists of a RCA-certificate (anchor),

chain)	CA-certificate and the Subscriber certificates signed by the CA.
Certification Practice Statement (CPS)	A statement of the practices, which a CA employs in issuing and revoking Certificates, and providing access to same. The CPS defines the equipment and procedures the CA uses to satisfy the requirements specified in the CP that are supported by it.
Common Criteria	Common Criteria for Information Technology Security Evaluation is an international standard (ISO/IEC 15408) for information technology security certification.
Compromise	A violation (or suspected violation) of a security policy, in which an unauthorized disclosure of, or loss of control over, sensitive information may have occurred. With respect to private keys, a Compromise is a loss, theft, disclosure, modification, unauthorized use, or other compromise of the security of such private key.
Confidentiality	The property that information is not made available or disclosed to unauthorized individuals, entities, or processes [ISO/IEC 13335-1:2004].
Cryptographic domain (for HSM)	Trusted environment that contains one or several keys and managed with dedicated activation data. This trusted environment is deployed in a Hardware Security Module (HSM) to activate and use keys.
Consent Protocol	Document in which the Customer specifies all of the rules to be followed by a given Customer Application using the Protect and Sign (Personal signature) Service, including: (i) the definition of the actions to be carried out by the Subscriber to sign the document proposed by the Customer, (ii) the terms and conditions of Subscriber, (iii) the methods used by the Protect and Sign (Personal signature) Service to authenticate the Subscriber for the signature operation and therefore the Subscriber key pair and certificate generation, and (iv) the type of file submitted by the Customer to be signed (XML/PDF…).
Digital Signature	The result of a transformation of a message by means of a cryptographic system using keys such that a person who has received a digitally signed message can determine: • Whether the transformation was created using the private signing key that corresponds to the signer's public verification key. • Whether the message has been altered since the transformation was made.
Directory	A directory system that conforms to the ITU-T X.500 series of Recommendations.
Disaster Recovery Plan	A plan defined by a CA to recover its all or part of PKI services, after they've been destroyed following a disaster, in a delay define in the CP/CPS.
Distinguished Name	A string created during the certification process and included in the Certificate that uniquely identifies the Subscriber within the CA domain.
Encryption Key Pair	A public and private Key Pair issued for the purposes of encrypting and decrypting data.
Federal Information	Federal standards that prescribe specific performance requirements,

Processing Standards (FIPS)	practices, formats, communications protocols, etc. for hardware, software, data, telecommunications operation, etc. U.S. Federal agencies are expected to apply these standards as specified unless a waiver has been granted in accordance with agency waiver procedures.
Hardware Security Module (HSM)	An HSM is a hardware device used to generate cryptographic Key Pairs, keep the Private Key secure and generate digital signatures. It is used to secure the CA keys, and in some cases the keys of some applications (Subscribers).
Hardware Token	A hardware device that can hold Private Keys, digital Certificates, or other electronic information that can be used for authentication or authorization. Smart card and USB tokens are examples of hardware tokens.
Hash Function	A function which maps string of bits to fixed-length strings of bits, satisfying the following two properties: - It is computationally infeasible to find for a given output an input which maps to this output; - It is computationally infeasible to find for a given input a second input which maps to the same output [ISO/IEC 10118-1].
Internet Engineering Task Force(IETF)	The Internet Engineering Task Force is a large open international community of network designers, operators, vendors, and researches concerned with the evolution of the Internet architecture and the smooth operation of the Internet.
Integrity	Refers to the correctness of information, of originator of the information, and the functioning of the system which processes it.
Interoperability	Implies that equipment and procedures in use by two or more entities are compatible, and hence that it is possible to undertake common or related activities.
Key Ceremony (KC)	A Key Ceremony (KC) is an operation enabling the management (generation and destruction) of cryptographic key pairs and CA life-cycle (certificate signature and revocation). A key ceremony requires a minimum number of trusted employees whom represent the owner of the PKI.
Key Generation	The process of creating a Private Key and Public Key pair.
Object Identifier (OID)	An object identifier is a specially-formatted sequence of numbers that is registered with an internationally-recognized standards organization.
OCSP	Protocol useful in determining the current status of a digital Certificate without requiring CRLs.
Operational Period of a Certificate	The operational period of a Certificate is the period of its validity. It would typically begin on the date the Certificate is issued (or such later date as specified in the Certificate), and end on the date and time it expires as noted in the Certificate or earlier if revoked.
Organization	Department, agency, partnership, trust, joint venture or other association.
PIN	Personal Identification Number. See activation data for definition

PKCS #10	Public-Key Cryptography Standard #10, developed by RSA Security Inc., which defines a structure for a Certificate Signing Request.
PKI Disclosure Statement (PDS)	Defined by IETF's RFC 3647 as "An instrument that supplements a CP or CPS by disclosing critical information about the policies and practices of a CA/PKI. A PDS is a vehicle for disclosing and emphasizing information normally covered in detail by associated CP and/or CPS documents. Consequently, a PDS is not intended to replace a CP or CPS.
PKIX	IETF Working Group chartered to develop technical specifications for PKI components based on X.509 Version 3 Certificates.
Private Key	The Private Key of a Key Pair used to perform Public Key cryptography. This key must be kept secret.
Public Key	The Public Key of a Key Pair used to perform Public Key cryptography. The Public Key is made freely available to anyone who requires it. The Public Key is usually provided via a Certificate issued by a Certification Authority and is often obtained by accessing a repository.
Public Key Infrastructure (PKI)	A set of policies, processes, server platforms, software and workstations used for the purpose of administering Certificates and public-private Key Pairs, including the ability to issue, maintain, and revoke Public Key Certificates.
Public/Private Key Pair (also named Key Pair)	Two mathematically related keys, having the properties that (i) one key can be used to encrypt data that can only be decrypted using the other key, and (ii) knowing one of the keys which is called the Public Key, it is computationally infeasible to discover the other key which is called the Private Key.
Sub-CA domain space	Sub-CA domain space is the set of all the certificates delivered by the Sub-CA.
Registration	The process whereby a user applies to a Certification Authority for a digital Certificate.
Repository	Publication service providing all information necessary to ensure the intended operation of issued digital Certificates (e.g.: CRLs, encryption Certificates, CA Certificates).
Revocation	To prematurely end the Operational Period of a Certificate from a specified time forward.
RFC3647	Document published by the IETF, which presents a framework to assist the writers of Certificate Policies or certification practice statements for participants within Public Key infrastructures, such as certification authorities, policy authorities, and communities of interest that wish to rely on Certificates. In particular, the framework provides a comprehensive list of topics that potentially (at the writer's discretion) need to be covered in a Certificate Policy or a certification practice statement.
RSA	A public key cryptographic system invented by Rivest, Shamir, and Adelman.
Signature Key Pair	A public and private Key Pair used for the purposes of digitally signing

	electronic documents and verifying digital signatures.
Trusted Role	Those individuals who perform a security role that is critical to the operation or integrity of this PKI.
Trustworthy System	Computer hardware, software, and/or procedures that: (a) are reasonably secure from intrusion and misuse; (b) provide a reasonable level of availability, reliability, and correct operation; (c) are reasonably suited to performing their intended functions, and (d) adhere to generally accepted security procedures.
Valid Certificate	A Certificate that (1) a Certification Authority has issued, (2) the Subscriber listed in it has accepted, (3) has not expired, and (4) has not been revoked. Thus, a Certificate is not "valid" until it is both issued by a CA and has been accepted by the Subscriber.

1.6.2 Acronyms

Acronym	Means
AES	Advanced Encryption Standard
ARL	Authority Revocation List
CA	Certification Authority
CDS	Adobe Certified Document Services
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certification Revocation List
CSR	Certificate Signing Request
DES	Data Encryption Standard
DN	Distinguished Name
EAL	Evaluation assurance level, ISO 15408 (Common Criteria) norm for certification of security products
FIPS	United States of America, Federal Information Processing Standards
HTTP	Hypertext Transport Protocol
IP	Internet Protocol
ISO	International Organization for Standardization

LDAP	Lightweight Directory Access Protocol
MBUN	“Meaningless But Unique Number” a number that is assigned by the PKI to assist in differentiating Subscribers with otherwise similar attributes.
MofN	M out of N (Threshold Scheme)
O	Organization
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OU	Organizational Unit
PIN	Personal Identification Number
PKCS	Public-Key Cryptography Standard
PKI	Public Key Infrastructure
PS	Publication Service
RCA	Root Certification Authority
RFC	Request For Comment
RSA	Rivest, Shamir, Adleman
SHA	Secure Hash Algorithm
SSL	Secure Socket Layer
SSCD	Secure Signature Creation Device
Sub-CA	Subordinate CA
TDES	Triple DES
TLS	Transport Layer Security

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

The Publication Service is responsible for making available the any published information related to the Sub-CA services.

The PS shall be deployed so as to provide high levels of reliability (24 out of 24 hours, 7 out of 7 days) with 99.9 availability.

2.2 Publication of Certification Information

The PS publishes the following data:

- CP: https://www.docusign.fr/societe/politiques-de-certifications
- CA certificate: https://www.docusign.fr/societe/politiques-de-certifications
- The PDS is published for qualified certificates only (the URL is in the certificate profile in the appendix).
- CRL: refer to section 10 below.

The last CRL of each expired CA is put on line with the entire AC chain in the above repository used for CP.
It will be also accessible online using the CRL DP URL.

CA ensures that terms and conditions are made available to Subscribers and Relying Party as following:

– Subscriber: terms and conditions are shown to the Subscriber during the Consent Protocol or in the RA portal.
– Relying Party: terms and conditions and information as required by ETSI to be published for Relying party are already contained in the present CP in sections; 1.4, 4.4, 4.5.2, 4.9.6, 5.5, 9, 9.6, 9.7, and 9.8.
– Customer is responsible to establish and make available particular terms and conditions to complete ETSI requirements for Relying Party and Subscriber.

2.3 Time or Frequency of Publication

Information identified in section 2.2 above is made available:

- CP:
  - Before start of service for the initial CP.
  - Best effort after any CP update or replacement is approved by the PMA.

- CA certificate:
  - Before start of service for the initial CA and best effort after generation of CA certificates following a renewal or re-key.

2.4 Access Controls on Repositories

The PS is responsible for the security policy set granting access to the published information.

Access to read information is publicly and internationally available through the Internet, in readily language, for the following information for CP and CA certificate.

3 IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of Names

The attribute fields for “Issuer Name” and “Subject” shall be compliant with RFC 5280. Details for the type of use coding are given below.

3.1.1.1 Sub-CA

The DN content for Sub-CA certificates is detailed in section 10 below.

3.1.1.2 Subscriber

The DN content for Subscriber certificates is detailed in section 10 below.

3.1.2 Need for Names to Be Meaningful

The certificates issued pursuant to this CP are meaningful only if the names that appear in the certificates can be understood and used by Relying Parties. Names used in the certificates must identify the person to which they are assigned in a meaningful way and shall be in line with the identity card of the Subscriber

3.1.2.1 Sub-CA

A key pair can be linked with only a unique CN for each Sub-CA certificate.

3.1.2.2 Subscriber

In all cases, the identity set in the Subscriber certificate is the built using at least one of first name and last name as written in official ID of the Subscriber

RA is sole responsible to define identity of Subscriber.

Only Subscribers certificates with the RA’s or DRA’s name in the “OU” field can be issued (refer to section 10.3 and 10.4 below) by the Sub-CA.

3.1.3 Anonymity or Pseudonymity of Certificate

This policy does not permit anonymous certificates. All certificates shall contain information from the enterprise directory or manually entered by the RA.

3.1.4 Rules for Interpreting Various Name Forms

3.1.4.1 Sub-CA

Relying parties shall use the subject name contained in the certificate (refer to section 3.1.1) to identify the Sub-CA.

3.1.4.2 Subscriber

Subscriber certificates can be identified using the CN field contained in the DN. The CN field is not guaranteed to be unique.

3.1.5 Uniqueness of Names

3.1.5.1 Sub-CA

Names contained in any Sub-CA certificate (refer to section 3.1.1 above) shall be unique in the ICA trust domain, and all names shall be provided to the entity providing ICA services for inclusion in the appropriate name constraint values of the Sub-CA Certificate.

3.1.5.2 Subscriber

A certificate's uniqueness is based on the uniqueness of its serial number within the domain of the CA.

The RA shall be responsible for ensuring DN uniqueness in Certificates issued by the Sub-CA, and for handling DN-related conflicts. To do so, the RA must create a unique TransNUM for each Subscriber and signed document to be inserted by CA in the DN of Subscriber Certificate.

3.1.6 Recognition, Authentication, and Role of Trademarks

No stipulations.

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

3.2.1.1 Sub-CA

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

3.2.1.2 Subscriber

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, chosen by Customer, used and applied as part of the Protect and Sign (Personal signature) Service when the certificate request is made.

3.2.2 Authentication of Organization Identity

Not applicable. The CA doesn't include any information related to the legal entity of the Subscriber in the Certificate. The CA only sets the name of the legal entity that is RA in an OU field of the Subscriber's DN.

The RA legal entity is authenticated by CA during contractual phase with RA.

3.2.3 Authentication of Physical Person Identity

3.2.3.1 Subscriber

The RA is also 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 phone number).

The enrollment of a Subscriber prior to issuing a Subscriber Certificate is performed directly by the RA.

Subscriber identity verification rules are left to the discretion of the RA, which is in charge of managing the Subscriber.

Subscriber shall be authenticated using an official ID document (passport, national ID card, residence permit and Austrian driving license only in Austria and only model of driving license issued after March 01 2006 on a card model with a photo and security features as described here : http://www.consilium.europa.eu/prado/en/prado-documents/AUT/F/docs-per-category.html).

The particular rules below shall be implemented by the Customer according its OID choice.

3.2.3.1.1 OID: 1.3.6.1.4.1.22234.2.8.3.7, 1.3.6.1.4.1.22234.2.8.3.20 and 1.3.6.1.4.1.22234.2.14.3.31

RA shall carry out the authentication of the Subscriber identity, under RA rules and meeting the requirements contractually defined by the CA audited as compliant against ETSI 319 411-2. Initial registration is used to collect identity, email and phone number of the Subscriber. Initial registration is also used to securely distribute the secure authentication means to the Subscriber for remote access to the RA portal if RA has such function.

The RA shall verify at the time of initial registration, by appropriate means and in accordance with national law, the identity and, if applicable, any specific attributes of the person to which a qualified Certificate is issued:

- by the natural presence of the natural person; or
- remotely, using electronic identification means, for which prior to the issuance of the qualified Certificate, a physical presence of the natural person was ensured and which meets the requirements set out in Article 8 of the eIDAS regulation with regard to the assurance levels ‘substantial’ or ‘high’; or
- by means of a Certificate of a qualified electronic signature or of a qualified electronic seal; or
- by using other identification methods recognised at national level which provide equivalent assurance in terms of reliability to physical presence, within the meaning of article 24(1) of the eIDAS regulation. The equivalent assurance shall be confirmed by a conformity assessment body.

Evidence shall be provided of:

- full name (including surname and given names consistent with the national identification practices);
- date and place of birth, reference to a nationally recognised identity document, or other attributes which can be used to, as far as possible, distinguish the person from others with the same name.

If evidence is provided of a nationally recognised identity document, the DRA shall check that this document is still valid and authentic.

3.2.3.1.2 OID: 1.3.6.1.4.1.22234.2.8.3.9 and 1.3.6.1.4.1.22234.2.14.3.32

RA shall collect either direct evidence, or an attestation from an appropriate and authorized source, of the identity (e.g. name) and, if applicable, any specific attributes of subscriber to whom a certificate is issued. Submitted evidence may be in the form of either paper or electronic documentation. Verification of the Subscriber’s identity shall be at time of registration by appropriate means and in accordance with national law.

For Subscriber, evidence shall be provided of:

– Full name (included surname and given names consistent with the applicable law and national identification practices).

– Date and place of birth, a nationally recognized identity number, or other attributes which may be used to, as far as possible, distinguish the person from others with the same name.

It is recommended that the place be given in accordance to national conventions for registering births.

RA shall

3.2.4 Validation of Authority

The authentication and identification of an authority of a subscriber’s is done by the RA using and verifying information required by section 3.2.2 above.

Any Certificates issued by any CA that contain explicit or implicit Subscriber entity affiliation shall be issued only pursuant to the stipulations of section 3.2.2 above.

3.2.5 Non-Verified Subscriber Information

There is no non verified information used by the RA to fill a certificate.

3.2.6 Criteria for Interoperation

Certificates delivered by PKI components are managed according to the rules and requirements stated by the CA and Customer in compliance with Adobe and ETSI requirements.

3.3 Identification and Authentication for Re-key Requests

3.3.1 Identification and Authentication for Routine Re-key

3.3.1.1 Sub-CA

Same procedures as described in section 3.2 above apply.

3.3.1.2 Subscriber

For this section, Subscriber is already registered by RA and has been successfully issued a first certificate. Then RA can define a process to issue again others Certificates for the Subscriber. But in this case, as major and most important information used initially to register Subscriber may stayed valid, RA may want to avoid to register again completely the subscriber as in section 3.2 above.

This section deals with a new certificate with a new key pair for the Subscriber (Refer to section 4.7).

The RA is also responsible for updating, collecting and storing the required information in order to provide evidence of the Subscriber identity set in the certificate during renewal operation.

The enrollment for renewal of a User prior to issuing a Subscriber Certificate is performed directly by the RA.

Subscriber identity verification rules are left to the discretion of the RA, which is in charge of managing the Subscriber for renewal operation.

The procedure for identifying, authenticating and validating a request to issue a new certificate is described in the Proof Management Policy and in the Consent Protocol used for each Customer using Subscriber Certificates, and is supplemented by a procedure specific to the RA's line of business defined by the Customer.

The method of assigning this identity for a new certificate is therefore defined by the Customer, which enrolls all of its Users with its identification data and authentication data.

The particular rules below shall be implemented by the Customer according its OID choice.

RA shall check the existence and validity of the certificate (not revoked) to be renewed ant that the information used to verify the identity and attributes of the subscriber is still valid.

If any of the CA terms and conditions have changed, these shall be communicated to the Subscriber.

If any information of Subscriber to be set in Subscriber certificate (refer to section 3.1.1 above) have changed then the registration shall be performed against procedure as defined in section 3.2 above at least concerning information that have changed.

Information used to authenticate Subscriber during consent protocol (like email address and phone number) can only be modified by Subscriber after verification performed by RA in order to be sure that update information are linked to the Subscriber for consent protocol.

3.3.2 Identification and Authentication for Re-key After Revocation

3.3.2.1 RCA, ICA and CA

Same procedures as described in section 3.2 above apply.

3.3.2.2 Subscriber

Same procedures as described in section 3.2 above apply.

RA shall document its rules for re-key for depending on the type of revocation causes.

3.4 Identification and Authentication for Revocation Request

3.4.1.1 Sub-CA

Sub-CA revocation requests shall only be authorized by PMA members.

3.4.1.2 Subscriber

For Subscribers, the authentication is done according RA procedure approved by DOCUSIGN FRANCE.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

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.

4.1.1 Who Can Submit a Certificate Application

4.1.1.1 Sub-CA

The authorized representative of the Sub-CA shall submit the certificate request as directed by the PMA.

4.1.1.2 Subscriber

Certificate request is under responsibility of RA.

4.1.2 Enrollment Process and Responsibilities

4.1.2.1 Sub-CA

Sub-CA certificates must be authorized by the PMA prior to issuance. The issuance process will include documenting the following information:

- Identity to set in the certificate (refer to section 3.1.1 above).
- Legal Entity identification data, i.e. full name and legal status of the associated legal person or other organizational entity and any relevant existing registration information (e.g. company registration) of the associated legal person or other organizational entity.
- CSR associated with the generated key pair (refer to section 6.1.1). The CSR shall be included in the application.

4.1.2.2 Subscriber

Certificate application shall contain the following information:

– The Subscriber shall provide a physical address, or other attributes, which describe how the subscriber may be contacted.

– All required information to construct the Subscriber's identity to be set in the Certificate as described in section 3.1.1 (included surname and given names consistent with the applicable law and national identification practices).

– Subscriber's identification number of its official ID containing its name and first name, country of issuance of its official ID, ID type and ID validity period.

4.1.2.2.1 OID: 1.3.6.1.4.1.22234.2.8.3.9 and 1.3.6.1.4.1.22234.2.14.3.32

In addition, certificate request shall contain the following information:

- Identity of RA and if needed the DRA;
- Localization of the RA;
- RA or CA collect the ratification of the TOU (Subscriber agreement) by the Subscriber during the Consent Protocol or in the RA portal using a click in a check box.

4.1.2.2.2 OID: 1.3.6.1.4.1.22234.2.8.3.7, 1.3.6.1.4.1.22234.2.14.3.20 and 1.3.6.1.4.1.22234.2.14.3.31

In addition, certificate request shall contain the following information:

- Identity of the RA and if needed the DRA;
- Subscriber's mobile phone number.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

4.2.1.1 Sub-CA

Requests are submitted by an authorized representative at the discretion of the PMA prior to issuance. It is the responsibility of the PMA to authenticate the authorized representative as described in section 3.2 above, and to verify that the information in Certificate request is accurate for the CA.

4.2.1.2 Subscriber

It is the responsibility of the RA to verify that the information in Certificate request is accurate for a Physical person (refer to sections 3.2.2 and 3.2.5 above).

Verification of identity of Subscriber is made during face to face meeting between RA and Subscriber.

4.2.2 Approval or Rejection of Certificate Applications

4.2.2.1 Sub-CA

The PMA shall be responsible for approving or rejecting the Sub-CA certificate applications.

4.2.2.2 Subscriber

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

4.3 Certificate Issuance

4.3.1 CA Actions during Certificate Issuance

4.3.1.1 Sub-CA

The PMA shall transmit the certificate request to the OA and Root CA. The OA shall authenticate the certificate request prior to the generation of the Sub-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.

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

- Issuance of Sub-CA keys
- Backup of Sub-CA private key
- Generation of Sub-CA CSR (The CSR shall include the Sub-CA's public key)

The key ceremony shall be documented and a copy shall be provided to the DOCUSIGN FRANCE PMA. The following actions must occur during a ICA Key Ceremony:

- Generation of Sub-CA certificate.
- Use of ICA private key to sign Sub-CA certificate.

4.3.1.2 Subscriber

RA transmits the technical certificate request to the CA containing Subscriber's information (name, first name, optionally email if required by the CA and phone number) and data to be signed by the Subscriber.

Subscriber uses the activation data according the Consent Protocol chosen by Customer (refer to section 6.4 below). During the Consent Protocol, the Customer shall make available to the Subscriber for validation all the information used to construct the Subscriber identity in the DN (Refer to section 3.1 above).

CA authenticates the Subscriber using the activation data.

CA generates the Subscriber's Subscriber certificate.

Protect and Sign (Personal signature) service signs the document transmitted by Customer and includes Subscriber certificate inside the document.

After signature of the document, Subscriber key pair is destroyed.

Protect and Sign (Personal signature) service transmits the document to the RA.

4.3.1.2.1 OID: 1.3.6.1.4.1.22234.2.8.3.7, 1.3.6.1.4.1.22234.2.14.3.20 and 1.3.6.1.4.1.22234.2.8.3.31

If the Subscriber accepts to sign the document, then it confirms its choice to the RA using RA procedure (click on a screen …) and RA means during face to face meeting (refer to section 4.2 above).

4.3.1.2.2 OID: 1.3.6.1.4.1.22234.2.8.3.9 and 1.3.6.1.4.1.22234.2.14.3.32

If the Subscriber accepts to sign the document, then it confirms its choice to the RA using RA procedure (click on a screen …) and its IT mean.

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

Not applicable

4.4 Certificate Acceptance

4.4.1 Conducting Certificate Acceptance

4.4.1.1 Sub-CA

Acceptance of the Sub-CA certificate shall be performed by the PMA. The Sub-CA shall neither issue certificates nor sign CRLs until the Sub-CA certificate has been accepted.

4.4.1.2 Subscriber

If there is a mistake in the Subscriber certificate, then RA shall be alerted by the person (RA or Subscriber) who performs the verification.

4.4.1.2.1 OID: 1.3.6.1.4.1.22234.2.8.3.7, 1.3.6.1.4.1.22234.2.14.3.20 and 1.3.6.1.4.1.22234.2.8.3.31

Acceptance of the certificate is realized by RA verifying with Subscriber the content of the signed document and signature.

4.4.1.2.2 OID: 1.3.6.1.4.1.22234.2.8.3.9 and 1.3.6.1.4.1.22234.2.14.3.32

Acceptance of the certificate is realized by Subscriber verifying the content of the signed document and signature.

4.4.2 Publication of the Certificate by the PS

Subscriber Certificate is contained in the signed document signed during the Consent Protocol. Therefore Customer shall make available the signed document in order to make available the certificate. RA collects the consent of Subscriber about Subscriber certificate management during the collect of the signed agreement as specified in section 4.1 above.

For Relying Party, the Subscriber certificate of a particular Subscriber is also contained in the associated signed document and therefore will be available to a Relying Party if the Relying Party has the signed document.

Relying party can test the certificate using information published by CA (refer to section 2.2 above).

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

Customer and RA are notified of certificate issuance by CA according Protect and Sign (Personal signature) services.

4.5 Key Pair and Certificate Usage

4.5.1 Private Key and Certificate Usage

Subscribers and the Sub-CA shall use their Private Keys for the purposes set forth in section 1.4 above. Usage of a key pair and the associated certificate shall also be performed as indicated in the certificate itself, via extensions related to key pair usage (refer to section 6.1.7 below).

4.5.2 Relying Party Public Key and Certificate Usage

Relying parties use the trusted certification path and associated public keys for the purposes constrained by the certificates extensions (such as key usage, extended key usage, certificate policies, etc.) and to authenticate the trusted common identity of Subscriber certificates.

Relying parties has to be aware of the security rules to be deployed in the Customer electronic transaction for the usage of a Subscriber certificate. A Subscriber certificate is used to identify, for example, Subscriber as a physical person who sometimes belongs to an External Entity. Relying party has to check additional information (key usage, OID policy ...) in order to accept and use the right Subscriber certificate in the electronic transaction. The relying party has to use all the required information in the certificate (DN as described in section 3.1.1 above, extensions ...) in order to be sure to accept the right Subscriber.

A Subscriber certificate can’t be used without preliminary check from Relying party like for example trusted path, additional information only known from Subscriber and Relying party (in order to register the Subscriber’s certificate) and Customer information about Subscriber enrollment and use of signed document verifiable using Subscriber certificate.

4.6 Certificate Renewal

According to RFC 3647, certificate renewal is a process in which only the validity period and the serial number of the certificate are changed (neither the public key nor any other information in the certificate are changed).

This practice is not allowed for Subscriber certificates. If a new certificate is created, a new key pair is created. This practice is authorized for CA and procedure remains the same as for the first CA certificate.

4.7 Certificate Re-key

Certificate re-key shall be processed when a key pair reaches the end of its life (refer to section 6.3.2 below), the end of operational use, or when the public key is compromised. A new key pair shall be generated in all cases.

4.7.1 Sub-CA

The same procedures as those applied for initial generation shall apply for a new Sub-CA certificate and associated key pair generation (refer to sections 4.1.1, 4.1.2, 4.2.1, 4.2.2, 4.2.3**Error! Reference source not found.**, 4.3.1, 4.4.1 and 4.4.2 above).

4.7.2 Subscriber

Refer to section 4.1.1, 4.1.2, 4.2.1, 4.2.2, 4.2.3**Error! Reference source not found.**, 4.3.1, 4.4.1 and 4.4.2 above but for authentication it is the section 3.3 that shall be applied.

4.8 Certificate Modification

According to RFC 3647, certificate modification is the process of generating new certificates using the same key pair.

This practice is not allowed for Subscriber certificates. If a new certificate is created, a new key pair is created. This practice is authorized for CA and procedure remains the same as for the first CA certificate.

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for Revocation

Any certificate shall be revoked when the binding between the certificate and the public key it contains is no longer considered valid. Examples of circumstances that invalidate the binding are:

- The RCA or ICA issuing CA in the chain is revoked or ceases activity.
- The subscriber fails to comply with the necessary obligations and security rules in the CP or CPS.
- The subscriber ceases operating, or is otherwise no longer associated with the issuing organization.
- The private key is suspected of compromise or is compromised or is suspected of being compromised.
- Change in policy as directed by the PMA, including requirements for key length, algorithm, validity date, or other certificate attributes.
- Other reasons as directed by the PMA.

4.9.1.1 Sub-CA

Sub-CA certificate revocation may only be directed by the PMA. In addition to the above, a Sub-CA certificate may be revoked when:

- The PMA directs that the Sub-CA is to cease operating.
- If the Sub-CA loses its license to issue certificates.
- The Sub-CA violates this CP or its own internal CP, at the discretion of the PMA.
- The entity owning the Sub-CA ceases to operate, or ends its Sub-CA services to DOCUSIGN FRANCE.

4.9.1.2 Subscriber

A certificate is revoked when the binding between the certificate and the public key it contains is considered no longer valid. Circumstances for physical person that invalidate the binding are:

- The CA is revoked.
- DN information filled incorrectly.
- The physical person or RA failed to comply with the necessary obligations and security rules in the CP and CPS.
- The certificate corresponding to the private key has been lost or compromised or suspected to be.
- Any other reasons indicated by PMA.

4.9.2 Who Can Request Revocation

4.9.2.1 Sub-CA

Only the PMA has the authority to request Sub-CA certificate revocation.

4.9.2.2 Subscriber

The physical person can submit a revocation request in the following cases:

- DN information filled incorrectly.
- The certificate corresponding to the private key has been lost or compromised or suspected to be.

The RA can submit a revocation request in the following cases:

- DN information filled incorrectly.
- The certificate corresponding to the private key has been lost or compromised or suspected to be.

The PMA can submit a revocation request in the following cases:

- The CA is revoked.
- The physical person or RA failed to comply with the necessary obligations and security rules in the CP and CPS.
- The certificate corresponding to the private key has been lost or compromised or suspected to be.
- Any other reasons indicated by PMA

4.9.3 Revocation Request Procedure

4.9.3.1 Sub-CA

The revocation of a Sub-CA certificate shall require the authorization of the PMA. The PMA shall direct the revocation by issuance of a signed document instructing the revocation to the ICA.

The revocation by the ICA shall be performed according to the written procedures of the ICA service provider.

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 revocation request to the CA.

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

The Sub-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

4.9.4.1 Sub-CA

The ICA shall process revocation of Sub-CA certificates upon receipt of direction from the PMA. This revocation shall be processed as quickly as possible not to exceed 10 business days.

4.9.4.2 Subscriber

There is no revocation grace period. Responsible parties must request revocation as soon as they identify the circumstances under which revocation is required.

4.9.5 Timeframe within which CA Must Process the Revocation Request

4.9.5.1 Sub-CA

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

4.9.5.2 Subscriber

The Sub-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 after RA has authenticated the request.

CRLs issued by CA “Cloud Signing CA” and “DocuSign Premium Cloud Signing CA - SI1” contain the extension "ExpiredCertsOnCRL" with the date for "start date" corresponding to the date and time of the first CA certificate of the AC.

4.9.6 Revocation Checking Requirement for Relying Parties

Use of revoked Certificates could have damaging or catastrophic consequences in certain applications. The matter of how often new revocation data should be obtained is a determination to be made by the Relying Party. If it is temporarily infeasible to obtain revocation information, then the Relying Party must either reject use of the Certificate, or make an informed decision to accept the risk, responsibility, and consequences for using a Certificate whose authenticity cannot be guaranteed to the standards of this policy. Such use may occasionally be necessary to meet urgent operational needs.

CRL issued by CA « Cloud Signing Personal Signature CA » and « DocuSign Premium Cloud Signing CA – SI1 » contains all expired revoked certificate and the extension « expiredCertsOnCRL ».

It should be noted that an unexpired certificate with a revoked status given by the OCSP service may have a valid status in the CRL because the OCSP is based on the CA database while the CRL is issued every 24 hours. This status difference can only last a maximum of 24 hours (the difference no longer exists with the next CRL). However, an expired, unqualified and revoked certificate will no longer be in the CRL but will have a revoked status given by the OCSP.

4.9.7 CRL Issuance Frequency

CA issues a CRL every 24 hours but CRL. CRL contains the expired revoked certificates.

CRL contains the expired revoked certificates.

The latest CRL issued by the “Cloud Signing CA Signature CA” and “DocuSign Premium Cloud Signing CA - SI1” is published with a validity date of December 31, 9999, 11:59:55 pm ("99991231235959Z").

Revocation information will always be available from the CA that publishes a LRC. In the event of the CA's end of life or the Service stopping with this CA or even in the event of a compromised CA key, a last CRL is generated and archived at DocuSign France. The latter CRL is published on the DocuSign France website until the TSP expires and on the CRL distribution URL contained in the Certificate until the last Certificate issued by the CA expires.

4.9.8 Maximum Latency for CRLs

CA issues CRL every 24 hours but CRL is valid for 6 days.

4.9.9 On-line Revocation/Status Checking Availability

If CA doesn’t include CRL in the signed document, therefore CAs shall support online status checking (OCSP service) in order to include an OCSP response in the signed document.

4.9.10 On-line Revocation Checking Requirements

The response of the OCSP system for CA validity status is based on the CA information (CA data base).

OCSP shall have the following format:

Field	Requirements
version	1
Responder ID	OCSP's public key hash
ProducedAT	Date and time of the OCSP response signature
CertID	Subscriber's certificate serialNumber, Sub-CA issuerKeyHash and Sub-CA issuerNameHash
This Update	Date and time of the verification of the Subscriber's certificate status made in the CRL.
Next Update	Date of the next CRL.
CertStatus	"Good", "Revoked" or "unknown"
nonce	Used if and only if the user Application provides a value for this field and reused in full.
extensions	No extension referenced

4.9.11 Other Forms of Revocation Advertisements Available

Not applicable.

4.9.12 Specific Requirements in the Event of Private Key Compromise

Entities that are authorized to submit alert are required to do so as quickly as possible after being informed of the compromise of the private key.

For Sub-CA Certificates, notification of compromise of private keys shall be performed according to the policies of the ICA service provider.

4.9.13 Suspension of token

Not applicable.

4.9.13.1 Circumstances for Suspension

Not applicable.

4.9.13.2 Who can Request Suspension

Not applicable.

4.9.13.3 Procedure for Suspension Request

Not applicable.

4.9.13.4 Limits on Suspension Period

Not applicable.

4.9.13.5 Resume certificate request

Not applicable.

4.10 Certificate Status Services

4.10.1 Operational Features

The OCSP service uses the Sub-CA information data base.

OCSP responses have an expiry date as follow:

- 24 hours for valid certificate.
- 72 hours for revoked certificate.
- 15 minutes for unknown certificate.

4.10.2 Service Availability

The certificate status service is available according needs of Protect and Sign (Personal signature) service. The service OCSP and CRL is available 24 hours a day, 7 days a week with an availability rate of 99.9.

The OCSP service is cut off after the end of the CA's life and only the last CRL is the only information available see 4.9.7.

4.11 End of Subscription

The contract between Customer and DOCUSIGN FRANCE deals with end of relationship.

4.12 Key Escrow and Recovery

4.12.1 Subscriber

4.12.1.1 Which key pair can be escrowed

Not applicable.

4.12.1.2 Who Can Submit a Recovery Application

Not applicable.

4.12.1.3 Recovery Process and Responsibilities

Not applicable.

4.12.1.4 Performing Identification and Authentication

Not applicable.

4.12.1.5 Approval or Rejection of Recovery Applications

Not applicable.

4.12.1.6 KEA and KRA Actions during key pair recovery

Not applicable.

4.12.1.7 KEA and KRA Availability

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 and Construction

The location and construction of the facility of the OA housing CA, RA and PS and remote Subscriber SSCD equipment shall be consistent with facilities used to house high value and sensitive information. The site location and construction, when combined with other physical security protection mechanisms such as guards and intrusion sensors, shall provide robust protection against unauthorized access to equipment and records.

5.1.2 Physical Access

CA and RA Equipment and Subscriber PSM SSCD shall always be protected from unauthorized access and damage. The physical security mechanisms for equipment 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 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 an authorized employee.
– Ensure an access log is maintained and inspected periodically.
– Provide at least three layers of increasing security such as perimeter, building, and operational room.
– Require two person physical access controls for both the cryptographic HSM and activation data for CA and SSCD.

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

– The equipment is in a state appropriate for the current mode of operation.
– For off-line components, all equipment is shut down.
– Any security containers (tamper-proof envelopes, safes ...) are properly secured.
– Physical security systems (e.g., door locks, vent covers, electricity ...) are functioning properly.
– The area is secured against unauthorized access.

Removable cryptographic modules shall be deactivated prior to storage. When not in use, removable cryptographic modules and the activation data used to access or enable cryptographic modules shall be placed in secure containers. 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.

5.1.3 Power and Air Conditioning

The OA ensures that power and air conditioning facilities are sufficient to support the operation of the PKI system, using primary and back-up installations.

5.1.4 Water Exposures

The OA ensures that systems are protected in a way that minimizes impact from water exposure.

5.1.5 Fire Prevention and Protection

The OA ensures that systems are protected with fire detection and suppression systems.

5.1.6 Media Storage

Media used within the OA are securely handled to protect media from damage, theft and unauthorized access. Media management procedures are implemented to protect against obsolescence and deterioration of media within the period of time that records are required to be retained.

Sensitive data shall be protected against being through re-used storage objects (e.g. deleted files) being accessible to unauthorized users.

CA shall maintain an inventory of all information assets and shall assign a classification for the protection requirements to those assets consistent with the risk analysis.

5.1.7 Waste Disposal

All media used for the storage of sensitive information such as keys, activation data or files shall be destroyed before being released for disposal.

5.1.8 Off-site Backup

Full back-ups of CA systems online, sufficient to enable recovery from system failure, shall be made after PKI deployment according to DOCUSIGN FRANCE policies. Back-up copies of essential business information and software are made regularly. Adequate back-up facilities are provided to ensure that all essential business information and software can be recovered following a disaster or media failure. Back-up arrangements for individual systems shall be regularly tested to ensure that they meet the requirements of the OA business continuity plan (for CA). At least one full back-up copy shall be stored at an offsite location (disaster recovery OA). The back-up copy shall be stored at a site with physical and procedural controls commensurate to that of the operational CA system.

5.2 Procedural Controls

5.2.1 Trusted Roles

CA shall ensure that roles are defined to operate the ETSI trusted roles functions in support of the PKI services (deployed by DocuSign France only) with an appropriate separation of duties.

All personnel are formally appointed to trusted roles by the PMA and/or the OA (for CA), as described in the CPS. For OID 1.3.6.1.4.1.22234.2.8.3.20 and 1.3.6.1.4.1.22234.2.14.3.31, PSM software dedicated role shall be implemented according [PSM SSCD].

Customer is responsible to define and documented trusted roles and associated operation compliant with ETSI. Customer shall define trusted to manage RA and RA personal shall be formally appointed by senior manager.

5.2.2 Number of Persons Required per Task

The number of persons who provide PKI services is detailed in the CPS for CA and Customer document for RA. The number of persons is defined to guarantee trust for all services (key generation, certificate generation, revocation, certificate request …), so that no malicious activity may be conducted by a single person acting on behalf of the PKI. All participants shall serve in a trusted role as defined in section 5.2.1 above.

Sub-CA keys are under dual control at minimum.

The following tasks shall be completed by two persons authorized for PKI system operations:

- key generation
- key activation
- key backup
- CA Certificate revocation.

The number of person required for each operation are defined in the CPS.

For OID 1.3.6.1.4.1.22234.2.8.3.20 and 1.3.6.1.4.1.22234.2.14.3.31, PSM software dedicated role shall be implemented according [PSM SSCD].

Customer shall appoint and define role to make at least a separation between personal in charge of RA services and personal in charge of RA software to proceed the following operation; configuration, installation, backup, maintain and recovery.

5.2.3 Identification and Authentication for Each Role

All necessary checks must be completed before any individual enters a trusted role within the PKI components.

For OID 1.3.6.1.4.1.22234.2.8.3.20 and 1.3.6.1.4.1.22234.2.14.3.31, PSM software dedicated role shall be implemented according [PSM SSCD].

All persons assigned a role, as described in this CP, are identified and authenticated to guarantee that said role enables them to perform their PKI duties. The CPS describes the mechanisms used to identify and authenticate individuals.

5.2.4 Roles Requiring Separation of Duties

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 above.

For OID 1.3.6.1.4.1.22234.2.8.3.20 and 1.3.6.1.4.1.22234.2.14.3.31, PSM software dedicated role shall be implemented according [PSM SSCD].

No individual shall be assigned more than one identity unless approved by the PMA.

The part of the CA concerned with certificate generation and revocation management shall be independent of other organizations for its decisions relating to establishing, provisioning and maintaining and suspending of services in conformance with the applicable certificate policies; in particular its senior executive, senior staff and staff in trusted roles, shall be free from any commercial, financial and other pressures which might adversely influence trust in the services it provides.

5.3 Personnel Controls

5.3.1 Qualifications, Experience, and Clearance Requirements

PMA and OA components employ a sufficient number of personnel who possess expert knowledge, experience and appropriate qualifications necessary for the job functions and services offered. PKI personnel fulfill the requirements of "expert knowledge, experience and qualifications" through formal training and credentials, actual experience, or a combination of the two. Trusted roles and responsibilities, as specified in the CPS, are documented in job descriptions and clearly identified. PKI personnel sub-contractors have job descriptions defined to ensure separation of duties and least privilege, and position sensitivity is determined based on the duties and access levels, background screening and employee training and awareness. PKI personnel shall be appointed to trusted roles by the PMA.

5.3.2 Background Check Procedures

PMA and OA employees in trusted roles shall be free from conflicting interests that might prejudice the impartiality of the PKI operations. The Customer and OA shall not appoint to trusted roles or management any person who is known to have a conviction for a serious crime or other offence which affects his/her suitability for the position.

5.3.3 Training Requirements

The PMA and OA ensure that all personnel performing duties with respect to operations receive comprehensive training in:

- PKI security principles and mechanisms
- Software versions in use in the PKI system
- PKI business Processes and workflows
- Duties they are expected to perform
- Dispute operations and procedures
- Sufficient IT knowledge.
- Disaster recovery and business continuity procedures

5.3.4 Retraining Frequency and Requirements

Individuals in trusted roles shall be aware of changes in the PKI operations, as applicable. Any significant change to the operations shall be accompanied by a training (awareness) plan, and the execution of said plan shall be documented.

5.3.5 Job Rotation Frequency and Sequence

The PMA and OA Entity ensure that any change in staff will not affect the security of the system.

5.3.6 Sanctions for Unauthorized Actions

Appropriate administrative disciplinary sanctions are applied to any PKI component's personnel violating the DOCUSIGN FRANCE CP.

5.3.7 Independent Contractor Requirements

Contractors employed to perform PKI component functions are subject to the all personnel controls defined in section 5.3. Contractors can perform PKI system operations (refer to section 5.2 above) with approval of the PMA or the Customer according the PKI component.

5.3.8 Documentation Supplied to Personnel

PKI components make available to their personnel the present CP and the corresponding CPS, and any relevant statutes and policies. Other technical, operational and administrative documents (e.g., Administrator Manual, User Manual, etc.) are provided to enable the trusted personnel to perform their duties.

5.4 Audit Logging Procedures

5.4.1 Types of Events Recorded

Audit log files are generated by 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 (for CA and for RA if RA uses HSM and SSCD).
- 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 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.

In addition to that, RA shall record all the information used:

– To verify the subject's identity.
– If applicable, any specific attributes of the subject, including any reference number on the documentation used for verification, and any limitations on its validity (refer to section 3.2 above).
– To create the certificate request (means all information described in section 4.1.2.2 above.
– The list of all RA Operator that are authorized to enroll and manage Subscriber.
– The technical Consent Protocol.

- According choice made by the Customer, record with the proof file (as defined in [PSMP]) as proof of the certificate request. If not, DocuSign France record the proof file in an archive system according [PSMP] also as proof of certificate request from RA.

5.4.2 Log Processing Frequency

PKI operation audit logs are reviewed on an annual basis by the member of the OA responsible for audits, who conducts a reasonable search for any evidence of malicious activity, and following each important operation.

A statistically significant sample of security audit data generated by their PKI business entity since the last review shall be examined (where the confidence intervals for each category of security audit data are determined by the security ramifications of the category and the availability of tools to perform such a review), as well as a reasonable search for any evidence of malicious activity. OA review log on day to day basis for IT and physical security.

The OA shall explain all significant events in log audit report. 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 shall be documented.

5.4.3 Retention Period for Audit Logs

Records related to PKI operation are held on the OA site for at least one year before being archived.

5.4.4 Protection of Audit Log

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.

5.4.5 Audit Log Backup Procedures

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.

5.4.6 Audit Collection System (Internal vs. External)

Audit processes shall be invoked at system start up, and end only at system shutdown. The audit collection system has to maintain the integrity and availability of all data collected. If necessary, the audit collection system protects the integrity of the data. If a problem appears during the process of the audit collection system, the PMA determines whether it has to suspend operations until the problem is solved and inform the impacted component.

5.4.7 Event-Causing Subject Notification

Where an event is logged by the audit collection system, it guarantees that the event is linked to a trusted role.

5.4.8 Vulnerability Assessments

The role 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:

– Implement detection and prevention controls under the control of the OA 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 (i) after any system or network changes that the PMA determines are significant for CA and Customer for RA, and (ii) at least once per quarter, on public and private IP addresses identified by the OA as the PKI's systems (for CA).

– 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 for CA and Customer for RA determines are significant.

– 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

5.5.1 Types of Records Archived

PKI component archived records shall be detailed enough to establish the validity of a signature and of the proper operation of the PKI. At minimum, the following data shall be archived:

- PKI events records:
  - Physical facility access log of OA (3 months minimum).
  - Video facility access log of OA (3months maximum).
  - Video of key ceremony for CA only (minimum 7 years after certificate expiration).
  - Trusted roles management log for OA (minimum 7 years after certificate expiration).
  - IT access log for OA (minimum 7 years after certificate expiration).
  - Subscriber and CA key creation, use and destruction log (minimum 7 years after certificate expiration) kept by DocuSign France.
  - Activation data management log for OA (minimum 7 years after certificate expiration).
  - IT and network log for OA (minimum 7 years after certificate expiration).
  - PKI documentation for OA (minimum 7 years after certificate expiration).
  - Security incident and audit report for OA (minimum 7 years after certificate expiration).
- PKI audit documentation (minimum 7 years after certificate expiration) kept by PMA.
- CP document (minimum 7 years after certificate expiration) kept by PMA.
- CPS documents (minimum 7 years after certificate expiration) kept by PMA.
- Contract between DOCUSIGN FRANCE and acting RA(minimum 7 years after certificate expiration) kept by PMA.
- System equipment, software and configuration (minimum 7 years after certificate expiration) for DocuSign France.
- Certificates (or other revocation information) (minimum 7 years after certificate expiration) kept by CA.
- Certificate request (minimum 7 years after certificate expiration) records in CA system.
- Other data or applications sufficient to verify archive contents (minimum 7 years after certificate expiration).
- All work related to or from the PMA and compliance auditors (minimum 7 years after certificate expiration).
- RA record (minimum 7 years after certificate expiration).

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.

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

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

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 PMA and OA personnel are allowed to access archives.

5.6 Key Changeover

5.6.1 Sub-CA Certificate

The Sub-CA private key validity period is defined in compliance with cryptographic security recommendations for key size length. The Sub-CA certificate validity period is defined in section 6.3 below.

The Sub-CA cannot generate Subscriber certificates whose validity period would be superior to the Sub-CA certificate validity period. A new key pair for the Sub-CA requires a new Sub-CA certificate be generated.

The Subscriber certificate has a fixed validity period which cannot be changed due to end of life of Sub-CA.

As soon as a new key pair is generated for the Sub-CA, only the new private key is used to sign Subscriber certificates.

Previous Sub-CA certificates shall be used for the validation process of the certification path for all Subscriber certificates signed by the previous Subscriber.

The PMA reserves the right to change the key at any time.

5.6.2 Subscriber Certificate

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 the CA CP.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

This system shall be supported by the DOCUSIGN FRANCE enterprise computing infrastructure and its incident, compromise and business continuity plans. These plans shall be periodically tested, reviewed and updated, as directed by the DOCUSIGN FRANCE.

If a PKI component (for DocuSign France) 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 PMA in order to determine if the PKI needs to be rebuilt, if only some certificates need to be revoked, and/or if the PKI has been compromised. In addition, the PMA determines which services are to be maintained (revocation and certificate status information) and how, in accordance with the PMA business continuity plan.

Incident, Compromise and Business continuity are covered in the CPS, which may also rely upon other enterprise resources and plans for implementation.

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.

Incident, Compromise and Business continuity are covered in the Customer documentation, which may also rely upon other enterprise resources and plans for implementation.

If any of the algorithms, or associated parameters, used by the CA becomes insufficient for its intended remaining use, then CA:

• Informs all RA with which CA has agreements or other forms of established relationships. In addition, this information is made available to other relying party;

• Revokes all relevant certificates.

The discovered vulnerabilities are processed within 48 hours of their knowledge by the PMA and the ANSSI and Adobe is alerted by the PMA in 24H00 after knowledge of the major incident affecting the security of the service or personal data.

5.7.2 Corruption of Computing Resources, Software, and/or Data

If PKI equipment is damaged or rendered inoperative, but signature keys are not destroyed, the operation is re-established as quickly as possible, with priority given to the ability to generate certificate status information.

5.7.3 Entity Private Key Compromise Procedures

If a CA key is compromised, lost, destroyed or suspected of being compromised:

- The PMA investigates on the “key-issue” and revokes the associated certificate.
- A new key pair is generated and a new certificate is created.
- Alert the Customer.

If system used by Protect and Sign (Personal signature) service to generate Subscriber key pair is compromised, then PMA alert the Customer and gives a list of detailed risk and consequence for Customer and Subscriber due to the compromising.

When any of the algorithms, or associated parameters, used by the CA or its Subscriber becomes insufficient for its remaining intended usage then the CA shall inform the Customer and change the used algorithms.

5.7.4 Business Continuity Capabilities after Disaster

The business continuity plan addresses all necessary operations as described in section 5.7.1 above.

5.8 Termination

One or more components of the PKI may be required to cease operations or transfer to another entity for various reasons.

The CA shall make arrangements to cover the costs of meeting these minimum requirements in the event that the CA goes bankrupt or for other reasons is unable to cover these costs on its own, subject as far as possible to the constraints of applicable bankruptcy legislation.

Transfer of activity is defined as the termination of activity of a component of the PKI that does not affect the validity of certificates issued prior to the transfer under consideration and the resumption of that activity organised by the CA in collaboration with the new entity.

The PMA must keep the ANSSI informed.

The cessation of activity is defined as the end of activity of a component of the PKI involving an impact on the validity of certificates issued prior to the cessation in question.

5.8.1 Transfer of activity or cessation of activity affecting a TGI component

In order to ensure a constant level of trust during and after such events, the CA shall:

- Implement procedures to ensure a consistent service, in particular with respect to archiving (e.g. archiving of Subscriber certificates and certificate information)
- Ensures revocation continuity (acknowledgement of a revocation request and publication of CRLs), in accordance with the availability requirements for its functions defined in the CP.

Details of the following commitments must therefore be announced by the CA in its CP:

- To the extent that the proposed changes may affect commitments to certificate RP or Subscriber, the CA shall notify them as soon as necessary.

5.8.2 Sub-CA

In the event of the termination of the PKI service, the PMA provides notice prior to the termination, and:

- Inform Customer.
- Destroys the Sub-CA private key.
- Revoke the CA certificate.
- Publishes the most recent revocation status information (CRL signed by CA) to all Relying parties (if any).
- The Sub-CA signed by the ICA stops delivering certificates in accordance with and referring to this CP and in accordance with its CP.
- In the case of a compromised Sub-CA, the PMA and OA both use secure means to notify Subscribers and relying parties that they must delete all trust certificates representing the Sub-CA with the compromised(s) key pair(s).
- Archives all audit logs and other records prior to terminating the PKI.
- Archived records are transferred to the PMA.

In the event of the termination of the OA services, the OA is responsible for keeping all relevant records regarding the needs of Subscriber and PKI components. The OA then transmits its records to the PMA.

5.8.3 RA

In the event of the termination of the RA service, the Customer provides notice prior to the termination, and:

- Inform PMA by register letter.
- Destroys all private keys used to secure communication with CA.

- Publishes the most recent revocation status information (CRL signed by CA) to all Relying parties (if any).
- The RA stops delivering certificates request to the CA.
- In the case of a compromised RA, the Customer use secure means to notify Subscribers and relying parties that they must not trust Subscriber certificate identified in the list provided by Customer.
- Archives all audit logs and other records prior to terminating the PKI.
- Archived records are transferred to an entity designated by Customer.

In the event of the termination of the OA services, the OA is responsible for keeping all relevant records regarding the needs of Subscriber and PKI components. The OA then transmits its records to the Customer.

6 TECHNICAL SECURITY CONTROLS

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

6.1.1.1 Sub-CA

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

The operation of the Sub-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.

Sub-CA key pair generation 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. Sub-CA key generation is carried out within a hardware security module (refer to section 6.2 below). Witnesses are persons other than the operational personnel. Sub-CA HSM activation and initialization is under the control of Sub-CA activation data holders. During the key ceremony, the Sub-CA key pair is backed up (refer to section 6.2. below).

6.1.1.2 Subscriber

Protect and Sign (Personal Signature) software shall request generation of the Subscriber signature key pair. The generation is performed using a HSM (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.

6.1.2 Private Key Delivery

Not applicable.

6.1.3 Public Key Delivery to Certificate Issuer

6.1.3.1 Sub-CA

Sub-CA public keys are securely delivered to the relevant ICA 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 Sub-CA checked identities to the public keys to be certified using the Pkcs#10 format.

6.1.3.2 Subscriber

A Subscriber’s public key is securely delivered by Protect and Sign (Personal Signature) software to the Sub-CA for certificate issuance. The delivery mechanism binds the verified identities to the public keys to be certified using the Pkcs#10 format.

6.1.4 CA Public Key Delivery to Relying Parties

Refer to section 2 above.

6.1.5 Key Sizes

6.1.5.1 Sub-CA

The key pair is 2048 bits long for the RSA algorithm.

RSA algorithm is used with SHA-2 as hash function.

6.1.5.2 Subscriber

The key pair is 2048 bits long for the RSA algorithm.

RSA algorithm is used with SHA-2 as hash function.

6.1.6 Public Key Parameters Generation and Quality Checking

6.1.6.1 Sub-CA

Public key parameters shall always be generated and checked in accordance with the standard that defines the crypto-algorithm for the parameters that are to be used.

Sub-CA keys are generated in accordance with the cryptography tools of the hardware security modules (refer to section 6.2.11 below).

6.1.6.2 Subscriber

Public key parameters shall always be generated and checked in accordance with the standard that defines the crypto-algorithm in which the parameters are to be used.

Subscriber keys are generated in accordance with the cryptography tools of the hardware security modules or tokens used to protect the keys (refer to section 6.2.11 below).

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

The use of the "key usage" extension in the "Subscriber" certificate (and also the "Extended Key Usage" extension when present) and in CA certificates is described in § 10 in the certificate profiles and indicates the purpose of the key usage.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

6.2.1.1 Sub-CA

The Sub-CA generates its key pairs and stores their private keys within an HSM that is certified according to the rating specified in section 6.2.11 below.

6.2.1.2 Subscriber

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 (N out of M) Multi-Person Control

6.2.2.1 Sub-CA

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

6.2.2.2 Subscriber: OID different from 1.3.6.1.4.1.22234.2.8.3.20 and 1.3.6.1.4.1.22234.2.14.3.31

Subscriber’s key pair is activated after successful authentication of the Subscriber using its activation data according Consent Protocol chosen by Customer.

6.2.2.3 Subscriber: OID 1.3.6.1.4.1.22234.2.8.3.20 and 1.3.6.1.4.1.22234.2.14.3.31

Subscriber's key pair is activated after successful authentication of the Subscriber using its activation data (OTP code send by SMS to the Subscriber) according Consent Protocol defined in the [PSM SSCD].

6.2.3 Private Key Escrow

6.2.3.1 Sub-CA

Under no circumstances shall a Sub-CA private key be escrowed by any PKI component or third party.

6.2.3.2 Subscriber

Under no circumstances shall the private key be escrowed by a third party or by PKI components.

6.2.4 Private Key Backup

6.2.4.1 Sub-CA

Sub-CA private signature keys shall be backed up under the same multi-person control as the operational ones. A single back-up copy of the signature key shall be stored in the Sub-CA systems location. A second back-up copy shall be kept at the Sub-CA off-site backup location. All locations must be accepted by the PMA.

6.2.4.2 Subscriber

Not applicable.

6.2.5 Private Key Archival

6.2.5.1 Sub-CA

Sub-CA private keys shall never be archived.

6.2.5.2 Subscriber

Not applicable.

6.2.6 Private Key Transfer Into or From a Cryptographic Module

6.2.6.1 CA Private Key

In the case of private key transfer, the Sub-CA key pair is transferred to another Hardware Security Module (HSM) of the same specification as described in section 6.2, by direct token-to-token copy, via a trusted path under N out of M multi-person control (refer to section 6.2).

Sub-CA keys are generated, activated and stored in HSMs or in an encrypted format. When they are not stored onto HSMs, Sub-CA private keys are encrypted. An encrypted Sub-CA 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 Subscriber

Not applicable.

6.2.7 Private Key Storage on Cryptographic Module

6.2.7.1 Sub-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 those mentioned in the security policy attached to the approved HSM.

6.2.7.2 Subscriber: OID different from 1.3.6.1.4.1.22234.2.8.3.20 and 1.3.6.1.4.1.22234.2.14.3.31

Dedicated HSM for Protect and Sign (Personal signature) service stores Private Keys in any form as long as the keys are not accessible without authentication mechanisms that are compliant with those mentioned in the security policy attached to the approved HSM and according Consent Protocol.

6.2.7.3 Subscriber: OID 1.3.6.1.4.1.22234.2.8.3.20 and 1.3.6.1.4.1.22234.2.14.3.31

Dedicated partition in HSM for Protect and Sign (Personal signature) service stores Private Keys in any form as long as the keys are not accessible without authentication mechanisms that are compliant with those mentioned in the security policy attached to the approved HSM and according Consent Protocol defined in the [PSM SSCD].

6.2.8 Method of Activating Private Key

6.2.8.1 Sub-CA

Several trusted roles with activation data are required to perform the initial activation of the HSM that contains the Sub-CA key pair corresponding to a Sub-CA Certificate. Once the HSM containing the Sub-CA key and the Sub-CA key are operational, only the authorized services of the PKI system can use the Sub-CA key pair within the HSM, by using the mutual authenticated interface of the PKI systems.

6.2.8.2 Subscriber: OID different from 1.3.6.1.4.1.22234.2.8.3.20 and 1.3.6.1.4.1.22234.2.14.3.31

Subscriber key pair is activated according the Customer’s Consent Protocol. Consent Protocol shall require a technical activation data (for example: OTP code, authentication certificate used by the Subscriber to be authenticated by CA or OTP token).

6.2.8.3 Subscriber: OID 1.3.6.1.4.1.22234.2.8.3.20 and 1.3.6.1.4.1.22234.2.14.3.31

Subscriber’s key pair is activated according Consent Protocol defined in the [PSM SSCD]. Consent Protocol shall require from the Subscriber an OTP code transmitted by PSM by SMS using mobile phone number transmitted by RA.

6.2.9 Method of Deactivating Private Key

6.2.9.1 Sub-CA

A Sub-CA HSM that has been activated is never left available to unauthorized access.

After being used, HSMs are deactivated. After deactivation, the use of the HSM-based Sub-CA key pair shall require the presence of the trusted roles with the activation data in order to reactivate said Sub-CA key pair (refer to section 6.2).

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

6.2.9.2 Subscriber

Subscriber’s key pair is used to sign document during a transaction requested by RA, according [PSPM] and Customer Consent Protocol and Customer Signature Policy, and destroyed immediately after usage.

6.2.10 Method of Destroying Private Key

6.2.10.1 Sub-CA

Destroying a Sub-CA private key inside an HSM requires destroying the key(s) inside the HSM using the zeroization function of hardware in such a way that no information can be used to recover any part of the private key. All the Sub-CA private key back-ups must be destroyed using the same level of security. If the HSM functions 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 5.1above) by personnel in trusted roles (refer to section 5.2 above) under at least dual supervision.

6.2.10.2 Subscriber

Destroying a Subscriber's private key inside an HSM requires destroying the key(s) inside the HSM using the zeroization function of hardware in such a way that no information can be used to recover any part of the private key. If the HSM functions are not accessible in order to destroy the key contained inside, then the HSM has to be physically destroyed.

6.2.11 Cryptographic Module Rating

6.2.11.1 Sub-CA

The Hardware Security Module used to generate RCA key pairs is at least approved in accordance with FIPS 140 - 2 Level 3 standard or EAL4+ Common Criteria equivalent.

6.2.11.2 Subscriber: OID different from 1.3.6.1.4.1.22234.2.8.3.20 and 1.3.6.1.4.1.22234.2.14.3.31

The Hardware Security Module used to generate Subscriber key pairs is at least approved in accordance with FIPS 140 - 2 Level 2 standard or EAL4+ Common Criteria equivalent.

6.2.11.3 Subscriber: OID 1.3.6.1.4.1.22234.2.8.3.20 and 1.3.6.1.4.1.22234.2.14.3.31

The Hardware Security Module used to generate Subscriber key pairs is at least approved in accordance with FIPS 140 - 2 Level 3 standard or EAL4+ Common Criteria equivalent and certified as a SSCD compliant with Annex III requirements of Directive 1999/93/EC.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

Public keys are archived as part of certificate archival as described in section 5.5 above.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

6.3.2.1 Sub-CA

The maximum operational period for a Sub-CA private key is five (5) years.

The maximum operational period for a Sub-CA certificate is 5 (5) years.

6.3.2.2 Subscriber

A Subscriber private key can be used as long as the associated certificate is valid, and can be used for decrypting encrypted data as long as is necessary.

The Subscriber certificate validity period is given in section 10.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

6.4.1.1 Sub-CA

Sub-CA activation data used to protect HSM containing Sub-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. Some of the most critical activation data are backup (CPS gives exact details).

The 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 Subscriber: OID different from 1.3.6.1.4.1.22234.2.8.3.20 and 1.3.6.1.4.1.22234.2.14.3.31

The Consent Protocol (refer to section 4.3 above) requires a technical activation data (for example: OTP code, authentication certificate used by the Subscriber to be authenticated by CA or OTP token).

This activation data is generated either by RA or Protect and Sign (Personal signature) platform or accepted by Customer (for example, Customer can accept to use certificate delivered to Subscriber in order to authenticate Subscriber during Consent Protocol). When an activation data is generated by Customer or accepted by Customer, then this activation data shall be securely transmit to the Protect and Sign (Personal signature) in order to be used by Protect and Sign (Personal signature) to authenticate Subscriber.

6.4.1.3 Subscriber: OID 1.3.6.1.4.1.22234.2.8.3.20 and 1.3.6.1.4.1.22234.2.14.3.31

The Consent Protocol (refer to section 4.3 above) requires a technical activation data that is an OTP code send by SMS.

This OTP code is generated by Protect and Sign (Personal signature) platform according Consent Protocol defined in the [PSM SSCD].

6.4.2 Activation Data Protection

6.4.2.1 Sub-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 PMA requires that activation data holders store their activation data in a safe for which access is controlled by both the holder and other employees in trusted roles.

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

6.4.2.2 Subscriber: OID different from 1.3.6.1.4.1.22234.2.8.3.20 and 1.3.6.1.4.1.22234.2.14.3.31

A Subscriber is responsible for ensuring the protection of his/her activation data.

When activation data are managed by Customer, RA and/or Protect and Sign (Personal signature) then these entities are also responsible of the protection of the protection of the activation data in a way to avoid use of activation data by other entity than the Subscriber.

6.4.2.3 Subscriber: OID 1.3.6.1.4.1.22234.2.8.3.20 and 1.3.6.1.4.1.22234.2.14.3.31

A Subscriber is responsible for ensuring the protection of his/her activation data.

When activation data are managed by Sign (Personal signature) then these entities is also responsible of the protection of the protection of the activation data in a way to avoid use of activation data by other entity than the Subscriber.

6.4.3 Other Aspects of Activation Data

6.4.3.1 CA

Activation data are changed if hardware security modules are re-keyed or returned to the manufacturer for maintenance. Other aspects of activation data management are given in the CPS.

6.4.3.2 Subscriber (physical person)

Not applicable.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

The following computer security functions are provided by the operating system, or through a combination of operating system, software, and physical safeguards. PKI components implement the following functionalities (CA and RA IT system when applicable):

- Require authenticated logins for trusted roles.
- Provide discretionary access control.
- Require use of authentication for session communication.
- Require user identification.
- Provide domain isolation for processes involving roles using PKI services.
- Remove unwanted services and ports from the PKI components.

When the PKI equipment is hosted on platforms certified for computer security assurance requirements, the system (hardware, software and operating system), when possible, operates in said certified configuration. At minimum, such platforms use the same version of the computer operating system as the one which received the evaluation rating. OA computer systems are configured with minimum required accounts, network services, and no remote login.

Sub-CA key pair generation is performed on the online HSMs, except during PKI system set-up where the HSM used online will be set up in an offline environment.

PSM software shall be installed according [PSM SSCD].

Key ceremony workstations are dedicated to key ceremony operations and not connected to any public network. Computers used in the administration of the PKI systems are dedicated to this task only.

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 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.

6.5.2 Computer Security Rating

No stipulations. For OID 1.3.6.1.4.1.22234.2.8.3.20 and 1.3.6.1.4.1.22234.2.14.3.31, PSM software is certified according [PSM SSCD].

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

The system development controls for the PKI are as follows:

- Use software that has been designed and developed under a formal, documented development methodology according to Common Criteria evaluation (for CA).

- Hardware and software procured shall be purchased in such a way so as to reduce the likelihood that any particular component was tampered with.

- Hardware and software shall be developed in a controlled environment, and the development process shall be defined and documented. This requirement does not apply to commercial off-the-shelf hardware or software.

- All hardware 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 shall be dedicated to performing the PKI activities. There shall be no other applications; hardware devices, network connections, or component software installed which are not part of the PKI operation.

- Proper care shall be taken to prevent malicious software from being loaded onto the equipment.

Only applications required to perform the PKI operations shall be obtained from sources authorized by local policy. PKI 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.

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 formal configuration management methodology 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 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 PMA monitors the maintenance scheme requirements to ensure the same level of trust.

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

The PKI system shall implement appropriate security measures to ensure they are guarded against denial of service and intrusion attacks. Such measures shall include the use of guards, firewalls and filtering routers. Unused network ports and services shall be turned off. Any network software present shall be necessary to the functioning of the PKI system.

The following rules apply:

- Any boundary control devices used to protect the network on which PKI equipment is hosted shall deny all but the necessary services to the PKI equipment even if those services are enabled for other devices on the network.
- Segment PKI equipment into networks or zones based on their functional, logical, and physical (including location) relationship. Only authorized flow, used for administration and PKI services, between PKI equipment shall be authorized.
- 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 (front-end and back-end like N-Thirds architecture shall be in place).
- Implement and configure an administration network (a system used to provide security support functions, such as authentication, network boundary control, audit logging, audit log reduction and analysis, vulnerability scanning, anti-virus when it is applicable and IT administration) that protects systems and communications between PKI systems and communications with non-PKI systems outside those zones (including those with organizational business units that do not provide PKI-related services) and those on public networks.

– 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 at least a weekly basis (for CA) and according Customer security policy for RA 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.

– Implement strong authentication for each component of the PKI system that supports multi-factor authentication.

– 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.

For OID 1.3.6.1.4.1.22234.2.8.3.20 and 1.3.6.1.4.1.22234.2.14.3.31, PSM software shall be installed according [PSM SSCD].

6.8 Time-Stamping

Electronic or manual procedures shall be used to maintain system time. Clock adjustments are auditable events as listed in section 5.4 above. Key ceremony uses a manual procedure.

For secured time on audit records, all Sub-CA system components shall regularly synchronize with a time service such as Network Time Protocol (NTP) Service. Time derived from the time service shall be used for establishing the time of:

- Initial validity time of a Subscriber Certificate.

- Initial validity time of CRL and OCSP response.

Additional information is given in the applicable CPS. Customer shall take care about the RA system to control system time.

7 CERTIFICATE, CRL AND OCSP PROFILES

7.1 Certificate Profile

7.1.1 Version Numbers

Issued certificates are X.509 v3 Certificates (populate version field with integer "2").

7.1.2 Certificate Extensions

Any Sub-CA asserting critical private extensions shall be interoperable in their intended community of use.

Issuer Sub-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 these Certificate profiles.

7.1.3 Algorithm Object Identifiers

Certificates issued under this CP shall use the following OIDs for signatures:

sha256WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha256WithRSAEncryption(11)}

Certificates issued under this CP shall use the following OIDs for signatures:

Sha1WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha256WithRSAEncryption(5)}

Certificates under this CP shall use the following OID for identifying the subject public key information:

rsaEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) rsaEncryption(1)}

7.1.4 Name Forms

The Subject and Issuer fields of the Certificate shall be populated with a unique Distinguished Name in accordance with one or more of the X.500 series standards, with the attribute type as further constrained by [RFC5280] and section 3.1.

7.1.5 Name Constraints

The Sub-CA asserts critical or non-critical name constraints beyond those specified in the Certificate profiles in section 10 below for the Sub-CA certificate and Subscriber Certificate.

7.1.6 Certificate Policy Object Identifier

The Sub-CA shall not contain the Certificate policy OIDs defined in this CP, listed in section 1.2 of this CP, in the certificate policy extension if it issues a Subscriber certificate which contains an OID listed in section 1.2.

The Subscriber certificate shall have only one OID, listed in section 1.2 of this CP, in the certificate policy extension.

7.1.7 Usage of Policy Constraints Extension

Not applicable.

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 as described in section 10 below.

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 as described in section 10 below.

7.2 CRL Profile

Refer to section 10 below.

7.3 OCSP Profile

Refer to section 10 below.

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1 Frequency or Circumstances of Assessment

The PKI components are subject to periodic compliance audits at least once a year, to allow the PMA to authorize or not (based on the audit result) PKI components hosted by the OA to operate under this CP according to the “PKI audit guide” provided by the ICA.

The PMA has the right to require non periodic compliance audit of PKI components (especially RA) that operate under this CP. The PMA states the reason for any non-periodic compliance audit.

During the period in which the CA issues Certificates, the PMA shall monitor adherence to its Certificate Policy, Certification Practice Statement and RA Requirements and strictly control its service quality by performing self-audits on at least a yearly basis against a randomly selected sample of the greater of one certificate or at least three percent of the Certificates issued by it during the period commencing immediately after the previous self-audit sample was taken.

Before to authorize a Customer to use Protect and Sign (Personal signature) service using a certified OID, PMA audit the RA procedure and RA management defined by the Customer to be sure that it is coherent with requirement set in the PC. If the RA procedures are compliant with CP requirements, then PMA authorizes Customer to use Protect and Sign (Personal signature) service with its RA.

In addition to that, PMA mandates regularly, according ANSSI and eDIAS requirements, external auditor to asset the compliancy of CA to ETSI requirements.

When a Customer wants to use Protect and Sign (Personal signature) service with a certified OID, then Customer (as RA) shall be audited by external auditor, selected by the PMA, to asset its compliancy against this CP and ETSI requirements according to the selected OID. If not Customer can’t claim that the Subscriber certificate is compliant with a certified OID. The audit program is planned according the following with an audit each year for RA:

- First audit is realized by external audit.
- First year after the initial audit, the audit is realized according DOCUSIGN FRANCE audit program.
- Second year after the initial audit, the audit is realized by external auditor.

In case of major findings discovered during internal audit made by DOCUSIGN FRANCE, RA as to fix it and an external audit will be conduct during the same year in order to check the findings.

8.2 Identity/Qualifications of Assessor

Compliance auditors shall demonstrate competence in the field of compliance audits and shall be thoroughly familiar with requirements of these CP. Compliance auditors must perform such compliance audits as a primary responsibility. The PMA should carefully review the methods employed to audit PKI components for its own audit requirements base. The PMA is responsible for selecting the auditor for its own PKI components. In addition, the PMA must approve selected auditors.

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

The PMA determines whether a compliance auditor meets these requirements in order to audit CA and RA.

8.3 Topics Covered by Assessment

The purpose of a compliance audit shall be to verify that a component operates in accordance with this CP and the corresponding CPS.

For CA, the perimeter of audit is OA, CA, Customer contractual relationship and RA control by PMA.

For RA, the perimeter of audit is:

- Protection according this CP, KWS CP and PSMP document, use and management of the KWS keys pairs used to protect communication with CA.
- Protection according this CP, KWS CP and PSMP document, use and management of the Protect and Sign (Personal signature) Client software provide by DocuSign France.
- Creation of the technical certificate request.
- RA records against requirements set in this CP.
- “RA procedure” defined by Customer to identify, authenticate and manage certificate request to the CA.
- RA Consent Protocol and the implementation of “WYSWSY” for information to be set in the certificate as defined in section 4.3 above.
- Subscriber personal data protection and management.

8.4 Actions Taken as a Result of Deficiency

The PMA may determine that PKI components do not comply with obligations set forth in this CP. In the case of non-compliance, the PMA may suspend operation of the non-compliant PKI component, or may decide to discontinue relations with the affected PKI component, or decide that other corrective actions have to be taken.

When the compliance auditor finds a discrepancy with the requirements of this CP, the following actions shall be performed:

- The compliance auditor notes the discrepancy.
- The compliance auditor notifies the Entity of the discrepancy. The auditor and the Entity shall notify the PMA promptly.
- The party responsible for correcting the discrepancy determines what further notifications or actions are necessary pursuant to the requirements of this CP, and then proceeds to make such notifications and take such actions without delay in relation with the approval of PMA.

Depending upon the nature and severity of the discrepancy, and how quickly it can be corrected, the PMA may decide to temporarily halt operation of a PKI component (typically end relationship with a Customer temporally or definitively), to revoke a certificate issued by the PKI component, or take other actions it deems appropriate. Based on the audit result the PMA can decide to revoke CA.

8.5 Communication of Results

An Audit Compliance Report, including identification of corrective measures taken or being taken by the component, is provided to the PMA as well as the dedicated persons in the entity. The report identifies the versions of the CP and CPS and any other auditing criteria used as the basis for assessment.

The Audit Compliance Report is not available on the Internet for relying parties. However, it may be provided to law of court or any official body based on legal request. In addition, it should be available, in part or in whole, to the Audited entity according to the PMA decision.

9 OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

9.1.1 Certificate Issuance or Renewal Fees

These services are defined in the contract established between DOCUSIGN FRANCE and Customer.

9.1.2 Certificate Access Fees

No fees.

9.1.3 Revocation or Status Information Access Fees

Not applicable.

9.1.4 Fees for Other Services

These services are defined in the contract established between DOCUSIGN FRANCE and Customer.

9.1.5 Refund Policy

These services are defined in the contract established between DOCUSIGN FRANCE and Customer.

9.1.6 Fines List

These services are defined in the contract established between DOCUSIGN FRANCE and Customer.

9.2 Financial Responsibility

9.2.1 Insurance Coverage

DOCUSIGN FRANCE maintains reasonable levels of insurance coverage.

9.2.2 Other Assets

DOCUSIGN FRANCE maintains sufficient financial resources to maintain operations and fulfill PKI services.

9.2.3 Insurance or Warranty Coverage for Subscribers

If there is damage for a Customer due to DOCUSIGN FRANCE fault, DOCUSIGN FRANCE will activate its insurance to cover part of the customer damage in the limits stated in contractual arrangements between DOCUSIGN FRANCE and Customer.

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

PMA guarantees a special treatment for the following confidential information:

- Records and archive of OA.
- Personal identity data.
- Sub-CA private keys.
- Subscriber private key.
- Subscriber certificate request.
- Sub-CA activation data.
- Audit result and reports.
- Business continuity plan.
- Contractual and agreement with Customer.

- Internal facility security policy.
- Activation data.
- CPS.

The treatment of confidential business information provided by RA and Customer in the context of submitting a certificate request for Subscriber will be in accordance with the terms of the contract entered into between the applicable Customer and DOCUSIGN FRANCE.

Each RA and 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, and shall treat such information with the same degree of care and security as the CA treats its own most confidential information.

9.3.2 Information Not Within the Scope of Confidential Information

All information that is published by the PS (CP and CA certificates) is considered to be not confidential.

9.3.3 Responsibility to Protect Confidential Information

PKI components shall be responsible for protecting the confidential information they possess in accordance with the applicable laws and contracts. PKI components must not disclose certificate or certificate-related information to any third party unless authorized by this policy, required by law, government rule or regulation, or order of a court of competent jurisdiction.

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

For the purposes of the PKI related services, PKI components may collect, store, or process personally identifiable information. Any such use or disclosure shall be in accordance with applicable laws and regulations, specifically the European Data Protection Act and the present Certification Policy.

DocuSign France manage Subscriber personal data according applicable laws and regulations, specifically the European Data Protection Act and the present Certification Policy.

Entity RAs shall develop a privacy policy, according to European Law, and stipulate in the contract between Customer and DOCUSIGN FRANCE how they protect any personally identifiable information they collect.

Subscribers must be given access and the ability to correct or modify their personal or organization information upon appropriate request to the Customer according Protect and Sign (Personal signature) service policy and Customer rules. Such information must be provided only after taking proper steps to authenticate the identity of the requesting party.

When personal or organization information for Subscriber's has to be modified, then it shall be done before certificate generation. Once the Subscriber certificate is generated, it is not possible for Subscriber to request modification and deletion of RA and CA record that concerned its private personal data. Customer is the sole point of contact for the Subscriber to have access to its personal data according Customer terms and condition.

Details are given to the Subscriber in the Terms of Use signed by the Subscriber.

9.4.2 Information Treated as Private

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

9.4.3 Information Not Deemed Private

Any and all information within a certificate is inherently public information and shall not be considered confidential information.

9.4.4 Responsibility to Protect Private Information

PMA, OA and PKI component shall have the responsibility to protect private information and shall refrain from disclosing it unless by order of the Sub-CA and RA pursuant to law enforcement.

9.4.5 Notice and Consent to use Private Information

All private information coming from a PKI component cannot be used without any explicit consent from the Subscriber (refer to section 4.1) and PMC for dedicated treatment.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

Sub-CA is compliant with its national law and has secure procedures to clear access to private data.

RA is compliant with its national law and has secure procedures to clear access to private data.

9.4.7 Other Information Disclosure Circumstances

The PMA obtains consent from PKI Components to transfer its private data in case of a transfer of activity as described in section 5.8.

9.5 Intellectual Property Rights

The PMA shall maintain intellectual ownership of CA certificates that it publishes. This CP shall be the property of the PMA. Any service mark, trademark, or trade name contained within a certificate or certificate application shall remain the property of its owner. The Sub-CA key-pairs and corresponding certificate shall be the property of the PMA.

9.6 Representations and Warranties

9.6.1 PMA Representations and Warranties

The PMA defines the present CP and the corresponding CPS. The 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 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 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 PMA has the responsibility to audit the RA and approve RA's procedures before allows Customer (RA) uses the Protect and Sign (Personal signature) service with one of the OID referenced in section 1.2 above.

9.6.2 Sub-CA Representations and Warranties

The Sub-CA has the responsibility to:

- Protect and guarantee integrity and confidentiality of their activation data and/or private key.
- Only use their private key and certificate, with associated tools specified in CPS, for what purpose they have been generated.
- Respect and operate the section(s) of the CPS that deals with their duties (this part of CPS has to be transmitted to the corresponding component).
- Allow the auditor team to control and check the compliance with the present CP and with the components CP/CPS and communicate the requested information to them, in accordance with the intentions of the PMA.
- Document their internal procedures to complete the global CPS.
- Use every means (technical and human) necessary to achieve the realization of the CP/CPS it has to implement and for which they are responsible.

- If the Subscriber's private key has been lost, stolen potentially compromised due to compromise of activation data or other reason notify Customer.
- Shall carry out a risk assessment to evaluate business risks and determine the necessary security requirements and operational procedures. The risk analysis shall be regularly reviewed and revised if necessary.
- Shall implement and define CP and CPS according principals set in DOCUSIGN FRANCE security policy.

9.6.3 RA Representations and Warranties

The RA has the responsibility to:

- For OID 1.3.6.1.4.1.22234.2.8.3.7, 1.3.6.1.4.1.22234.2.8.3.20, 1.3.6.1.4.1.22234.2.14.3.31 and 1.3.6.1.4.1.22234.2.14.3.32: Ensure that Subscriber is properly identified and authenticated, and that Subscriber certificate request, accurate and duly authorized.
- For OID 1.3.6.1.4.1.22234.2.8.3.9: Ensure that evidence of Subscriber's and subject's identification and accuracy of their names and associated data are either properly examined as part of the defined service or, where applicable, concluded through examination of attestation from appropriate and authorized sources, and that certificate requests are accurate, authorized and complete according to the collected evidence or attestation.
- Before entering into a contractual relationship with a subscriber, the RA shall inform the subscriber of the terms and condition regarding use of the certificate. The RA shall communicate this information though a durable (i.e. with integrity over time) means of communication, which may be transmitted electronically, and in readily understandable language.
- Submit accurate and complete information to the CA in the certificate request according PSMP document.
- Make Subscriber be able to view information that will be set in Subscriber certificate to create its identity (refer to section 4.3 above) during Consent Protocol.
- Let auditor team audit and communicate the requested information to them, according to the PMA intention, control and check the compliance with the present CP and with the components CPS and the RA procedure.
- Alert PMA when there is a security incident about the CA services that the OA performed.
- Respect the CP and corresponding CPS.
- Protect its information system and guaranty the security of the data transmitted to the PKI.
- Collect and verify Subscriber information in order to create the Subscriber certificate.
- Records and archive
- Authenticates and identify the Subscriber.
- Submit accurate and complete information about the Subscriber to the Sub-CA.
- Protect information of the Subscriber.
- Exercise reasonable care to avoid unauthorized use of the subject's private key.
- Designate and maintain a list of all RA Operator.
- Alert Customer in case of incident related to CP and RA procedure.
- Respect contract established between Customer and DOCUSIGN FRANCE.

9.6.4 Customer Representations and Warranties

Make available the signed document to the Subscriber.

- Exercise reasonable care to avoid unauthorized use of the private key of "Protect and Sign Personal signature".
- Notify Subscriber in case of Customer private key has been lost, stolen potentially compromised due to compromise of activation data or other reason.
- Notify Subscriber in case of Subscriber private key has been lost, stolen potentially compromised due to compromise of activation data or other reason.
- In case of being informed that the CA which issued the Subscriber's certificate has been compromised, ensure that the certificate is not used by the Subscriber or a Relying Party.

- Establishes contract with RA and OA entity when they are different legal entity from it with clear identification of PKI services run by the entity and all RA's and OA's obligations and warranties according PKI services managed.
- Defines RA procedure and RA management procedure.
- Select OID level from this CP.
- Alert PMA in case of incident due to RA.
- Select and defines Consent Protocol.
- Respect the CP and corresponding CPS.
- Protect its information system and guaranty the security of the data transmitted to the PKI.
- Let auditor team audit and communicate the requested information to them, according to the PMA intention, control and check the compliance with the present CP and with the components CPS, the contract between DOCUSIGN FRANCE and the Customer, the RA procedure and PSMP.

9.6.5 OA Representations and Warranties

The OA has the responsibility to:

- Respect its security policy.
- Protect and guarantee integrity and confidentiality of their secret data and/or private key.
- Allow the auditor team to control and check the compliance with the present CP/ auditing criteria and components of the CPS as well as the OA's security policy and communicate every useful piece of information to them, in accordance with the intentions of the PMA.
- Alert PMA when there is a security incident with the PKI services that the OA performed.
- Respect and operate the section(s) of the CPS that deals with their duties (this part of CPS has to be transmitted to the corresponding component).
- Protect identity token and associated activation data.
- Protect and guarantee integrity and confidentiality of their secret data and/or private key.
- Document their internal procedures to complete the global CPS and its security policy.
- Respect the total or parts of the agreement(s) that binds it to the PMA and to the Customer.

9.6.6 Subscriber

The physical person has the responsibility to:

- Accurately represent themselves in all communications with the RA.
- Only use activation data through the Customer application according the Protect and Sign (Personal signature) service and Consent Protocol.
- When they are used, protect their activation data at all times and prevent them from unauthorized access in accordance with this policy, as stipulated in their Subscriber agreement.
- Abide by all the terms, conditions, and restrictions levied on the use of their Certificates, as set forth in this CP and the Subscriber agreement.

- Use Certificates provided by the Sub-CA only for authorized and legal purposes in accordance with the Entity CP.

- Cease to use such issued Certificates if they become invalid and remove them from any applications they have been installed on.

9.6.7 Representations and Warranties of Other Participants

9.6.7.1 Relying Party Representations and Warranties

Any relying party has the responsibility to validate a digital certificate using:

- Only accept the use of the Certificate for the purposes indicated in the Certificate keyUsage extensions.
- Verify the validity of the Certificate, using the procedures described in [RFC5280], prior to any reliance on said Certificate.
- Check the OID contained in each certificate of the trusted certification path in order to be sure to accept the right kind of certificate.
- Establish trust in the Sub-CA who issued the Certificate by the methods outlined elsewhere in this CP, and using the path validation algorithm outlined in [RFC5280].
- Preserve the 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 said signature.
- Cease to use such issued Certificates (Subscriber, Sub-CA ...) if they become invalid and remove them from any applications they have been installed on.

9.7 Disclaimers of Warranties

The PMA guarantees through the PKI services:

- Identification and authentication of Sub-CA, with the Sub-CA Certificate generated by the ICA.
- Management of corresponding certificates and certificate status information regarding the present CP.
- Subscriber certificate content according RA transmitted information about Subscriber.
- Subscriber key pair is used by the sole Subscriber according Consent Protocol chosen by Customer and activation data required from Subscriber.

The RA guarantees trough the PKI services:

- Identification and authentication of Subscriber, with Subscriber certificate generated by the applicable Sub-CA.
- When it is applicable, transmission of activation data to the right Subscriber.

PMA provides no warranty, express, or implied, statutory or otherwise and disclaims any and all liability for the success or failure of the deployment of the PKI or for the legal validity, acceptance or any other type of recognition of its own certificates otherwise mentioned above. No more guarantees can be pinpointed by the PMA and relying parties in their contractual relationship (if there is any).

9.8 Limitations of Liability

DOCUSIGN FRANCE makes no claims with regard to the suitability or authenticity of certificates issued under this CP. Relying parties may only use these certificates at their own risk. The PMA assumes no liability what so ever in relation with the use of certificate or associated public/private key pairs for any use other than those described in the present CP/CPS.

RA is liable as regards the accuracy of all information contained in the Subscriber certificate and Subscriber enrollment used for Consent Protocol.

9.9 Indemnities

DOCUSIGN FRANCE makes no claims as to the suitability of certificates issued under this CP for any purpose whatsoever. Relying parties use these certificates at their own risk. DOCUSIGN FRANCE has no obligation to make any payments regarding costs associated with the malfunction or misuse of certificates issued under this CP.

9.10 Term and Termination

9.10.1 Term

This CP and subsequent versions shall be effective upon approval by the PMA.

9.10.2 Termination

In the event that the PKI services ceases to operate, a public announcement must be made by the PMA. Upon termination of service, the PMA will properly archive its records including certificates issued, CP, CPS and ARL according to section 5.8 above.

9.10.3 Effect of Termination and Survival

End of validity of the present CP stops all obligation and liability for the PMA.

Sub-CA cannot continue delivering electronic certificate referred to by the present CP.

9.11 Individual Notices and Communications with Participants

The PMA provides all participants with new version of CP via the PS, as soon as it is validated by the PMA.

9.12 Amendments

9.12.1 Procedure for Amendment

The PMA reviews CP and CPS at least yearly. Additional reviews may be enacted at any time at the discretion of the PMA. Spelling errors or typographical corrections which do not change the meaning of the CP are allowed without notification. Prior to approving any changes to this CP, PMA notifies PKI components.

If the PMA wishes to recommend amendments or corrections to the CP, such modifications shall be circulated to appropriate parties identified by PMA. The PMA collects, sums up and proposes CP modifications according to approval procedures.

9.12.2 Notification Mechanism and Period

The PMA notifies PKI components on its intention to modify CP/CPS no less than 2 months before entering in a modification process of CP/CPS and according to the scope of modification.

9.12.3 Circumstances under Which OID Must Be Changed

The present CP OIDs have to be changed if the PMA determines that a change in the CP modifies the level of trust provided by the CP requirements or CPS material.

9.13 Dispute Resolution Provisions

Provisions for resolving disputes between DOCUSIGN FRANCE and its Customers shall be set forth in the applicable contract between the parties.

9.14 Governing Law

Subject to any limits appearing in applicable law, the laws of FRANCE, shall govern the enforceability, construction, interpretation, and validity of the CP, irrespective of contract or other choice of law provisions and without the requirement to establish a commercial nexus in the State of France.

This governing law provision applies only to the CP. Contract with Customer 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

The CP is subject to applicable French and European laws, rules, regulations, ordinances, decrees, and orders including, but not limited to, restrictions on exporting or importing software, hardware, or technical information and topics related to privacy and signature.

Customer and DOCUSIGN FRANCE agree to conform to applicable laws and regulations in their contract.

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

This CP constitutes the entire understanding between the parties and supersedes all other terms, whether expressed or implied by law. No modification of this CP shall be of any force or effect unless in writing and signed by an authorized signatory. Failure to enforce any or all of these sections in a particular instance or instances shall not constitute a waiver thereof or preclude subsequent enforcement thereof. All provisions in this CP which by their nature extend beyond the term of the performance of the services such as without limitation those concerning confidential information and intellectual property rights shall survive such term until fulfilled and shall apply to any party's successors and assigns.

9.16.2 Assignment

Except where specified by other contracts, only the PMA may assign and delegate this CP to any party of its choice.

9.16.3 Severability

Should it be determined that one section of this CP is incorrect or invalid, the other sections of this CP shall remain in effect until the CP is updated. The process for updating this CP is described in section 9.12.

9.16.4 Waiver of Rights and obligation

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 the CP are for convenience only and cannot be used in interpreting the CP.

9.16.5 Force Majeure

DOCUSIGN FRANCE shall not be liable for any failure or delay in its performance under the 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, natural disasters, fire, epidemic, flood, earthquake, riot, war, failure of equipment, failure of telecommunications lines, lack of Internet access, sabotage, and governmental action or any unforeseeable events or situations.

DOCUSIGN FRANCE HAS NO LIABILITY FOR ANY DELAYS, NON-DELIVERIES, NON-PAYMENTS, MIS-DELIVERIES OR SERVICE INTERRUPTIONS CAUSED BY ANY THIRD PARTY (like RA or Customer) ACTS OR THE INTERNET INFRASTRUCTURE OR ANY NETWORK EXTERNAL TO DOCUSIGN FRANCE.

9.17 Other Provisions

9.17.1 Interpretation

All references in this CP to “sections” refer to the sections of this CP. As used in this CP, neutral pronouns and any variations thereof shall be deemed to include the feminine and masculine, and all terms used in the singular shall be deemed to include the plural, and vice versa as the context may require. The words “hereof,” “herein” and “hereunder” and other words of similar import refer to this CP as a whole, as the same may from time to time be amended or supplemented, and not to any subdivision contained in this CP. The words "include" and “including” when used herein are not intended to be exclusive and mean, respectively, "include, without limitation" and “including, without limitation.”

9.17.2 Conflict of Provisions

In the event of a conflict between the provisions of this CP, the CPS and any subscriber agreement, the order of precedence shall be CP, CPS, and then subscriber agreement.

9.17.3 Limitation Period on Actions

Any legal actions involving a dispute that is related to this PKI or any services provided involving a certificate issued by this PKI shall be commenced prior to the end of date defined in contract between DOCUSIGN FRANCE and Customer the period in dedicated by PMA after either the expiration of the certificate in dispute, or the date of provision of the disputed service or services involving the PKI certificate, whichever is earlier If any action involving a dispute related to a certificate issued by this PKI or any service involving certificates issued by this PKI certificate is not commenced prior to such time, any such action shall be barred.

9.17.4 Notice of Limited Liability

This CP makes no claims that should be construed to be an agreement between any parties, nor does it imply any liability for any parties.

10 CERTIFICATE, CRL AND OCSP PROFILE

10.1 "DocuSign Premium Cloud Signing CA – SI1" CA

10.1.1 Natural person qualified signature with SSCD : 1.3.6.1.4.1.22234.2.14.3.31

<table>
<tr><th>Basic Certificate Fields</th><th colspan="3">Value</th></tr>
<tr><td>Version</td><td colspan="3">2 (=version 3)</td></tr>
<tr><td>Serial number</td><td colspan="3">Defined by the software</td></tr>
<tr><td>Issuer</td><td colspan="3">C = FR
O = DocuSign France
OU = 0002 81261115
CN = DocuSign Premium Cloud Signing CA - SI1</td></tr>
<tr><td>NotBefore</td><td colspan="3">YYYY/MM/DD HH:MM:SS Z (certificate issuance date minus 1 hour)</td></tr>
<tr><td>NotAfter</td><td colspan="3">YYYY/MM/DD HH:MM:SS Z 10 days</td></tr>
<tr><td rowspan="9">Subject</td><td>Attribute type</td><td>Attribute value</td><td>Directory String[1]</td></tr>
<tr><td>C</td><td>Country code on 2 character ISO 3166-1
Country where the legal entity acting as RA or DRA is officially registered</td><td>PrintableString</td></tr>
<tr><td>OU</td><td>RA or DRA <name></td><td>UTF8String</td></tr>
<tr><td>OU</td><td><Transaction identification number></td><td>UTF8String</td></tr>
<tr><td>serialNumber</td><td>random value of 16 bytes of entropy generated by PSM</td><td>PrintableString</td></tr>
<tr><td>pseudonym</td><td>Equal to serialNumber or transmitted by RA. This field can be here only if givenName and surname are not present.</td><td>UTF8String</td></tr>
<tr><td>givenName</td><td>First name of the signatory if transmitted by RA if not the field is empty.</td><td>UTF8String</td></tr>
<tr><td>surName</td><td>Last name of the signatory if transmitted by RA if not the field is empty.</td><td>UTF8String</td></tr>
<tr><td>CN</td><td>First name and last name of the Signatory or equal to pseudonym when RA transmits the pseudonym value.</td><td>UTF8String</td></tr>
<tr><td rowspan="2">Subject Public Key Info</td><td>Key generation (algorithm & OID)</td><td colspan="2">rsaEncryption (1.2.840.113549.1.1.1)</td></tr>
<tr><td>Key size</td><td colspan="2">2048</td></tr>
<tr><td>Signature (algorithm & OID)</td><td colspan="3">sha256WithRSAEncryption (1.2.840.113549.1.1.11)</td></tr>
</table>

Extensions	**Criticality (True/False)**	**Value**

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

Extensions	Criticality (True/False)	Value
Authority Key Identifier	**FALSE**	
keyIdentifier		Defined by issuer CA (in its Subject Key Identifier)
Subject Key Identifier	**FALSE**	
Methods of generating key ID		Defined by Software (SHA1 160bits of the subject public key)
Key Usage	**TRUE**	
Non Repudiation		Set
Extended Key Usage	**FALSE**	
Adobe-AuthenticDocumentTrust		Set
Certificate Policies	**FALSE**	
policyIdentifier		1.3.6.1.4.1.22234.2.14.3.31
policyQualifier-cps		https://www.docusign.fr/societe/politiques-de-certifications
Basic Constraint	**TRUE**	
cA		False
CRL Distribution Points	**FALSE**	
distributionPoint		http://crl.dsf.docusign.net/docusignpremiumcloudsigningcasi1.crl
Authority Information Access	**FALSE**	
Ocsp		http://ocsp.dsf.docusign.net/docusignpremiumcloudsigningcasi1
caIssuers		http://crt.dsf.docusign.net/docusignpremiumcloudsigningcasi1.p7c
Qualified Certificate Statements	**FALSE**	
esi4-qcStatement-1		*No value (QcCompliance)*
esi4-qcStatement-4		*No value (SSCD)*
esi4-qcStatement-6		QcType=id-etsi-qct-esign
esi4-qcStatement-5		EN: https://pds.dsf.docusign.net/docusignpremiumcloudsigningcasi1.pdf

10.1.2 Natural person qualified signature with SSCD with DTM : 1.3.6.1.4.1.22234.2.14.3.31

Basic Certificate Fields	Value
Version	2 (=version 3)
Serial number	Defined by the software
Issuer	C = FR O = DocuSign France OU = 0002 81261115

	CN = DocuSign Premium Cloud Signing CA - SI1		
NotBefore	YYYY/MM/DD HH:MM:SS Z (certificate issuance date minus 1 hour)		
NotAfter	YYYY/MM/DD HH:MM:SS Z 10 days		
Subject	**Attribute type**	**Attribute value**	**Directory String[2]**
	C	Country code on 2 character ISO 3166-1 Country where the legal entity acting as RA or DRA is officially registered	PrintableString
	OU	RA or DRA <name>	UTF8String
	OU	<*Transaction identification number*>	UTF8String
	OU	<Envelope number>	UTF8String
	serialNumber	random value of 16 bytes of entropy generated by PSM	PrintableString
	pseudonym	Equal to serialNumber or transmitted by RA. This field can be here only if givenName and surname are not present.	UTF8String
	givenName	First name of the signatory if transmitted by RA if not the field is empty.	UTF8String
	surName	Last name of the signatory if transmitted by RA if not the field is empty.	UTF8String
	CN	First name and last name of the Signatory or equal to pseudonym when RA transmits the pseudonym value.	UTF8String
Subject Public Key Info	Key generation (algorithm & OID)	rsaEncryption (1.2.840.113549.1.1.1)	
	Key size	2048	
Signature (algorithm & OID)	sha256WithRSAEncryption (1.2.840.113549.1.1.11)		

Extensions	**Criticality (True/False)**	**Value**
Authority Key Identifier	**FALSE**	
keyIdentifier		Defined by issuer CA (in its Subject Key Identifier)
Subject Key Identifier	**FALSE**	
Methods of generating key ID		Defined by Software (SHA1 160bits of the subject public key)
Key Usage	**TRUE**	
Non Repudiation		Set
Extended Key Usage	**FALSE**	
Adobe-AuthenticDocumentTrust		Set

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

Extensions	Criticality (True/False)	Value
Certificate Policies	**FALSE**	
policyIdentifier		1.3.6.1.4.1.22234.2.14.3.31
policyQualifier-cps		https://www.docusign.fr/societe/politiques-de-certifications
Basic Constraint	**TRUE**	
cA		False
CRL Distribution Points	**FALSE**	
distributionPoint		http://crl.dsf.docusign.net/docusignpremiumcloudsigningcasi1.crl
Authority Information Access	**FALSE**	
Ocsp		http://ocsp.dsf.docusign.net/docusignpremiumcloudsigningcasi1
caIssuers		http://crt.dsf.docusign.net/docusignpremiumcloudsigningcasi1.p7c
Qualified Certificate Statements	**FALSE**	
esi4-qcStatement-1		*No value (QcCompliance)*
esi4-qcStatement-4		*No value (SSCD)*
esi4-qcStatement-6		QcType=id-etsi-qct-esign
esi4-qcStatement-5		EN: https://pds.dsf.docusign.net/docusignpremiumcloudsigningcasi1.pdf

10.1.3 OCSP Responder certificate

Basic Certificate Fields	Value		
Version	2 (=version 3)		
Serial number	Defined by the software		
Issuer	C = FR O = DocuSign France OU = 0002 81261115 CN = DocuSign Premium Cloud Signing CA - SI1		
NotBefore	YYYY/MM/DD HH:MM:SS Z (certificate issuance date)		
NotAfter	YYYY/MM/DD HH:MM:SS Z 1 year		
Subject	**Attribute type**	**Attribute value**	**Directory String[3]**
	C	FR	PrintableString
	O	DocuSign France	UTF8String

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

	OU	0002 812611150	UTF8String
	CN	OCSP Responder <*date*>	UTF8String
Subject Public Key Info	Key generation (algorithm & OID)	rsaEncryption (1.2.840.113549.1.1.1)	
	Key size	2048	
Signature (algorithm & OID)	sha256WithRSAEncryption (1.2.840.113549.1.1.11)		

Extensions	**Criticality (True/False)**	**Value**
Authority Key Identifier	**FALSE**	
keyIdentifier		Defined by issuer CA (in its Subject Key Identifier)
Subject Key Identifier	**FALSE**	
Methods of generating key ID		Defined by Software (SHA1 160bits of the subject public key)
Key Usage	**TRUE**	
Digital Signature		Set
Basic Constraint	**TRUE**	
cA		False
Extended Key Usage	**FALSE**	
id-kp-OCSPSigning		Set
OCSPNoCheck	**FALSE**	
NULL		NULL

10.1.4 Certificate Revocation List

CRL Fields	**Value**
Version	1 (=version 2)
Issuer	C = FR O = DocuSign France OU = 0002 81261115 CN = DocuSign Premium Cloud Signing CA - SI1
ThisUpdate	YYYY/MM/DD HH:MM:SS Z (CRL issuance date)
NextUpdate	YYYY/MM/DD HH:MM:SS Z =thisUpdate + 6 days
Signature (algorithm & OID)	sha256WithRSAEncryption (1.2.840.113549.1.1.11)

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
Expired Certs On CRL	**FALSE**	
expiredCertsOnCRL		2017/03/08 11:35:50 Z

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

10.2 “DocuSign Cloud Signing CA – SI1” CA

10.2.1 Natural person remote certificate LCP : 1.3.6.1.4.1.22234.2.14.3.32

Basic Certificate Fields	Value		
Version	2 (=version 3)		
Serial number	Defined by the software		
Issuer	C = FR O = DocuSign France OU = 0002 81261115 CN = DocuSign Cloud Signing CA - SI1		
NotBefore	YYYY/MM/DD HH:MM:SS Z (certificate issuance date minus 1 hour)		
NotAfter	YYYY/MM/DD HH:MM:SS Z 10 days		
Subject	**Attribute type**	**Attribute value**	**Directory String[4]**
	C	Country code on 2 character ISO 3166-1 Country where the legal entity acting as RA is officially registered	PrintableString
	OU	RA <name>	UTF8String
	OU	*<Transaction identification number>*	UTF8String
	serialNumber	random value of 16 bytes of entropy generated by PSM	PrintableString
	pseudonym	Equal to serialNumber or transmitted by RA. This field can be here only if givenName and surname are not present.	UTF8String

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

	givenName	First name of the signatory if transmitted by RA if not the field is empty.		UTF8String
	surName	Last name of the signatory if transmitted by RA if not the field is empty.		UTF8String
	CN	First name and last name of the Signatory or equal to pseudonym when RA transmits the pseudonym value.		UTF8String
Subject Public Key Info	Key generation (algorithm & OID)		rsaEncryption (1.2.840.113549.1.1.1)	
	Key size		2048	
Signature (algorithm & OID)	sha256WithRSAEncryption (1.2.840.113549.1.1.11)			

Extensions	Criticality (True/False)	Value
Authority Key Identifier	**FALSE**	
keyIdentifier		Defined by issuer CA (in its Subject Key Identifier)
Subject Key Identifier	**FALSE**	
Methods of generating key ID		Defined by Software (SHA1 160bits of the subject public key)
Key Usage	**TRUE**	
Digital Signature		Set
nonRepudiation		Set
Extended Key Usage	**FALSE**	
Adobe-AuthenticDocumentTrust		Set
Certificate Policies	**FALSE**	
policyIdentifier		1.3.6.1.4.1.22234.2.14.3.32
policyQualifier-cps		https://www.docusign.fr/societe/politiques-de-certifications
Basic Constraint	**TRUE**	
cA		False
pathLenConstraint		None
CRL Distribution Points	**FALSE**	
distributionPoint		http://crl.dsf.docusign.net/docusigncloudsigningcasi1.crl
Authority Information Access	**FALSE**	
Ocsp		http://ocsp.dsf.docusign.net/docusigncloudsigningcasi1
caIssuers		http://crt.dsf.docusign.net/docusigncloudsigningcasi1.p7c

10.2.2 Natural person remote certificate LCP with DTM : 1.3.6.1.4.1.22234.2.14.3.32

<table>
<tr><th>Basic Certificate Fields</th><th colspan="3">Value</th></tr>
<tr><td>Version</td><td colspan="3">2 (=version 3)</td></tr>
<tr><td>Serial number</td><td colspan="3">Defined by the software</td></tr>
<tr><td>Issuer</td><td colspan="3">C = FR
O = DocuSign France
OU = 0002 81261115
CN = DocuSign Cloud Signing CA - SI1</td></tr>
<tr><td>NotBefore</td><td colspan="3">YYYY/MM/DD HH:MM:SS Z (certificate issuance date minus 1 hour)</td></tr>
<tr><td>NotAfter</td><td colspan="3">YYYY/MM/DD HH:MM:SS Z 10 days</td></tr>
<tr><td rowspan="10">Subject</td><td>Attribute type</td><td>Attribute value</td><td>Directory String5</td></tr>
<tr><td>C</td><td>Country code on 2 character ISO 3166-1
Country where the legal entity acting as RA is officially registered</td><td>PrintableString</td></tr>
<tr><td>OU</td><td>RA <name></td><td>UTF8String</td></tr>
<tr><td>OU</td><td><Transaction identification number></td><td>UTF8String</td></tr>
<tr><td>OU</td><td><Envelope number></td><td>UTF8String</td></tr>
<tr><td>serialNumber</td><td>random value of 16 bytes of entropy generated by PSM</td><td>PrintableString</td></tr>
<tr><td>pseudonym</td><td>Equal to serialNumber or transmitted by RA. This field can be here only if givenName and surname are not present.</td><td>UTF8String</td></tr>
<tr><td>givenName</td><td>First name of the signatory if transmitted by RA if not the field is empty.</td><td>UTF8String</td></tr>
<tr><td>surName</td><td>Last name of the signatory if transmitted by RA if not the field is empty.</td><td>UTF8String</td></tr>
<tr><td>CN</td><td>First name and last name of the Signatory or equal to pseudonym when RA transmits the pseudonym value.</td><td>UTF8String</td></tr>
<tr><td rowspan="2">Subject Public Key Info</td><td>Key generation (algorithm & OID)</td><td colspan="2">rsaEncryption (1.2.840.113549.1.1.1)</td></tr>
<tr><td>Key size</td><td colspan="2">2048</td></tr>
<tr><td>Signature (algorithm & OID)</td><td colspan="3">sha256WithRSAEncryption (1.2.840.113549.1.1.11)</td></tr>
</table>

Extensions	Criticality (True/False)	Value
Authority Key Identifier	**FALSE**	

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

Extensions	Criticality (True/False)	Value
keyIdentifier		Defined by issuer CA (in its Subject Key Identifier)
Subject Key Identifier	**FALSE**	
Methods of generating key ID		Defined by Software (SHA1 160bits of the subject public key)
Key Usage	**TRUE**	
Digital Signature		Set
nonRepudiation		Set
Extended Key Usage	**FALSE**	
Adobe-AuthenticDocumentTrust		Set
Certificate Policies	**FALSE**	
policyIdentifier		1.3.6.1.4.1.22234.2.14.3.32
policyQualifier-cps		https://www.docusign.fr/societe/politiques-de-certifications
Basic Constraint	**TRUE**	
cA		False
pathLenConstraint		None
CRL Distribution Points	**FALSE**	
distributionPoint		http://crl.dsf.docusign.net/docusigncloudsigningcasi1.crl
Authority Information Access	**FALSE**	
Ocsp		http://ocsp.dsf.docusign.net/docusigncloudsigningcasi1
caIssuers		http://crt.dsf.docusign.net/docusigncloudsigningcasi1.p7c

10.2.3 OCSP Responder certificate

Basic Certificate Fields	Value
Version	2 (=version 3)
Serial number	Defined by the software
Issuer	C = FR O = DocuSign France OU = 0002 81261115 CN = DocuSign Cloud Signing CA - SI1
NotBefore	YYYY/MM/DD HH:MM:SS Z (certificate issuance date)

NotAfter	YYYY/MM/DD HH:MM:SS Z 1 year		
Subject	**Attribute type**	**Attribute value**	**Directory String[6]**
	C	FR	PrintableString
	O	DocuSign France	UTF8String
	OU	0002 812611150	UTF8String
	CN	OCSP Responder <*date*>	UTF8String
Subject Public Key Info	Key generation (algorithm & OID)	rsaEncryption (1.2.840.113549.1.1.1)	
	Key size	2048	
Signature (algorithm & OID)	sha256WithRSAEncryption (1.2.840.113549.1.1.11)		

Extensions	Criticality (True/False)	Value
Authority Key Identifier	**FALSE**	
keyIdentifier		Defined by issuer CA (in its Subject Key Identifier)
Subject Key Identifier	**FALSE**	
Methods of generating key ID		Defined by Software (SHA1 160bits of the subject public key)
Key Usage	**TRUE**	
Digital Signature		Set
Basic Constraint	**TRUE**	
cA		False
Extended Key Usage	**FALSE**	
id-kp-OCSPSigning		Set
OCSPNoCheck	**FALSE**	
NULL		NULL

10.2.4 Certificate Revocation List

CRL Fields	Value
Version	1 (=version 2)
Issuer	C = FR O = DocuSign France

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

	OU = 0002 81261115 CN = DocuSign Cloud Signing CA - SI1
ThisUpdate	YYYY/MM/DD HH:MM:SS Z (CRL issuance date)
NextUpdate	YYYY/MM/DD HH:MM:SS Z =thisUpdate + 6 days
Signature (algorithm & OID)	sha256WithRSAEncryption (1.2.840.113549.1.1.11)

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