docusign

DS France ETSI Registration Policy and Practice for Remote Signature

DS FRANCE ETSI REGISTRATION POLICY AND PRACTICE FOR REMOTE SIGNATURE

Document version:	1.7	Pages	35
Document status:	☐ Project	☒ Final version	
Editor of the document:	RSSI DocuSign France		

Mailing list:	☒ External	☒ Internal DocuSign France
	Public	Public

Revision history:				
Date	Version	Author	Comments	Verified by
04/04/2018	0.9	EM	Creation of the version 0.9	
16/06/2019	1.0	EM	Creation of the version 1.0 and update of the document due to stop of signature of GTU by Subscriber for AES level.	
04/03/2021	1.1	EM	Creation of the version 1.1 and update of the document due to maintain signature of GTU by Subscriber for AES level only when DS France is RA and deletion of DRA for the level LCP.	
07/04/2021	1.2	EM	Logo change.	
15/04/2022	1.3	EM	Add the use case with RVIP	
09/05/2023	1.4	CG	Corrections and proofreading	EM
27/10/2023	1.5	EM	Integration of Identity Wallet for QES.	
25/02/2025	1.6	EM	Delete reference to PSMP and QSCD as they are in the CP and update of the OID of CP to add new CAs G2.	
23/04/2025	1.7	EM	CP version update.	

CONTENTS

1 INTRODUCTION

1.1 Overview

This Registration Policy (*RP*) is an amendment to the document [CP] of DOCUSIGN FRANCE (DSF). DSF is the Registration Authority (RA) in the meaning of the [CP].

The present document describes the rules of DSF to implement the RA and manage Subscribers.

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: Electronic Signatures and Infrastructures (ESI); Cryptographic Suites.
    - [319 401]: ETSI EN 319 401 V2.3.1: Electronic Signatures and Infrastructures (ESI), General Policy Requirements for Trust Service Providers.
    - [319 412]:
        - ETSI EN 319 412-1: Electronic Signatures and Infrastructures (ESI); Certificate Profiles, Part 1: Overview and common data structures.
        - ETSI EN 319 412-2: Electronic Signatures and Infrastructures (ESI), Certificate Profiles, Part 2: Certificate profile for certificates issued to natural persons.
        - ETSI EN 319 412-5 : Electronic Signatures and Infrastructures (ESI), Certificate Profiles, Part 5: QCStatements.
    - [319 411]:
        - ETSI EN 319 411-1: Electronic Signatures and Infrastructures (ESI), Policy and security requirements for Trust Service Providers issuing certificates, Part 1: General requirements.
        - ETSI EN 319 411-2: 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.

- [CP]: "DSF_Protect and Sign Personal Signature ETSI CP v 3.0" (*applicable OID is 1.3.6.1.4.1.22234.2.14.3.31, 1.3.6.1.4.1.22234.2.14.3.32, 1.3.6.1.4.1.22234.2.14.3.45 and 1.3.6.1.4.1.22234.2.14.3.46*).

1.2 Document Name and Identification

"DS France ETSI Remote Signature, Registration Policy". This RP manages 2 level of security:

- QES: to provide qualified electronic signature according eIDAS regulation and ETSI requirements. They are 2 types of service for QES:
    - QES remote: this service uses certified RIVSP by ANSSI (https://www.ssi.gouv.fr/en/actualite/publication-of-the-requirement-rule-set-for-remote-identity-verification-service-providers/). The abbreviation for this service is [QES RIVSP].
    - QES in face to face: this service uses Customer as DRA to perform the face to face with Subscriber. The abbreviation for this service is [QES FtoF].

- LCP: to provide certified advanced signature according eIDAS regulation and ETSI requirements.

In the RP, difference in the security requirements due to level of security are referenced specifically with the acronym [LCP] and [QES FtoF] and [QES RIVSP]. Others security requirements applies for all level.

1.3 PKI Components

1.3.1 Policy Management Authority (*PMA*)

The PMA is the PKI lead authority and is managed by DOCUSIGN FRANCE (refer to [CP]).

PMA main mission for RA:

- Approves RA services and RP.
- Approve DRA Registration Policy.
- Approve RISVP provider.
- Approves the list of country where the service can be deployed and the type and model of ID document to be used for ID proofing.
- Approves the dedicated risk analysis made for RA services.
- Approves DRA (*Delegated Registration Authority*) creation and revocation.
- Approves compliance between security practice documents and related policies.
- Approves final annual internal audit report of all the PKI's components.
- Approves external audit report of DRA performed by DSF.
- Manage external audit of DRA and RIVSP.
- Approves the chosen Consent Protocol defined with DocuSign France.
- Approves procedures defined by DRA for Subscriber management.
- Guarantees the validity and the integrity of the RP published information.
- Ensures that a proper process to manage security incidents within the RA services and RA components is in place.
- Arbitrates disputes relating to the RA services and the use of ide and ensures that the resolution of such disputes is published.

1.3.2 Registration Authority (RA)

DSF is RA.

RA supports the following PKI services:

- Authentication and identification of the Subscriber via an ID proofing process using the official ID.
- Authentication of Delegate Registration Authority (DRA).
- Audit of DRA.
- Authorization of DRA.
- Transmission of certificate request to the CA.
- Revocation process.
- Transmission of revocation request to CA.
- Log trail generation and record of registration information.

An RA operates its services according to the [CP], the corresponding CPS and the present RP. An RA cannot start operation without prior approval of the PMA.

1.3.3 Operational Authority (*OA*)

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

RA components are operated by:

- DSF designated entity that is the OA for the RA and PS.

- DSF uses DocuSign to run part of the DRA service (*DocuSign Signature Application*).

- Customer designates entity that is the OA for the DRA service implemented by itself.

An OA operates its services according to the [CP], the corresponding CPS and the present RP. An OA cannot start operation without prior approval of the PMA.

1.3.4 Delegate Registration Authority (*DRA*)

DRA is an entity (*named Customer*) bound by contract to DSF by a Service Agreement.

DRA is only used in [QES FtoF] service.

The DRA supports the following PKI services:

- Authentication and transmission of revocation request to RA.

- Log trail generation and record of registration information.

- Transmission of the Certificate request application to the RA.

- Initial authentication of the subscriber during face-to-face meeting.

- Initial identity validation of the Subscriber.

- Verification and update of the official ID Document and of registration data (*email, phone number, etc*).

- If applicable, authentication of the Subscriber with secured means of authentication for remote access to the DRA portal.

The DRA defines, implements, and maintains a DRA Registration Policy. The DRA Registration Policy is defined to describe the dedicated implementation of the RP by the Customer.

DRA designates the DRA agent, a person related to the DRA (staff or contractor), in charge of performing face to face identification for Signers, according to the DRA Registration Policy.

A DRA operates its services according to the [CP], the corresponding CPS, the present RP and its dedicated DRA Registration Policy.

A DRA cannot start operation without prior approval of the PMA.

A list of DRAs is established and maintained by the RA.

1.3.5 Remote Identity Verification Service Provider (RIVSP)

RIVSP is an entity bound to DSF by a Service Agreement and a contract.

RISVP is only used in [QES RIVSP] service.

The RIVSP supports the following PKI services:

- Log trail generation and record of registration information.

- Transmission of the Certificate request application to the RA.

- Initial authentication of the subscriber remotely according ANSSI's requirements.

- Initial identity validation of the Subscriber.

- Verification of the the Subscriber's ID and of data collection during identification operation (*email, phone number, etc*).

The RIVSP defines, implements and maintains an Identification Policy.

RIVSP shall be certified by ANSSI before being authorized for use in the [QES RIVSP] perimeter, according to the following rules: https://www.ssi.gouv.fr/en/actualite/publication-of-the-requirement-rule-set-for-remote-identity-verification-service-providers/.

A list of RIVSPs is established and maintained by the RA.

1.3.6 Publication Service (PS)

PS is owned by DSF.

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

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

1.3.7 Other Participants

1.3.7.1 Customer

A Customer is a Legal Entity that establishes a contract with DSF to use DocuSign Application service for QES and/or LCP level. In case of [QES FtoF], Customer designates a DRA entity. In the service agreement between Customer and DSF all DRA obligations are included.

In case of [QES FtoF], the Customer defines DRA services and security rules DRA and DRA agents shall implement, and selects the level of trust for Subscriber Certificate.

The customer is in charge of elaborating and transmitting electronic Documents to be signed by Subscriber to DocuSign Application.

1.3.7.2 Subscriber

A Subscriber is a physical person whose identity appears as subject in a Subscriber Certificate and who signs a document using LCP and/or QES services. The Subscriber key pair and certificate generation are linked to the signature operation performed by Subscriber according [CP] and present RP.

Subscribers abide to the CP and the associated procedures as described in the present RP, and summarized in each dedicated GTU, by signing the GTU during Consent Protocol.

1.3.7.3 Relying Parties

Relying Parties are entities which 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

The uses of private key are the following:

- Used to sign electronic Document(*s*) and GTU(*s*) by using a Consent Protocol (*with a technical activation data*).
- Used to sign CSR (*Pkcs#10 format*) for certificate issuance.

The uses of certificate are the following:

- Used to verify electronic signature applied on electronic Document(*s*) and GTU(*s*).

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

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

1.5 Policy Administration

1.5.1 Organization managing the Document

The PMA is responsible for all aspects of this RP and its associated practice.

1.5.2 Person of contact

The PMA contact is provided in web or by postal mail with the following details:

– PMA of DocuSign France.

– https://www.docusign.fr/ (*contact information is provided on the website*).

– DocuSign France – 9-15 rue Maurice Mallet - 92131 Issy-les-Moulineaux Cedex – France.

1.5.3 Person Determining pratice Suitability for the RP

The PMA approves the RP and associated practice. The RA and DRA will be audited periodically to verify compliance as per PMA guidelines and standards approved by the PMA. The Audit ensures that the practice is implemented correctly and is compliant with the RP. Further, the PMA reserves the right to audit the RA and DRA as set in section 0 of this CP.

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

1.5.4 Practice Approval Procedures

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

1.6 Definitions and Acronyms

1.6.1 Definitions

Term	Definition
Conformity Assessment Body (or CAB)	Is a third party accredited by a European Member State to perform conformity assessment of CA and RA based on the ETSI applicable standard for the activity of issuing qualified certificates. The current Applicable standard is ETSI EN 319 411-2 and French ANSSI requirements (*Agence Nationale de la Sécurité des Systèmes d'Information*).
Consent Protocol	Designates the procedure according to which the user is asked for his/her consent to receive a Certificate with the Signer Identity, to accept signing the electronic Document via the Service and to accept signing the GTU(*s*). The Consent Protocol is executed by the Signer within the Service accessible via the DocuSign Signature Application.
DocuSign Signature Application	Designates the DocuSign, Inc. Transaction service, which provides online electronic Document management and viewing, Signer's Identity (*first name, last name, email and mobile phone*) registration, DRA role management,

	electronic Document viewer, creation of Certificate of Completion (*COC*), and interface to the Service. Only DocuSign Signature Application platforms located in Europe are used to access the Service. DocuSign Signature Application is used by DR, DRA Agent and Signer.
eDocument(s)	Designates a document(s) in electronic form that is deposited by the Customer via the Service and submitted to the RA via the DocuSign Signature application in order to be signed by the Signatory. The electronic Document may also be signed by other signatories and by the Customer with same or different level of security for the signature (*basic, advanced or qualified*).
eIDAS	Means EU Regulation No. 910/2014.
ID	"ID Document (ID)" for purposes of the Service means a passport, a national identity card or a residence permit meeting the security requirements defined by The National Cybersecurity Agency of France (*ANSSI*).
Identity Wallet	Means an optional service provided to the Signer to securely store Signer Identity, RIVR and Signer information (email and mobile phone number) for use of Signer Identity in Transaction and signature of eDocument and terms without performing a PVID identification process.
GTU	Designates the General Terms of Use of the service that forms a legal agreement between the Signer and DocuSign France. GTU(s) are signed by the Signer during the Consent Protocol cinematic. There is a GTU for LCP and another one for QES.
Proof File(s)	Designates a file generated, signed and time stamped by DocuSign France that contains all the information related to the authentication during the ID proofing made by the RA and the signature process (including the copy of the official ID document). A dedicated Proof File is associated to each Transaction. Proof files are only available to DocuSign France in its role as Trust Service Provider.
Proof of DocuSign Signature Application (*Certificate of Completion, "COC"*)	Designates a file generated by DocuSign Signature Application that contains all the information related to the Signer, sender of the eDocument, unique identifier of the transaction used to manage the electronic Document. A dedicated COC associated to each electronic Document, Signer and sender is generated in the purpose of proving the validity of a Transaction. The COC is sealed by DocuSign Inc. and is made available to the Customer.
RIVR	"Remote Identity Verification Result ("*RIVR*")" *means the signed information sent by the RIVSP to the RA, including the result (successful or unsuccessful) of the remote identity verification of Signer, the reason for the failure if any, the information required by the RA (name, email and mobile phone number of Signer*) and extracted information from the Signer's ID document verified by the RIVSP (*date of birth, ID serial number, ID expiration date, ID issuing country, and ID type*)."Transaction(s)" designates the performance of a signature process, defined by a set of electronic Documents submitted for electronic signature by one or more Signer(s).
RIVSP	"Remote Identity Verification Service Provider" (or "RIVSP") designates the third-party service provider responsible for acquiring and verifying the facial image and ID document in order to identify the signer. The RIVSP produces the evidence file and sends the Result of the Remote Identity Verification to the RA. The RVISP is certified by ANSSI (*the French supervisory body*

	according eIDAS).
Signer Identity	Designates the set of personal data (*first and last name, email address, mobile phone number, and copy of an official ID document*) used to identify a Signer.
Transaction(s)	Designates the performance of a signature process, defined by a set of electronic Documents submitted for electronic Signature by one or more Signers.

2   PUBLICATION AND REPOSITORY RESPONSIBILITIES

The RP is published at the following url : https://www.docusign.fr/societe/politiques-de-certifications.

PMA approves version to be published signing it.

3   IDENTIFICATION AND AUTHENTICATION

3.1   Naming

The certificates issued in accordance with this RP are meaningful only if the names appearing 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 ID of the Subscriber.

Subscriber's certificates are issued with the following value in the Certificate (*precision for Certificate profile defined in the [CP]*):

- OU=RA DocuSign France, the RA's name.
- C=FR , Country field "FR" for France.
- CN: at least one Name and at least one First Name in the order selected by the Subscriber and as filled in DocuSign Signature Application or as contained in the Subscriber's ID.

3.2   Initial Identity Validation

3.2.1   Method to Prove Possession of Private Key

The Subscriber has sole control of his/her private key thanks to Consent Protocol and OTP code received on his/her telephone mobile number.

3.2.2   Authentication of Organization Identity

Not applicable.

CA doesn't issue Certificate with Subscriber's entity information. Neither RA nor DRA verify Subscriber affiliation with entity.

3.2.3   Authentication of Physical Person Identity

3.2.3.1   [QES FtoF]

The DRA shall carry out the authentication of the Subscriber identity, under DRA rules and meeting the requirements contractually defined by the RA. Initial registration is used to collect Subscriber identity to be set in the Certificate, and email address and telephone number in order to contact the Subscriber. Initial

registration is also used to securely distribute the secure authentication means to the Subscriber for remote access to the DRA portal if the DRA has such function.

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

- The physical presence of the natural person.
- 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'.
- By means of a Certificate of a qualified electronic signature or of a qualified electronic seal.
- 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 for:

- Subscriber identity.
- Date and place of birth of Subscriber, reference to a nationally recognised ID document (*like serial number of ID*), or other attributes which can be used to, as far as possible, distinguish the Subscriber from others with the same identity.

The DRA shall check that the Subscriber ID's document is still valid and authentic.

DRA practices are described in DRA Registration Policy.

3.2.3.2 [QES RIVSP]

RIVSP shall carry out the authentication of the Subscriber identity, under ANSSI rules and meeting the requirements contractually defined by the RA. Initial registration is used to collect Subscriber identity to be set in the Certificate; at least one first name and one last name as written in the Subscriber's ID, email address and telephone number of the Subscriber. After the initial identification with the RIVSP, the Subscriber has the option to create an Identity Wallet, it will request in such case to also create a DocuSign account, using a device and its name, mobile phone number and email as registered during identification operation.

The RVISP identifies the Subscriber and it's ID according to the rules defined by ANSSI and set in the RIVSP's Identification Policy.

Evidence shall be provided for:

- Subscriber identity.
- Date and place of birth of Subscriber, reference to a nationally recognised ID document (*like serial number of ID*), or other attributes which can be used to, as far as possible, distinguish the Subscriber from others with the same identity.

The RIVSP shall check that the Subscriber ID's document is still valid and authentic.

After identification of the Subscriber, the RIVSP generates and signs a RIVR.

RIVSP policy and practice is described in each RIVSP Identification Policy published by each RIVSP.

CA keeps records of the RIVSP Identification Policy.

3.2.3.3 LCP

The RA collects direct evidence of the Subscriber's identity through the RA interface (*refer to section 4.2 below*).

Subscriber uploads a copy of his/her valid official ID document in the RA interface and at the same time uploads his/her telephone number.

3.2.4 Validation of Authority

Not applicable (*refer to section 3.2.1 above*).

3.2.5 Non-Verified Subscriber Information

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

3.3 Identification and Authentication for Re-key Requests

3.3.1 Identification and Authentication for Routine Re-key

3.3.1.1 [QES FtoF]

For this section, Subscriber is already registered by DRA and has been successfully issued a first certificate. Then RA can define a process to issue again other Certificates for the Subscriber. But in this case, as major and most important information used initially to register Subscriber may stayed valid, DRA may want to avoid registering 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 DRA 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 Subscriber prior to issuing a Certificate is performed directly by the DRA.

The DRA is in charge of managing the Subscriber for renewal operation.

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

The DRA shall check the existence and validity of the certificate (*not revoked*) to be renewed and that the information used to verify the identity and telephone number and email of the subscriber is still valid.

If any information of the Subscriber to be set in the certificate (*refer to section 3.1 above*) has changed then the registration shall be performed against procedure as defined in section 3.2 above at least concerning the information that has changed.

Information used to authenticate Subscriber during the consent protocol cinematic (*eg email address and phone number*) can only be modified by the Subscriber after verification performed by the DRA in order to confirm that the updated information is/are linked to the Subscriber for the Consent Protocol.

This practice, to have a new certificate without doing the initial identification as described in section 3.2 above, is limited in the duration to 3 years maximum. After Subscriber is obliged to re do an initial complete identification process to begin a new cycle of 3 years.

The DRA practices are described in DRA Registration Policy.

3.3.1.2 [QES RIVSP]

The RA applies the same procedure as described for the initial Certificate (*Refer to section 3.2.3.2 above*) or requires the Subscriber to authenticate himself or herself to its Identity Wallet using the device of the Subscriber and activates a key, enrolled, and deployed in the device during the initial identification of the Subscriber (*refer to section 3.2.3.2 above*), to establish a secured technical authentication with the DocuSign platform. This Identity Wallet is used by Subscriber to be authenticated by RA to be issued another Certificate using name as registered on its official ID used during the initial identification process (refer to Section 3.2 above).

This practice, to have a new certificate without doing the initial identification as described in section 3.2 above, is limited in the duration to 3 years maximum. Subscriber can be issued as many Certificates as it is requested by Transaction requiring signature of Subscriber (there is no limitation). Subscriber can keep on using Identity Wallet if and only if RIVSP is still certified by ANSSI and ID used by Subscriber at time of initial identification process is still an approved ID by ANSSI.

After Subscriber is obliged to re do an initial complete identification process to begin a new cycle of 3 years.

Subscriber can at any time delete its Identity Wallet in the interface of DocuSign platform using its account in DocuSign platform.

If Subscriber:

- Want to change email or name or mobile phone number, Subscriber shall do an initial complete identification as described in section 3.2 above process to begin a new cycle of 3 years with a new Identity Wallet.

- To have another Identity Wallet (for example due to lost of its key due to device deletion, broken…, Subscriber shall do an initial complete identification as described in section 3.2 above process to begin a new cycle of 3 years with a new Identity Wallet.

3.3.1.3 LCP

The RA applies the same procedure as described for the initial Certificate (*Refer to section 3.2.3.3 above*).

3.3.2 Identification and Authentication for Re-key After Revocation

Same procedures as described in section 3.2 above apply.

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

3.4 Identification and Authentication for Revocation Request

In all cases, the authentication of revocation request from Subscriber, to be done here: https://docusign.fr/revocation in the RA portal, is done by RA using an OTP code sent to the email of the Subscriber recorded by the RA during the identification operation (*refer to section 3.2*).

For [QES FtoF], the DRA can also request revocation to RA and DRA practices as described in the DRA Registration Policy.

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 QES [FtoF]

Certificate request is under responsibility of the DRA.

4.1.1.2 [QES RIVSP]

Certificate request is under responsibility of the Customer.

4.1.1.3 LCP

Certificate request is under responsibility of the Customer.

4.1.2 Enrollment Process and Responsibilities

4.1.2.1 [QES FtoF]

The Certificate request shall contain the following information:

- At least one Name and at least one First Name of the Subscriber.

- Subscriber's email and telephone number.

The Certificate request is filled in the DocuSign Signature Application by the DRA.

The DRA practices are described in DRA Registration Policy.

4.1.2.2 [QES RIVSP]

A Certificate request shall contain the following information:

- At least one Name and at least one First Name of the Subscriber.

- Subscriber's email and optionally the telephone mobile number. If the mobile phone is not communicated in the Certificate request, then the Subscriber will declare it in the RIVSP portal.

A Certificate request is filled in DocuSign Signature Application by the Customer.

4.1.2.3 LCP

Certificate requests shall contain the following information:

- At least one Name and at least one First Name of the Subscriber.

- The Subscriber's email.

Certificate requests are first filled in DocuSign Signature Application for the above information by the Customer and finalized by the Subscriber who confirms email and fills telephone number in DocuSign Signature Application.

4.2 Certificate Application Processing

4.2.1 [QES FtoF]

After having submitted a Certificate request (*refer to section 4.1 above*), and having been authenticated by the DRA, DocuSign Signature Application sends to the Subscriber an electronic Document to be signed.

The Subscriber is then invited to upload a copy of its valid official ID document in the RA interface. In the eventuality where the invitation to sign is sent to the Subscriber via email, the email notification contains an internet link to be used by the Subscriber to connect to DocuSign Signature Application.

The RA verifies (*ID proofing*) the genuineness of the Subscriber official ID document and coherence with the identity provided by DocuSign Signature Application in the Certificate request (*refer to section 4.1 above*). The Verification uses transliteration of Subscriber's identity.

If the result of the verification is positive, then the RA accepts to issue a Certificate (*refer to section 4.3 below*).

If the result of the verification is negative, then the RA refuses to issue Certificate and the Transaction is canceled.

4.2.2 [QES RIVSP]

After having submitted a Certificate request (*refer to section 4.1 above*), and having been authenticated by RIVSP, the DocuSign Signature Application receives the RIVR, verifies it, and sends to the Subscriber an electronic Document to be signed if the RIVR verdict is good. If the RIVR verdict is not good, then the Subscriber can't sign. The RIVR can be used to sign during 24H00 maximum, after that the Subscriber shall redo a remote identification with the RIVSP. During this step the Subscriber has the option to create an Identity Wallet (refer to section 3.3.1.2).

In the case where the invitation to sign is sent to the Subscriber via email, the email notification contains an internet link to be used by the Subscriber to connect to the DocuSign Signature Application. The DocuSign Signature Application redirects the Subscriber to the RA portal and gives to the RA portal the RIVR and fingerprint of the electronic Document to be signed.

The RA verifies the signature of the RIVR and uses the information of Subscriber contained in the RIVR (*email, mobile phone number and name*).

If the result of the RIVR verification is good, then the RA accepts to issue a Certificate (*refer to section 4.3 below*).

If the result of the RIVR verification is not good, then the RA refuses to issue a Certificate and the Transaction is canceled.

4.2.3 [LCP]

After having submitted a Certificate request (*refer to section 4.1 above*), and having been authenticated by the RA, the DocuSign Signature Application sends to the Subscriber an electronic Document to be signed.

The Subscriber is then invited to upload a copy of its valid official ID document in the RA interface. In the case where the invitation to sign is sent to the Subscriber via email, the email notification contains an internet link to be used by the Subscriber to connect to the DocuSign Signature Application.

The RA verifies (*ID proofing*) the genuineness of the Subscriber official ID document and coherence with the Subscriber Identity provided by the DocuSign Signature Application in the Certificate request (*refer to section 4.1 above*). The Verification uses transliteration of Subscriber's identity.

If the result of the verification is good, then the RA accepts to issue a Certificate (*refer to section 4.3 below*). If the result of verification is not good, then the RA refuses to issue a Certificate and the Transaction is canceled.

4.3 Certificate Issuance

The RA presents the Consent Protocol to the Subscriber in order to continue with the signing process. The Subscriber can accept or refuse to sign the electronic Document and the GTU (*GTUs are viewable in the Consent Protocol*). During the Consent Protocol presentation, the Subscriber confirms his/her identity (*to be set in Certificate*), his/her telephone number and email. In any mistake appears in the aforementioned data, the Subscriber shall refuse to sign.

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

Then, a dedicated signing Private Key is uniquely generated by the CA and in a secure way assigned to the Subscriber for the duration of the electronic Document and GTU signature transaction. The private key is generated, stored, and destroyed after the signature Transaction in a way that it cannot be used for any other Transaction. The private key is associated with a Certificate, generated by the CA, and contains the identity. This Certificate has a validity of 10 days.

The CA generates and archives a Proof File. DocuSign can provide the Customer with the Proof File and the COC for evidence management purpose. The Proof File contains:

- The reference of the electronic Document and GTU presented to the Signer before signature.

- The signature of the electronic Document and GTU.

- The date and time of the signature operation.

- The Consent Protocol as executed between the Signer and the CA.

- The Registration information used to run Consent Protocol and to fill the Certificate.

- ID proofing result in case of [LCP] and [QES FtoF] and RIVR in case of [QES RIVSP].

- A Copy of Subscriber's ID or extracted information from Subscriber's ID.

- The personal data contained in the Subscriber ID.

The DocuSign Signature Application builds and stores the COC.

The COC can be downloaded with the electronic Document by the Signer in DocuSign Signature Application.

Once signed, the electronic Document can be downloaded from DocuSign Signature Application by the Subscriber, te Customer and in case of [QES FtoF] by the DRA immediately after the signature process.

In any case, the signed electronic Document and the COC may be transmitted to the Subscriber on the subscriber's email after having been signed.

Once signed, the GTU is sent by email by the RA to the Subscriber immediately after the signature process. The Used email address is the one indicated in the Consent Protocol.

4.4 Certificate Acceptance

4.4.1 Conducting Certificate Acceptance

If there is a mistake in the Subscriber certificate; the DRA, in case of [QES FtoF], shall be alerted by the person (*DRA or Subscriber*) who performs the verification, or the Subscriber in any cases, and revocation shall be performed by DRA or the Subscriber, in case of [QES FtoF], or Subscriber alone in case of [QES RIVSP] and [LCP].

Acceptance of the certificate is realized after verification of the content of the Certificate in the signed electronic Document. Acceptance can only be done during Certificate validity period minus 24 hours to be able to revoke Certificate in the case of mistakes.

4.4.2 Notification of Certificate Issuance by the CA to Other Entities

Customer, and DRA in case of [QES FtoF], are notified of certificate issuance by DocuSign Signature Application notifying the Customer and the Subscriber, and the DRA, about successful Transaction.

4.5 Key Pair and Certificate Usage

Refer to [CP].

4.6 Certificate Renewal

This practice is not allowed for Subscriber certificates. If a new certificate is created, a new key pair is created.

4.7 Certificate Re-key

Certificate re-key shall be processed when a key pair reaches the end of its life (*refer to section **Error! Reference source not found.** below*), the end of operational use, or when the public key is compromised.

A new key pair shall be generated in all cases.

Refer to section 3.3, 4.1, 4.2, 4.3 and 4.4.

4.8 Certificate Modification

This practice is not allowed for Subscriber certificates.

If a new certificate is created, a new key pair is created.

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for Revocation

A Subscriber Certificate is revoked when:

- Subscriber's identity information has been filled incorrectly.
- The Certificate corresponding to the private key has been compromised or is suspected to be (*e.g., Signer lost his mobile phone, and its email box has been hacked*).
- Subscriber's identity has never been verified in face to face by a DRA Agent or the DRA Agent has not requested Subscriber to present his/her official ID document.
- The CA is revoked.
- DRA, RIVSP or RA failed to comply with their obligation in identifying the Subscriber.
- The Certificate corresponding to the Private Key has been or is suspected by CA to be lost or compromised.
- Any other reasons legitimately indicated by the CA.
- The DRA failed to comply with its obligations.

4.9.2 Who Can Request Revocation

The Subscriber can request a revocation request, when:

- The Subscriber's identity information has been filled incorrectly.
- The Certificate corresponding to the private key has been compromised or is suspected to be (*e.g., Signer lost his mobile phone, and its email box has been hacked*).
- The Subscriber's identity has never been verified in face to face by a DRA Agent or the DRA Agent has not requested the Subscriber to present his/her official ID document.

The DRA can request a revocation request when:

- The Subscriber's identity information has been filled incorrectly.
- The Certificate corresponding to the private key has been compromised or is suspected to be (*e.g., Signer lost his mobile phone, and its email box has been hacked*).
- The Subscriber's identity has never been verified in face to face by a DRA Agent or the DRA Agent has not requested Subscriber to present his/her official ID document.
- The DRA failed to comply with its obligations.

The RA can request a revocation request when:

- The CA is revoked.
- DRA, RIVSP or RA failed to comply with their obligation to identify Subscriber.
- The Certificate corresponding to the Private Key has been or is suspected by CA to be lost or compromised.
- Any other reasons legitimately indicated by the CA.

4.9.3 Revocation Request Procedure

Revocation requests are authenticated by the DRA.

The revocation request is stored in the DRA's logs in case of [QES FtoF] and in RA's logs in any cases.

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

The DRA transmits the revocation request to the RA in case of [QES FtoF].

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 CA.

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

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

The DRA shall inform the Subscriber about the new status of the certificate.

4.9.4   Revocation Request Grace Period

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 DRA Must Process the Revocation Request

Contract between Customer and RA defines the different timeframe that shall be respected by Customer and the RA to have a Certificate revoked 24 hours maximum after revocation request has been authenticated by DRA.

4.10 End of Subscription

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

5   FACILITY, MANAGEMENT AND OPERATIONAL CONTROLS

5.1   Physical Controls

The RA requirements are defined in the [CP].

[QES FtoF]: the PMA audits the DRA to verify security of DRA location according to PMA audit program (*refer to section 8 below*).

[QES FtoF]: the DRA Registration Policy gives synthesis of location of DRA used to run DRA service.

5.2   Procedural Controls

5.2.1   Trusted Roles

The RA roles are defined by PMA.

The Customer is responsible for defining and documenting trusted roles and associated operations compliant with ETSI and DRA services.

The Customer shall define trusted roles to manage DRA and DRA staff shall be formally appointed.

[QES FtoF]: The Customer designates the DRA Agents for authentication and revocation according DRA Registration Policy.

5.2.2   Number of Persons Required per Task

The RA roles are defined by PMA with the segregation of duty rules.

[QES FtoF]: The Customer shall appoint and define roles to make at least a separation between staff in charge of DRA services and staff in charge of DRA software to proceed to the following operation :
- Configuration
- Installation
- Backup.
- Maintain and recovery.

The DRA Registration Policy gives details about roles and segregation of duty.

5.2.3 Identification and Authentication for Each Role

The RA uses multi-factor authentication to be authenticated to each RA interface directly involved in sensitive operation (*administration of production and configuration of production*).

[QES FtoF]: DRA agents shall use multi-factor authentication to run DRA services.

DRA Registration Policy details the multi-factor authentication used by DRA Agent.

5.3 Personnel Controls

The RA requirements are defined in the [CP].

[QES FtoF]: DRA roles shall be trained:

- To respect state-of-the-art legal requirements for ID verification and face-to-face meetings in accordance with ANSSI requirements.
- To revoke Subscriber Certificates.
- To inform the Subscriber about GTU(*s*) and revocation processes.

The DRA Registration Policy gives details about DRA training.

5.4 Audit Logging Procedures

5.4.1 Events Recorded

The RA records the following information:
- Copy of ID document used for ID proofing.
- Proof Files.
- All other logs requested in [CP].

[QES FtoF]: The DRA shall record all the information used and detailed below:
- The list of all DRA Agents that are authorized to enroll and manage Subscribers.
- Training records of DRA roles.
- Revocation requests.
- COC.
- The identities of DRA Agent who have registered Subscribers if it is not already included in the COC.

[QES RIVSP]:
- RIVSP shall record the following information:
    - o Video of Subscriber ID made during the remote identification.
    - o Video of Subscriber Face made during the remote identification.
- DocuSign platform: record the Identity Wallet use and life cycle.

The RA protects log as required in [CP].
The DRA Registration Policy gives details about log management.
The RIVSP Identification Policy gives details about log management and the contract between CA and RIVSP defines the duration of retention for RIVSP records which is at least 7 years.

Recorded information are protected in such a way that only authorized roles can access them.

Where an event is logged by the audit collection system, it guarantees that the event is linked to a role (*name and first name of the person having the role or makes it possible to have the link with the person having the role*).

5.4.2 <u>Vulnerability Assessments</u>

The RA requirements are given in the [CP].

[QES FtoF]: when the DRA uses an IT system to manage Subscriber information used to issue Certificates, then it shall be covered by a vulnerability and patch management.

The DRA Policy gives details about vulnerability and patch management.

5.5 Records Archival

The RA archives the following information (*for at least 7 years and one month*):

- Copy of ID document used for ID proofing.
- Proof File.
- All other logs requested in [CP].
- Registration Policy.
- DRA Registration Policy.
- List of DRA entity/entities.
- GTU(*s*) and DRA agreement(*s*).

[QES FtoF]: The DRA archives the following information (*for at least 7 years and one month*):

- The list of all DRA Agents authorized to enroll and manage Subscribers.
- Training records of DRA roles.
- Revocation requests.
- COC.
- The identities of DRA Agent who have registered Subscribers if it is not already included in the COC
- The DRA Registration Policy.

The RIVSP archives the records as defined in section 5.4 above.

The RA protects archives as required in [CP].

The DRA Registration Policy gives details about archive management.

Archived information are protected in such a way that only authorized roles can access them.

5.6 Compromise and Disaster Recovery

The RA requirements are given in [CP].

[QES RIVSP] and [QES FtoF]: The discovery of major vulnerabilities and security breaches (*including security breach on personal data*) are processed within 48 hours of their knowledge by the Customer, the DRA, the RIVSP and the RA is alerted by the Customer 24H00 after having taken knowledge of the major incident affecting the security of the DRA IT system used to manage Certificate requests or personal data.

5.7 RA And DRA Termination

The RA termination is treated according the [CP].

In the event of the termination of the DRA service for a Customer, the Customer provides notice prior to the termination, and:

- Inform the RA by registered letter.
- Destroys all secrets used to connect to the DRA service (*DocuSign Signature Application*).
- The DRA stops delivering Certificates request to the RA.
- In the case of a compromised DRA, the Customer uses secure means to notify Subscribers and relying parties that they must not trust Subscriber certificates identified in the list provided by the Customer.
- Archives all audit logs and other records prior to terminating the DRA.
- Archived records are transferred to RA.

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

In the case of the termination of RIVSP services, the RIVSP manages the record according ANSSI rules and contract between the RIVSP and the CA.

6 TECHNICAL SECURITY CONTROLS

6.1 Subscriber Activation Data

The Consent Protocol (*refer to section 4.3 above*) requires a technical activation data that is an OTP code generated by CA and transmitted to the Subscriber on his/her telephone number.

6.2 RA and DRA technical Security Controls

All security rules defined in the [CP] applies to the RA.

[QES FtoF]: the PMA audits the DRA to verify the security of DRA IT systems used to manage Subscribers according to the PMA audit program (*refer to section 8 below*).

7 CERTIFICATE, CRL AND OCSP PROFILES

Refer to [CP].

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1 Frequency or Circumstances of Assessment

The RA audit requirements are the same as the CA as defined in [CP]. The RA is audited every 2 years by external accredited auditors. The RA in audited by PMA internal auditors every year.

Before authorizing a Customer to use the DRA service, the PMA must audit the DRA procedure and the DRA management defined by the Customer in the DRA Registration Policy, to be sure that it is coherent with the requirement set in the CP, the Registration Policy and the DRA Registration Policy and agreement signed with the RA. If the DRA Registration Policy comply with CP requirements and the Registration Policy, then the PMA authorizes Customers to use the DRA Service with its DRA entities. After validation of the DRA Registration Policy by PMA, the DRA Registration Policy is signed by the Customer and the RA.

After initial audit of the DRA (*interview of Customer and DRA Registration Policy review*), an onsite audit is planned by the PMA. Onsite audit is conducted based on a sample of Customers and DRA site according to audit strategies defined by PMA.

8.2 Identity/Qualifications of Assessor

The RA is audited by a CAB.

The DRA is audited by the RA internal compliance team.

Compliance auditors shall demonstrate competence in the field of compliance audits and shall be thoroughly familiar with PKI requirements, CP and Registration Policy. Compliance auditors must perform such compliance audits as a primary responsibility. The PMA carefully reviews 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.

8.3 Topics Covered by Assessment

For the RA, the perimeter of audit is:

- The OA

- The Registration Policy implementation

- The Customer contractual relationship.

For the DRA, the perimeter of audit is:

- The Content and availability of the agreement between Customer and potential third parties to whom all or part of DRA missions are sub-contracted.

- The DRA management of Signer identification and authentication data.

- Authentication and identification of Signer by the DRA.

- Delivery Management of signed electronic Documents to Signers.

- The Designation, training, and authentication of DRA Agents.

- Management, protection, and storage of Customer logs relevant to the DRA activity.

- Customer management of secrets used to connect to the DocuSign Signature Application platform.

- Management of revocation request procedures.

- Physical and IT protection of all systems used by the DRA to manage Signer Identity data, and revocation data.

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 RP. 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 RP, 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 RP, 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 operations 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 necessary. Based on the audit result the PMA can decide to revoke the CA.

If it is suspected that the DRA and/or one or more DRA Agents are in breach of the agreement signed with the RA, or if the CAB or an entitled government authority makes the express request, DocuSign France also reserves the right to conduct an unannounced audit on the premises of the Customer and the relevant DRAs at any time, to determine any noncompliance with the agreement and/or the applicable CP.

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 RP and DRA Registration Policy and any other audit criteria used as the basis for the 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 Financial Responsibility

DocuSign France maintains reasonable levels of insurance coverage.

CA requirements applies to RA.

A Contract established between RA and Customers describes this aspect.

9.2 Confidentiality of Business Information

9.2.1 Scope of Confidential Information

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

- Records and archives of OA.
- Subscriber identity and information data.
- RA service private keys.
- Subscriber certificate request.
- Revocation request.
- RA activation data.
- Audit results and reports.
- Business continuity plan.
- Contract and agreement with Customer.
- Internal facility security policy.
- Practice to implement Registration Policy.

Each DRA 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.

[QES FtoF]: the Customer guarantees a special treatment for the following confidential information:

- Records and archives of OA.
- Subscriber identity and information data.
- DRA activation data to connect to DRA service.
- Subscriber certificate request.
- Revocation request.
- Audit result and reports.
- Contractual and agreement with RA and DRA.
- Internal facility security policy.
- Practice to implement DRA Registration Policy.

9.3 Privacy of Personal Information

9.3.1 Privacy Plan

All data collected and verified directly by the RA, and copies of Signer Identity transmitted by DRA to the RA are governed by rules defined by DocuSign France in order to be compliant with eIDAS regulation as a qualified Trust Service Provider (TSP) issuing Qualified Certificates.

In its role of controller, the Customer shall:

- Respect provisions related to Signer's Personal data in DRA Registration Policy.

- Define its own complementary security rules if they remain compliant with 2016/679 European Regulation (*GDPR*) for Signer's personal data collected by DRA.

- Designate DocuSign France as its processor according to GDPR regulation.

- Delete the personal data controlled by the Customer and stored in DocuSign Signature Application, using the DocuSign Signature Application appropriate function, beyond acceptable retention period as per GDPR.

- Ensure communication of these rules to the Signer according to GDPR requirements.

The DRA collects the following personal data:

- Subscriber name and first name.

- Subscriber mobile phone number

- Subscriber email

- A copy of Subscriber official ID document.

The CA and RA collect the following personal data :

- Subscriber name and first name.

- Subscriber mobile phone number.

- Subscriber email.

- A copy of Subscriber official ID document.

These personal data are collected and processed by DRA, RA and CA as per the requirements of the 2014/910 European Regulation to issue Qualified Certificates. Subscribers are informed that the RA will use an automated process to verify Subscriber identity against the copy of Subscriber official ID document, as described in DRA Registration Policy, prior to the issuance of Subscriber Certificate. The issuance of

Subscriber certificate is not based on that sole automatic process but also relies on the DRA verification. Inside DRA, RA and CA, only restricted group of authorized persons can have access to these data for evidence management and incident resolution only. If Subscribers refuse this process, Subscribers cannot be issued a Certificate and sign electronic Documents.

Subscribers are informed that the right to restriction of processing is associated to their right to not continue the identification and signing process, as described in the DRA Registration Policy, if Subscribers detect a mistake in Subscriber name and/or in Subscriber mobile phone number and/or in Subscriber email. This right is also associated to Subscriber capability to request a revocation as described in GTU(*s*).

Subscribers are informed that the IP address of the device used for the Consent Protocol is recorded in the Proof File and in the COC, for the only purpose of evidence management.

The personal data is collected as described above for the sole purposes of :

a) Identification of the Subscriber by the RA.

b) Creation of the Subscriber's Certificate.

c) Authentication of the Subscriber during the Consent Protocol.

d) Revocation of the Subscriber Certificate.

Personal data stored and already used in Certificates, logs and archives can't be modified and deleted as they constitute an evidence of Subscriber consent to sign the electronic Documents.

Personal data are stored by:

- DocuSign in the Proof File (*all data collected by DRA, RIVSP in RIVR, RA and CA only*) for a proper term, based on the legal and regulatory requirements, and in order notably to ensure the service's continuity and to provide any proof required in case of dispute. These data are kept at least 7 years after Certificate issuance, and maximum of 17 years due to log system of the CA.

- The DRA in the COC (*excluding the copy of the official ID document except if the DRA wants to do it on its own needs required by regulation associated to electronic Document signature*).

- DocuSign Signature Application (*excluding the copy of the official ID document*) and potentially the Customer (*all data collected by the DRA only*). The DRA defines its own personal data maximum retention period, depending on the legal requirements regarding the electronic Documents managed by the Customer.

For any legitimate request related to Subscriber personal data, under 2016/679 European Regulation (GDPR), please contact https://www.docusign.com/company/privacy-policy.

9.3.2 Disclosure Pursuant to Judicial or Administrative Process

The RA is compliant with French law and has secure procedures to clear access to private data to duly authorized personnel based on request by official legal entities.

9.4 Representations and Warranties

9.4.1 PMA Representations and Warranties

The PMA defines the present RP and the corresponding practice.

The PMA establishes that PKI components are compliant with the present RP.

The processes, procedures and audit framework used to determine compliance are documented within the practices.

The PMA establishes and approves the dedicated risk analysis for RA services.

The PMA approves list of countries and types of official ID document to be used for ID proofing run by the RA.

The PMA ensures that all requirements on a PKI component, as detailed in the present RP and in the corresponding practice, are implemented as applicable to deliver and manage registration and revocation services.

The PMA has the responsibility for compliance with the procedures prescribed in this RP and DRA Registration Policy, even when PKI component functionality is undertaken by sub-contractors. PKI components provide all their registration and revocation services consistent with their practice.

The PMA has the responsibility to audit the DRA and approve DRA's Registration Policy before allowing Customer (RA) usage of the DRA service with the OID referenced in section 1.2 above.

9.4.2 RA Representations and Warranties

The RA has the responsibility to:

- [QES FtoF] and [QES RIVSP]: Ensure that Subscribers are properly identified based on ID proofing verification, and that Subscriber certificate requests are accurate and duly authorized.

- [QES]: Receive from authenticated DRA or RIVSP, and use Subscribers telephone numbers and email addresses for Certificate requests.

- [LCP]: Ensure that Subscribers are properly identified and authenticated, and that Subscriber certificate requests are accurate and duly authorized.

- [LCP]: Collect telephone numbers and email addresses of Subscribers for Certificate requests.

- Send GTU(s) to the email address registered by the DRA or the Customer.

- Only accept official ID document for ID proofing based on risk analysis.

- Verify Subscriber identity with IDP proofing or with RIVR, received from DRA or RIVSP, to be set in the Certificate.

- Transmit the valid and verified Subscriber identity, as received from the DRA or the Customer, to the CA to be set in the Certificate if ID proofing verification.

- Before entering into an agreement relationship with a Subscriber, the RA shall inform the Subscriber of the terms and condition regarding use of the Certificate (GTU(s)) during the Consent Protocol cinematic.

- Submit accurate and complete information about the Subscriber to the CA.

- Allow the Subscriber to be able to view information that will be set in Subscriber certificate to create its identity and used to interact with Subscriber (*telephone number and email address*) during Consent Protocol cinematic.

- Let auditor team audit and communicate the requested information to them, according to the PMA intention, control and check the compliance with the present RP and with the associated practices.

- Alert PMA when there is a security incident about the RA and DRA services.

- Respect the RP and corresponding practices.

- Protect its information system and guaranty the security of the data transmitted to the PKI.

- Records and archives all requested information.

- Protect Subscriber information.

- Exercise reasonable care to avoid unauthorized use of the Subscriber's private key.

- Designate and maintain a list of all trusted roles.

- Alert Customer in case of incident related to the RP and the RA procedures.

- Respect GDRP regulation.

9.4.3 DRA Representation and Warranties

The DRA is responsible for:

- Ensuring that Subscribers are properly identified and authenticated in face-to-face meetings or equivalent, and that Subscriber certificate requests are accurate and duly authorized.

- Collecting telephone numbers and email addresses of Subscribers for Certificate requests.

- Verifying identity of subscribers and authenticate Subscribers according to DRA Registration Policy.

- Transmitting the Subscriber identity to be set in the Certificate to the RA.

- Authenticating revocation requests and transmit them to the RA.

- Submitting accurate and complete information about Subscribers to the RA.

- Making available the signed electronic Document to the Subscriber.

- Letting auditor team audit and communicate the requested information to them, according to the PMA intention, control and check the compliance with the present RP and with the associated practices.

- Alerting the PMA when there is a security incident about the DRA services.

- Respecting the DRA Registration Policy and corresponding practices and agreements signed with the RA.

- Protecting its information system and guarantying the security of the data transmitted to the DRA.

- Recording and archiving all requested information.

- Protecting information of the Subscriber.

- Exercising reasonable care to avoid unauthorized use of the Subscriber's private key.

- Exercising reasonable care to avoid unauthorized access to DocuSign Signature Application.

- Designating and maintaining a list of all trusted roles.

- Alerting Customer in case of incident related to DRA Registration Policy and DRA procedures.

- Notifying Subscribers in case of DocuSign Signature Application access or DRA service or RA/CA services compromise resulting in Subscriber compromised Certificate issuance.

- Respecting GDRP regulation.

9.4.4 Customer Representations and Warranties

The Customer is responsible for:

- [LCP]: Collecting email address and name (*and optionally mobile phone number*) of Subscriber for Certificate request.

- Transmitting the Subscriber identity to be set in the Certificate to the RA.

- Submitting accurate and complete information about the Subscriber to the RA.

- Making available the signed document to the Subscriber.

- Protecting information of the Subscriber.

- Exercising reasonable care to avoid unauthorized use of the Subscriber's private key.

- Exercising reasonable care to avoid unauthorized access to DocuSign Signature Application.

- Alerting the RA in case of incident related to the DRA Registration Policy and DRA procedures.

- Notifying Subscriber in case of DocuSign Signature Application access or DRA service or RA/CA services compromise and result in Subscriber compromised Certificate issuance.

- Establishing contract with the OA entity when they are different legal entities from it with clear identification of DRA services run by the entity and all DRA's and OA's obligations and warranties according to the DRA services managed.

- Establishing a contract with the DRA entity when they are different legal entity from it with clear identification of DRA services run by the entity and all DRA's and Customer's obligations and warranties according to the DRA services managed.

- Defining the DRA Registration Policy, the DRA management procedure and the Subscriber management procedure.

- Selecting OID level from this RP.

- Respecting the DRA Registration Policy and corresponding practices and agreement signed with the RA and the DRA.

- Protecting its information system and guarantying the security of the data transmitted to the DRA and RA.

- Recording and archiveing all requested information (*COC*).

- Protecting information of the Subscriber.

- Letting auditor team audit and communicate the requested information to them, according to the PMA intention, control and check the compliance with the present RP, DRA Registration Policy and with the associated practices.

- Respecting GDRP regulation.

9.4.5 OA Representations and Warranties

The OA has the responsibility for:

- Respecting its security policy and contract signed with the entity for which service are run/operated.

- Protecting and guaranteeing integrity and confidentiality of secret data and Subscriber data according to the contract signed with the RA and/or the DRA according to the entity services supported.

- Allowing the auditor team to control and check the compliance with the present RP/DRA Registration Policy/auditing criteria and components of the practices 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.

- Alerting the PMA when there is a security incident with the PKI services that the OA performed.

- Respecting and operating the section(*s*) of the practices that deals with their services run and communicated in contract.

- Documenting their internal procedures to complete the global practice and its security policy.

- Respecting GDRP regulation.

9.4.6 RIVSP

RIVSP has to:

- Record and archive all requested information.
- Protect information of the Subscriber.
- Exercise reasonable care to avoid unauthorized access to DocuSign Signature Application.
- Respect their Identification Policy.
- Be certified by ANSSI.
- Alert CA in case of incident related to Identification Policy and certification process.
- Respect GDRP regulation.

9.4.7 Subscriber

The physical person has the responsibility to:

- Gives his/her telephone number and email address for Certificate request and guaranty it is under his/her sole control.
- Upload his/her valid secured official ID document in the RA interface.
- Verify and confirm his/her information during Consent Protocol and refuse to sign in case of mistake discovered during Consent Protocol cinematic.
- Accurately represent themselves in all communications with the DRA and the Customer.
- Notify the DRA or Customer in case of compromission or change of his/her email address, telephone or identity.
- Only use OTP code in the Consent Protocol and protect it to be the sole to have knowledge of it.
- Abide by all the terms, conditions, and restrictions levied on the use of their Certificates (*described in GTU*(*s*)), as set forth in this RP and in the GTU(*s*).
- Notify the DRA in case of mistake in the information contained in Consent Protocol and in the Certificate.
- Request revocation when revocation reasons are met.

9.5 Disclaimers of Warranties

The PMA guarantees through the RA services:

- Management of corresponding certificates and certificate status information, based on received revocation request, regarding the present RP.
- Subscriber certificate content according to the DRA, the Customer and the Subscriber transmitted information about the Subscriber.
- Subscriber key pair is used by the sole Subscriber according to the Consent Protocol, with OTP code sent to telephone number (*registered by the Subscriber or the DRA*).

The RA guarantees trough the RA services:

- [QES FtoF] and [QES RIVSP]: Identification of Subscriber, with Subscriber certificate generated by the applicable CA.
- [LCP]: Identification and authentication of Subscriber, with Subscriber certificate generated by the applicable CA.

The 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*).

9.6 Limitations of Liability

DocuSign France makes no claims regarding the suitability or authenticity of certificates issued under this RP. Relying parties may only use these certificates at their own risk. The PMA assumes no liability whatsoever in relation with the use of certificates or associated public/private key pairs for any use other than those described in the present RP and associated practices.

[QES FtoF] and [QES RIVSP]: the RA is liable as regards for the accuracy of all information contained in the Subscriber certificate.

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

9.7 Indemnities

Indemnities are defined in the agreement between Customer and RA.

9.8 Term and Termination

9.8.1 Term

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

9.8.2 Termination

If the RA services ceases to operate, a public announcement must be made by the PMA.

Upon termination of service, the PMA will properly archive its records.

9.8.3 Effect of Termination and Survival

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

The DRA cannot continue registering Subscriber referred to by the present RP.

9.9 Individual Notices and Communications with Participants

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

9.10 Amendments

9.10.1 Procedure for Amendment

The PMA reviews the RP, dedicated risk analysis and associated practices at least yearly.

Additional reviews may be enacted at any time at the discretion of the PMA especially about official ID document to use for ID proofing by RA. 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 RP, the PMA notifies PKI components.

If the PMA wishes to recommend amendments or corrections to the RP, such modifications shall be circulated to appropriate parties identified by the PMA.

The PMA collects, sums up and proposes RP modifications according to approval procedures.

9.10.2 <u>Notification Mechanism and Period</u>

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

9.11 Dispute Resolution Provisions

Provisions for resolving disputes between DocuSign France and its Customers are set forth in the applicable agreement between the parties.

9.12 Governing Law

Subject to any limits appearing in applicable law, the laws of France, shall govern the enforceability, construction, interpretation, and validity of the RP, 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 RP. Agreement with Customers incorporating the RP 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 RP separate and apart from the terms of such other agreements, subject to any limitations appearing in applicable law.

9.13 Compliance with Applicable Law

The RP 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.

Customers and DocuSign France agree to conform to applicable laws and regulations in their contract.

9.14 Miscellaneous Provisions

9.14.1 <u>Entire Agreement</u>

This RP constitutes the entire understanding between the parties and supersedes all other terms, whether expressed or implied by law. No modification of this RP shall be of any force or effect unless in writing and signed by an authorized signatory. Failure to enforce any or all these sections in a particular instance or instances shall not constitute a waiver thereof or preclude subsequent enforcement thereof. All provisions in this RP 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 assignees.

9.14.2 <u>Assignment</u>

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

9.14.3 <u>Severability</u>

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

9.14.4 <u>Waiver of Rights and obligation</u>

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

9.14.5 Force Majeure

DocuSign France shall not be liable for any failure or delay in its performance under the RP 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 DRA or Customer) ACTS OR THE INTERNET INFRASTRUCTURE OR ANY NETWORK EXTERNAL TO DOCUSIGN FRANCE.

9.15 Other Provisions

9.15.1 Interpretation

All references in this RP to "sections" refer to the sections of this RP. As used in this RP, 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 RP as a whole, as the same may from time to time be amended or supplemented, and not to any subdivision contained in this RP. The words "include" and "including" when used herein are not intended to be exclusive and mean, respectively, "include, without limitation" and "including, without limitation."

9.15.2 Conflict of Provisions

In the event of a conflict between the provisions of this RP, the associated practices and any subscriber agreement, the order of precedence shall be RP, associated practices, and then Customer agreement.

9.15.3 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 the 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.

9.15.4 Notice of Limited Liability

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