DocuSign

DS France ETSI Registration Policy and Practice for Remote Signature

DS FRANCE ETSI REGISTRATION POLICY AND PRACTICE FOR REMOTE SIGNATURE

Version	1.3	**Pages**	33
Status	☐ Draft	☒ Final	
Author	DocuSign France		

Diffusion List	☒ External	☒ Internal DocuSign
	Public	Public

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 PVID	

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 Subscriber.

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 QSCD]: “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).
- [CP]: “DSF_Protect and Sign Personal Signature ETSI CP v 2.2” (applicable OID is 1.3.6.1.4.1.22234.2.14.3.31 and 1.3.6.1.4.1.22234.2.14.3.32).

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 Consent Protocol chosen 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 designates 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) contractually bound 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.
- Verify and update of the official ID Document and of registration data (email, phone number…).
- If applicable, authentication of the Subscriber with a secure means of authentication for remote access to 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 DRA agent, person contractually or hierarchically related to the DRA, in charge of performing face to face identification for Signers, according to the DRA Registration Policy.

An DRA operates its services according to the [CP], the corresponding CPS, the present RP and its dedicated DRA Registration Policy. An 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 contractually bound to DSF by a Service Agreement. 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.
- Verify the Subscriber's ID and of collect data during identification operation (email, phone number…).

The RIVSP defines, implements and maintains an Identification Policy. RIVSP shall be certified by ANSSI before to be used for [QES RIVSP] according 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

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 entity that is DRA. In the service agreement between Customer and DSF all DRA obligations are included.

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

Customer is in charge to elaborate and transmit eDocument to DocuSign Application and to be signed by Subscriber.

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. 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 summarizes in each dedicated GTU, signing the GTU during Consent Protocol.

1.3.7.3 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

The uses of private key are the following:

- Used to sign electronic eDocument(s) and GTU according 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 eDocument(s) and GTU.

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 Administering the Document

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

1.5.2 Contact Person

To contact PMA using contact provided in web or by postal mail:

- PMA of DocuSign France.
- https://www.docusign.fr/ (contact information is provided here).
- 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	Means the procedure according to which You consent to receive a Certificate with the Signer Identity, to accept signing the eDocument via the Service and to accept signing this GTU. The Consent Protocol is executed by the Signer within the Service accessible via the DocuSign Signature Application.
DocuSign Signature Application	Means DocuSign, Inc. Transaction service, which provides online eDocument management and viewing, Signer's Identity (first name, last name, email and mobile phone) registration, DRA role management, eDocument viewer, creation of 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 DRA and DRA Agent and Signer.
eDocument(s)	Mean(s) 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 eDocument 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).
GTU	Means the General Terms of Use of the service that forms a legal agreement between the Signer and DocuSign France. GTU are signed by Signer during Consent Protocol. There is a GTU for LCP and another one for QES.
Proof File(s)	Mean(s) 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 file is only available to DocuSign France in its role as Trust Service Provider.
Proof of DocuSign Signature Application (Certificate of Completion, "COC")	Means 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 eDocument. A dedicated COC associated to each eDocument, Signer and sender is generated in the purpose of proving the validity of a Transaction. COC is sealed by DocuSign Inc. COC 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 verdict (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 (Your date of birth, IDs serial number, IDs expiration date, IDs issuing country, and IDs type)."Transaction(s)" means the performance of a signature process, defined by a set of eDocuments submitted for electronic signature by one or more Signer(s).
RIVSP	"Remote Identity Verification Service Provider" (or "RIVSP") means the third party service provider responsible for acquiring and verifying Signer's facial image and Signer's ID document in order to identify You, producing the evidence file and sending the Result of the Remote Identity Verification to the RA. The RVISP is certified by ANSSI (the French supervisory body according eIDAS).
Signer Identity	Means the set of personal data (containing name, email address, mobile phone number, and copy of an official ID document) used to identify a Signer.
Transaction(s)	Means the performance of a signature process, defined by a set of eDocuments submitted for electronic Signature by one or more Signers.

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

The RP is published here: 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 pursuant to this RP 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 ID of the Subscriber.

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

- The RA's name in the "OU" field: "DocuSign France".
- Country field is "FR".
- 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

Subscriber has sole control of its private key thanks to Consent Protocol and OTP code received on its 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]

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, email and telephone number of 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 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:

- 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:

- 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 and telephone number of the Subscriber.

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

Evidence shall be provided of:

- 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 a RIVR and signed it.

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

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

Subscriber uploads a copy of its valid official ID document in the RA interface. During this upload, in same time Subscriber upload its 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.

DRA, which 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, which enrolls all of its Users with its identification data and authentication data.

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

If any information of Subscriber to be set in Subscriber certificate (refer to section 3.1 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 DRA in order to be sure that update information are linked to the Subscriber for Consent Protocol.

DRA practices are described in DRA Registration Policy.

3.3.1.2 [QES RIVSP]

RA apply same procedure as described for the initial Certificate (Refer to section 3.2.3.2 above).

3.3.1.3 LCP

RA apply 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.

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 OTP code sent to email of Subscriber recorded by RA during the identification operation (refer to section 3.2).

For [QES FtoF], DRA can also requests revocation to RA and DRA practices are described in 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 DRA.

4.1.1.2 [QES RIVSP]

Certificate request is under responsibility of Customer.

4.1.1.3 LCP

Certificate request is under responsibility of Customer.

4.1.2 Enrollment Process and Responsibilities

4.1.2.1 [QES FtoF]

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.

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

DRA practices are described in DRA Registration Policy.

4.1.2.2 [QES RIVSP]

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. When mobile phone is no filled in the Certificate request, then Subscriber fills it in the RIVSP portal.

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

4.1.2.3 LCP

Certificate request shall contain the following information:

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

Certificate request is 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 submit a Certificate request (refer to section 4.1 above), and having been authenticated by DRA, DocuSign Signature Application send to the Subscriber an eDocument to be signed.

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 Subscriber to connect to DocuSign Signature Application.

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

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

4.2.2 [QES RIVSP]

After having submit a Certificate request (refer to section 4.1 above), and having been authenticated by RIVSP, DocuSign Signature Application receives the RIVR, verifies it, and sends to the Subscriber an eDocument to be signed if RIVR verdict is good. If not RIVR verdict is not good, then the Subscriber can't sign. The RIVR can be used to sign during 24H00 maximum, after that Subscriber shall do again a remote identification with the RIVSP.

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 Subscriber to connect to DocuSign Signature Application. DocuSign Signature Application redirects the Subscriber to RA portal and gives to RA portal the RIVR and finger print of eDocument 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 verification of RIVR is good, then RA accepts to issue a Certificate (refer to section 4.3 below). If the result of verification of RIVR is not good, then RA refuse to issue Certificate and Transaction is canceled.

4.2.3 [LCP]

After having submit a Certificate request (refer to section 4.1 above), and having been authenticated by RA, DocuSign Signature Application send to the Subscriber an eDocument to be signed.

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 Subscriber to connect to DocuSign Signature Application.

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

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

4.3 Certificate Issuance

RA presents the Consent Protocol to Subscriber to enable Subscriber continuing with the signing process. Subscriber can accept or refuse to sign the eDocument and the GTU (GTU are viewable in the Consent Protocol). During Consent Protocol, Subscriber verifies its identity (to be set in Certificate), telephone number and email. In case of mistake in these above data, Subscriber shall refuse to sign.

RA transmits the technical certificate request to the CA containing 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 CA and in a secure way assigned to Subscriber for the duration of the eDocument 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 containing your 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 eDocument and GTU presented to the Signer before signature.
- The signature of the eDocument and GTU.
- The date and time of the signature operation.
- The Consent Protocol as executed between the Signer and the CA.

- 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].
- Copy of Subscriber's ID or extracted information from Subscriber's ID.
- Your personal data contained in the Subscriber ID.

DocuSign Signature Application builds and stores the COC. COC can be downloaded with the eDocument by the Signer in DocuSign Signature Application.

Once signed, the eDocument can be downloaded from DocuSign Signature Application by the Subscriber, Customer and in case of [QES FtoF] by DRA immediately after the signature process. In any case, the signed eDocument and the COC may be transmitted to Subscriber on subscriber's email after having been signed.

Once signed, the GTU is sent by email by RA to Subscriber immediately after the signature process. 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; then DRA, in case of [QES FtoF], shall be alerted by the person (DRA or Subscriber) who performs the verification, or Subscriber in any cases, and revocation shall be performed in any cases by DRA or Subscriber, in case of [QES FtoF], or Subscriber in case of [QES RIVSP] and [LCP].

Acceptance of the certificate is realized verifying with the content of Certificate in the signed eDocument. Acceptance can only be done during Certificate validity period minus 24 hours to be able to revoke Certificate in case of mistake.

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 Subscriber, and DRA in in case of [QES FtoF], 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 Your official ID document.
- 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.
- The DRA failed to comply with its obligations.

4.9.2 Who Can Request Revocation

Subscriber can request a revocation request, 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 Your official ID document.

DRA can request a revocation request 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 Your official ID document.
- The DRA failed to comply with its obligations.

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”.

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 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

RA requirements are defined in the [CP].

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

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

5.2 Procedural Controls

5.2.1 Trusted Roles

RA roles are defined by PMA.

Customer is responsible to define and documented trusted roles and associated operation compliant with ETSI and DRA services. Customer shall define trusted role to manage DRA and DRA personal shall be formally appointed.

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

5.2.2 Number of Persons Required per Task

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

[QES FtoF]: Customer shall appoint and define role to make at least a separation between personal in charge of DRA services and personal in charge of DRA software to proceed the following operation; configuration, installation, backup, maintain and recovery. DRA Registration Policy gives details about roles and segregation of duty.

5.2.3 Identification and Authentication for Each Role

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 agent 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

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 meeting in accordance with ANSSI requirements.
- To revoke Subscriber Certificate.
- To inform the Subscriber about GTU and revocation process.

DRA Registration Policy gives details about DRA training.

5.4 Audit Logging Procedures

5.4.1 Events Recorded

RA record the following information:

- Copy of ID document used for ID proofing.
- Proof File.
- All others logs requested in [CP].

[QES FtoF]: DRA shall record all the information used:

- The list of all DRA Agent that are authorized to enroll and manage Subscriber.
- Training record of DRA roles.
- Revocation request.
- COC.
- DRA Agent identity who has registered Subscriber if it is not already included in the COC.

[QES RIVSP]: RIVSP shall record the following information:

- Video of ID of Subscriber made during the remote identification.
- Video of face of Subscriber made during the remote identification.

RA protects log as required in [CP].
DRA Registration Policy gives details about log management.
RIVSP Identification Policy gives details about log management and the contract between CA and RIVSP defines duration retention for RIVSP record that 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 Vulnerability Assessments

RA requirements are given in the [CP].

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

5.5 Records Archival

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

- Copy of ID document used for ID proofing.
- Proof File.
- All others logs requested in [CP].
- Registration Policy.
- DRA Registration Policy.
- List of DRA entity.
- GTU and DRA agreements.

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

- The list of all DRA Agent that are authorized to enroll and manage Subscriber.
- Training record of DRA roles.
- Revocation request.
- COC.
- DRA Agent identity who has registered Subscriber if it is not already included in the COC.
- DRA Registration Policy.

RIVSP archives the records as defined in section 5.4 above.

RA protects archives as required in [CP].

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

RA requirements are given in [CP].

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

5.7 RA And DRA Termination

RA termination is treated according [CP].

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

- Inform RA by register letter.
- Destroys all secret used to connect to DRA service (DocuSign Signature Application).
- The DRA stops delivering Certificates request to the RA.
- In the case of a compromised DRA, 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 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 Subscriber and PKI components. The OA then transmits its records to the Customer.

In case of termination of RIVSP, RIVSP manages the record according ANSSI rules and contract between RIVSP and 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 Subscriber on its telephone number.

6.2 RA and DRA technical Security Controls

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

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

7 CERTIFICATE, CRL AND OCSP PROFILES

Refert to [CP].

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1 Frequency or Circumstances of Assessment

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

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

After initial audit of the DRA (interview of Customer and DRA Registration Policy review), an onsite audit is planned by PMA. Onsite audit is made based on sample of Customer and DRA site principal according audit strategy defined by PMA.

8.2 Identity/Qualifications of Assessor

RA is audited by a CAB.

DRA is audited by RA internal compliance team.

Compliance auditors shall demonstrate competence in the field of compliance audits and shall be thoroughly familiar with requirements PKI, CP and Registration Policy. Compliance auditors must perform such compliance audits as a primary responsibility. 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 RA, the perimeter of audit is; OA, Registration Policy implementation and Customer contractual relationship.

For DRA, the perimeter of audit is:

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

- DRA management of Signer identification and authentication data.
- Authentication and identification of Signer by the DRA.
- Management of the delivery of signed eDocuments to Signers.
- Designation, training and authentication of DRA Agents.
- Management, protection and storage of the Customer's log relevant to Delegated Registration Authority activity.
- Customer management of secret used to be connected to the DocuSign Signature Application platform.
- Management of revocation request procedure.
- Physical and IT protection of all system used by 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 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.

If it is suspected that the DRA and/or one or more DRA Agents are in breach of the agreement signed with 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 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 Financial Responsibility

DOCUSIGN FRANCE maintains reasonable levels of insurance coverage. CA requirements applies to RA.

Contract established between RA and Customer describes this aspect.

9.2 Confidentiality of Business Information

9.2.1 Scope of Confidential Information

PMA guarantees a special treatment for the following confidential information:

- Records and archive of OA.
- Subscriber identity and information data.
- RA service private keys.
- Subscriber certificate request.
- Revocation request.
- RA activation data.
- Audit result and reports.
- Business continuity plan.
- Contractual 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]: Customer guarantees a special treatment for the following confidential information:

- Records and archive 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 of 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 Certificate.

In its role of controller, Customer shall:

- Respect provisions related to Signer's Personal data in DRA Registration Policy.
- Define its own complementary security rules provided that they remain compliant with 2016/679 European Regulation (GDPR) for Signer's personal data collected by DRA.
- Designate DocuSign 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.

DRA collects the following personal data; Subscriber name and first name, Subscriber mobile phone number, Subscriber email and a potentially a copy of Subscriber official ID document.

CA and RA collect the following personal data; Subscriber name and first name, Subscriber mobile phone number, Subscriber email and 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 Certificate. Subscriber are informed that RA will use an automatic 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 person can have access to these data for evidence management and incident resolution only. If Subscriber refuse this process, Subscriber cannot be issued a Certificate and sign eDocument.

Subscriber are informed that the right to restriction of processing is associated to Your right to not continue the identification and signing process, as described DRA Registration Policy, if Subscriber 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.

Subscriber 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 and (d) revocation of the Subscriber Certificate.

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

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 DRA wants to do it for on its own needs required by regulation associated to eDocument signed).
- DocuSign Signature Application (excluding the copy of the official ID document) and potentially the Customer (all data collected by DRA only). The DRA defines its own personal data maximum retention period, depending on the legal requirements in regard to the eDocuments managed by 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

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

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. PMA establishes and approves the dedicated risk analysis for RA services. PMA approves list of countries and types of official ID document to be used for ID proofing run by 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 allows Customer (RA) uses 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 Subscriber is properly identified based on ID proofing verification, and that Subscriber certificate request, accurate and duly authorized.
- [QES]: Receive, from authenticated DRA or RIVSP, and use Subscriber telephone number and email address for Certificate request.
- [LCP]: Ensure that Subscriber is properly identified and authenticated, and that Subscriber certificate request, accurate and duly authorized.
- [LCP]: Collect telephone number and email address of Subscriber for Certificate request.
- Send GTU to the email address registered by DRA or Customer.
- Only accept official ID document for ID proofing based on risk analysis.
- Verify the 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 DRA or Customer, to CA to be set in the Certificate if ID proofing verification is good.
- 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) during the Consent Protocol.
- Submit accurate and complete information about the Subscriber to the CA.
- Make Subscriber 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.
- 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 archive all requested information.
- Protect information of the Subscriber.
- 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 RP and RA procedures.
- Respect GDRP regulation.

9.4.3 DRA Representation and Warranties

DRA is responsible to:

- Ensure that Subscriber is properly identified and authenticated in face to face meeting or equivalent, and that Subscriber certificate request, accurate and duly authorized.
- Collect telephone number and email address of Subscriber for Certificate request.
- Verify identity of subscriber and authenticate Subscriber according DRA Registration Policy.
- Transmit the Subscriber identity to be set in the Certificate to RA.
- Authenticate revocation request and transmit it to RA.
- Submit accurate and complete information about the Subscriber to the RA.
- Make available the signed eDocument to the Subscriber.
- 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 DRA services.
- Respect the DRA Registration Policy and corresponding practices and agreement signed with RA.
- Protect its information system and guaranty the security of the data transmitted to the DRA.
- Records and archive all requested information.
- Protect information of the Subscriber.
- Exercise reasonable care to avoid unauthorized use of the Subscriber's private key.
- Exercise reasonable care to avoid unauthorized access to DocuSign Signature Application.
- Designate and maintain a list of all trusted roles.
- Alert Customer in case of incident related to DRA Registration Policy and DRA procedures.
- Notify Subscriber in case of DocuSign Signature Application access or DRA service or RA/CA services has been compromised and result in Subscriber compromised Certificate issuance.
- Respect GDRP regulation.

9.4.4 Customer Representations and Warranties

Customer is responsible to:

- [LCP]: Collect email address and name -and optionally mobile phone number) of Subscriber for Certificate request.
- Transmit the Subscriber identity to be set in the Certificate to RA.
- Submit accurate and complete information about the Subscriber to the RA.
- Make available the signed document to the Subscriber.
- Protect information of the Subscriber.
- Exercise reasonable care to avoid unauthorized use of the Subscriber's private key.
- Exercise reasonable care to avoid unauthorized access to DocuSign Signature Application.
- Alert RA in case of incident related to DRA Registration Policy and DRA procedures.
- Notify Subscriber in case of DocuSign Signature Application access or DRA service or RA/CA services has been compromised and result in Subscriber compromised Certificate issuance.
- Establishes contract with OA entity when they are different legal entity from it with clear identification of DRA services run by the entity and all DRA's and OA's obligations and warranties according DRA services managed.
- Establishes contract with 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 DRA services managed.
- Defines DRA Registration Policy, DRA management procedure and Subscriber management procedure.
- Select OID level from this RP.
- Respect the DRA Registration Policy and corresponding practices and agreement signed with RA and DRA.
- Protect its information system and guaranty the security of the data transmitted to the DRA and RA.
- Records and archive all requested information (COC).
- Protect information of the Subscriber.
- 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, DRA Registration Policy and with the associated practices.
- Respect GDRP regulation.

9.4.5 OA Representations and Warranties

The OA has the responsibility to:

- Respect its security policy and contract signed with the entity for which service are run/operated.
- Protect and guarantee integrity and confidentiality of secret data and Subscriber data according contract signed with RA and/or DRA according entity services supported.
- Allow 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.
- Alert PMA when there is a security incident with the PKI services that the OA performed.

- Respect and operate the section(s) of the practices that deals with their services run and communicated in contract.
- Document their internal procedures to complete the global practice and its security policy.
- Respect GDRP regulation.

9.4.6 RIVSP

RIVSP has to:

- Records 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 its telephone number and email address for Certificate request and guaranty it is under its sole control.
- Upload its valid secured official ID document in the RA interface.
- Verify and confirm its information during Consent Protocol and refuse to sign in case of mistake discovered during Consent Protocol.
- Accurately represent themselves in all communications with the DRA and Customer.
- Notify DRA or Customer in case of compromission or change of its email address, telephone or identity.
- Only use OTP code in the Consent Protocol and protect it in order 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), as set forth in this RP and in the GTU.
- Notify DRA in case of mistake in the information contained in Consent Protocol and in the Certificate.
- Request revocation when revocation reason 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 DRA, Customer and Subscriber transmitted information about Subscriber.
- Subscriber key pair is used by the sole Subscriber according Consent Protocol, OTP code sent to telephone number (registered by Subscriber or 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.

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 with regard to 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 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 RP and associated practices.

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

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

In the event that 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.

DRA cannot continue registered Subscriber referred to by the present RP.

9.9 Individual Notices and Communications with Participants

The PMA provides all participants with new version of 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 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, 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 PMA. The PMA collects, sums up and proposes RP modifications according to approval procedures.

9.10.2 Notification Mechanism and Period

The PMA notifies 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 Customer 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.

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

9.14 Miscellaneous Provisions

9.14.1 Entire Agreement

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 of 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 assigns.

9.14.2 Assignment

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

9.14.3 Severability

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 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 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 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.