REGISTRATION POLICY

Amendment to DOCUSIGN FRANCE's Certificate Policy for using the QUICKSIGN platform as a registration service to identify Subscribers

QuickSign, 19-21 rue Poissonnière 75002 Paris - RCS : Paris B 450 439 963
Phone: +33 1 825 20 500 – www.quicksign.com

Version	2.11	
Status	☐ Draft	☒ Final
Author	Margo Companie	QUICKSIGN

Diffusion List	☐ Internal	☒ External
		Public

History				
Version	Date	Author	Comments	Status
V.1.0	27/09/2016	MC		Verified by XR Published
V.1.99	28/08/2017	FV	Update to prepare post Art51 transitional period Draft version	Waiting for DocuSign and audit Approbation
V2.04	12/09/2019	XR	Review with CA and approbation of PMA (September, 12th, 2019)	Approbation
V2.05	02/12/2019	XR	Review with the CA of the authentication of the Revocation request.	Approbation
V2.10	16/02/2021	AB	Adding new workflow with a manual signature validated by a Registration Officer	Modification
V2.10	23/02/2021	AB	Review and validation with CA	Approbation
V2.11	06/07/2021	AB	Review and minor update of document	Modification and Approbation

TABLE OF CONTENTS

1. Introduction

1.1. Overview

This registration policy (RP) is an amendment to the document “DBD_Protect and Sign Personal Signature ETSI CP” of DOCUSIGN FRANCE. It explains how the online registration service [QUICKSIGN QES ONBOARD ID] operated by QUICKSIGN fulfils the requirements laid out for Registration Authorities (RA) issuing qualified Certificates with ETSI EN 319 411-2 QCP-n-qscd.

In this context QUICKSIGN operates as the Registration Authority (RA) and uses QUICKSIGN’s platform as the registration service to identify Subscribers requesting personal signatures based on Certificates issued by a Certification Authority (CA).

This RP is based on:

- [CP]: DBD_Protect_and_Sign_Personal_Signature_ETSI_CP_v_1_8.
- [PSMP]: “Proof Signature and Management Policy, version 6 minimum that defined the technical process for electronic signature and interaction with Customer.
- RFC 3647 « Certificate Policy and Certification Practices Framework » issued by the Internet Engineering Task Force (IETF).
- ETSI documents:
    - [119 312]: “ETSI TS 119 312 V1.1.1 (2014-11): 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. »;
    - [319 411]:
        - « 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 ».

- [ETSI 319 411] :
    - « Electronic Signatures and Infrastructures (ESI), Policy and security requirements for Trust Service Providers issuing certificates, Part 1: General requirements »
    - « 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 ».

The numeration of the document is in line with DBD_Protect and Sign Personal Signature ETSI CP.

1.2. Document name and identification

In the context of this document the DOCUSIGN FRANCE CP OID to consider is:

- OID = 1.3.6.1.4.1.22234.2.14.3.31: This profile is implemented by the new DocuSign France CA and is eIDAS qualified with the new certificate profile.

Note that the CP for this two OID is identical, taking this information into account CA OID migration will not impact Quicksign Registration Policy.

1.3. PKI components

1.3.1. Registration Authority (RA)

The RA is owned and operated by QUICKSIGN.

The RA supports the following PKI services for all cases:

- Authentication of the Subscriber via a challenge using the Identity Document;
- Authentication and authorization of Delegate Registration Authority (DRA);
- Establishment of contractual relationship with the DRA committing the DRA to fulfil its obligations as per the present Registration Policy;
- Training of the DRA;
- Collaboration with the CA in the control and audit activities directed to the DRA;
- Sending of Certificate request to the CA;
- Revocation authentication and revocation process, and in particular sending of Certificate revocation request to the CA;
- Log trail generation and record of registration information;

When running the RA runs the Consent Protocol (use case noted as *QS Consent Protocol* in the document to identify specific requirement to this use case) a collection of the handwritten signature of a Subscriber in a Face-to-Face signature process using the Tablet of a DRA is performed.

1.3.2. Delegate Registration Authority (DRA)

The DRA acts under the supervision and rules established by QUICKSIGN as a RA.

QUICKSIGN only enters in a contractual relationship with DRAs which are, because of the nature of the services they provide, compelled to ensure that its organization has been

trained to respect state-of-the-art legal requirements for ID verification and face-to-face meeting in accordance with due diligence rules for institutions selling financial products or equivalent rules.

The DRA is audited by the RA or the Policy Management Authority (PMA) before entering in a contractual relationship with the RA.

A list of DRAs, including reference of the contract, audit plan, and reference persons authorized to handle revocation requests for each DRAs, is established by the RA.

The DRA supports the following PKI services:

- Initial identification and authentication of the Subscriber;
- If applicable, update of the official Identity Document and of registration data (email, phone number…) after having duly verified that the link between the updated registration data and the Subscriber remain accurate;
- If applicable, authentication of the Subscriber with a secure means of authentication with a remote access through a DRA portal;
- Sending of a Certificate request to the RA;
- Sending of a Certificate revocation request to the RA;
- Log trail generation and record of registration information.

All information exchanged between the RA and the DRA is exchanged securely, according to the procedures defined by the RA in its technical specifications.

The DRA obligations are defined in the contract between the RA and the DRA.

1.4. Certificate Usage

The only Certificate usage covered by this RP is to verify the electronic signature applied on documents using QUICKSIGN's registration service. QUICKSIGN is not responsible for any other use.

1.5. Policy Administration

A reference person has been assigned within the RA to:

- report all security incidents to the CA;
- manage the changes within this registration policy document upon validation of the PMA;
- ensure that the operational procedures related to the RA activity are performed in compliance with the present registration policy.

The person to contact is:

M Ahmed Boussadia
QUICKSIGN
19-21 rue Poissonnière
75002 PARIS

1.6. Definitions

Term	Definition
Authentication	A process whereby one party has presented an identity and claims to be that identity and the second party confirms that this assertion of identity is true.
Certificate	A Certificate is a data structure that is digitally signed by a Certification Authority, and that contains the following pieces of information: • the identity of the Certification Authority issuing it; • the identity of the certified Subscriber; • a public key that corresponds to a private key under the control of the certified Subscriber; • the operational period; • a serial number; • the Certificate format in accordance with ITU-T Recommendation X.509 version 3.
Certification Authority	An authority trusted by one or more users to create and assign Certificates. More specifically, in the context of this document, the CA is responsible for: • issuing Certificates; • defining rules governing user identification and ensuring they are respected; • ensuring the reliability of the digital signature service for third parties. The CA operates a CA signing platform. In the context of this document, the CA is DOCUSIGN FRANCE.
Client	An entity using the CA signing service in order to ask its Subscribers to digitally sign a submitted document. In the context of this document, the Client acts as a Delegate Registration Authority.
Delegate Registration Authority	An entity that is responsible, under RA rules and within the framework of a contract with the RA, for collecting the user identification documents, checking the user identity, collecting contact details to authenticate the user online, authenticating the users online for them to update their identification documents or

	contact details, and requesting the certificate Revocation when necessary.
Identity Documents	The user identity documents can be either: • an official identity document (passport, ID card); • or any electronic identification scheme that has been notified by a Member State to the European Commission according to article 9 of eIDAS regulation (regulation n°910/2014); or any other electronic identification document that has been issued after a face-to-face meeting during which an official identity document has been checked.
MRZ	Machine Readable Zone: a zone included in an official document that contains all the information of the document and can be read by a machine.
Qualified Certificate	A Certificate that meets the requirements listed in article 3 and in Annex I of the eIDAS regulation.
Policy Management Authority	The entity in charge of managing the PKI components and services. The PMA approves Certificate Policy (CP) and Certification Practices Statement (CPS) used to support the PKI certification services. The PMA reserves the right to audit the PKI as set in section 8 of this RP. In the context of this document, the PMA is managed by DOCUSIGN FRANCE.
Registration Authority	An entity that is responsible, under CA control and in the framework of a contract with the CA, for identifying and authenticating subjects of Certificates. Optionally, the RA can transmit the signed documents to the Subscriber and store the user registration file. In the context of this document, the RA is managed by QUICKSIGN.
Registration Officer	A person contractually or hierarchically related to the DRA, who is responsible for identifying and/or authenticating Subscribers during a face-to-face meeting. The DRA ensures that this officer has been trained to respect state-of-the-art customer due diligence rules for institutions selling financial products or equivalent rules.
Revocation	A process whereby the Operational Period of a Certificate is prematurely ended. The Operational Period for Certificates requested by the RA is defined in the CA Certificate policy.
Secure Signature Creation Device	A signature creation device meeting the requirements laid down in Directive 1999/93/EC of the European Platform and of the European Council and recognised in the eIDAS regulation under article 51.
Qualified electronic signature creation devices	A Qualified Electronic Signature Device is a Secure Signing Creation Device that is certified against ETSI EN 319-411-2 and can be used to generate a Qualified Electronic Signature.
QUICKSIGN Consent Protocol	Consent Protocol run by QUICKSIGN as the RA in the case of the collection of the handwritten signature of a Subscriber in a Face-to-Face signature process using the Tablet of a DRA.

Subscriber	The physical person receiving a Certificate from the Certification authority and using a private key that is kept in a SSCD to digitally sign the document that is sent by the Client.
Tablet	Hardware provided by the DRA in order to display and execute the Consent Protocol in a secure manner under the sole control of the Registration Officer.
Transaction Identification Number	A unique identifier that is composed randomly out of letters and digits assigned to one single request of identification and that ensures the uniqueness of the Certificate.

2. Publication and repository responsibilities

This document is published by the RA on the company's website: http://www.quicksign.com/.

It can also be published by the Policy Management Authority as an amendment to the Certificate Policy according to its own publication rules.

3. Identification and Authentication

3.1. Naming

Naming in Certificates requested by the RA complies with Recommendation ITU-T X.509 or IETF RFC 5280 and CA Certificate Policy (section 10).

3.2. Initial Identity Validation

3.2.1. Method to Prove Possession of Private Key

Proof of ownership of the private key corresponding to the Subscriber Certificate used for signing purposes is provided by the technical and organizational resources of the CA Signing Platform.

3.2.2. Authentication of Organization Identity

This part is not applicable. the RA accepts requests only from natural persons requesting qualified electronic certificates submitted on their own behalf and not for third parties, Subject being equivalent to Subscriber. Hence the RA's registration service includes no process to verify the association of a person with an organization or legal person.

3.2.3. Authentication of Physical Person Identity

First, the DRA carries out the Authentication of the physical person (Subscriber) identity, under RA rules and meeting the requirements contractually defined by the RA.

The DRA verifies at the time of initial registration, by appropriate means and in accordance with national law, the identity and, if applicable, any specific attributes of the person to whom a qualified Certificate is issued.

Evidence of the identity against a natural person is checked either:

- 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 is confirmed by a conformity assessment body.

Evidence is provided of:

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

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

The DRA collects the reference of the ID document, or, optionally, uploads a copy of the ID document. The DRA also collects the Subscriber's phone number as well as his email address. The DRA updates the registration information if it has changed.

If applicable, the DRA provides the Subscriber with a secure means of authentication securely managed by the DRA according to banking security rules, securely associated with the Subscriber and considered as controlled by the Subscriber

The DRA records the registration information for a minimum of 7 years after certificate expiration.

3.2.4. Validation of Authority

This part is not applicable. The RA accepts orders only from individuals requesting qualified electronic certificates submitted on their own behalf and not for third parties. Hence the RA's registration service includes no process to verify the association of a person with an organization or legal person.

3.2.5. Non-Verified Subscriber Information

As described above, all personal details and information to be stored in the Certificate is verified by the DRA before the RA sends any information to the CA. There is no non-verified information used by the RA to fill a Certificate.

3.2.6. Criteria for Interoperation

Certificates delivered by PKI components are managed according to the rules and requirements stated by the CA and Customer in compliance with Adobe and ETSI 319-411 requirements.

3.3. Identification and Authentication for Re-key requests

In case of a rekey request, the Subscriber's registration data is updated according to the procedure described in paragraph 3.2 of the RA's Certification Practices Statement.

3.4. Identification and Authentication for Revocation Request

The Authentication of the requester is performed by the RA following the procedure described in the Certification Practices Statement.

4. Certificate Life-Cycle operational requirements

4.1. Certificate Application

During the Subscriber's authentication, the DRA checks if the ID used during the initial registration is still valid. If the ID is not valid, the Subscriber is requested by the DRA to update his ID information. In any case, the DRA only sends to the RA the identity information registered during the initial identity validation.

In the case of the QS Consent Protocol:

- The Subscriber performs on the Tablet his/her handwritten signature in the Consent Protocol presented by QUICKSIGN during the Face to Face with the Registration Officer
- The Registration Officer verifies and compares that the handwritten signature created on the Tablet is the same as the image of the signature of the Subscriber present on the ID document presented by the Subscriber. In case of difference, the signature process is cancelled. Otherwise, the Registration Officer confirms that the handwritten signature shown in the Consent Protocol is the same as the one contained in the ID Document,

In any case, the DRA then requests a certificate. This DRA certificate request is sent securely to the RA with at least the following information:

- At least one first Name(s);
- At least one last Name(s);
- Current email address;
- Mobile Phone number;
- Information for identifying the Subscriber
    - ID Type
    - ID Number
    - ID Expiry date or issuing date
    - Country of issuing
    - Date of birth
    - Either a Copy of the official identity document with the following information readable: ID Type, ID Number, ID Expiry or issuing date, country of issuing, Date of birth
    - Optionnal: the MRZ band of the ID Document to be checked by the RA.
- DRA Officer Identification (Name, Surname, or Unique identification number) Optional : copy of the official Identity Document;
- Reference of the DRA;
- The document to be signed.

4.2. Certificate Application Processing

The RA further checks, in the RA's registration service interface, the Subscriber's identity by:

(a) asking the Subscriber to fill in a form, provided by the RA's registration service interface, with a technical challenge on the ID if the MRZ band is not provided, or
(b) By checking the validity of the MRZ band and the presence of the ID Document in the MRZ band.

In case of (a):

- if the certificate application is performed during a face-to-face meeting, the DRA ensures that only the Subscriber himself fills this form, with technical means that are under his sole control, and
- This information is collected securely by the RA according to its own procedures and on its own interface. The RA checks the consistency between the information filled in by the Subscriber in the RA interface, on the one hand, and the ID information sent by the DRA IT system, on the other hand.

If these checks cannot be performed by the RA, the RA's registration service does not send any Certificate request to the CA and rejects the application made by the Subscriber.

4.3. Certificate Issuance

In order to proceed to the Certificate Issuance, 2 cases are possible:

- Described in § 4.3.1: The authentication of the Subscriber is performed via an OTP code sent via SMS , in this case, once the registration process is completed, and the Subscriber has agreed to the terms and conditions of the service, the RA calls the CA signing platform to submit a Certificate request, transmitting the following information of the Subscriber:
  - At least one first Name(s);
  - At least one last Name(s);
  - Current email address;
  - Mobile Phone number.
- Described in § 4.3.2: The authentication of the Subscriber is performed by verification of the manual signature, in this case, once the registration process is completed, and the Subscriber has agreed to the terms and conditions of the service, the RA runs the Consent Protocol and securely calls the CA signing platform to submit a Certificate request, transmitting the following information of the Subscriber:
  - At least one first Name(s);
  - At least one last Name(s);
  - Current email address.

At the end of the process, the RA calls the CA signing platform to seal the Proof-file transmitting at least DRA certificate request information (ref §4.1. Certificate Application).

This information is exchanged securely.

4.3.1. Certificate Issuance in case of authentication of the Subscriber with an OTP code sent by SMS

The CA authenticates the RA.

The CA runs the Consent Protocol with the Subscriber in order to collect his/her consent to sign the Document and the Subscriber agreement.

The CA authenticates the Subscriber using an OTP code sent by the CA to the Subscriber by SMS on the mobile phone number transmitted by the RA.

The CA issues Certificates securely to maintain their authenticity.

The CA signs the Document with the Subscriber's private key and deletes the Subscriber's private key.

The CA makes the Certificate contained in the signed document (contained in the Proof file) available to the RA.

The RA collects the Proof file from the CA.

4.3.2. Certificate Issuance in case of authentication of the Subscriber by verification of his manual signature

The RA runs the Consent Protocol with the Subscriber in order to collect his/her consent to sign the Document and the Subscriber agreement.

The RA authenticates the Subscriber by asking the latter to affix his handwritten signature on the Consent Protocol on the Tablet. The RA then asks the Registration Officer to compare the affixed hand signature with the hand signature present on the ID Document used to identify the Subscriber. If these 2 images match, the DRA Officer is invited to validate the Subscriber Signature. The RA records this validation and authenticates the Subscriber by this action.

The RA transmits the document to be signed and the Subscriber identification to the CA.

The CA authenticates the RA. The RA securely hosts the authentication key in a certified Hardware Secure Module (FIPS 140-2 Level 3 or CC EAL 4+) that is under its responsibility.

The CA issues Certificates securely to maintain their authenticity.

The CA signs the Document with the Subscriber's private key and deletes the Subscriber's private key.

The CA makes the Certificate contained in the signed document (contained in the Proof file) available to the RA.

The RA collects the Proof file from the CA.

4.4. Certificate Acceptance

The terms and conditions (Subscriber agreement) of the service offered by the CA and the RA indicates what constitutes acceptance of the Certificate. Before entering in a contractual relationship with a Subscriber, the RA informs the Subscriber of the terms and conditions of the service regarding the use of the Certificate. These terms and conditions mention at least:

- The applicable qualified Certificate policy;
- The limitations of use of the service;
- The Subscriber's obligations;
- The Certificate terms of Revocation;
- The conditions in which registration information and event logs are recorded and archived;
- The fact that the Certificate is not published;
- The limitations of liabilities;
- Data privacy rules.

The terms and conditions are made available through a durable means of communication and signed by the Subscriber (refer to section 4.3 above).

The name and the first name of the Subscriber are mentioned on the signing page as information to be validated by the Subscriber to be included in the Certificate. The Subscriber accepts the terms and conditions of the service by ticking at least one box (refer to section 4.3 above).

If the ID was valid for the certificate request, the RA makes the signed Document with the embedded Certificate available to the Subscriber and to the DRA.

If the ID was not valid for the certificate request, then the RA does not give the signed Document with the embedded Certificate to the Subscriber and to the DRA. The DRA has a maximum of 5 days, just after certificate issuance, to check and verify the new ID document. If the new ID document is not valid, the DRA submits a Revocation request to the RA. If the new ID document has not been checked within 5 days, the RA submits a revocation request to the CA as well. In both cases, the proof file is not archived by the RA and is destroyed by the CA. If the new ID document is valid, the RA makes the signed Document with the embedded Certificate available to the Subscriber and to the DRA.

4.5. Key pair and Certificate usage

Subscribers use their private keys for the purpose set forth in section 1.4. above.

4.6. Certificate Renewal

This part is not applicable, in accordance with the CA Certificate Policy.

4.7. Certificate Re-key

Certificate re-key is performed according to the procedures described in paragraphs 4.1. to 4.4. For the Subscriber authentication, paragraph 3.3. applies.

4.8. Certificate Modification

This part is not applicable, in accordance with the CA Certificate Policy.

4.9. Certificate Revocation and Suspension

4.9.1. Circumstances for Revocation

A Revocation request is possible for 8 days after the Certificate has been issued.

4.9.2. Who Can Request Revocation

The Subscriber can submit a Revocation request to the RA in the following cases:

- DN information filled incorrectly;
- the Certificate corresponding to the private key has been lost or compromised or is suspected to be;
- the DRA failed to comply with its obligations and with the security rules described in this RP;

The DRA shall submit a Revocation to the RA in the following cases:

- DN information filled incorrectly;
- the Certificate corresponding to the private key has been lost or compromised or is suspected to be;
- the valid identity document required to fulfil a remote transaction (in case the identity document that has been used for the initial face-to-face identity validation is not valid): has been checked and is not valid;

The RA shall submit a Revocation to the CA in the following cases:

- DN information filled incorrectly;

- the Certificate corresponding to the private key has been lost or compromised or is suspected to be;
- the DRA failed to comply with its obligations and with the security rules described in this RP.

4.9.3. Revocation request procedure

If the Revocation is requested by the Subscriber, he shall address the request by sending an email to a dedicated email address of the RA. The email address, as well as the information to be included in the Revocation request, is displayed in the terms and conditions of the service. The email address is available 24 hours a day. There is no customer service that can be contacted by phone.

In order to authenticate the Revocation request, the Subscriber must be available during the eight (8) business hours following its submission. During this period of eight (8) business hours, he will be contacted by the RA Revocation Officer on the phone number provided to generate the designated Certificate. If the Subscriber does not answer the phone the Revocation request is deemed invalid and the RA shall not proceed with the Revocation request. If the Subscriber still wishes to revoke his certificate, he shall submit a new Revocation request from the begging.

When the Revocation request is authenticated, the RA follows the procedure described in paragraph 4.9.3 of the Certificate Policy. Once the CA Signing Platform has confirmed the Revocation, the RA informs the DRA and the Subscriber via e-mail within an hour. Revocation is performed in less than 24 hours.

If the Revocation is requested by the DRA, the DRA shall address the request by sending an email to a dedicated email address of the RA. The email address, as well as the information to be included in the Revocation request, is displayed in the contract between QUICKSIGN and the DRA. The email address is available 24 hours a day. After the Revocation request is authenticated, the RA follows the procedure described in paragraph 4.9.5. of the Certificate Policy. Once the CA Signing Platform has confirmed the Revocation, the RA informs the DRA and the Subscriber via e-mail within an hour. Revocation is performed in less than 24 hours.

If the Revocation is requested by the RA, the RA shall follow the procedure described in paragraph 4.9.5. of the Certificate Policy. Once the CA Signing Platform has confirmed the Revocation, the RA informs the DRA and the Subscriber via e-mail within an hour. Revocation is performed in less than 24 hours.

Revocation requests and the following actions are recorded manually by the RA.

5. Facility, Management and Operational Controls

5.1. Physical controls

All physical controls, including inspection of the premises and construction of the data center facilities being used to run the registration service are checked by an independent technical auditor.

Physical access to the RA's offices are restricted to authorized persons only. Non-authorized persons shall always be accompanied by authorized staff and their access to the offices shall be recorded. The access to the main data centers are be limited to authorized persons only.

Controls are implemented to avoid loss, damage or compromise of the assets and interruption to business activities; to avoid compromise or theft of information and information processing facilities; and to prevent RA assets from being taken without authorisation. These controls are described in the risk assessment and management process as well as in the Business Continuity Plan.

A protected security perimeter is defined to protect components that are critical against intrusion; access to that security perimeter is controlled, especially with alarms in order to detect intrusion.

5.2. Procedural controls

All roles to perform within the RA and the DRA are well identified in a way that separation of duties is implemented. Each role is described and documented and each person assigned to a role is identified.

The RA and the DRA administer user access of each role. The administration includes user account management and timely modification or removal of access. Access to information and application system functions are restricted in accordance with the access control policy. Personnel is identified and authenticated before using critical applications of the registration service, and is accountable for their activities through event log or classic log.

5.3. Personnel controls

The DRA and RA personnel in charge of the enrolment process, running the infrastructure or delivering support to Subscribers is well qualified and trained.

The DRA and RA personnel not working along the established rules and procedures shall face disciplinary sanctions according to the French labour law.

Security roles and responsibilities are documented in job descriptions and are made available to all concerned personnel. Personnel are aware of the segregation of duties and least privilege, according to the position sensitivity.

Personnel exercise administrative and management procedures and processes that are in line with the RA's information security management procedures.

Managerial personnel possess experience or training in esignature and information security.

Staff making decisions on the enrolment process is free from any conflict of interest and has full power of decision, except in crisis situations.

Personnel is formally appointed to trusted roles by senior management according to the principle of "least privilege". Personnel have access to trusted roles only after having proven their qualification for the described roles. the RA staff prove trustworthiness by presenting their criminal record as well as good references from former employers.

5.4. Audit Logging Procedures

Audit log files are generated for all events related to security and RA and DRA services. Where possible, security audit logs are automatically collected. Where this is not possible, a logbook or another physical mechanism shall be used. All security logs, both electronic and non-electronic, are retained and made available during compliance audits.

The privacy of subject information is maintained.

Audit logs are protected in such a way that only authorized users can access and/or use them. Audit logs are logged in such a way that they cannot be easily deleted or destroyed (except for transfer to long term media) within the period of time that they are required to be held. Audit logs are protected in such a way so as to remain readable for the duration of their storage period. Audit logs and audit summaries are backed up via enterprise backup mechanisms.

A vulnerability scan on public addresses is done on a monthly basis. A vulnerability scan on private IP addresses is done on a yearly basis.

Audit logs delivering information on potential malicious activity are reviewed by the system administrator on a regular basis. If a security system alerts the system administrator about a potential security issue, the logs are reviewed immediately.

5.4.1. Registration Authority

Logging includes at least the following topics:

- Physical facility access;

- Trusted roles management;
- Logical access;
- Backup management;
- Log management;
- Revocation authentication and request;
- Collect of proof file from the CA;
- Registration data sent by the DRA;
- In case of QS Consent Protocol: acceptance of the handwritten signature by the Registration Officer;
- IT and network management.

5.4.2. Delegate Registration Authority

Logging includes at least the following topics:

- the identification and the authentication of the Subscriber, including the Subscriber's ID document information, email and phone number;
- the circumstances of the identification of and the authentication of the Subscriber;
- management of the Subscriber's means of authentication;
- Logical access;
- Backup management;
- trusted role management;
- access log management; in particular, the DRA shall have a list of all the accesses that are authorized to enroll and manage Subscribers;
- IT and network management.

5.5. Records Archival

5.5.1. Registration Authority

The RA records at least:

- the following registration information:
  - Identity of the DRA;
  - The method used to validate identification documents (i.e. face-to-face meeting);
  - The role of QUICKSIGN as a RA;
  - Registration logs.
- the Subscriber's agreement to his obligations:
  - consent to the keeping of a record by the RA and/or DRA of information used in registration, any specific attributes of the subject placed in the Certificate, and the passing of this information to third parties under the same conditions as required by this policy in the case of the RA terminating its services;

- whether, and under what conditions, the Subscriber requires and the subject's consents to the publication of the Certificate;
- confirmation that the information held in the Certificate is correct.

The record is archived for at least seven years after certificate expiration.

The confidentiality and integrity of current and archived records concerning qualified Certificates is maintained. Records are completely and confidentially archived in accordance with disclosed business practices; they shall be made available if required for the purposes of providing evidence of certification for the purpose of legal proceedings. In particular, the archive system and the methods applied make sure that:

- All media being used for archiving RA records are being protected against damage and stored in access restricted areas only. The media is encrypted and needs special access control to be read;

- Media is being supervised by the archive system to identify media that is in danger of obsolescence or deterioration. Identified media has to be exchanged by the system administrator making sure that the data is not being lost or recovered from the mirror of the archive system;
- All media being used to store personal details is being deleted and destroyed at the end of its lifetime;

- All media being used in the archive system cannot being used or re-used in another context because of the encrypted file system used which is different from the ones being used to store operational data.

5.5.2. Delegate Registration Authority

The DRA records the following registration information:

- Type of document presented by the Subscriber to support registration;
- ID number or, if applicable, copy of the ID document;
- Registration logs;
- Storage location of copies of applications and identification documents, including the signed Subscriber agreement;
- Proof files for all Certificate generated by CA;
- The method used to validate identification documents (i.e. face-to-face meeting);

The record is archived for at least seven years after certificate expiration.

The confidentiality and integrity of archived records concerning qualified Certificates is maintained. Records are completely and confidentially archived in accordance with disclosed business practices; they shall be made available if required for the purposes of

providing evidence of certification for the purpose of legal proceedings. In particular, the archive system and the methods applied make sure that:

- All media being used for archiving DRA records are being protected against damage and stored in access restricted areas only. The media is encrypted and needs special access control to be read;

- Media is being supervised by the archive system to identify media that is in danger of obsolescence or deterioration. Identified media has to be exchanged by the system administrator making sure that the data is not being lost or recovered from the mirror of the archive system;

- All media being used to store personal details is being deleted and destroyed at the end of its lifetime;

- All media being used in the archive system cannot being used or re-used in another context because of the encrypted file system used which is different from the ones being used to store operational data.

5.6. Key Changeover

The Subscriber Certificate validity is defined in the CA Certificate policy.

5.7. Compromise and Disaster Recovery

QUICKSIGN has a business continuity plan. It identifies the risks and describes actions and measures to cope with incidents and other compromising events.

5.8. Termination

5.8.1. Registration Authority

If QUICKSIGN foresees a termination of its role as Registration Authority for the CA, it shall:

- give notice to the CA prior to the termination according to the procedures agreed in the commercial contract,
- send a registered letter to the PMA,
- destroy all private keys used to secure communication with CA on the day following the day of termination,
- stop to deliver Certificate requests,
- notify Subscribers and relying parties in the case that it has been compromised in its role of being Registration Authority.

The decision on the entity to which QUICKSIGN has to deliver archived records to has to be taken by the CA.

5.8.2. Delegate Registration Authority

If the DRA foresees a termination of its role as Delegate Registration Authority, it shall:

- give notice to the RA prior to the termination according to the procedures agreed in the commercial contract,
- send a registered letter to the RA,
- stop to deliver Certificate requests,
- notify Subscribers and relying parties in the case that it has been compromised in its role of being Delegate Registration Authority.

The decision on the entity to which the DRA has to deliver archived records is contractually defined between the RA and the DRA.

6. Technical Security Controls

6.1. Key pair generation and installation

The CA generates keys securely and the private key is secret. The CA verifies that the device is certified as a qualified QSCD meeting the requirements of eIDAS Regulation.

6.2. Private Key Protection and Cryptographic Module Engineering

CA key pair generation is carried out according to the CA's CP.

6.3. Other aspects of Key Pair Management

Other aspects of Key Pair Management are carried out by the CA according to the CA's CP.

6.4. Activation Data

The consent protocol, including activation data generation, installation and protection, is implemented by the CA according to its own procedures. In particular, there are two use cases to activate the private key:

- Generic use case: the Subscriber uses an OTP code generated by the CA and transmitted to the phone number registered for the Subscriber,
- QS Consent Protocol: the affix of the manual signature and the validation of the Regsitration Officer against the image of the signature contained on the presented ID Document.

6.5. Computer Security Controls

Controls (e.g. firewalls) protect the RA's and the DRA's internal network domains from unauthorized access. Firewalls are also configured by the RA and the DRA to prevent all protocols and accesses not required by relevant operation. The RA and the DRA ensure that system access is limited to properly authorized individuals.

Sensitive data is protected against being revealed through re-used storage objects being accessible to unauthorized users.

6.6. Life cycle security control

The RA and the DRA use trustworthy systems and products that are protected against modification and ensure the technical security and reliability of the processes supported by them.

An analysis of security requirements is carried out at the design and requirements specification stage of any project undertaken by the RA, in particular to ensure that security is built into the DRA IT system.

Change control procedures apply for releases, modifications and emergency software fixes for any operational software and changes to the configuration. The procedures include documentation of the changes.

The integrity of the RA's and the DRA's systems and information is protected against viruses, malicious and unauthorized software. Damage from security incidents and malfunctions is minimized through the use of incident reporting and response procedures. Media used within the RA and the DRA is securely handled to protect media from damage, theft and unauthorized access. Media management procedures protect against obsolescence and deterioration of media within the period of time that records are required to be retained. Procedures are established and implemented for all trusted and administrative roles that impact on the provision of certification services.

Procedures are specified and applied to ensure that security patches are applied within a reasonable time after they come available, that security patches are not applied if they introduce instabilities that outweigh the benefits of applying them, and that the reasons for not applying any security patches are documented and chosen by the RA and the DRA team.

6.7. Network Security Controls

The RA and the DRA maintain and protect all their systems in at least a secure zone and implement and configure a security procedure that protects systems and communications between layers of the system inside secure zones.

6.8. Time Stamping

Electronic or manual procedures are used to maintain system time. For secured time on audit records, the RA regularly synchronizes with a time service.

7. Framework for the definition of other Certificate policies built on the present document

The RA has no other Registration Policy than this document.

8. Compliance Audit and other assessments

8.1. Frequency or circumstances of assessment

8.1.1. Registration Authority

Registration Service after the end of the transitional period (art 51 of eIDAS), an ETSI evaluation according to will be carried out by an external auditor.

Before to run its service, RA shall be audited by external auditor against ETSI 319 411-2 (QCP-n-qscd).

The first year following the external audit, an audit may be performed by the CA on the RA according to the CA Signing Platform's audit program.

The second year after an external audit, a new external audit has to be performed.

In case of major findings discovered during an internal audit made by the CA, the RA will resolve these issues and an external audit will be performed within the same year.

8.1.2. Delegate Registration Authority

The RA controls the DRA's compliance with its commitments and this Registration Policy. An audit plan is defined by the RA and approved by the PMA.

The DRA accepts that the RA or the PMA will conduct a compliance audit, before starting its role as a DRA.

The DRA accepts that the RA and the PMA will conduct an audit whenever needed to ensure that it complies with this Registration Policy and with the CP.

If a major non-conformity is revealed during one of these audits, the Delegate Registration Authority shall comply without delay to the RP and the CP. If the issue is not solved within a delay determined by the auditor, the RA will suspend its services until effective compliance is achieved, under the conditions provided for in the contract between the RA and the DRA.

8.2. Topics Covered by Assessment

8.2.1. Registration Authority

The perimeter of an audit of QUICKSIGN as a Registration Authority is:

- Protection, use and management of the key pairs used to protect the communication with CA;
- Creation of the technical Certificate request;

- RA records against requirements set in the CP;
- Registration procedure defined by the RA to identify, authenticate and manage Certificate request to the CA;
- Revocation procedure;
- Trusted role management;
- IT and incidents management;
- Physical security;
- Proof file management;
- Subscriber personal data protection and management.

8.2.2. Delegate Registration Authority

The perimeter of an audit of the DRA is:

- Registration procedures requirements level defined by the RA in paragraph 1.3.2 to identify, authenticate and manage Certificate applications;
- Protection, use and management of the means used to protect the communication with the RA;
- Proof file management;
- Trusted role management;
- Subscriber secure authentication means type and management;
- IT and incidents management used to manage Subscriber and DRA portal;
- Physical security;
- Subscriber personal data protection and management.

9. Other Business and Legal Matters

9.1. Fees

These services are defined in the contract established between the RA and the DRA.

9.2. Financial Responsibility

The RA maintains reasonable levels of insurance coverage and sufficient financial resources to maintain operations. The insurance or warranty coverage is defined in the contract between the RA and the DRA.

9.3. Confidentiality of Business Information

The RA maintains the confidentiality of confidential business information, including personal identity data, Subscriber Certificate request, audit results and reports, business continuity plan and contract with the DRA.

9.4. Privacy of Personal Information

9.4.1. Registration Authority

The RA protects the confidentiality and integrity of registration data, according to the applicable European law on data privacy. The RA's set of Data Privacy Rules is documented in its ISSP. These rules are presented to each Subscriber before any transaction in the terms and conditions of the service, which have to be agreed upon by the Subscriber by clicking on a check box.

QUICKSIGN as a Registration Authority is supervised by the Data Protection Authority of Paris (CNIL) and appoints a Data Protection officer. His contact details are the following:

David Leroy

QUICKSIGN

19-21 rue Poissonnière

75002 PARIS

9.4.2. Delegate Registration Authority

The DRA protects the confidentiality and integrity of the registration data. The DRA's set of Data Privacy Rules are documented and are in compliance with the applicable European law on data privacy.

9.5. Intellectual Property Rights

This part is not applicable. The PMA maintains intellectual ownership of the CA Certificates that it publishes.

9.6. Representations and Warranties

9.6.1. Registration Authority

The RA alerts the PMA in case of a security incident.

The RA informs the Subscriber about the terms and conditions regarding the use of a Certificate before submitting a Certificate request to the CA. The Subscriber agrees to the terms and conditions of the service by clicking on a check box on the screen. The RA either sends to the Subscriber an e-mail containing the terms and conditions of the service, or, optionally, makes these terms available on its website.

The RA protects its information system and guarantees the security of the data transmitted to the PKI.

The RA authenticates the DRA and the Subscriber.

The RA approves the DRA procedure and the secure authentication means used by the DRA for subscriber authentication before authorising a DRA to use the service. The method used to authorise a DRA is approved by the PMA.

The RA establishes a contractual relationship with a DRA committing the DRA to fulfil its obligations as per the present Registration Policy

The RA shall make its best efforts to ensure over time that the DRA respects its obligations as per the present Registration Policy

The RA collaborates with the CA in the control and audit activities performed on the DRA.

The RA informs PMA for all new DRA which want to use the service and transmit a synthesis of DRA procedure.

The RA notifies the Subscriber in case the Subscriber’s private key has been lost, stolen or potentially compromised due to compromise of activation data or other reasons.

The RA makes sure that no Certificate is being used by the Subscriber or a relying party, if it has been told by the CA that the Subscriber’s Certificate has been compromised.

The RA only transmits authenticated revocation requests to the CA.

The RA shall support the audit teams in a constructive way and make any reasonable effort needed to complete an audit and to communicate the results.

In case of QS Consent Protocol, the RA shall run the Consent Protocol and the activation of the Signature with a Tablet according to the process approved by the CA.

9.6.2. Delegate Registration Authority

The DRA obligations are contractually defined between the RA and the DRA.

The DRA ensures that each Subscriber for which a Certificate application is submitted to the CA via the RA has been identified and authenticated properly and that the Certificate request has been accurate and duly authorized. The DRA makes sure that the submitted Certificate request contains accurate and complete information only.

The DRA ensures that its organization possesses the necessary expertise, reliability, experience and qualifications and has received proper training regarding security and personal data protection rules for identification and authentication in accordance with due diligence rules for institutions selling financial products or equivalent rules.

The DRA protects its information system and guarantees the security of the data transmitted to the RA.

The DRA protects the confidentiality and integrity of registration data.

The DRA must run and secure the Tablet according to the rules approved by the RA and CA.

9.7. Disclaimers of Warranties

The DRA guarantees initial identity validation and Authentication of the Subscriber. The RA guarantees that it will only enter in a contractual relationship with DRAs which are, because of the nature of the services they provide, compelled to ensure that its organization has been trained to respect state-of-the-art legal requirements for ID verification and face-to-face meeting in accordance with due diligence rules for institutions selling financial products or equivalent rules.

The RA also guarantees that it will make sure of the DRA's financial capacity. The RA provides no other warranty, express or implied, statutory or otherwise and disclaims all liability for the initial identity validation and Authentication of the Subscriber.

As a consequence, provided that the DRA has fulfilled its role as described in this document, the RA guarantees identification and authentication of the Subscriber. The RA provides no warranty, express or implied, statutory or otherwise and disclaims all liability for the success or failure of the deployment of the PKI or for the legal validity or acceptance of the CA Certificates.

9.8. Limitations of Liability

The RA makes no claim 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 RA assumes no liability in relation with the use of Certificate for any other use than that described in the present document.

The DRA is liable as regards the accuracy of all registration information, subject to the terms of the contract between The RA and the DRA. The RA has no liability for any delay, non-delivery, non-payment, misdelivery or service interruption caused by any third party, including the DRA.

9.9. Indemnities

The RA makes no claim with regard to the suitability or authenticity of Certificates issued under this RP. There is no obligation to make any payments regarding costs associated with the malfunction or misuse of personal details being verified for a Certificate request.

9.10. Term and termination

The RP and subsequent versions are effective upon approval by the PMA.

In the event that the RA ceases to operate, the RA shall follow the procedure described in paragraph 5.8. of this document.

9.11. Individual notices and communications with participants

QUICKSIGN as a Registration Authority provides a new version of this registration policy via its website.

9.12. Amendments

The RA reviews this document and its certification practices statement at least once a year. Additional reviews may be enacted at any time at the discretion of the RA. Any amendment is approved by the PMA.

9.13. Dispute Resolution Provisions

Provisions for resolving disputes between the DA and the DRA are set forth in the applicable contract between the parties.

9.14. Governing Law

Subject to any limitation in applicable law, the laws of FRANCE govern the enforceability, construction, and validity of this policy, irrespective of the contract or other choice of law provisions and without the requirement to establish a commercial nexus in FRANCE.

This governing law provision applies only to the registration policy. Contracts with a Client referring to this policy may have their own governing law provisions, provided that this section governs the enforceability, construction and validity of this policy apart from the terms of such other agreements.

9.15. Compliance with Applicable Law

This registration policy is subject to applicable French and European laws, rules, regulations, ordinances, decrees and orders. The DA and the DRA agree to comply with applicable laws and regulations in their contracts.

9.16. Miscellaneous Provisions

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 is 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 does not constitute a waiver or preclude subsequent enforcement. All provisions in this RP which by nature extend beyond the term of the performance of the services (for example confidential information and intellectual property rights) service such terms and apply to any party’s successor.

If one section of this RP is incorrect or invalid, the other sections of this RP remain in effect until the RP is updated.