REGISTRATION POLICY

Amendment to DocuSign France's Certificate Policy for using the QUICKSIGN platform as a registration service to identify Subscribers remotely

09/03/2026

QUICKSIGN 19 Rue Poissonnière, 75002 Paris | RCS: 450 439 963 Paris

Phone: 01 82 52 05 00 | www.quicksign.com

Version	1.1	
Status	☒ Draft	□ Final
Author	Ahmed Boussadia	QUICKSIGN

Mailing list	□ Internal	☒ External
		Public

History				
Version	Date	Author	Comments	Status
V.0.9	16/06/2022	A. Boussadia	Document creation	Draft
V.0.91	30/11/2022	A. Bedeau	Document update	Draft
V0.91	23/10/2023	A. Boussadia	Review and integration of compliance comments from a partner AC	Draft
V1.0	27/10/2023	A. Boussadia	Document validation following a meeting with the compliance officer of a partner AC	Valid
V1.1	19/11/2025	A. Boussadia	Generalization of RP to third-party CAs without mention of the CA	Valid
V 1.2	09/03/2026	A. Boussadia	Update of the applicable OID for DocuSign France	Valid

Table of Contents

1. Introduction

1.1. Overview

This registration policy (RP) complements the document “Certificate Policy and Public Certificate Practice Statement Protect and Sign Personal Signature : Utilisateur ETSI” of DocuSign France for the Registration Authority registration service. It explains how a Client's registration service operated by QuickSign meets the requirements for Registration Authorities (RAs) issuing advanced certificates.
In this context, the QuickSign Client acts as a Registration Authority (RA) and uses the QuickSign platform as a registration service to identify Subscribers requesting personal signatures based on Certificates issued by the Certification Authority (CA), “DOCUSIGN PREMIUM CLOUD SIGNING CA – G2 ».
This roleplay is based on:

- [PC] : 1.3.6.1.4.1.22234.2.14.3.45
- RFC 3647 "Certificate Policy and Certification Practices Framework" published by the Internet Engineering Task Force (IETF).

.

1.2. Name and identification of the document

In the context of this document, the OID of The CP to consider is:

- OID = 1.3.6.1.4.1.22234.2.14.3.45 : This profile is implemented by the CA «DOCUSIGN PREMIUM CLOUD SIGNING CA – G2 and complies with Article 26 of eIDAS.

1.3. Key Management Infrastructure (KMI) Components

1.3.1. Registration Authority (RA)

The AE, which is QuickSign's client, is an institution subject to anti-money laundering and counter-terrorist financing legislation. It is an institution supervised by a banking regulatory authority, such as the ACPR in France.
AE relies on the RA Technical Provider platform, which is owned and operated by QUICKSIGN.
The RA covers the following IGC services in all cases:

- Define the rules for entering into a relationship with the Signatory in accordance with the requirements of the banking regulator;

- Initial identification and authentication of the Subscriber in accordance with the rules established in this PE;
- The collection, verification and storage of identity documents (e.g. a national identity card) and contact information (e.g. email and mobile phone number) used to identify the Signatory;
- The collection and storage of Evidence Files generated by the RA Technical Provider;
- The implementation of the Consent Protocol using AE's Technical Provider;
- If necessary, update the official identity document and registration data (email, telephone number, etc.) after duly verifying that the link between the updated registration data and the Signatory remains accurate;
- Where applicable, authentication of the subscriber by a secure authentication method with remote access via an RA portal;
- Establishing a contractual relationship with one or more technical service providers responsible for carrying out identity verification checks;
- Creation of a logbook and recording of registration information.

1.3.2. Technical service provider for the Registration Authority

AE's technical service provider is QUICKSIGN.
The technical service provider carries out the processing defined by the RA under the security conditions compliant with this PE.
The technical service provider handles the following services:

- Send the certificate application and the documents to be signed to the AC;
- Create the Evidence File and have it sealed and time-stamped;
- Make the Evidence File available to the AE;
- Deploy the Consent Protocol;
- Retrieve the contact and identity information of the Signatory.

All information exchanged between the RA and its service provider is done so securely, according to the procedures defined by the RA in its technical specifications.
The obligations of the service provider are defined in the contract between the RA and the service provider.

1.4. Using the certificate

The only use of the Certificate covered by this RP is the verification of the electronic signature affixed to documents using the QUICKSIGN registration service. QUICKSIGN is not responsible for any other use.

1.5. Policy administration

A designated contact person has been appointed within the RA for:

- Report all security incidents to AEAE's technical service provider;
- AE's Technical Service Provider undertakes to notify the CA of any security incident

- Manage changes to this registration policy document in the event of a major change to the identity verification rules;
- Ensure that operational procedures related to RA activity are carried out in accordance with this registration policy.

The email address to contact is:

securite@quicksign.com

QUICKSIGN,

19 Rue Poissonnière, 75002 Paris.

1.6. Definitions

Term	Definition
Registration Agent	A person contractually or hierarchically linked to the Insurance Agency (IA), who is responsible for identifying and/or authenticating subscribers during a face-to-face meeting or by validating the information submitted by the subscriber. The IA ensures that this agent has been trained in compliance with best practices in customer due diligence for institutions selling financial products or equivalent regulations.
Authentication	A process by which one party presents an identity and claims to be that identity, and the second party confirms that this claim of identity is true.
Certification Authority	An authority that one or more users trust to create and issue certificates. More specifically, in the context of this document, the CA is responsible for: ● Issuance of certificates; ● To guarantee the reliability of the digital signature service for third parties. The CA operates an CA signing platform.

Registration Authority	The entity responsible for identifying and authenticating certificate subjects. Optionally, the EA can transmit signed documents to a subscriber and store the user registration file. Within this document, the EA is managed by QUICKSIGN.
Policy Management Authority	The entity responsible for managing the components and services of the IGC. The PMA approves the Certification Policy (CP) and the Statement of Certification Practices (SCP) used to support the IGC's certification services. The PMA reserves the right to audit the IGC as outlined in Section 8 of this PE.
Certificate	A certificate is a data structure that is digitally signed by a certification authority and contains the following information: ● The identity of the certification authority that issues it; ● The subscriber's identity; ● A public key that corresponds to a private key under the exclusive control of the subscriber; ● The expiry date; ● A serial number; ● The certificate format in accordance with ITU-T Recommendation X.509 version 3.
Advanced Certificate	A certificate that meets the requirements listed in Article 26 of the eIDAS Regulation.
Client	An entity using the CA's signature service and the QuickSign RA Technical Provider's technical platform to request its subscribers to digitally sign a submitted document. In the context of this document, the Client acts as the Registering Authority.
Identity documents	The user's identity documents can be either: ● An official form of identification (passport, identity card); ● Or any electronic identification system that has been notified by a Member State to the European Commission in accordance with Article 9 of the eIDAS Regulation (Regulation No 910/2014); Or any other electronic identification document that was issued after a face-to-face interview during which an official identity document was verified.

Proof File (QS)	This refers to a file generated by QuickSign, sealed in QuickSign's name and time-stamped with a qualified timestamp, containing all information related to the signing and identification of one or more signatories. A dedicated Proof File will be attached to each transaction to prove the validity of the electronic signature in the event of legal proceedings or an investigation. The Proof File is made available only to the Electronic Signature Authority (EA). The Proof File contains the name(s) of the document(s) that are the subject of the transaction.
Hash function	A cryptographic function that transforms a string of any size into a string of a fixed, and generally smaller, size. This function satisfies, among other things, two properties: ● the function is "one-way": it is difficult for an image of the given function to calculate the associated antecedent; ● the function is "collision-free": it is difficult to find two different preimages of the function having the same image.
Hash	Result of a hash function
HSM (Hardware Security Module)	CC EAL 4+ or FIPS 140-2 level 3 certified hardware cryptographic resource that is used by the CA to generate, use and manage Signatory keys.
LCBFT	Combating Money Laundering and Terrorist Financing
Transaction identification number	A unique identifier composed randomly of letters and numbers assigned to a single identification request and which guarantees the uniqueness of the Certificate.
Technical service provider for the Registration Authority	An entity that is responsible, according to the rules of the RA and under a contract with the AE, for collecting user identification documents (if applicable), verifying user identity (if applicable), collecting contact information to authenticate the user online (if applicable) and forwarding the certificate request to the CA.
Consent Protocol	This refers to the set of consent collection rules managed by the Agency and the Agency's Technical Provider for a signature operation within a given transaction, namely (i) the definition of the actions to be taken by the Signatory to sign the Document(s), (ii) the information used to create the Signatory identity, and (iii) the methods for viewing the presented Document and the associated acceptance (or refusal) message. The Consent Protocol is implemented by the Agency with the support of the Agency's Technical Provider.
Revocation	A process by which the operational period of a certificate is prematurely terminated. The operational period of certificates requested by the RA is definedin the CA certification policy. Not applicable in the context of this PE.

Signatory	The individual who receives a certificate from the certification authority and uses a private key stored in a HSM to digitally sign the document sent by the CA. The Signatory is the Holder as defined in the Certification Policy (also called a signatory).

2. Responsibilities regarding publication and archiving

This document is published by the RA on the company website [https://quicksign.com].
It can also be published by the Policy Management Authority as an amendment to the certification policy according to its own publication rules.

3. Identification and authentication

3.1. Number

The naming in the certificates requested by the RA is in accordance with ITU-T Recommendation X.509 or IETF RFC 5280 and the CA certification policy (section 10).

3.2. Initial identity validation

3.2.1. Method to prove possession of a private key

Proof of ownership of the private key corresponding to the subscriber's certificate used for signing purposes is provided by the technical and organizational resources of the CA's signing platform.

3.2.2. Organization Identity Authentication

This section is not applicable. The RA only accepts applications from natural persons requesting qualified electronic certificates in their own name and not on behalf of third parties, the subject being equivalent to the subscriber. Therefore, the RA registration service does not include any process to verify an individual's association with an organization or legal entity.

3.2.3. Authentication of the identity of the natural person

The RA verifies at the time of initial registration, by appropriate means and in accordance with national legislation, the identity and, where applicable, the specific attributes of the person to whom a certificate is issued.
Proof of a natural person's identity is verified either:

- By the face-to-face presence of the physical person and the presentation of a valid identity document;
- Remotely, through the use of the service ID Pulp provided by QuickSign. This remote identification method is an asynchronous unassisted Identity verification process. This process involves : (a) the capture of identity documents through a video capture or via NFC scanning of a compatible ID document, (b) the capture of the video of the face of the subscriber and biometric identification of the subscriber, (c) the verification of the conformity of the captured identification elements by a trained QuickSign operator. This method must be compliant with the TS 119 461 by August 29th 2027 in order to be compliant with Level of Assurance High.
- Remotely, using a notified eID of level High[1].

[1] https://ec.europa.eu/digital-building-blocks/sites/spaces/EIDCOMMUNITY/pages/48762251/Overview+of+pre-notified+and+notified+eID+schemes+under+eIDAS

The following identity and contact information is recorded by the RA:

- Subscriber name (including family name and at least one first name in accordance with national identification practices);
- Email ;
- Telephone number;
- If applicable: The 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 other persons with the same name;

- If applicable: information of the face to face agent performing the identification and place of identification.

Where appropriate, the RA provides the subscriber with a secure authentication method managed by the RA, securely associated with the subscriber and considered to be controlled by the subscriber.
The RA records the registration information (proof file) for a period of time of at least 7 years after the expiration of the generated certificate.

3.2.4. Validation of authority

This section is not applicable. The RA only accepts orders from individuals requesting electronic certificates submitted in their own name and not on behalf of third parties. Therefore, the RA registration service does not include any process for verifying an individual's association with an organization or legal entity.

3.2.5. Unverified information about the subscriber

As described above, all personal details and information to be stored in the certificate are verified by the RA (first and last name). No unverified information is used by the RA to complete a certificate.

3.2.6. Interoperability criteria

Certificates issued by PKI components are managed according to the rules and requirements set forth by the CA and the client, in accordance with Adobe requirements.

3.3. Identification and authentication for renewal requests

Not applicable because the certificates have a lifespan of 5 minutes plus 1 hour.
A new Certificate cannot be provided to the Signatory without renewing the corresponding key pair. The procedure for a new Certificate is either the same as the initial procedure (see § 3.2) or equivalent. For example, the Client can authenticate the Signatory once and provide them with login credentials for their Client portal, ensuring that it is indeed the

Signatory logging in. In this case, it will be necessary to regularly verify the Signatory's identity (first and last name, at least every 10 years for the identity) and that the means used for the Consent Protocol are still valid (email and telephone numbers).

3.4. Identification and authentication for the revocation request

Not applicable because the certificates have a lifespan of 5 minutes plus 1 hour.

4. Operational requirements of the certificate lifecycle

4.1. Certificate application

The RA requests a certificate following the collection of information from the Signatory (see § 3.2). This certificate request is sent securely to the RA Technical Provider with at least the following information:

- At least one first name(s);
- At least one surname;
- Current email address;
- Mobile phone number;
- If applicable, a copy of the official identity document with the following information legible: Ty RP of identity document, identity document number, expiry or issue date of the identity document, country of issue, date of birth.
- The document to be signed.

4.2. Processing of certificate requests

The RA verifies the information collected in Section 3.2 according to its own rules. The RA may define rules for automatically validating certificate requests, enabling the generation of advanced certificates without human validation. These rules must be reviewed by the RA. The RA verifies the identity of the Signatory before or after the Certificate request and therefore the signing process. In all cases, the Signatory's contact and identity information must be retrieved and verified by the RA before publishing the certificate (and thus the signed document) to the subscriber.
These controls are documented in internal RA documents, they are carried out by technical means specific to the RA or via its technical service provider.

4.3. Issuance of the certificate

To generate the Certificate, the subscriber is authenticated via an OTP code sent by SMS. The documents to be signed, the Signatory's information, and their consent to sign are processed within the framework of the Consent Protocol implemented by the RA using the RA Technical Provider's platform. Once the registration process is complete, and the Signatory has accepted the terms and conditions of the service, the RA provider calls the CA's signature platform to submit a Certificate request, transmitting the following subscriber information:

- At least one first name(s);
- At least one surname;
- The hash of the document(s) to be signed.

This information is exchanged securely.

4.3.1. Certificate issuance process

The CA authenticates the RA provider.
The CA (a) generates a Certificate, (b) signs the hash(s) of the Document(s) to be signed, with the Signatory's private key, (c) then deletes the Signatory's private key, (d) timestamps, and (e) if necessary affixes an electronic seal according to the choice of the AE's Technical Provider.
The CA makes the certificate and the result of the signature available to the RA provider.
The RA provider retrieves the certificate generated by the CA along with the signed hashes and generates a document in PDF format conforming to the PDF/A standard.
At the end of the process, the RA provider generates a proof file containing traces of events and seals it. The RA technical provider calls the CA's signature platform to seal and timestamp the Proof File by transmitting at least the certificate request information (ref § 4.1. Certificate Request).
The RA provider makes the Proof File available to the RA.
The RA must in all cases retrieve the Proof File for all Signatories and keep it (See § 5.5).

4.4. Acceptance of the certificate

Before entering into a contractual relationship with a Subscriber, the RA collects the subscriber's consent under the Consent Protocol.
The subscriber's first and last name are listed on the Consent Protocol page as information that the subscriber must validate in order to be included in the Certificate. The subscriber gives their consent by checking at least one box.
If the Subscriber's identity was deemed valid for the certificate application according to the AE's rules, the RA makes the signed document with the integrated certificate available to the Subscriber.
Otherwise, the RA does not give the signed document with the integrated certificate to the subscriber and destroys it.

4.5. Using the key pair and the certificate

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

4.6. Certificate renewal

This section is not applicable, in accordance with the CA certification policy.

4.7. Re-key of the certificate

The certificate re-key is carried out according to the procedures described in paragraphs §4.1. to §4.4. For subscriber authentication, paragraph 3.3. applies.

4.8. Certificate modification

This section is not applicable, in accordance with the CA certification policy.

4.9. Revocation and suspension of certificates

This section is not applicable, in accordance with the CA certification policy.

5. Controls of facilities, management and operations

5.1. Physical checks

Physical access to the premises housing the information system and the personnel implementing the services of the RA and the RA Technical Provider is restricted to authorized personnel only. Unauthorized individuals must always be accompanied by authorized personnel, and their access to the offices must be logged. Access to the main data centers is limited to authorized personnel only.
Controls are in place to prevent the loss, damage, or compromise of assets and the disruption of business operations; to prevent the compromise or theft of information and information processing facilities; and to prevent the unauthorized removal of the assets of the Enterprise and the Enterprise's Technical Provider. These controls are described in the risk assessment and management process and the business continuity plan.
A security perimeter is defined to protect critical components against intrusions; access to this security perimeter is controlled, notably by alarms to detect intrusions.

5.2. Procedure checks

All trusted roles within the RA and the AE's Technical Provider are clearly defined to ensure the separation of duties is implemented. Each role is described and documented, and each person assigned to a role is identified by name.
The Accounting Authority (AA) and the AA's Technical Provider administer access for each role. This administration includes managing user accounts and modifying or deleting access in a timely manner. Access to information and application system functions is restricted according to the access control policy. Staff are identified and authenticated before using critical registration service applications and must report their activities through the event log or traditional log.

5.3. Staff checks

The staff of the RA and the RA Technical Provider responsible for the operation of the infrastructure or the implementation of this RP are qualified and trained.
AE and RA Technical Provider staff who do not comply with established rules and procedures are subject to disciplinary sanctions in accordance with French labor law.
Security roles and responsibilities are documented in job descriptions and made available to all relevant staff. Staff are aware of the separation of duties and the principle of least privilege, depending on the sensitivity of the position.
Staff apply administrative and management procedures and processes that are consistent with the information security management procedures of the RA and the RA Technical Provider.

The management staff have experience or training in electronic signatures and information security.
Staff who make decisions regarding the onboarding process are free from any conflict of interest and have full decision-making power, except in the event of a crisis.
Staff are formally appointed to trusted roles by the EA and the EA Technical Provider according to the principle of least privilege. Staff are only granted access to trusted roles after demonstrating their qualifications for the roles described. EA and EA Technical Provider staff demonstrate their reliability by submitting a criminal record check and positive references from previous employers.

5.4. Audit logging procedures

Audit log files are generated for all events related to the security and services of RA and AE's Technical Provider. Where possible, security audit logs are collected automatically. When this is not possible, a logbook or other physical mechanism is used. All security logs, whether electronic or not, are retained and made available during compliance audits.
The confidentiality of information on the subjects is preserved.
Audit logs are protected so that only authorized users can access and/or use them. Audit logs are stored in a way that prevents them from being easily deleted or destroyed (except for transfer to long-term storage) during their retention period. Audit logs are protected to remain readable throughout their retention period. Audit logs and audit summaries are backed up using enterprise backup mechanisms.
A vulnerability analysis of private and public IP addresses is performed on a monthly basis.
Audit logs providing information on potential malicious activity are reviewed regularly by the system administrator. If a security system alerts the system administrator to a potential security issue, the logs are reviewed immediately.

5.4.1. Registration Authority

The log includes at least the following topics:

- Access to physical facilities;
- Management of trusted roles;
- Logical access;
- Backup management;
- Log management;
- Collection of the evidence file;
- Management of registration data;
- Information technology and network management;
- Identification and authentication of the subscriber;
- The circumstances of the subscriber's identification and authentication;

- Management of subscriber authentication methods;
- Management of trusted roles;

5.5. Document archiving

5.5.1. Registration Authority

The RA records at least:

- The method used to validate the Subscriber's identity;
- Documents used to verify the identity of the Signatory;
- The identity and contact information of the Signatory;
- The Subscriber's consent.

The file and the Proof File are archived, whether or not the Signatory wants products from the signed Documents and whether or not the Signatory's identity is valid, for a period in accordance with banking regulations and for at least 5 years to comply with the PC.

The confidentiality and integrity of current and archived certificate records are maintained. Records are archived fully and confidentially in accordance with disclosed business practices; they are made available if necessary to provide evidence of certification for legal proceedings. In particular, the archiving system and methods applied ensure that:

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

- The storage media are monitored by the archiving system to identify those that are at risk of becoming obsolete or deteriorating. Identified media must be exchanged by the system administrator, ensuring that data is not lost or recovered from the archiving system's mirror.
- All media used to store personal data are deleted and destroyed at the end of their lifespan;
- Not all media used in the archiving system can be used or reused in another context because of the encrypted file system used, which is different from those used to store operational data.

5.6. Key change

The validity of the subscriber's certificate is defined in the CA's certificate policy.

5.7. Compromise and recovery after a disaster

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

5.8. Termination

5.8.1. Registration Authority

If QUICKSIGN plans to terminate its role and that of the Technical Provider of the RA for the AC, it will have to apply the reversibility clause defined in the contract between the CA and the RA provider.

If the RA plans to terminate its role as AE, then the RA shall retain its Evidence File in accordance with the rules of this RP and make it available on request from the CA for 5 years, for audit and investigation purposes arising from a French administrative authority, from the end of the contract.

6. Technical safety checks

6.1. Generating and installing key pairs

The CA manages the Signatories' keys in accordance with the AC's PC.

6.2. Private key protection and cryptographic module engineering

The Signatory activates their private signing key using an OTP code received on their mobile phone, which must be entered into the Consent Protocol interface.

6.3. Other aspects of key pair management

The other aspects of key pair management are performed by the CA in accordance with the CA's PC.

6.4. Activation data

The consent protocol, including the generation, installation and protection of activation data, is implemented by the RA according to the procedures of the RA Technical Provider.
The OTP code is generated by the RA Provider and delivered by the RA Provider to the Signatory. A different code is required for each transaction.

6.5. Computer security controls

Controls (e.g., firewalls) protect the internal network domains of the EA and the EA's Technical Provider from unauthorized access. The firewalls are also configured by the EA and the EA's Technical Provider to block all protocols and access not required for relevant operations. The EA and the EA's Technical Provider ensure that system access is restricted to duly authorized personnel.
Sensitive data is protected from disclosure by reused storage objects accessible to unauthorized users.

6.6. Safety monitoring throughout the lifecycle

The RA and the RA Technical Provider use trustworthy systems and products, protected against any modification and guaranteeing the technical security and reliability of the processes they support.

A security requirements analysis is carried out at the design and requirements specification stage of any project undertaken by the RA and the AE's Technical Provider.

Change control procedures apply to versions, modifications, and emergency software fixes for all operational software and configuration changes. These procedures include documenting the changes.
The integrity of the systems and information of the Certification Authority (CA) and the CA's Technical Provider is protected against viruses, malware, and unauthorized access. Damage caused by security incidents and malfunctions is minimized through the use of incident reporting and response procedures. Media used within the CA and the CA's Technical Provider are handled securely to protect them against damage, theft, and unauthorized access. Media management procedures protect against obsolescence and deterioration of media during the document retention period. Procedures are established and implemented for all trusted and administrative roles that impact the delivery of certification services.
Procedures are specified and applied to ensure that security patches are applied within a reasonable time after they are made available, that security patches are not applied if they introduce instabilities that outweigh the benefits of their application, and that the reasons for not applying security patches are documented and chosen by the RA and the AE's Technical Provider.

6.7. Network security controls

The RA and the RA Technical Provider maintain and protect their systems in at least one secure area and implement and configure a security procedure that protects systems and communications between system layers within secure areas.

6.8. Timestamp

Automatic (e.g., NTP synchronization) or manual procedures are used to maintain the system time. To ensure accurate timekeeping for audit records, the auditing firm and its technical service provider regularly synchronize with a time service.

7. Profil de Certificat, CRL et OCSP.

Cf. PC de l'AC.

8. Compliance audit and other assessments

8.1. Frequency or circumstances of the assessment

The registration service is audited regularly by the banking authorities applicable to the RA.
In the event of a critical security incident or at the request of a regulator and in accordance with the AC's PC, the RA and the AE's Technical Provider may be audited by DocuSign France in order to verify compliance with this RP and PC.

8.2. Topics covered by the assessment

The Accounting Authority (AC) may conduct checks on registration activity in the event of suspected fraud detected by the CA or as part of an audit of the Accounting Entity (AE) and the AE's Technical Provider as defined in the AC's Policy. The sole purpose of this audit will be to verify that the rules of this Policy and the contracts that implement it are fully understood and correctly implemented.

9. Other legal matters and issues

9.1. Registration fees

These services are defined in the contract established between the RA and the AE's technical service provider.

9.2. Financial responsibility

The RA maintains reasonable levels of insurance coverage and sufficient financial resources to maintain operations. The insurance or guarantee coverage is defined in the contract between the RA and the AE's technical service provider.

9.3. Confidentiality of business information

AE maintains the confidentiality of confidential business information, including personal identity data, the subscriber's certificate application, audit results and reports, the business continuity plan and the contract with AE's service provider.

9.4. Confidentiality of personal information

The Agency and its Technical Provider protect the confidentiality and integrity of registration data in accordance with applicable European data privacy legislation. All of the Agency's and its Technical Provider's data privacy rules are documented in their Information Security Policy (ISSP). These rules are presented to each subscriber before any transaction in the service's terms and conditions, which must be accepted by the subscriber by clicking a checkbox.
QUICKSIGN, as the Technical Service Provider for the AE, and the RA comply with the French Data Protection Act and the GDPR. QuickSign has appointed a Data Protection Officer. Their contact details are as follows:

dpo@quicksign.comQUICKSIGN

19 Rue Poissonnière, 75002 Paris

9.5. Intellectual property rights

This section is not applicable. The PMA retains the intellectual property rights to the CA certificates it publishes.

9.6. Declarations and warranties

The RA alerts the RA Technical Provider in the event of a security incident.
The AE's Technical Provider alerts the CA in the event of a security incident.

The RA collects the Subscriber's consent. The Subscriber accepts the terms and conditions of the service by clicking a checkbox on the screen.
AE protects its information system and guarantees the security of data transmitted to AE's technical service provider.
The RA establishes a contractual relationship with the RA Technical Provider, committing the latter to fulfill its obligations in accordance with this registration policy.
The RA complies with its obligations under this registration policy.
The RA ensures that each Subscriber for whom a certificate request is submitted to the CA via the RA provider has been identified and authenticated in accordance with its procedures and that the certificate request was accurate and duly authorized.

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

The RA protects its information system and guarantees the security of the data collected.
The RA protects the confidentiality and integrity of registration data.
The RA retains all Evidence Files of all Signatories for a minimum of 5 years.
The RA guarantees compliance of the validation rules of the onboarding process with a Signatory with regard to its banking regulator and this PE.

9.7. Exclusion of warranties

Non applicable.

9.8. Limitations of liability

The RA assumes no responsibility in connection with the use of the certificate for any purpose other than that described in this document.
The RA is responsible for the accuracy of all registration information, subject to the terms of the contract between the RA and its technical service provider. The RA is not liable for delays, non-delivery, non-payment, incorrect delivery, or service interruptions caused by any third party, including the AE's technical service provider.

9.9. Compensation

The compensation in the event of liability of the RA is defined in the general terms of use of the RA service which the Signatory accepts before being able to sign in accordance with this PE.

9.10. Duration and termination

The RP and its subsequent versions enter into force upon their approval by the RA.
In the event that the RA ceases to function, the RA must follow the procedure described in paragraph 5.8 of this document.

9.11. Individual notices and communications with participants

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

9.12. Amendments

QUICKSIGN reviews this document at least once a year. Further revisions may be made at any time at QUICKSIGN's discretion.

9.13. Provisions relating to the settlement of disputes

The provisions relating to the settlement of disputes between RA and AE's Technical Provider are set out in the applicable contract between the parties.

9.14. Applicable law

Subject to any limitations under applicable law, the laws of FRANCE shall govern the execution, construction and validity of this policy, regardless of contractual provisions or any other choice of law and without the need to establish a commercial relationship in FRANCE.
This applicable law provision applies only to the registration policy. Contracts with a client that reference this policy may have their own applicable law provisions, provided that this section governs the applicability, interpretation, and validity of this policy regardless of the terms of those 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 RA and the RA service provider agree to comply with applicable laws and regulations in their contracts.

9.16. Miscellaneous provisions

This Agreement constitutes the entire agreement between the parties and supersedes all other terms, whether express or implied by law. No modification of this Agreement shall be effective unless made in writing and signed by an authorized signatory. The failure to enforce any or all of these sections in a particular instance shall not constitute a waiver of such provision and shall not preclude subsequent enforcement. All provisions of this Agreement that, by their nature, extend beyond the term of the services (for example,

confidential information and intellectual property rights) shall be enforceable against the successor of either party.

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