Remote QSCD Management Policy
Provision of a Server Signature Application Service (SSASP)

ISSUER	RECIPIENTS	CC
CERTINOMIS	PUBLIC	

Certinomis

Docaposte Certinomis SAS with a capital of €40,156.

Head office: 45-47, Boulevard Paul Vaillant-Couturier

94200 Ivry sur Seine – France. Créteil Trade and Companies Register B 433 998 903

History of the versions

DATE	VERSION	DEVELOPMENTS	AUTHOR
30/09/2025	0.1	Document creation	Y. THOMASSIER
23/12/2025	1.0	Initial document	Y. THOMASSIER
20/02/2026	1.1	Supplement following the rQSCD qualification audit	Y. THOMASSIER

Table of contents

WARNING

1 INTRODUCTION

1.1 OVERVIEW

1.1.1 Certinomis QES service

The QES (Qualified Electronic Signature) service of Docaposte Certinomis is used by signature-creation applications (SCAs) to generate the qualified electronic signature of a document hash.

To this end, the Service generates and manages the lifecycle of an individual's or professional's private signing key (Signatory).

The QES Service is in contact with the Service for issuing the qualified signature certificate of a CA, for which it manages the private keys associated with the public keys that the latter has certified.

1.1.2 Purpose of the document

The document describes the Server Signature Application Service Policy applied to the QES Service provided by Docaposte Certinomis.

The Policy covers the management of the signature key pair on behalf of a Signatory, associated with the signature certificate issued by the Certinomis CA, within a QSCD-level remote cryptographic device (HSM).

The Policy also covers the exclusive use of the Signatory's private signature key for calculating the cryptographic value of electronic signatures of hashes of electronic documents.

The Policy complies with Appendix A of the [ETSI 119 431-1] standard.

1.2 DOCUMENT IDENTIFICATION

The Object Identifier (OID) designation of this document is: 1.2.250.1.86.7.1.1.1

This document covers a single Signature Server Application Policy, for which an OID has been assigned.

The ETSI Policy adopted as the basis is specified in the table below.

OID	*Usage*	*ETSI / RGS Compliance*
1.2.250.1.86.7.1.1.1	Qualified policy for the remote production management of QSCD	EUSPv2: 0.4.0.19431.1.1.4

1.3 ENTITIES INVOLVED IN THE SERVICE

1.3.1 Server Signature Application Service Provider

The company Docaposte Certinomis is the Server Signature Application Service Provider (SSASP).

Docaposte Agility provides it with the Signatory's Identification and Authentication Service for a private signature key. Identification and authentication are carried out by various technical means, depending on the use.

Docaposte Certinomis is also a qualified electronic certification service provider (ECSP) within the meaning of the RGS and the eIDAS regulation. Through this qualified Service, it manages the qualified signature certificates of the Signatories, associated with the key pairs managed in the remote QSCD.

1.3.2 Service Subscribers and Signatories

Docaposte Certinomis client entities (Subscribers) interface via APIs with the Service and implement signature creation applications (SCA) within the meaning of the standard [ETSI 119431-1].

The SCAs interact with the service to request from it:

- The creation of a key pair within the remote QSCD, for a Signatory duly identified and authenticated by the Service;
- The cryptographic calculation of an electronic signature, for a duly authenticated signatory, based on a supplied document hash, using the signatory's private key managed within the remote QSCD.

The Signatories are customers of the Service Subscribers. This guarantees them exclusive access to their signature private key associated with their qualified signature certificate, stored in the remote QSCD,

1.4 USE OF THE SERVICE

The Service is consumed by signature creation applications (SCA), in contractual relationship with Docaposte Certinomis and produces a qualified signature within the meaning of the eIDAS v2 regulation.

1.5 POLICY MANAGEMENT

This Policy applies to the QES service for remote QSCD management by Docaposte Certinomis.

This Policy is reviewed and updated annually.

The French version of this document shall be the reference. This document is also translated into English.

1.5.1 Entity managing the Policy

This Service Policy for the Server Signature Application is the responsibility of Docaposte Certinomis.

1.5.2 Contact point

Certinomis general manager
45-47, Boulevard Paul Vaillant-Couturier
94200 Ivry sur Seine
Telephone: 0810 184 956
Email: ld-Politiquecertification@certinomis.fr

1.5.3 Entity determining compliance of a DPSSAS with this Policy

The Management of Certinomis determines the compliance of the Statement of Service Practices of the Server Signature Application Service (DPSSAS) with the PSSAS Policy, either directly or indirectly through the use of independent experts specialised in the field of security and Trust Services.

The Management of Docaposte Certinomis has appointed a compliance officer from among the company's employees, responsible, among other things, for regularly monitoring changes in the requirements of the eIDAS regulation and the ETSI standards referenced by the acts implementing this regulation.

1.5.4 DPSSAS compliance approval procedures

Docaposte Certinomis guarantees the application of the DPSSAS with the PSSAS Policy.

Docaposte Certinomis is responsible for the management (updating, revisions) of the DPSSAS. Any request to update the DPSSAS follows the approval process put in place.

A body of the Policy Management Authority (PMA) may request the review of the DPSSAS in accordance with the procedures in force.

1.6 DEFINITIONS AND ACRONYMS

1.6.1 Acronyms

The acronyms used in this Policy are as follows:

- CA Certification Authority
- RA Registration Authority
- API Application Programming Interface
- PMA Policy Management Authority
- CC Common Criteria
- DPSSAS Server Signature Application Service (SSAS) Practice Statement
- ECDSA Elliptic Curve Digital Signature Algorithm
- ETSI European Telecommunications Standards Institute
- IDP IDentity Provider
- OID Object Identifier
- PKI Public Key Infrastructure
- PSSAS Server Signature Application Service (SSAS) Policy
- ECSP Electronic Certification Service Provider
- RIVP Remote Identity Verification Provider
- QSCD Qualified Signature Creation Device
- RSA Rivest Shamir Adelman
- SAD Signature Activation Data
- SAP Signature Activation Protocol
- SCA Signature Creation Application
- SAM Signature Activation Module
- ISS Information Systems Security
- SSAS Server Signature Application Service (SSAS)
- URL Uniform Resource Locator

1.6.2 Definitions

Certification Authority (CA):

Within an ECSP, a Certification Authority looks after, in the name and under the responsibility of this ECSP, the application of at least one Certification Policy and is therefore identified as the issuer (certificate's "issuer" field), in the certificates issued pursuant to this Certification Policy. As part of this CP, the term ECSP is not used elsewhere than in the present chapter and chapter 1.1, while only the term CA is used. It appoints Docaposte Certinomis responsible for the application of the Certification Policy, meeting the requirements of this CP, within the ECSP wishing to have the corresponding family of certificates qualified.

Policy Management Authority (PMA):

For the uses that relate to it, the Policy Management Authority determines the security-related needs and requirements in the overall process for the certification and usage of the certificates. It establishes guidelines, which may take the form of a Policy canvas to be followed by all Certification Authorities it accredits. It validates and monitors any change to the certification policies of the Certification Authorities that it accredits.

It plays the role of a moral authority, and its accreditation indicates the trust that one can put in a Certification Authority.

Certificate:

Electronic attestation that links the data related to the encryption or verification of signatures, exchanges, messages and electronic documents to a subject, in order to ensure their confidentiality or to ensure their authentication and integrity.

Signatory

A natural person, identified in accordance with the Certificate's PC, and authenticated by the identity provider (IDP), who has a pair of signature keys generated by the SERVICE and which they use, under their sole control, to perform the electronic document signature.

Subscriber

Legal entity that contracts with Docaposte Certinomis for the use of the Server Signature Application to interface it through an API with its signature-creation application (SCA).

Policy:

Set of rules, identified by a name (OID), defining the requirements with which an entity complies in the implementation and provision of its services and indicating the applicability of a certificate to a particular community and/or a class of applications with common security requirements. A POLICY may also, if necessary, identify obligations and requirements relating to other stakeholders, including beneficiaries and users of certificates.

Signature Server Application Practice Statement (DPSSAS):

A DPSSAS identifies the practices (organisation, operational procedures, technical and human resources) that the SERVICE applies in the context of the provision of its Signature Server Application Services to users and in accordance with the Signature Server Application Policy(ies) that it has undertaken to comply with.

Electronic Certification Service Provider (ECSP):

Any person or entity that is responsible for the management of electronic certificates throughout their life cycle, vis-à-vis the beneficiaries and users of these certificates. An ECSP can provide various families of certificates corresponding with different purposes and/or different security levels. An ECSP has at least one CA, but can have several based on its organisation. An ECSP's various CAs can be independent of one another and or linked by hierarchical or other links (Root CAs / Daughter CAs). An ECSP is identified in a certificate for which it is responsible through its CA that issued this certificate, which is itself directly identified in the certificate's "issuer" field.

Service:

Means the Signature Server Application Service, within the meaning of the ETSI standard 119 431-1, operated by Docaposte Certinomis.

2 RESPONSIBILITIES REGARDING THE PROVISION OF INFORMATION HAVING TO BE PUBLISHED

2.1 ENTITIES IN CHARGE OF PROVIDING INFORMATION

The information is made available by Docaposte Certinomis, through its website https://www.certinomis.com.

2.2 INFORMATION HAVING TO BE PUBLISHED

Docaposte Certinomis is obliged to publish at least the following information to users of its Service:

- This Policy
-

2.3 PUBLICATION TIMEFRAMES AND FREQUENCIES

Information relating to the service must be published whenever necessary to ensure that published information is always consistent with the service provider's actual commitments, resources and procedures.

In particular, any new version must be communicated to Subscribers (SCA clients of the Service) with reasonable notice before its publication. The systems publishing this information must be available on working days and during working hours.

2.4 PUBLISHED INFORMATION ACCESS CONTROL

All published information is freely accessible in read-only mode.

Access to modify publication systems (addition, deletion, modification of published information) must be strictly limited to authorised internal roles within Docaposte Certinomis, at least through an access control based on long passwords and a strict password management policy.

Docaposte Certinomis SAS with capital of 40,156 euros.
Head office: 45-47 Boulevard Paul Vaillant-Couturier
94200 Ivry-sur-Seine. Créteil Trade and Companies
Register B 433 998 903

3 INITIALISATION OF THE SIGNATURE KEY

3.1 GENERATION OF THE SIGNATURE KEY

Signatories' private signature keys must be generated in a QSCD-level hardware device (certified in accordance with EN 419 241-5).

The private signature keys thus generated must remain in the hardware device. A secure protocol, an integral part of the security target of the hardware device, must allow the synchronisation of keys between all the hardware devices comprising the Service.

The modules of signature key pairs must be generated using the RSA or ECDSA algorithm and must be 3072 or 4096 bits long for RSA, and at least the P-256 for ECDSA.

The signature key pair of a Signatory is generated by the Service and, simultaneously, the corresponding signature certificate must be signed by the ECSP CA.

In the case of ephemeral certificates (lifespan of 30 minutes), the Signatory's signature key pair must be generated and used during the same and single signature session.

3.2 MEANS OF IDENTIFICATION

The Signatory must be identified by the CA in accordance with the Certificate's PC (for example through an identification service provided by a qualified RIPV, a high-level electronic identification means, or during a face-to-face identity verification). They must accept the CA's General Conditions of Use before being issued his signature certificate.

The Signatory must be authenticated before signing either:

- using the La Poste Digital Identity (LPDI) application (digital identity notified at the substantial level)
- using an OTP / SMS transmitted to their mobile phone and entered within the same session
- using an OTP / SMS sent to their mobile phone and entered under the supervision of a notary.

These means of authentication require prior enrolment by the CA of the LPDI identifier or the Signatory's mobile phone.

Authentication may be delegated to an external IDP and must in all cases result in an access token containing a unique identifier for the Signatory.

The IDP must ensure that the identification presented by the authentication method used by the Signatory matches the identity associated with their signature certificate.

If the Signatory's authentication is delegated to an external IDP, authentication with the QSCD SAM module must be carried out using a token, derived from the identification token issued by the IDP and signed by a signature key residing in an HSM.

Where applicable, Docaposte Certinomis must ensure coverage of the requirements incumbent on the external IDP.

In the case of ephemeral certificates, the identification, key generation and authentication of the Signatory must be carried out within the same functional session

3.3 LINK WITH SIGNATURE CERTIFICATE

The Signatory's signing certificate and private signing key must be associated in the Service's QSCD.

The electronic signature created by the Signatory using their private key must be produced after the issuance of their signature certificate by the CA.

The CA PKI and the QSCD SAM module must ensure the integrity of the signature key and the corresponding certificate.

3.4 PROVISION OF THE MEANS OF IDENTIFICATION

Not Applicable, Docaposte Certinomis does not provide any means of identification to the Signatories.

4 LIFE CYCLE OF THE SIGNATURE KEY

4.1 ACTIVATION OF THE SIGNATURE

The Signatory's private signature key must be activated under the Signatory's exclusive control.

Activation of the private key requires successful authentication of the Signatory. The activation of the signature must necessarily follow an explicit action by the Signatory, in order to proceed with the electronic signature of documents.

Activation data (SAD) must be sent directly to the QSCD SAM module. An SAD may contain the references to several documents that will be signed during the same session.

The activation protocol (SAP) must ensure that the signature is produced from the data sent by the Signatory, using their private signing key.

The private key access token must contain the Signatory's unique identifier and the reference of its issuer.

The signature request must come from an SCA with which Docaposte Certinomis has a contractual relationship. The consent of the Signatory of the private key, through the SCA's General Conditions of Use, governs the use of electronic signatures.

The selected algorithms must be deemed reliable for use in electronic signatures. The following are deemed reliable:

- RSA keys with a module length of at least 2048 bits (certificates generated before 31/12/2025)
- RSA keys with a module length of 3072 bits or more (certificates generated after 31/12/2025)
- ECDSA keys whose algorithm is at least P-256
- The SHA-2 family hash algorithms

4.2 DELETION OF SIGNATURE KEYS

The signature key pair must be deleted from the QSCD following expiry or revocation of the associated signature certificate.

4.3 BACKUP AND RESTORATION OF SIGNATURE KEYS

The signature key pairs generated by the Service must remain in the QSCDs.

The contents of the QSCDs comprising the Service must be synchronised with each other.

5 NON-TECHNICAL SECURITY MEASURES

5.1 PHYSICAL SECURITY MEASURES

The technical rooms, which house the hardware devices that comprise the Service, must be well protected against intrusions.

The level of protection of the technical premises is essential to ensuring the security of the Service's resources and their operation.

5.1.1 Geographical location and construction of the sites

This Policy does not set out any specific requirements regarding the geographical location of sites.

The construction of the sites must comply with the regulations and standards in force and, where applicable, specific requirements in the face of risks such as earthquakes or explosions (proximity to an area of factories or warehouses of chemical products, etc.).

5.1.2 Physical access

In order to avoid any loss, damage and compromise of the resources of the SERVICE and the interruption of the Docaposte Certinomis Services, access to the premises of the various components of the SERVICE must be controlled.

Access must be strictly limited to persons authorised to enter the premises and the traceability of access must be ensured. Outside working hours, security must be reinforced by the implementation of physical and logical intrusion detection means.

In order to ensure the availability of the systems, access to the machines must be limited only to persons authorised to perform operations requiring physical access to the machines.

Note - Machines mean all servers, cryptographic boxes, stations and active elements of the network used to implement these functions.

5.1.3 Power supply and air conditioning

The characteristics of the electrical power supply and air conditioning equipment must make it possible to comply with the conditions of use of the equipment of the Service as set by their suppliers.

They must also enable compliance with the requirements of this Policy, as well as the commitments made by Docaposte Certinomis in its DPSSAS, in terms of the availability of its functions.

5.1.4 Vulnerability to water damage

The means of protection against water damage must make it possible to comply with the requirements of this Policy, as well as the commitments made by Docaposte Certinomis in its DPSSAS, regarding the availability of its functions.

5.1.5 Fire prevention and protection

The means of fire prevention and fighting must make it possible to comply with the requirements of this Policy, as well as the commitments made by Docaposte Certinomis in its DPSSAS, in terms of the availability of its functions.

5.1.6 Safekeeping of media

As part of the risk analysis, the various information involved in the activities of the SERVICE must be identified and their security needs defined (in terms of confidentiality, integrity and availability).

Docaposte Certinomis must maintain an inventory of this information. Docaposte Certinomis must put in place measures to avoid the compromise and theft of this information.

The media (paper, hard drive, USB stick, DVD / CD, etc.) corresponding to this information must be managed according to procedures that comply with these security requirements. In particular, they must be handled securely in order to protect the media against damage, theft and unauthorised access.

Management procedures must protect these media against obsolescence and deterioration during the period in which Docaposte Certinomis undertakes to retain the information they contain.

5.1.7 Media taken out of service

At their end-of-life, the media must be either destroyed or reinitialised for reuse, depending on the confidentiality level of the corresponding information.

The procedures and means of destruction and reset must comply with this level of confidentiality.

5.1.8 Backups

The components of the Service, with the exception of the QSCD, must implement remote backups enabling the rapid resumption of these functions following the occurrence of a disaster or an event that severely and permanently affects the provision of these services (destruction of the site, etc.).

The information backed up must comply with the same requirements of this Policy regarding the protection of confidentiality and integrity of such information.

5.2 PROCEDURAL SECURITY MEASURES

5.2.1 Trust roles

Each component of the Service distinguishes at least the following seven functional trust roles:

Security Manager - The Security Manager is responsible for implementing the Component Security Policy. They manage the controls on the physical access to the component's system hardware. They are authorised to review the archives and are in charge of analysing the event logs in order to detect any incident, anomaly, attempted compromise, etc.

Application Manager - The Application Manager is responsible, within the component to which they report, for implementing the Policy and reporting SERVICE practices at the application level for which they are responsible. Their responsibility includes all of the functions provided by this application and the corresponding performances.

System Engineer - They are in charge of the start-up, configuration and technical maintenance of the component's IT hardware. They provide the technical administration of the component's systems and networks.

Operator - An operator within a component of the Service carries out, as part of their responsibilities, the operation of applications for the functions implemented by the component.

Controller - A person designated by a competent authority whose role is to regularly perform compliance checks on the implementation of the functions provided by the component with respect to the Certification Policies, statements of Service certification practices and the Security Policies of the component.

In addition to these trust roles within each component of the Service, Docaposte Certinomis also distinguishes, as a trust role, the roles of holder of shares of secrets of the Service.

These bearers of secret shares are responsible for ensuring the confidentiality, integrity and availability of the shares entrusted to them.

5.2.2 Number of persons required per task

Depending on the type of operation undertaken, the number and capacity of the persons that must be present, as participants or witnesses, can be different.

For security reasons, sensitive functions are allocated between several persons. This Policy sets out a number of requirements regarding this allocation, in particular for operations related to the Service's cryptographic modules.

5.2.3 Identification and authentication for each role

All Docaposte Certinomis staff members must have their identity and authorisations verified before:

- their name is added to the list of access to the premises of Docaposte Certinomis; or
- their name is added to the list of persons authorised to physically access the Docaposte Certinomis system.

All participants in the Docaposte Certinomis system, or another component of the SERVICE, must have their identity and authorisation verified before:

- a certificate can be provided to them in order to carry out their assigned role; or
- a system account can be opened in their name.

Each of these certificates and accounts (with the exception of the signature certificates of Docaposte Certinomis):

- is assigned directly to a person;
- must not be shared;
- should only be used for the tasks authorised for the assigned role; a control mechanism is in place.

Remote operators working on the Docaposte Certinomis system must be identified using strong cryptographic mechanisms.

Docaposte Certinomis and the components of the Service ensure that any verification process they use makes it possible to supervise all the activities of the persons who hold privileged roles within them.

5.2.4 Roles requiring a separation of duties

Several roles can be assigned to a given person, provided that this accumulation of duties does not compromise the security of the implemented functions.

With regard to trust roles, the following positions must not be aggregated:

- security manager and system engineer / operator
- controller and any other role
- system engineer and operator

5.3 SECURITY MEASURES RELATIVE TO THE PERSONNEL

5.3.1 Required qualifications, skills and authorisations

The manager of Docaposte Certinomis must ensure that all members of staff who perform tasks relating to the operation of the Service:

- are appointed to a position with a detailed and written description;
- are linked by contract or by law to the positions that they occupy;
- have received the necessary training to perform their tasks;
- are required by contract or by law not to disclose information relating to the security of Docaposte Certinomis, clients or Signatories; a confidentiality clause is expressly included in the employment contracts of Docaposte Certinomis staff members;

5.3.2 Background verification procedures

Each entity operating a component of the Service must implement all legal means at its disposal to ensure the honesty of its personnel working within the component. In particular, these members of staff must not have a criminal conviction that is incompatible with their duties.

In this respect, the employer may ask these employees to provide a copy of bulletin no. 3 of their criminal record.

The employer may decide, if the employee refuses to provide this copy or if there is a court ruling incompatible with the employee's duties, to withdraw those duties from the employee.

Persons with a trust role must not be affected by conflicts of interest that are detrimental to the impartiality of their duties.

These checks must be conducted prior to being assigned to a trust role and reviewed regularly (at least every 3 years).

5.3.3 Requirements regarded to initial training

Staff must be previously trained in the software, hardware and internal operating and security procedures that they implement and must comply with, corresponding to the component in which they operate.

Personnel must be aware of and understand the implications of the operations for which they are responsible.

5.3.4 Continuing training requirements and frequency

The personnel concerned must receive adequate information and training prior to any changes in the systems, procedures, organisation, etc., depending on their nature.

5.3.5 Rotation frequency and sequence between the various duties

Not applicable.

5.3.6 Penalties in case of unauthorised actions

The sanctions must be specified in the DPSSAS.

5.3.7 Requirements relative to the personnel of external service providers

The personnel of external service providers working on the premises and/or on the components of the Service must also comply with the requirements of this chapter 5.3. This must be translated into adequate clauses in contracts with these service providers.

5.3.8 Documentation provided to the personnel

Each staff member must have at least adequate documentation regarding the specific operational procedures and tools they implement and the General Policies and Practices of the component in which they work. In particular, the Security Policy(ies) concerning them must be provided to them.

5.4 AUDIT DATA ESTABLISHMENT PROCEDURES

The logging of events involves making a record of these events, either manually or electronically by means of input or automatic generation.

The resulting files, in paper or electronic form, make it possible to trace and attribute the operations carried out.

5.4.1 Types of events to be logged

With regard to the systems linked to the functions that are implemented within the framework of the Service, each entity operating a component of the Service must at least log the events described below, in electronic form. Logging must be automatic, from the start of a system and without interruption until the system stops.

- creation / modification / deletion of user accounts (access rights) and of the corresponding authentication data (passwords, certificates, etc.);
- start-up and shutdown of the IT systems and applications;
- events related to logging: start and stop of the logging function, modification of the logging parameters, actions taken following a failure of the logging function;
- Events related to changes to audit parameters;
- connection / disconnection of users having trust roles, and any corresponding unsuccessful attempts.

Other events must also be collected, by electronic or manual means. These concern security and are not automatically produced by IT systems, in particular:

- the physical access points;
- the maintenance activities and changes to system configurations;
- changes to personnel;
- the actions to destroy and reinitialise storage media containing confidential information.

In addition to these logging requirements common to all components and functions of the Service, events specific to certain Service functions must also be logged, in particular:

- events related to the signature key pairs (generation and destruction);
- events related to electronic signatures executed;
- events related to the authentication of the Signatory and the management of signature data;

Each record of an event in a log must contain at least the following fields:

- type of event;
- name of the operator or reference of the system triggering the event;

- date and time of the event (the exact time of significant events of Docaposte Certinomis concerning the environment, key and certificate management must be recorded);
- outcome of the event (failure or success).

The accountability for an action lies with the person, organisation or system that executed it. The name or identifier of the executor must be explicitly indicated in one of the fields of the event log.

In addition, depending on the type of event, each record must also contain the following fields:

- recipient of the transaction;
- name of the requester of the operation or the reference of the system that made the request;
- name(s) of the people present (if this is an operation requiring several people);
- cause of the event;
- any information characterising the event (for example, for the generation of a certificate, the serial number of that certificate).

Logging operations must be carried out during the process.
In the case of manual entry, the entry must be made, subject to exceptions, on the same working day as the event.

The specific events and data to be logged must be documented by Docaposte Certinomis.

5.4.2 Processing frequency for event logs

See chapter 5.4.8.

5.4.3 Retention period for events logs

Event logs must be kept on site for at least one (1) month. They must be archived as soon as possible after their generation and at the latest within one (1) month (overlap possible between the on-site retention period and the archiving period).

5.4.4 Protection of the events logs

Logging must be designed and implemented in such a way as to limit the risks of circumvention, modification or destruction of event logs. Integrity control mechanisms must be in place to detect any voluntary or accidental modification of these logs.
Event logs must be protected to ensure availability (against partial or total loss and destruction, whether deliberate or not).
The event dating system must comply with the requirements of chapter 6.2.
The definition of the sensitivity of event logs depends on the nature of the information processed and the profession. It may result in a need for confidentiality protection.

5.4.5 Backup procedure for events logs

Each entity operating a component of the Service must implement the required measures to ensure the integrity and availability of event logs for the relevant component, in accordance with the requirements of this PC.

5.4.6 Collection system for event logs

Event logs must be forwarded to centralised log repositories in order to facilitate their processing.

5.4.7 Notification of an event's logging to the person responsible for the event

Not applicable.

5.4.8 Evaluation of vulnerabilities

Each entity operating a component of the Service must be able to detect any attempted violation of the integrity of the component in question.

Event logs must be checked once (1) per business day, in order to identify anomalies related to failed attempts.

The logs must be analysed in their entirety at least once every two weeks and as soon as an anomaly is detected.

This analysis will result in a summary in which the important elements are identified, analysed and explained. The summary must show the anomalies and falsifications found.

Furthermore, a reconciliation between the various function event logs that interact with each other must be carried out at least once a month, in order to verify the concordance between dependent events and thus contribute to revealing any anomaly.

5.5 DATA ARCHIVING

5.5.1 Types of data to be archived

Archiving arrangements must also be made by Docaposte Certinomis. This archiving must ensure the sustainability of the logs represented by the various components of the Service.

It must also allow the storage of paper documents related to technical operations.

The data to be archived are at least the following:

- software programs (executables) and configuration files for IT hardware;
- the Policies;
- the DPSSAS;
- contractual agreements with the CA;
- the event logs of the various entities of the Service

5.5.2 Retention period of the archives

5.5.2.1 Event logs

The event logs covered in chapter 5.4 must be archived for ten (10) years from the date of their creation. The measures put in place by Docaposte Certinomis for their archiving must provide the same level of security as that envisaged at the time of their creation. In particular, the integrity of records must be ensured throughout their life cycle.

5.5.3 Protection of the archives

For the entire duration of their retention, the archives and their backups must:

- be protected intact;
- be accessible to authorised persons;
- to be re-read and reused

Docaposte Certinomis will specify in its DPSSAS the measures put in place to archive the documents securely.

A copy of all archived or backed up IT materials is protected either solely by physical security measures, or by a combination of physical and cryptographic measures. The archiving site adequately protects the materials against natural dangers, for example excess temperatures, humidity and magnetism.

Docaposte Certinomis will verify the integrity of its archives at least every six (6) months.

In addition, the information stored or backed up by Docaposte Certinomis may be subject to the laws and regulations in force and applicable to archiving and retention.

5.5.4 Backup procedure for the archives

The level of protection of backups must be at least equivalent to the level of protection of the archives.

5.5.5 Data time-stamping requirements

Cf. chapter 5.4.4 for the dating of events logs.

Chapter 6.8 presents the requirements with regard to dating / time-stamping.

5.5.6 Archive collection system

The record collection system, whether internal or external, must comply with the requirements for the protection of the archives concerned.

5.5.7 Archive recovery and verification procedures

The (paper and electronic) archives must be able to be recovered within a period of less than two (2) working days, bearing in mind that only Docaposte Certinomis can access all the archives (as opposed to an entity operating a component of the Service which can only recover and consult the archives of the component in question).

5.6 RECOVERY AFTER COMPROMISE AND DISASTER

5.6.1 Procedure for forwarding and handling incidents and compromising

Each entity operating a component of the Service must implement procedures and means for reporting and processing incidents, in particular through awareness-raising and training of its personnel, and the analysis of the various event logs. These procedures and resources must make it possible to minimise damage due to security incidents and malfunctions.

In the case of a major incident, such as the loss, suspected compromise or actual compromise, theft of the private key of Docaposte Certinomis, the triggering event is the detection of this incident within the affected component, which must immediately inform Docaposte Certinomis. In the event of a major incident, it must be dealt with immediately upon detection, and, if applicable, information on certificate revocation must be published urgently

by any available means (press, website, acknowledgement of receipt, etc.). Docaposte Certinomis must also directly and immediately notify the contact point identified on the website https://cyber.gouv.fr.

Any practice not in compliance with the Policy or the DPSSAS currently in force must be considered an incident. A major non-compliance in the context of a certification audit must also be considered an incident.

Every incident must be reported and communicated to the appropriate authority.

The incident handling procedure must be specified in the DPSSAS.

If one of the algorithms, or associated parameters, used by Docaposte Certinomis or its servers becomes insufficient for the remainder of its intended use, then Docaposte Certinomis must:

- inform all clients (SCA) with whom Docaposte Certinomis has entered into agreements.

5.6.2 Recovery procedures in case of corruption of IT resources (hardware, software and/or data)

Each component of the Service must have a business continuity plan to meet the availability requirements of the different functions of the Service and the commitments of Docaposte Certinomis in its own policy.

This plan must be tested at least once every two years.

5.6.3 Business continuity capacities after a disaster

The various components of the Service must have the necessary means to ensure the continuity of their activities in accordance with the requirements of this Policy.

5.7 END OF LIFE OF THE SERVICE

One or more components of the Service may cease their activity or transfer it to another entity for various reasons.

Docaposte Certinomis must take the necessary measures to cover the costs to meet these minimum requirements in the event that Docaposte Certinomis is bankrupt or for other reasons is unable to cover these costs on its own, this, as far as possible, depending on the constraints of the applicable bankruptcy legislation.

The transfer of activity is defined as the end of the activity of a component of the Service that does not affect the validity of the key signature pairs produced prior to the transfer in question and the resumption of this activity organised by Docaposte Certinomis in collaboration with the new entity.

Cessation of activity is defined as the end of activity of a component of the Service having an impact on the validity of the key signature pairs produced prior to the cessation in question.

5.7.1 Transfer of activity or cessation of activity affecting a component of the Service

In order to ensure a constant level of confidence during and after such events, Docaposte Certinomis must, among other obligations, fulfil the following:

- Establish procedures whose objective is to ensure a constant Service, particularly in terms of archiving;
- Insofar as the planned changes may have an impact on the commitments vis-à-vis the Signatories of the signature key pairs, Docaposte Certinomis shall notify them, where necessary, within three months;
- Docaposte Certinomis must communicate to the contact point identified on the website https://cyber.gouv.fr/, the principles of the action plan implementing the technical and organisational means intended to deal with a cessation of activity or to organise the transfer of activity. In particular, it will present the systems put in place in terms of archiving in order to carry out or have carried out this function over the entire period initially provided for in its Policy. Docaposte Certinomis must communicate to ANSSI, for the various SERVICE components concerned,

the details of any changes that have occurred. Docaposte Certinomis will measure the impact and make an inventory of the consequences (legal, economic, functional, technical, communication, etc.) of this event. It shall present a plan of action designed to remove, or reduce the risk for the applications and any difficulties for subjects and users of certificates;

- Docaposte Certinomis must keep ANSSI informed of any obstacles or further delays encountered during the process.

5.7.2 Cessation of activity affecting Docaposte Certinomis

Cessation of activity may be total or partial (for example: cessation of activity for a given family of certificates only). The partial cessation of activity is gradual, so that only the obligations referred to below are to be performed by Docaposte Certinomis or a third-party entity taking over the activities.

In the event of total cessation of activity, Docaposte Certinomis or, in the event of impossibility, any entity replacing it by the effect of a law, a regulation, a court decision or an agreement previously concluded with this entity, must ensure the revocation of the certificates and the publication of the CRLs in accordance with the commitments made in this CP.

Docaposte Certinomis must include in its procedures the measures taken in the event of cessation of service. They must include:

- Notification of the entities affected;
- Transfer of its obligations to other parties;
- The deletion of the Bearers' signature key pairs.

6 TECHNICAL SECURITY MEASURES

6.1 MANAGEMENT OF SYSTEMS AND SECURITY

The Service supports privileged roles represented by various roles of trust, defined in chapter 5.3.1.

The rules set out in chapter 5.2.4 of this policy must be followed when assigning roles of trust.

Users who have system privileges must be identified by name and trained in the activities they will perform on the system. Only these users must have access to the QSCD of the Service. They must have extended privileges to administer the QSCD through a dedicated interface.

The Service also supports unprivileged roles:

- The Signatory is authorised to access the Service via the SAD using the SAP protocol, to request the electronic signature of data;
- The SCA (Subscriber) is authorised to send the data to be signed by the Signatory to the Service;
- The PKI (of the ECSP CA) is authorised to provide the Service with the Signatory's signature of signature certificate.

No user should have both a trust role and a non-privileged role.

6.2 SYSTEMS AND OPERATIONS

The Service and its technical components must be documented (DAT and DEX) in order to be operated in a secure manner, deployed while minimising the risk of failure and being protected against viruses and malware.

The clocks of the Service components must be synchronised to a reliable time source, referenced to UTC time.

6.3 SECURITY MEASURES FOR IT SYSTEMS

6.3.1 Technical security requirements specific to IT systems

A minimum level of security assurance provided for the SERVICE's IT systems must be defined in the internal DPSSAS of Docaposte Certinomis. It must meet at least the following security objectives:

- identification and strong authentication of users for system access (two-factor authentication, physical and/or logical),
- management of user rights (enabling the implementation of the Access Control Policy defined by Docaposte Certinomis, in particular the principles of least privilege, multiple controls and separation of duties),
- management of user sessions (disconnection after a period of inactivity, access to files controlled by role and user name),
- protection against computer viruses and all forms of compromising or unauthorised software and updates,
- management of user accounts, including the rapid modification and deletion of access rights,
- protection of the network against any intrusion by an unauthorised person,
- protection of the network in order to ensure the confidentiality and integrity of the data passing through it,
- audit functions (non-repudiation and nature of the actions performed),
- if necessary, management of retries on error.

Applications using component services may require additional security measures.

The protection of confidentiality and integrity of private or secret infrastructure and control keys (see chapter 1.4.1.2) must be subject to specific measures, which may result from the risk analysis.

Monitoring devices (with automatic alarms) and procedures for auditing system settings (in particular routing elements) must be put in place.

Docaposte Certinomis. must bring its practices into line with the ANSSI documents relating to the protection of the RA application workstation and the Docaposte Certinomis workstation.

In particular, Docaposte Certinomis must apply all the rules defined in the IT hygiene guide published by the ANSSI for the “standard” level.

6.3.2 IT systems security evaluation level

See Appendix 2 for requirements regarding the QSCD component of the Service.

6.4 SECURITY MEASURES FOR THE SYSTEMS DURING THEIR LIFECYCLE

6.4.1 Security measures linked to the development of the systems

The implementation of a system to implement the components of the SERVICE must be documented and must comply, as far as possible, with modelling and implementation standards. The system configuration of the components of the SERVICE as well as any modifications and upgrades must be documented and controlled.

Docaposte Certinomis must:

- guarantee that the safety objectives are defined during the specification and design phases,
- use reliable systems and products that are protected against modification.

6.4.2 Measures related to security management

Any significant change to a system or to a component of the SERVICE must be reported to Docaposte Certinomis for validation. It must be documented, included in the internal operating procedures of the relevant component, and comply with the conformity assurance maintenance scheme for evaluated products.

6.4.3 Security evaluation level of the systems lifecycle

Not applicable.

6.5 NETWORK SECURITY MEASURES

Interconnection to public networks must be protected by security gateways configured to accept only the protocols necessary for the operation of the component within the Service.

Docaposte Certinomis must guarantee that the components of the local network (e.g. routers) are kept in a physically secure environment and that their configurations are periodically audited to verify their compliance with the requirements specified by Docaposte Certinomis.

In addition, exchanges between components within the Service may require the implementation of specific measures depending on the level of sensitivity of the information (use of separate / isolated networks, implementation of cryptographic mechanisms using infrastructure and control keys, etc.).

7 COMPLIANCE AUDIT AND OTHER EVALUATIONS

This chapter only concerns the audits and assessments under the responsibility of Docaposte Certinomis in order to ensure the proper functioning of its Service.

7.1 FREQUENCY AND/OR CIRCUMSTANCES OF THE EVALUATIONS

Before the first commissioning of a component of its Service or following any significant modification within that component, Docaposte Certinomis must carry out a compliance check of the latter.

Docaposte Certinomis must also carry out a biennial compliance check of its entire Service.

7.2 IDENTITIES / QUALIFICATIONS OF THE EVALUATORS

The control of a component must be assigned by Docaposte Certinomis to a team of auditors competent in information system security and in the field of activity of the component controlled.

7.3 RELATIONS BETWEEN EVALUATORS AND THE EVALUATED ENTITIES

The audit team may not belong to the entity operating the component of the controlled Service, regardless of that component, and be duly authorised to perform the controls in question.

7.4 TOPICS COVERED BY THE EVALUATIONS

Compliance controls relate to a component of the Service (spot checks) or to the entire architecture of the Service (periodic checks) and are intended to verify compliance with the commitments and practices defined in this Policy and in the DPSSAS that responds to it as well as the resulting elements (operational procedures, resources implemented, etc.).

7.5 ACTIONS TAKEN AFTER THE CONCLUSIONS OF THE EVALUATIONS

At the end of a compliance check, the audit team gives Docaposte Certinomis one of the following opinions:

- “success”,
- “failure”,
- “to be confirmed”.

Depending on the rendered opinion, the consequences of the control are the following:

- In case of failure, and depending on the significance of the non-conformities, the audit team issues recommendations to Docaposte Certinomis which may be the (temporary or permanent) cessation of activity, the revocation of the certificate of the component, the revocation of all the certificates issued since the last positive control, etc. The choice of the measure to be applied is made by Docaposte Certinomis and must comply with its internal security policies.
- In the event of a "To be confirmed" result, Docaposte Certinomis gives the component an opinion specifying within what time frame the non-conformities must be repaired. A “Confirmation” control will then serve to verify that all of the critical points have been resolved.
- If successful, Docaposte Certinomis confirms to the controlled component that it complies with the requirements of this Policy and the associated DPSSAS.

7.6 COMMUNICATION OF THE RESULTS

The results of the compliance audits are made available to the qualification body in charge of the qualification of Docaposte Certinomis.

If the audit report contains information concerning the security of Docaposte Certinomis or information that it considers confidential, the report will not be published. A summary or extracts of the report may be obtained in electronic form upon express request.

Compliance audit certificates are made available to the public. A copy may be obtained in electronic form upon express request.

8 OTHER BUSINESS LINE AND LEGAL ISSUES

8.1 FINANCIAL LIABILITY

8.1.1 Insurance coverage

The guarantee associated with the electronic signature calculated by the Service is limited to the amount provided for in the contract. For any commercial transaction, or electronic exchange, the direct or indirect financial consequences of which are of an amount greater than the amount provided for, the parties involved in the Service may not be held liable vis-à-vis customers, beneficiaries and third-party users.

8.1.2 Other resources

No particular requirement.

8.1.3 Coverage and guarantee regarding the user entities

Electronic signatures guaranteed by this Policy carry a guaranteed level of assurance, specified by contract and accessible to the relying party.

8.2 CONFIDENTIALITY OF PERSONAL DATA

8.2.1 Perimeter of the confidential information

The following information is considered to be confidential:

- the private keys of the Signatories,
- the activation data associated with the private keys of the Signatories,
- all the secrets of the Service,
- the event logs of the components of the Service,
- The internal procedures and policies of Certinomis.

8.2.2 Information outside of the perimeter of confidential information

Not applicable.

8.2.3 Responsibilities for the protection of confidential information

Docaposte Certinomis is required to apply security procedures to guarantee the confidentiality of the information identified in chapter 8.2.1 in particular with regard to the permanent erasure or destruction of the media used to store it.

In addition, when this data is exchanged, Docaposte Certinomis must guarantee its integrity.

Docaposte Certinomis is required to comply with the legislation and regulations in force in France.

8.3 PROTECTION OF PERSONAL DATA

8.3.1 Personal data protection policy

European Regulation (EU) 2016/679 of 27 April 2016 on the protection of personal data as well as Law No. 78-17 of 6 January 1978 on information technology, files and freedoms amended by Law No. 2004-801 of 6 August 2004 on the protection of natural persons with regard to the processing of personal data applies to all documents held or transmitted by Docaposte Certinomis or by one of the components of the Service (CNIL website http://www.cnil.fr).

Pursuant to the laws, Subscribers and the Signatories have a right of access, rectification and opposition to the transfer of any information concerning them. This right may be exercised through the Service Agent, in particular the RA of the ECSP CA, having collected this information, at the address shown on the Docaposte Certinomis website.

Docaposte Certinomis rigorously complies with all applicable legal requirements and explains on its website the concrete terms of application of the law, particularly in the sections "legal notices & management of personal data".

The Policy complies with the fundamental principles of the protection of personal data enshrined in the law, the GDPR and any other international conventions that have entered into force.

8.3.2 Personal data

All data collected and held by Docaposte Certinomis relating to a natural or legal person are considered confidential and may not be disclosed without the prior consent of the Signatory.

Information concerning the identification or other personal data of the Signatory appearing on the certificates is considered confidential, unless the beneficiary has given its express prior consent to any distribution.

8.3.3 Non-personal data

Not applicable.

8.3.4 Responsibility for the protection of personal data

Cf. legislation and regulations in effect within France (notably cf. chapter 10 below)

8.3.5 Notification and consent to use personal data

Cf. legislation and regulations in effect within France (notably cf. chapter 10 below)

8.3.6 Conditions for the disclosure of personal information to legal or administrative authorities

Cf. legislation and regulations in effect within France (notably cf. chapter 10 below)

8.3.7 Other circumstances of disclosure of personal data

French law guarantees the secrecy of correspondence issued using telecommunication means. Any violation is punishable by article 226-15 of the criminal code for violations committed by an individual, and by articles 432-9 and 432-7 of the criminal code for violations committed by a person in a position of public authority.

In general, no employee of Docaposte Certinomis and no employee or subcontractor, in the context of their participation in the certification Services, has the right to intercept, open, divert, disclose, search for or use the documents submitted to Docaposte Certinomis, except in the cases provided for in this Policy, or within the framework of the regime of interceptions ordered by the judicial authority or security interceptions pursuant to law no. 91-646 of 10 July 1991.

8.4 INTELLECTUAL PROPERTY RIGHTS

All intellectual property rights held by Certinomis are protected by applicable law, regulations and other international conventions. Civil and criminal liability can result from non-compliance with them. For example, in accordance with Law No. 98-536 of 1 July 1998 (Official Journal of 2 July 1998, p.10075) and European Directive 96/6/EC of 11 March 1996, the databases produced by Certinomis are protected. The text of the law can be consulted on the following website: http://www.legifrance.gouv.fr.

8.5 CONTRACTUAL INTERPRETATIONS AND GUARANTEES

This chapter contains provisions relating to the respective obligations of Docaposte Certinomis, the personnel of Docaposte Certinomis, the various entities comprising the Service, the customers, and the Signatories. It also contains legal provisions, notably relative to the applicable law and the resolution of disputes.

The obligations common to the components of the Service are as follows:

- protect and guarantee the integrity and confidentiality of their secret and/or private keys,
- use their cryptographic keys (public, private and/or secret) only for the purposes provided for at the time of their issue and with the tools specified under the conditions set out in the Docaposte Certinomis Policy and the resulting documents,
- comply with and apply the part of the DPSSAS incumbent upon them (this part must be communicated to the corresponding component),
- accept the compliance checks carried out by the audit team mandated by Docaposte Certinomis (see chapter VIII) and the qualification body,
- comply with the agreements or contracts between them or with the CMs,
- document their internal operating procedures,
- implement the (technical and human) resources necessary for the performance of the services to which they are committed under conditions guaranteeing quality and safety.

8.5.1 Server Signature Application Provider

Docaposte Certinomis is required to:

- ensure that signature requests are made by authenticated users, using secure authentication methods.
- implement security mechanisms to ensure that signed data cannot be modified without being detected.
- prevent any unauthorised access to the data.
- ensure the resilience of the Service and the ability to recover quickly in the event of a breakdown.

Docaposte Certinomis is responsible for the compliance of its policy with the requirements set out in the applicable reference frameworks for the relevant security level. Docaposte Certinomis assumes any harmful consequences resulting from non-compliance with its CP, by itself or one of its components. It must make the necessary

arrangements to cover its responsibilities related to its operations and/or activities and have the financial stability and resources required to operate in accordance with this Policy.

In addition, Docaposte Certinomis acknowledges that it is liable in the event of fault or negligence, of itself or of one of its components, regardless of the nature and seriousness thereof, which would result in the reading, alteration or misappropriation of the personal data of the CM for fraudulent purposes, whether such data is contained or in transit in the Docaposte Certinomis certificate management applications.

Furthermore, Docaposte Certinomis acknowledges that it has a general duty to monitor the security and integrity of the certificates issued by it or one of its components. It is responsible for maintaining the level of security of the technical infrastructure on which it relies to provide its Services. Any modification having an impact on the level of security provided must be approved by the higher management of Docaposte Certinomis.

8.5.2 Signatories

The Signatory must comply with all requirements of this Policy.

It undertakes to comply with the contract binding it to the CA, which has delegated to the Service the management of the key pairs of signature of the Bearers of Signature Certificates that it issues.

If they suspect that a private key has been compromised, they must so inform the CA as quickly as possible, and according to the instructions provided by the latter.

Under no circumstances does the Signatory acquire ownership of the signature key pair issued by Docaposte Certinomis. They only acquire a usage right. Consequently all signature key pairs remain the property of Docaposte Certinomis which issued them.

8.6 GUARANTEE LIMIT

The generation and management of a signature key pair, in accordance with this Policy, does not make Docaposte Certinomis, any component of the Service, the person responsible for Docaposte Certinomis, Docaposte Certinomis personnel or other Service components a trustee, agent, guarantor or other representative of the beneficiary, the client or any other concerned party. Each party undertakes not to assume any commitment on behalf and in the name of the other party, which it can under no circumstances replace.

As a result, the Signatories and clients are legally and financially independent persons and, as such, do not have the power to represent or bind Docaposte Certinomis or any component of the Service liable to create legal obligations, either expressly or tacitly, on behalf of Docaposte Certinomis or any component of the Service. The Signature Server Application Services do not constitute a partnership or create any legal form of legal association that would impose liability based on the actions or deficiencies of the other. The contract constitutes neither an association, nor a company or other consortium, nor a mandate given by either of the parties to the other.

8.7 LIMIT OF LIABILITY

Docaposte Certinomis, the personnel of Docaposte Certinomis, the components of the Service, the customers, the beneficiaries, the third party users are liable for any damages arising from non-compliance with their respective obligations as defined under the terms of this Policy and the associated DPSSAS.

Docaposte Certinomis details the scope of liability limits in its DPSSAS.

8.8 COMPENSATION

The parties agree that in the event that any liability of one of the parties is found towards the other, the damages and indemnities incumbent upon it, for all causes combined, shall under no circumstances exceed the limits of liability mentioned in the contract concluded between Docaposte Certinomis and its client.

8.9 DURATION AND EARLY EXPIRY OF THE POLICY

8.9.1 Validity period

This Policy remains in force until the end of the life of the last certificate issued on the basis of a key pair generated by this Policy.

8.9.2 Early end of the validity

The publication of a new version of this Policy may lead, depending on the changes made, to the need for Docaposte Certinomis to change its corresponding DPSSAS.

Depending on the nature and importance of the changes made to the Policy, the deadline for compliance will be determined in accordance with the procedures provided for by the regulations in force.

8.9.3 Effects of the end of validity and clauses remaining in effect

Not applicable.

8.10 INDIVIDUAL NOTIFICATIONS AND COMMUNICATIONS BETWEEN PARTICIPANTS

In the event of a change of any kind occurring in the composition of the SERVICE, Docaposte Certinomis shall:

- no later than one month before the start of the operation, have this change validated through technical expertise, in order to assess the impacts on the level of quality and safety of the functions of Docaposte Certinomis and its various components;
- at the latest one month after the end of the operation, so inform the qualification institution.

8.11 POLICY AMENDMENTS

This chapter defines the requirements for the administration and management of this Certification Policy.

8.11.1 Amendment procedures

Docaposte Certinomis must ensure that any proposed modification to its POLICY remains compliant with the requirements of the applicable ETSI reference documents and any additional documents. In the event of a major change, Docaposte Certinomis will call on technical expertise to check the impact.

8.11.2 Mechanism and information period for amendments

No special requirement.

8.11.3 Circumstances in which the OID must be changed

The OID of the Docaposte Certinomis Policy must be updated whenever major changes occur in the requirements applicable to the Service.

8.12 PROVISIONS REGARDING THE RESOLUTION OF CONFLICTS

Docaposte Certinomis shall put in place policies and procedures for the handling of complaints and the resolution of disputes from entities for which it provides trusted electronic services or other matters related thereto.

8.13 COMPETENT JURISDICTIONS

This Certification Policy is expressly developed, governed, applied and interpreted in accordance with French laws and regulations, although the activities that result from this Policy may have legal effects outside the territory of the French Republic.

8.14 COMPLIANCE WITH LAWS AND REGULATIONS

The laws and regulations applicable to this Policy are, in particular, those set out in chapter 10 below.

8.15 MISCELLANEOUS PROVISIONS

8.15.1 Overall agreement

Not applicable.

8.15.2 Transfer of activities

Cf. chapter 5.8.

8.15.3 Consequences of an invalid clause

The inapplicability in a given context of a provision of the Policy does not affect the validity of the other provisions, nor of this provision outside the said context. The Policy continues to apply in the absence of the unenforceable provision, while respecting the intention of the parties.

The headings at the start of each article are intended only to facilitate reading, and can under no circumstances provide a pretext for any interpretation or denaturing of the clauses to which they relate.

8.15.4 Application and waiver

Any notice to be given under this Policy shall be deemed to have been given if it is sent by registered letter with acknowledgement of receipt or by fax sent to the address for service as indicated at the top of the Service contract and shall be deemed to have been received seven (7) days after the date of the postmark in the context of the registered letter with acknowledgement of receipt and one (1) day after the date of sending in the context of the fax.

8.15.5 Force majeure

Initially, force majeure situations will suspend the performance of the contract. If the duration of the force majeure situations is longer than as indicated in the contract, the contract will be automatically terminated, unless agreed otherwise between the parties. The performance of the obligations resumes its normal course once the force majeure situation has ended.

Docaposte Certinomis cannot be held liable and assumes no commitment, for any delay in the performance of obligations or for any non-performance of obligations resulting from this Policy when the circumstances giving rise thereto and which could result from the total or partial interruption of its activity, or its disorganisation, fall under force majeure within the meaning of Article 1148 of the French Civil Code.

It is formally agreed that the following will constitute cases of force majeure or fortuitous events, in addition to the situations normally accepted by the case law of the French courts and tribunals, of the contractual clauses contained in the associated Declaration of Practices, and any other agreements between the parties (for example the contract):

Total or partial strike, lock-out, riot, civil disturbance, insurrection, civil or foreign war, nuclear risk, embargo, confiscation, capture or destruction by any public authority, bad weather, epidemic, blocking of means of transport or supply for any reason whatsoever, earthquake, fire, storm, flood, water damage, governmental or legal restrictions, legal or regulatory changes in forms of marketing, computer breakdown, blocking of electronic communications, including telecommunications networks, any major scientific discovery calling into question in whole or in part the principles of asymmetric cryptography, any consequence of a technological development, not foreseeable by Docaposte Certinomis, calling into question the norms and standards of its profession and any other case beyond the control of the parties preventing the normal performance of this contract.

8.16 OTHER PROVISIONS

In accordance with articles 323-1 to 323-7 of the Criminal Code, applicable when an offence is committed within French territory, any hacking or attempted hacking of automated data processing systems will be punishable, which notably includes fraudulent access and remaining within the system, modifications, alterations, data hacking, etc.

The possible penalties vary from 2 to 5 years of imprisonment and a fine ranging from €30,000 to €375,000 for legal persons.

The infringement of trademarks, commercial and service marks, designs and models, distinctive signs, copyrights (for example: software, web pages, databases, original texts, etc.) is sanctioned by Articles L. 716-1 et seq. of the Intellectual Property Code

9 APPENDIX 1: REFERENCED DOCUMENTS

9.1 REGULATIONS

Reference	Document
[CNIL]	*Law n° 78-17 of 6 January 1978 relative to information technology, files and freedoms, modified by n° 2004-801 of 6 August 2004*
[EIDAS]	*REGULATION (EU) 2024/1183 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 11 April 2024 amending Regulation (EU) No 910/2014 as regards the establishment of the European framework for digital identity*
[ETSI 119431-1]	*Electronic Signatures and Trust Infrastructures (ESI); Policy and security requirements for trust service providers; Part 1: TSP services operating a remote QSCD / SCDev*
[GDPR]	*European Regulation EU 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC*

9.2 TECHNICAL DOCUMENTS

Reference	Document
[X.509]	*Information Technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks, Recommendation X.509, version March 2000 (supplemented by technical corrections No. 1 of October 2001, No. 2 of April 2002 and No. 3 of April 2004)*
[SOGIC-CRYPTO]	*SOG-IS Crypto Evaluation Scheme - Agreed Cryptographic Mechanisms - Current version.*

10 APPENDIX 2: SECURITY REQUIREMENTS OF THE SERVICE'S CRYPTOGRAPHIC MODULE

10.1 REQUIREMENTS REGARDING THE SECURITY OBJECTIVES

The cryptographic device used by the Service to generate, store and implement the key pairs of the Signatories must meet the following security requirements:

- guarantee that the generation of the key pair is carried out exclusively by authorised users and guarantee the cryptographic robustness of the generated key pair;
- ensuring the correspondence between the private key and the public key;
- authenticate the Signatory and identify their private signing key in a secure and reliable manner;
- generate a stamp or signature that cannot be forged without knowledge of the private key.

In addition, organisational, procedural or technical security measures must be put in place to:

- to detect faults during the initialisation, customisation and operation phases and to have secure techniques for destroying private keys;
- guaranteeing the private key's confidentiality and integrity;

10.2 QUALIFICATION REQUIREMENTS

The hardware cryptographic module used for the generation and implementation of the Signatories' keys must be assessed according to the Common Criteria at a minimum of EAL 4 [SOGIS-CRYPTO] and certified as a QSCD in accordance with Article 3 of the [EIDAS] regulation by a competent authority (see eIDAS Dashboard)).