Carrer d'Avila nº29 Pta 1 - 08005 Barcelona www.signaturit.com - Tel. 960 031 203

CERTIFICATION PRACTICE STATEMENT & CERTIFICATION POLICIES FOR

SIGNATURIT GLOBAL CA

1.3.6.1.4.1.50646.5.1

SIGNATURIT SOLUTIONS, S.L.U. - DIGITAL TRUST SERVICE PROVIDER

Signaturit Solutions, S.L.U.

Document date: 01/05/2023

VERSION CONTROL

Review	Date	Description
0	01/04/2023	Initial version (draft)
1	01/05/2023	It is specified that under this version 1 of the CPS only the "Citizen" certificate profile is included in Software support. However, practices applicable to centralized and certificates of attribute profiles are contemplated in case they are incorporated at a later date.

Interveners

Version	Date	Author	Reviewed by	Approved by
0	01/04/2023	France Vidal (compliance)	Sergio Serrano (PKI	Felix Esteban (CTO)
2	01/05/2023	France Vidal (compliance)	Sergio Serrano (PKI	Felix Esteban (CTO)

CONTENTS

1 INTRODUCTION

1.1 OVERVIEW

This document constitutes the Certification Practice Statement (hereinafter CPS) of "**Signaturit Global CA",** Certification Authority owned by the Trust Service Provider Signaturit Solutions, S.L.U. (hereinafter Signaturit), for the provision of the **SERVICE TO ISSUE QUALIFIED ELECTRONIC CERTIFICATES.**

Signaturit Global CA is an external Subordinate Certification Authority (hereinafter SubCA) under the root CA "**IvSign Root CA"** which is a Certification Hierarchy managed and owned by Ivnosys Soluciones, S.L.U. (hereinafter Ivnosys Soluciones) with NIF B-98333362 and address at C/ Acceso Ademuz nº12, 1º1 - 46980 Paterna (Valencia).

Therefore, this CPS is in compliance with the IvSign Root CA CPS of Ivnosys Solutions and its Certification Policies, and in particular with regard to the provisions on External Subordinate Certification Authorities.

Both companies, Signaturit and Ivnosys Soluciones, belong to the "Signaturit Group".

This service is provided in accordance with Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (hereinafter eIDAS) and Law 6/2020 of 11 November regulating certain aspects of electronic trust services.

Digital certificates issued under this CPS may be issued in the following modes or formats as new profiles are added:

- In software (PKCS#12 format) using the technical infrastructure of the Ivnosys Solutions PKI
- Centralised in Ivnosys Solutions' **IvSign** key management system which is reliably integrated with the IvSign Root CA PKI. (not available in version 1 of this CPS).
- Optionally, for some profiles, the issuance in Hardware devices (HSM or Smartcard) is available (not available in version 1 of this CPS).

For centralised services (not available under version 1 of this CPS), Signaturit uses the **IvSign Service** developed by Ivnosys Soluciones with the aim of enabling remote electronic signatures and seals, as enabled and encouraged by the eIDAS Regulation. For this reason, the Certification Authorities dependent on **IvSign Root CA,** can use the IvSign Remote Signature System as the preferred format for issuing certificates, as is the case of Signaturit Global CA.

According to the eIDAS Regulation, to ensure that a remote electronic signature management system managed by the Trusted Service Provider on behalf of the holder has the same legal recognition as those using a fully user-managed environment, specific security systems and procedures must be implemented to ensure that the environment is trusted and used under the sole control of the Signatory. **IvSign** has a 'Practice Statement (hereafter IvSign PS) that describes the procedures, practices and controls of the IvSign trusted system to ensure this objective.

For these reasons, this CPS will, at all times, refer to the following Service Practice Statements:

- CPS IvSign Root CA with OID 1.3.6.1.4.1.47304.3.1, localization: https://policy.ivnosys.com/
- Statement of Management Practices for the Remote Key Centralisation and Electronic Signature Service IvSign by Ivnosys Soluciones S.L.", with OID 1.3.6.1.4.1.47304.1.1, location: https://policy.ivnosys.com.

Signaturit Solutions, S.L.U. has registered the following root OID (or "arc") to identify all its policies:

OID	1.3.6.1.4.1.50646.
Description	Signaturit Solutions, S.L.U.

Signaturit Global CA is a multi-policy intermediate CA that can issue certificates for natural and legal persons (currently, only for natural persons under the initial version of this CPS) in accordance with the eIDAS Regulation and Law 6/2020. All certificate policies that are issued by the **Signaturit Global CA** in accordance with this CPS are identified by an OID with the prefix 1.3.6.1.4.1.50646.5.1.

In general, all certificates issued under this CPS have at least two certification policies:

- The standard policy for EU qualified certificates issued to natural or legal persons as defined by the European standard ETSI EN 319 411 and ETSI EN 319 412:
  - ETSI EN 319 412-2, for issuing qualified electronic certificates to natural persons:
    - **QCP-n**, for advanced electronic signatures based on a qualified certificate.
    - **QCP-n-qscd**, for qualified electronic signatures.
  - ETSI EN 319 412-3, for issuing qualified electronic certificates to legal entities:
    - **QCP-l**, for advanced electronic seals based on a qualified certificate
    - **QCP-l-qscd**, for qualified electronic seals.
- And an in-house policy to the CA that regulates the scope of use of the certificates. Under this CPS, the policies of this type are:
  - **Citizen**: Identifies a natural person without establishing any kind of linkage.
- In those certificates that allow it, a third policy is included that refers to **Certificate profiles based on Spanish Law 40/2015**. Consult the Policy Annex, which specifies the profiles compatible with this policy, if it has been created (not available in version 1 of this CPS).

The following table lists all the OIDs that identify the **Signaturit Global CA** qualified certification policies in force in each version of the approved CPS:

Qualified certificate type (PERSONAL)	OID POLICIES		MEDIUM
	S	SIGNATURIT SOLUTIONS	
	E	ETSI EN 319 411 2	
Citizen	S	1.3.6.1.4.1.50646.5.16.1.1.2	Software
	E	0.4.0.194112.1.0	

1.2 DOCUMENT IDENTIFICATION

This CPS has the following identification data:

Name	PRACTICES STATEMENT & CERTIFICATION POLICY FOR SIGNATURIT GLOBAL CA
Version	1
OID	1.3.6.1.4.1.50646.5.1
Location	https://policy.signaturit.com

1.3 COMMUNITY AND SCOPE OF APPLICATION

1.3.1 Certification authorities

A CA is the entity responsible for issuing and managing the lifecycle of digital certificates. It acts as a trusted third party, between the Certificate Holder and the Relying Party or Trusting Third Party, in electronic relations, linking a specific public key with a person. The CA has the ultimate responsibility for the provision of certification services. The CA is identified in the Subject (Issuer) field of the digital certificate.

A CA belongs to a Trusted Service Provider (TSP) that offers the service of issuing digital certificates. The TSP is a legal entity indicated in the organisation attribute (O) of the issuer field of the associated digital certificate.

A Certification Authority (CA) uses Registration Authorities (RA) to perform the tasks of checking and storing the documentation of the contents embedded in the digital certificate. At any time the CA can cover the tasks of an RA.

Signaturit Global CA is a Certification Authority subordinate to the Certification Authority of the following Hierarchy of the Ivnosys Solutions Root:

Distinguised Name (DN)	CN = IvSign Root CA O = IVNOSYS SOLUCIONES S.L.U. 2.5.4.97 = VATES-B98333362 OU = TRUST SERVICES S = VALENCIA C = ES
Fingerprint (SHA-256)	C94BFDADED2CFAF77469C871531956B1 455B24EC21148E66AE1C85E368323A8C
Publication URL	http://ca.ivsign.com/certs/ivsignrootca.crt

So under this CPS, Ivnosys Solutions manages the IvSign Root CA hierarchy.

The intermediate Certification Authority **Signaturit Global CA**, owned by Signaturit Solutions, S.L.U., has the following identification:

Distinguised Name (DN)	CN = Signaturit Global CA O = SIGNATURIT SOLUTIONS S.L.U. 2.5.4.97 = VATES-B66024167 S = BARCELONA C = ES
Fingerprint (SHA-256)	3BE056DA32623D5E006C90006A846615EFC4A7573FF339607FA0144BF920FAF4
Publication URL	https://policy.signaturit.com

1.3.2 Registration Authorities (RA)

An RA can be a natural or legal person that acts in accordance with this CPS and, where applicable, by means of an agreement signed with Signaturit, performing the functions of managing applications, identification, validation of documentation, registration of certificate applicants and validation of emissions. The RAs are delegated authorities of the CA, although the CA is ultimately responsible for the service.

In addition to the CPS itself, the following types of RA are recognised under the present practices:

- **External RA**: That managed by a public organisation or private entity for the distribution of certificates, in general, to individuals or entities with which it has established some type of relationship (labour, commercial, collegiate, etc.).
- **Remote RA**: Integrated External RA that communicates with the CA through the integration layer of Signaturit's PKI management platform.

- **PVP**: On-site Verification Point dependent on an RA. Its main mission is to cover the identification of the applicant and the delivery of documentation to the RA, which will validate it according to the applicable Policy in order to process the certificate issuance request.

For the purposes of this CPS, they may act as ARs:

- The Certification Authority itself.
- External Registration Authorities, as delegated entities of a CA, to which they are contractually bound, to carry out the complete registrations of Subjects/Signatories within the agreed scope of action.

In turn, any RA can delegate to the Presential Verification Points (PVP) the function of identifying the applicant's holder, collecting documentation and, if established, checking documentation and verifying its suitability. They are contractually bound to an RA by a standard contract provided by the TSP. On the basis of the documentation provided by the PVP, the RA operator checks the documentation and, if applicable, proceeds with the issuance of the certificate by the CA without the need for further verification of identity. In this CPS, for the sake of simplicity, we will refer to registration functions or obligations of the RA without distinguishing whether this is performed by the RA or the PVP, which is regulated contractually.

1.3.3 Applicant

The Applicant is the natural person who carries out the necessary procedures to obtain a digital certificate.

In the case of personal certificates, it is the person who applies for the certificate for him/herself or on behalf of a third party.

In electronic seal certificates (not available in version 1 of this CPS), it is the person with sufficient powers of representation to apply for the certificate on behalf of an Entity.

1.3.4 Subject/Holder, Signatory or Creator of the Seal

The Certificate Holder is the natural person or legal entity that will hold the certificate and whose identification details appear in the certificate.

The Signatory is understood to be the natural person who creates the electronic signature. In the Signaturit CA, the Signatory can be (depending on the profiles created):

- A natural person acting in his own name and in his own right
- A natural person representing an Entity with or without legal personality. (not available in version 1 of this CPS)
- A natural person authorised to be identified as being related to an Entity with or without legal personality (not available in version 1 of this CPS).

Creator of the Seal means the Holder legal person who is the creator of the seal in the electronic seal certificates (not available in version 1 of this CPS).

The Certificate Holder is described in the CN (Common Name) attribute of the DN (Distinguished Name) field of the certificate.

1.3.5 Subscribers

The subscribers of the certificates issued by the CA are natural persons or entities with or without legal personality that have contracted the certification service with Signaturit. Therefore, they will be the owners of the certificates.

Specifically:

- In the case of natural person certificates, the Subscriber is the natural person Holder of the Certificate.
- In the case of natural person certificates with a link or representation attribute with an Entity, the Subscriber is the Entity that contracts the service for the persons with whom it has a specific relationship (not available in version 1 of this CPS).
- In the case of legal person certificates (electronic seal certificates), the Subscriber is the Entity or its parent company (not available in version 1 of this CPS).

1.3.6 Relying party or certificate user

The *relying* party is the person who receives an electronic transaction carried out with a certificate issued by a CA included in this CPS and who voluntarily trusts the Certificate issued by the CA and, therefore, the trusted service that supports it.

1.3.7 Other participants

1.3.7.1 Entity

For natural person certificates, the Entity is the organisation with or without legal personality, public or private, individual or collective, recognised in law, which has a specific relationship with the natural person Holder. (not available in version 1 of this CPS).

In the case of electronic seal certificates (not available under version 1 of this CPS) the Entity is the legal entity that holds the certificate (the Holder).

1.3.7.2 Responsible for the certificate

The Responsible is the natural person responsible for the use of the private key associated with the certificate's public key.

In the case of natural person certificates, the Responsible is the Certificate Holder.

In the case of electronic seal certificates, without prejudice to the obligations of the Holder of the certificate, the Responsible is the Applicant or a person authorised by the Applicant (not available under version 1 of this CPS).

1.3.7.3 Accreditation Body or Supervisory Body

The Supervisory Body will be the corresponding management body that admits, accredits and supervises TSPs within a specific geographical area. This task within the Spanish State falls to the Ministry of Economic Affairs and Digital Transformation, being the competent authority depending on the Spanish State member of the European Union.

1.4 USE OF CERTIFICATES

1.4.1 Scope of Application and Uses

The certificates issued by the CAs listed in this CPS may be used under the terms established by the corresponding Certification Policies.

In general terms, certificates are allowed for the following uses:

- X.509v3 certificate-based authentication.
- Advanced electronic signature based on X.509v3 certificates.
- Advanced electronic signature based on X.509v3 qualified certificates.
- Qualified electronic signature based on X.509v3 certificates issued in remote QSCD.
- Asymmetric or mixed encryption, based on X.509v3 certificates.

1.4.2 Prohibited and Unauthorised Uses

Certificates may not be used outside the limits and uses for which they have been issued in each case and which are described in the corresponding certification policies.

Certificates are not designed, intended, and are not authorised for use or resale as hazardous situation monitoring equipment or for uses requiring fail-safe performance, such as the operation of nuclear facilities, airborne navigation or communications systems, or weapons control systems, where failure could directly result in death, personal injury or severe environmental damage.

Signaturit incorporates information on the limitation of use in the certificate, either in standardised fields in the attributes "key usage", "basic constraints" marked as critical in the certificate and therefore of mandatory compliance by the applications that use it, or limitations in attributes such as "extended key usage", "name constraints" and/or by means of texts incorporated in the "issuer's statement" field (user notice) marked as "non-critical" but of mandatory compliance by the certificate holder and user.

Although it is possible to encrypt data with the certificates, Signaturit shall not be liable for any damage caused by the loss of control of the holder of the private key required to decrypt the information.

1.5 ADMINISTRATION OF THE PSC

1.5.1 Organisation

The drafting, publication, review and revision of this CPS is the responsibility of:

Organisation	SIGNATURIT SOLUTIONS S.L.U.
E-Mail	info@signaturit.com
Website	https://www.signaturit.com

1.5.2 Contact person

For any questions about this SCP, please contact:

Organisation	SIGNATURIT SOLUTIONS S.L.U.
Responsible	Compliance Director
E-mail / Telephone	legal@signaturit.com / 960 031 203

1.5.3 Party responsible for determining this CPS's suitability with the policies

Signaturit's Quality & Compliance Department.

1.5.4 Policy approval procedure

The policies and this CPS are approved by Signaturit's TSP committee (formerly called "Coordination Committee"), according to the internal procedure established for this purpose. Each new version of CPS is published on Signaturit's website: https://www.signaturit.com/es/legalidad/autoridad-certificacion/.

1.6 DEFINITIONS AND ACRONYMS

1.6.1 Definitions

Trusted Service Provider (TSP): A trusted service provider is a natural or legal person who provides one or more trust services, either as qualified services or as non-qualified trust services.

Qualified Trust Service Provider (QTSP): A qualified trust service provider provides one or more trust services to which the supervisory body has granted qualification.

Trusted service: The trusted services defined in eIDAS include:

- The creation, verification and validation of electronic signatures. Certificates relating to these services are included.
- The creation, verification and validation of electronic seals. Certificates relating to these services are included.
- The creation, verification and validation of electronic time stamps. Certificates relating to these services are included.
- Certified electronic delivery. Certificates relating to these services are included.
- The creation, verification and validation of certificates for website authentication.
- The preservation of electronic signatures, seals or certificates relating to these services.

Qualified Trusted Service: a trusted service that complies with the applicable requirements set out in the eIDAS Regulation.

1.6.2 Acronyms

CA: Certification Authority

CPS: Certification Practice Statement

CRL: Certificate Revocation List

eIDAS: Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

HSM: Hardware Security Module

OCSP: Online Certificate Status Protocol

OID: Object Identifier

PC: Certificate Policy

PDS: PKI Disclosure Statement

PKI: Public Key Infrastructure

PS: Practice Statement

QSCD: Qualified Secure Creation Device

RA: Registration Authority

SubCA: Subordinate Certification Authority (Subordinate Certification Authority)

TSA: Time Stamp Authority

2 RESPONSIBILITIES FOR THE PUBLICATION OF INFORMATION

2.1 REPOSITORIES

Signaturit publishes the following CA data and information:

- The Certification Practice Statement and specific policies, which will be publicly available at https://policy.signaturit.com/ .
- The corresponding PDS (PKI Disclosure Statement) at the following URLs:
  - English: https://pds.signaturit.com/en
  - Spanish: https://pds.signaturit.com/es
- The Terms and Conditions of the services provided https://policy.signaturit.com/
- Links to CA certificate information
  - http://ca.ivsign.com/certs/ivsignrootca.crt
- Links to CRL and OCSP of the CA:
  - CRLs:
    - http://crl1.ivsign.com/ivsignroot.crl

- http://crl2.ivsign.com/ivsignroot.crl

- OCSP:
  - http://ocsp.ivsign.com
  - http://ocsp2.ivsign.com

Any changes to the specifications or conditions of service will be made available to users through the URLs specified for each repository, also accessible from the website https://www.signaturit.com/es/legalidad/autoridad-certificacion/ .

2.2 PUBLICATION OF CERTIFICATE INFORMATION

Signaturit publishes the following information about the certificates on the website: https://policy.signaturit.com/

- The public keys of certificates: http://ca.signaturit.com/certs/sitglobalca.crt
- Certificate revocation lists at the addresses:
  - http://crl1.signaturit.com/sitglobal.crl
  - http://crl2.signaturit.com/sitglobal.crl
- An on-line repository for querying the status of certificates, using OCSP protocol.
  - http://ocsp.signaturit.com
  - http://ocsp2.signaturit.com

2.3 UPDATE FREQUENCY

CA certificates are published by Signaturit in the corresponding repository on the date they become valid or are published in the trusted lists for the first time.

The end-entity certificates are published automatically and immediately after having been issued following approval by the Subject/Signatory, and their status can be consulted through the available means identified in point 2.2. Publication of certificate information.

Signaturit publishes immediately, once approved and in force, in the corresponding repositories, any modification to the Policies, CPS or PDS, maintaining the version history.

2.4 ACCESS CONTROL

All repositories specified in this point are publicly accessible and do not require any kind of access control by the subscriber or user of a certificate.

3 IDENTIFICATION AND AUTHENTICATION

3.1 NAMING POLICIES

3.1.1 Identifying name on certificates

The identifying name on the certificates is entered in the Subject field by means of a Distinguished Name (DN) according to the standard X.501 name type.

The structure, content and meaning of the data that make up the certificate DN are defined in the certificate profile documents for each of the types of certificates issued by the CA.

3.1.2 Meaning of names

All names used in the ND shall be meaningful.

3.1.3 Pseudonyms

Pseudonym certificates are not currently issued.

3.1.4 Rules used to interpret various name formats

Signaturit always complies with the X.500 reference standard in ISO/IEC 9594.

3.1.5 Uniqueness of names

Within the same CA, the name assigned in the Subject field of the certificate shall be unique, and shall identify the same identified certificate holder. A Subject/Holder name already assigned to a different Applicant cannot be assigned, which shall be controlled by incorporating the unique tax identifier or equivalent to the name string that distinguishes the Certificate Holder.

Several certificates can be issued to the same Subject as long as the type of certificate (Certificate description field) is different.

3.1.6 Recognition, authentication and function of trademarks and other distinctive signs

Signaturit makes no commitments when issuing certificates regarding the use of trademarks and other distinctive signs. Signaturit does not deliberately permit the use of a distinctive sign for which the Holder or Subscriber does not hold rights of use. However, neither Signaturit nor the RAs are obliged to search for evidence of rights of use over trademarks or other distinctive signs prior to issuing certificates.

3.2 INITIAL REGISTRATION

3.2.1 Methods of proof of possession of the private key

The generation of the private keys will be carried out by the CA when the certificates are issued. The control of the private key will be delivered directly to the Certificate Holder (or to the Responsible for electronic seal certificates), via the contact means indicated in the request (email address and/or mobile phone number):

- **In Software format:** They are delivered to the Holder by online generation of the protected file according to the PKCS#12 standard (not available under version 1 of this CPS).
- **In a centralised environment:** They will be generated directly in the IvSign certificate centralisation system, associated with the holder's account.
- **In Hardware format:** Keys can be delivered by the CA to the Holder, either directly or via an RA, on a Qualified Signature Creation Device (QSCD) like card or token that conforms to the requirements set out in Annex II of the eIDAS Regulation (not available in version 1 of this CPS).

However, the generation of private keys by the Holder shall be allowed, and the Holder shall prove possession of the private key by sending the RA a PKCS#10 request associated with the certificate request.

3.2.2 Authentication of Entities

(not available in version 1 of this CPS)

3.2.3 Authentication of an individual's identity

For the issuance of qualified certificates, the authentication of an individual's identity shall be verified by presenting one of the following documents to the RA:

- Spanish National Identity Card (DNI)
- Spanish Residence Card or Foreigner's Identity Card
- Spanish passport
- Identity card from any EU or EEA member country, along with the Foreigner's Identity Number Certificate (NIE).
- For foreigners who do not hold a NIE, passports and official identity documents from the country of origin will be accepted as long as the CA, RA or PVP operator understands the language of the document and can verify its authenticity through a reliable source such as the PRADO Public Register of Authentic identity and travel Documents Online database (https://www.consilium.europa.eu/prado/en/prado-start-page.html). In case of not knowing the language of the document or not having access to a database to corroborate its authenticity, the document should be submitted with the Hague Apostille and, if deemed necessary, with an official translation.

Certificates cannot be issued to minors who are not emancipated, legally incapacitated in whole or in part, or where there are reasonable grounds for suspecting that the applicant is not of sound mind.

Identity verification may be carried out:

- By physical personation before a CA, RA or PVP operator. Alternatively, the Applicant may choose to appear in person before a Notary and submit the request for issuance of the certificate with its signature authenticated in the presence of a Notary.

- Remotely, using electronic identification means, for which the presence of the natural person has been ensured prior to the issuance of the qualified certificate, and which meet the requirements set out in Article 8 (of the eIDAS Regulation) with regard to "substantial" or "high" security levels. Electronic identification schemes notified by a Member State under Article 9.1 of the eIDAS Regulation with a substantial or high security level (e.g. electronic ID in Spain) will be accepted.
- By means of another valid qualified certificate issued by a CA of Ivnosys Solutions or another Qualified Trust Service Provider, for the issuance of which the natural person had been identified in person or using electronic identification means in accordance with the previous point, provided that the identity data of the natural person (and, where appropriate, the attributes in the certificate requested) are contained in the certificate used. If necessary, the other Provider shall be asked to confirm when the last appearance took place.
- Signaturit may incorporate other nationally recognised identification methods, whose security is equivalent to physical personation, in accordance with the applicable standard, in particular the conditions and technical requirements established in Order ETD/465/2021, of 6 May, regulating remote video identification methods for issuing qualified electronic certificates.

Pursuant to Article 7.6 of Law 6/2020, a new personation is not required when the identity or other permanent circumstances of the certificate applicants are already known to the CA or RA by virtue of a pre-existing relationship of the applicants with the CA or RA, in which, for the identification of the interested party, the means indicated in paragraph 1 (physical personation) was used and the period of time elapsed since the identification was less than five years. Therefore, if such circumstances exist, the provisions of this point may not be applicable.

For non-qualified certificates, the corresponding policies shall be followed, with the organisation responsible for the RA establishing the rules for identification of the holders.

The RA shall register the data and documents relating to the identification and authentication of the natural person and/or the Entity. Pursuant to article 24.2.h) of the eIDAS Regulation, these registration activities may be carried out by electronic means whether the documents provided are legally valid electronic documents or paper documents. In the latter case, the RA Operator must keep a scanned copy and digitally sign it with its personal Certificate, to be kept in computer files held by the RA itself for the duration of the contractual relationship with the RA and when it is terminated by the RA during the required legal period.

3.2.4 Non-verified information on a Suscriber

All information in the Subject field of the certificate is verified.

3.2.5 Validation of authority for the application

The authority to apply for a certificate shall be validated at the time of verification of the identity of the holder and its concordance with the identity documents presented.

The authority to bind, represent or issue a certificate to an entity shall be validated by the documentation specified in points 3.2.2 Authentication and 3.2.3. Authentication of an individual's identity

3.2.6 Criteria for interoperability

Signaturit may interoperate with other CAs (e.g. cross certification), in particular the Ivsign Root CA Intermediate CAs on terms and criteria to be contractually established.

3.3 KEY RENOVATION

3.3.1 Identification and authentication for key renewal

Prior to renewal, the CA or RA shall verify that the information used to verify the identity and other details of the Signatory and the key holder is still valid.

These checks shall be carried out by authenticating the holder on the basis of the certificate to be renewed, which must be valid and have been issued by Signaturit.

If any Signatory or key holder information has changed, a new registration and issuance must be made, as set out in the relevant sections of this document.

This process cannot be carried out automatically if more than 5 years have passed since the last identification and authentication process of the Subscriber and/or Holder. In this case, a new certificate issuance process must be started.

3.3.2 Identification and authentication for key renewals after revocation

If the certificate is invalidated, it cannot be renewed automatically using the method indicated in point 3.3.1 above. A new certificate issue process must be started again.

If the revocation occurs in end-entity certificates as a result of a replacement process or due to an error in their issuance or loss, it is considered that the renewal after revocation can be carried out, provided that the information used to issue the revoked certificate is still valid. The supporting documentation provided for the issuance of the replaced certificate will be reused and the need for a new authentication of the holder will be eliminated as long as this occurred less than 5 years ago.

In no case may a certificate be replaced after revocation if:

- The certificate was revoked due to erroneous issuance to a person other than the person identified in the certificate.
- The certificate was revoked for unauthorised issuance by the natural person identified in the certificate.

3.4 REVOCATION OF THE KEY

Authentication of the Applicant to revoke or suspend a certificate is performed as follows:

- If it is the certificate Holder or the person responsible for the certificate:
    - By means of a signed request sent from the same e-mail address of the Holder or the Responsible in charge of the certificate on record to the TSP.

- Through the certificate management application made available to certificate applicants.
- By physical presence at the RA, upon presentation of one of the identification documents referred to in point 3.2.3 above. *3.2.3. Authentication of an individual's identity*.

- By the Subscriber different than the Subject or a representative of the Entity to which a certificate is bound:
  - By means of a written communication signed and sealed by a representative of the Entity accompanied by a document proving his or her powers of representation.
- By a third party:
  - This third party may report any circumstance that could lead to revocation, such as suspected fraud, misuse, erroneous data, etc. Such circumstances must be verified by the TSP or the RA who will take the revocation decision in accordance with the following point.
- The TSP, directly on its own initiative or through an RA, may request the revocation of a certificate if it knows or suspects that the subscriber's private key has been compromised, or if it knows or suspects any other event that makes it advisable to take such action. Additionally, the CA's authorised operators may process the request for mass revocation of certificates due to the CA or RA ceasing activity in accordance with the procedures of the TSP Termination Plan.

In any case, at the time of certificate revocation, an e-mail notification will be sent to the Subject/Holder or Responsible Party specifying the date and time and the reason for the revocation.

4 OPERATIONAL REQUIREMENTS OF THE CERTIFICATE'S LIFECYCLE

Signaturit uses Ivnosys Soluciones' RA platform for certificate lifecycle management. This platform allows the request, registration, publication and revocation of all issued certificates.

Signaturit guarantees that the trust services offered under this CPS are carried out under non-discrimination policies, so that:

- There are no procedures other than those specified in this CPS for the management of services.
- Notwithstanding the above, special application procedures and the rest of the certificate lifecycle processes may be enabled for subscribers with special needs due to any type of disability that prevents them from applying for the services in accordance with the procedures specified in this CPS.

- The services are accessible to any natural person who meets the necessary criteria for the issuance of a digital certificate according to the policies set out in this CPS, and no special conditions are required.

4.1 CERTIFICATES REQUEST

4.1.1 Who can initiate a certificate request

The application for a certificate can be made by the natural person or authorised representative whose identity coincides with the Subject of the certificate to be issued.

4.1.2 Request process

4.1.2.1 Individual application via website form

Requests for certificates are generally made in accordance with the following procedure:

(1) The Applicant must complete a form to initiate the process. For this purpose, the CA or RA will provide the necessary applications and access accounts to the users.
(2) During the registration process, the Applicant's email account (and/or mobile phone number) will be verified by sending an email (or sms), in which the Applicant will be asked to confirm through the CA or RA application the correction of his/her data (and, if applicable, those of the Entity) and the acceptance of the Terms and Conditions of use of the service and Privacy Policy.
Confirmation of the data and acceptance of the Terms and Conditions of use of the certificate may alternatively be formalised by the Applicant and, where applicable, the Subscriber within an operational process, internal or external, approved by the RA.
(3) With the submission of the request, the Applicant shall electronically submit the necessary documentation through the application provided and comply with the in-person identification requirement, if applicable, for identification and validation of the documentation.

4.1.2.2 Multiple application via batches

In this case, the Subscriber will send the RA a structured file with all Applicants' data. The RA will proceed to load these requests into the management application, continuing the management for each of the requests from step (2) of the previous point.

4.2 MANAGING REQUESTS

Requests are processed by an agent associated with the RA or the PVP.

4.2.1 Identification and authentication

Once a certificate request has been made, the agent will check:

(1) That the holder has been identified as specified in point 3.2. *Initial registration.*
(2) That the applicant has submitted all the documentation required for the type of certificate requested.

4.2.2 Approval or rejection of the application

Once the application has been validated by an agent, it will be processed by an RA Operator:

(1) The RA Operator verifies that the information provided in the request is compliant in order to issue the certificate.
(2) If the identification made or the information provided is not correct, in accordance with the provisions set out in point *3.2. Initial registration* of this CPS, the RA Operator shall request the necessary corrections, or shall reject the request, informing the Applicant of the reasons so that it can correct and redo the request again if it wishes to do so.
(3) In case the data is verified according to the established procedures the RA operator will approve the request to then issue the certificate.

Requests via web services are executed directly when they are received authenticated with a certificate previously recognised as RA by Signaturit.

4.2.3 Request processing time

There is no stipulated processing time for the requests.

4.3 ISSUANCE OF CERTIFICATES

4.3.1 CA actions to issue certificates

After approving the request, the RA operator will manage the issuance of the certificate with its authentication credentials.

For software certificates, the holder receives an e-mail with notification of the approval of the application and the procedure for generating and downloading the certificate in software format. A installation code will be needed for its installation, which has been provided in the request confirmation email.

For centralised certificates, this is done in accordance with the IvSign PS. The issuance is performed at the time the RA Operator executes it and signs the operation with its RA Operator certificate.

4.3.2 Notification to the subscriber of the issuance of the certificate

Once the certificate has been issued, the Subscriber will receive the private key activation PIN in the e-mail or mobile phone (via SMS) provided in the application.

For centralised certificates, the Subscriber will receive another message via one of the specified channels with the authentication means (user and password) to access the **IvSign** certificate management system. This message will only be received at the time of issuance of the first certificate in their IvSign account.

4.4 ACCEPTANCE OF CERTIFICATES

4.4.1 Conduct constituting acceptance of the certificate

Once the subscriber has been notified of the issuance of the certificate, he/she has a period of 7 calendar days to check that it has been correctly issued. After this time, the subscriber shall be deemed to have accepted the issued certificate.

If the certificate has not been issued correctly due to technical reasons, the certificate will be revoked and a new one will be issued, once the incident has been detected or communicated to the RA by the subscriber.

4.4.2 Publication of the certificate by the CA

Once issued, the certificate is immediately published in the certificate repository and is available for consultation of its status through the services enabled for this purpose (See point 2.2. Publication of certificate information).

4.4.3 Notification of the issuance of the certificate to other entities

There are no processes for the notification of the issuance of a certificate to other entities.

4.5 USE OF THE CERTIFICATES

4.5.1 Usage of the private key and certificate by the subscriber

The Certificate Holder, either directly or through an authorised third party (the Applicant or the Responsible for seals certificates), shall be obliged to comply with the provisions of the regulations, this CPS in its capacity as signatory/creator of the seal and the provisions of the Terms and Conditions imposed by the CA, which shall have been accepted prior to confirming the request for the certificate.

The subject must always use the certificate on the basis of the permitted uses, as indicated in point 1.4. *Use of certificates.*

4.5.2 Usage of the public key and the certificate by the relying party

It shall be the obligation of the Relying Party to comply with the provisions of the regulations in force and, in addition:

- Verify the validity of the certificates before accepting any operation carried out by the certificate holder. Signaturit has various mechanisms to perform this check, such as access to revocation lists (CRL) or online query services such as OCSP. Access to these mechanisms is described in this CPS.
- Know and agree to be bound by the guarantees, limits and responsibilities applicable to the acceptance and use of the certificates on which it relies, and agree to be bound by them (accessible from the "Certificate directives" field).

4.6 RENEWAL OF CERTIFICATES

4.6.1 Circumstances for the renewal of certificates

Certificates can be renewed in accordance with its certification policy.

Renewal must be made before expiry.

Only certificates in which none of their data has changed can be renewed, allowing only the modification of the e-mail address. If there are other data incorporated in the certificate that have changed, the certificate must be revoked and a new issue must be made.

4.6.2 Who can apply for renewal

The renewal must be requested by the certificate Holder or the natural person representing the certificate Holder in the case of certificates issued to entities (Certificate Applicant or the Responsible).

4.6.3 Renewal process

The renewal of certificates under this CPS is always carried out by issuing new keys, therefore, the technical issuing process is the same as that followed when a new request is made.

In the case of renewal of qualified certificates of natural persons, certificate issuance is allowed without repeating the identity verification process described in point 3.2.3. *Authentication of an individual's* identity*'s identity* up to a period of 5 years from the last face-to-face registration. Once this period has elapsed, the holder must carry out a face-to-face issuance process equal to the one carried out for the first issuance.

Before expiry, the CA sends four renewal notices to the certificate holder (30 days, 15 days, 7 days, 1 day) via email notifying that the certificate is about to expire.

The renewal process is initiated from the application provided by the TSP and indicated in the renewal emails. This process requires access to the private key of the valid (non-revoked) certificate to be renewed.

- The user must log in with his or her user account.
- Once identified, the software displays the data of the old certificate to the signatory and asks for confirmation of said data.
- The software allows the Signatory to modify only the email address assigned to the certificate.
- The request is added to the RA software, where the operator, once the data has been reviewed, asks the CA to issue the certificate.
- As a general rule, a new certificate is issued, taking the expiry date of the certificate to be renewed as the start of validity. In some cases, in the issuance processes via the web services, the renewal of the certificate is allowed with a date at the same time of renewal, subsequently proceeding to revoke the certificate to be renewed.

4.6.4 Notification of the new issued certificate to the subscriber

As this is a reissue of keys, the notification process is the same as described in point *4.3.2. Notification to the subscriber of the issuance* of the certificate.

4.6.5 Conduct constituting acceptance of the renewed certificate

As this is a new key issue, the acceptance process is the same as described in point *4.4.1. Conduct constituting acceptance of the certificate*.

4.6.6 Publication of the renewed certificate by the CA

As this is a new key issue, the publication process is the same as described in point 4.4.2. *Publication of the certificate by the CA.*

4.6.7 Notification of the issuance of the renewed certificate to other entities

There are no processes for notifying other entities of the renewal of a certificate.

4.7 RE-ISSUANCE OF CERTIFICATES

The renewal and issuance of new certificates after revocation, suspension or modification is always performed by generating new keys, therefore, there is no specific procedure under this CPS for the reissuance of a certificate with new keys.

4.8 AMENDMENT OF CERTIFICATES

Any need to modify certificates will involve a new request. First the certificate will be revoked and a new one will be issued with the corrected data. Therefore, there is no certificate modification procedure.

In the case of a certificate replacement process, this will be considered a renewal and will be taken into account when calculating the years of renewal without physical presence, as required by law.

Certificates may be replaced as a renewal when the attributes of the Signatory or key holder that are part of the uniqueness check foreseen for this policy have not changed.

4.9 SUSPENSION AND REVOCATION OF CERTIFICATES

4.9.1 Circumstances for revocation of certificates

Revocation shall be understood as a change in the status of a certificate due to the loss of validity of the certificate due to circumstances other than its expiry.

Possible reasons for revocation are:

- Request made by the Signatory, a person representing the Signatory or an authorized third party.
- Death of the Signatory or judicial modified capacity, total or partial
- Extinction of the legal personality or dissolution of the Creator of the seal
- Incorrect certificate data,
- Change since the time of issuance relating to the data or circumstances of the Signatory, of its power of attorney or relating to the entity that represents or to which the signatory is linked.
- Discovery of the falsity or inaccuracy of the data provided for the issuance of the certificate and contained therein, or subsequent alteration of the circumstances verified for the issuance of the certificate, such as those relating to the position.
- Violation or compromise of the key (theft, loss, ...).
- Violation, compromise or loss of control of the key activation data (PIN).
- Replacement of the certificate
- End of the stipulated suspension period
- When the cryptographic algorithms used were compromised, not allowing to ensure the relationship between the public and private key.
- Compromise of the CA keys

- If it is found that the cryptographic mechanisms used to generate the certificates do not meet the minimum security standards necessary to ensure their security.
- That the certificate no longer complies with the CPs
- Judicial or administrative resolution ordering it
- CA ceases operations or because the certificate no longer serves the purpose for which it was issued according to the contractual conditions agreed with the Subject and/or the Subscriber.

4.9.2 Who can request revocation

Revocation of a certificate may be requested by:

- The Subject/Holder
- The Authorised Applicant.
- The entity/organisation (through a representative of the entity/organisation)
- The Subscriber if different than the Subject
- The RA or the CA.
- It is also possible for third parties or interested parties to report any circumstances that could entail to revocation. Such circumstances must be verified by the PSC or the RA who will take the revocation decision.

4.9.3 Revocation process

Requests for revocation and suspension shall be made in accordance with the means of identification set out in point .3.4. *Revocation of the key'*. In addition, the CA or RA may make available additional methods for submitting the revocation request, provided that such methods allow for a correct identification of the Subject.

In the event of revocation due to non-payment of the price of the certificate issued, the RA or CA will previously and on two successive occasions request the Signatory to the contact email address to regularise this situation within 8 days, failing which, the revocation will be immediate.

Once the revocation request has been validated by a manager, it will be sent to an RA operator who will proceed with the revocation through the CA's certificate management application.

By procedure, it has been established that the RA operator that revokes a certificate must be different from the one that validated the issuance of that certificate. An exception to the above is the situation of an external RA with a single operator, in which case it will be allowed to perform validations and revocations under the control of the PSC RA, which must apply specific measures to prevent malpractice (control of deadlines between issuance and revocation, control of the reasons given, unannounced audits, etc.).

Once the certificate has been revoked, a notification is sent by email to the Subscriber informing them of the time of suspension and the reason for the suspension. If there is a Subscriber other than the Subject(s) holding the revoked certificates, the CA notifies the Subscriber with whom the CA has signed a specific agreement of the revocation.

4.9.4 Grace period for the revocation request

Not stipulated.

4.9.5 Revocation request processing period

The revocation period from the moment Signaturit or an RA has authenticated knowledge of the certificate revocation request will be a maximum of 24 hours from the confirmation of the data, being incorporated in the next CRL to be issued and in the database of the management platform where the OCSP responder is fed.

If the revocation request cannot be confirmed within this period due to lack of information or supporting documentation, it shall not be processed and the RA Operator shall inform the revocation applicant or the manager to remedy the defects.

4.9.6 CRL verification requirements

Relying Third Parties must check the status of the certificates prior to their use, checking in any case the last CRL issued, which can be downloaded at the URL that appears in the CRL Distribution Point extension of each certificate.

Signaturit always publishes CRLs signed by the CA that issued the certificate.

The CRL contains a field (NextUpdate) with the date of its next update.

4.9.7 CRL issue frequency

The frequency at which **Signaturit Global CA** updates CRLs is at most one day, and may be issued at a shorter interval in the event of a revocation.

Signaturit will issue the last CRL of a CA when all the certificates issued under that CA are expired or revoked, due to any of the possible circumstances (expiry or revocation of the CA).

4.9.8 Maximum latency for CRLs

CRLs will be immediately available in the repository once a new CRL is generated.

4.9.9 On-line revocation check available

Signaturit offers an OCSP query service at the address specified in each certificate and in this CPS. (see section 2.1 REPOSITORY)

The access addresses to these services are referenced in the digital certificate. For CRLs in the CRL Distribution Point extension and the OCSP address in the Authority Information Access extension.

Certificates may contain more than one access address to CRLs to ensure their availability.

Signaturit does not keep revoked certificates in the CRLs after their expiry. To query expired certificates, the OCSP consultation service must be employed.

The CRLs will remain published for a minimum period of 5 years from the expiry or revocation of the CA. The OCSP service may be interrupted indefinitely in case of expiration or revocation of the CA.

Due to the different natures of the OCSP and CRL services, in case of obtaining different answers for a certificate, the one offered by the OCSP shall be kept as valid answer.

4.9.10 Requirements for online verification of revocation

It should always be verified that the CRLs are signed by the CA that issued the revoked certificate.

OCSP responses are signed by "OCSP Responder" certificates signed by the CA that issues the certificate to be consulted, so this certificate is necessary to validate the response.

4.9.11 Other available dissemination methods of revocation information

There are no other forms of consultation.

4.9.12 Special revocation requirements for compromised keys

There are no special requirements.

4.9.13 Circumstances for suspension

Suspension involves revocation in which the certificate is placed on hold (thus a particular case of revocation). It consists of a cautionary revocation of a certificate until deciding whether or not to proceed with permanent revocation or its re-activation.

The possible reasons for suspension are:

- Request made by the Signatory, a person representing the Signatory or an authorized third party.
- Judicial or administrative resolution ordering it
- In case it is noticed that the cryptographic mechanisms used for the generation of the certificates do not comply with the minimum security standards necessary to guarantee their security.
- Doubt about possible violation or endangerment of the secrecy of the signature or seal creation data, or of the trust service provider, or improper use of such data by a third party.
- Doubt about possible falsity or inaccuracy of the data provided for the issuance of the certificate and contained therein, or subsequent alteration of the circumstances verified for the issuance of the certificate, such as those relating to the position.

A certificate in a suspended state shall be clearly visible in the revocation consultations to verify revocation as indicated in point *4.9.9. On-line revocation check available* and under the same conditions as revocation consultations (since it is a type of revocation).

4.9.14 Who can request the suspension of a certificate

By the same users as the revocation.

4.9.15 Certificate suspension request procedure

Same process as revocation, indicating that the suspension of the certificate is requested.

4.9.16 Timelines for suspension period

When a suspension occurs, Signaturit will have one week to decide the final status of the certificate: (revoked or active). If Signaturit does not have all the information necessary to verify

its definitive status within this period, Signaturit will revoke the certificate for an unknown reason.

4.10 CERTIFICATE CONSULTATIONS SERVICES

The CPS publishes an updated repository with the information of the certificates which can be consulted from the DN. (see section 2.1 REPOSITORY)

4.11 CERTIFICATE EXPIRY

The expiry of the certificates is established as specified in the certificate profiles.

4.12 KEY ESCROW AND RECOVERY

Signaturit does not directly escrow of keys in software format (PKCS#12).

The escrow of keys in centralised format is done in accordance with the IvSign PS on HSM devices, without consideration of QSCD or HSM with certification as QSCD. These keys cannot be exported and under the exclusive control of its holder.

5 PHYSICAL SECURITY, PROCEDURAL AND PERSONNEL CONTROLS

Signaturit Global CA is a Subordinate CA of Ivnosys Solutions, which uses the same technical infrastructure as the Ivnosys Solutions Root CA to operate. Therefore, at a general level, the controls defined in the **IvSign Root CA** CPS apply to it.

The specific aspects affecting Signaturit Global CA as a CA operator are detailed below.

As for the Centralised Key Management Platform (IvSign), the controls applied can be consulted in its own Statement Management Practices.

5.1 PHYSICAL SECURITY CONTROLS

Having contracted the infrastructure from which Signaturit Global CA provides its services to Ivnosys Soluciones, S.L.U., there are no additional stipulations to those specific to the infrastructure, which is subject to annual validations of the UNE-ISO/IEC 27001 standard for systems that support trust services, which in turn regulates the establishment of appropriate processes to ensure proper management of security in information systems.

5.1.1 DC Location and characteristics

The infrastructure used for the operation and contingency service of the CA is located in two Ivnosys Soluciones data centres (DC) that guarantee 24x7 availability of the communication systems and availability of the systems.

The DCs are located within the territory of the European Union.

5.1.2 Physical access control

The centre has the following physical security measures:

- Video surveillance and perimeter video recording in accesses, parking and installation areas.
- 24x7 staff at the centre
- Access control to the building:
    - The centre has an access control system that guarantees secure 24x7x365 access to the customer's authorised personnel to the contracted service area.
    - Accesses are logged individually with personal data of the customer's authorised personnel.
    - Multi-level access is restricted to all sensitive areas of the centre, with contactless card, fingerprint and/or key.
- Access to the security zones is protected with dual control and constantly monitored by CCTV and zone opening sensors.

5.1.3 Electric power and air conditioning

The centre has high availability energy services with the following infrastructures:

- Two alternate UPS rooms with 120kvAs UPS in 2N configuration.
- Backup generator sets in N+1 configuration
- Fuel tanks for an autonomy of more than 48 hours of operation of the centre.
- Room electrical panels supplied from independent UPS groups.

The climate control in the DC complies with ETSI EN 300 019 class 3.1, "Communication centres".

The technical rooms are air-conditioned with split air-condensing units, with air supply through a false floor and humidifier, with redundant and independent direct expansion in each room, in N + 1 rotary configuration. The external air supply for ventilation of the DP rooms is taken from the duct network coming from the external air supply fan, which passes through a filtering unit that maintains the biological conditions and active chemical substances.

5.1.4 Exposure to water

The DC is located in an area where the risk of flooding is null, being situated 1500 metres from an area of risk type 5, low frequency (less than 500 years).

5.1.5 Fire protection and fire prevention

The centre's fire extinguishing system covers technical rooms and critical facilities:

- Detection systems consisting of ionic smoke and flue gas detectors.
- Detection zones controlled by modular microprocessed analogue control panel with full autonomy of signalling, fire and fault centralisation.
- Extinguishing agent FE-13.

5.1.6 Media storage

Each removable Storage Media (tapes, cartridges, CDs, disks, etc.) remains accessible only to authorised personnel by physical access measures to the DC and the corresponding RACK cabinet.

5.1.7 Off-site backup

A backup copy shall be kept in a different DC from the one from which the service is provided with a frequency of less than 7 days.

5.2 PROCEDURAL CONTROLS

5.2.1 Trusted roles

The trusted roles for the **Signaturit Global CA** operation are shared with the Ivnosys Solutions trust roles, namely:

ROLE	DESCRIPTION
Internal Auditor	Responsible for compliance with operational procedures. Authorised to view TSP trusted services audit files and records. These functions will report to the Strategic Compliance Directorate.
Systems Administrator	Responsible for the proper functioning of communications and systems supporting the CA.
RA Operator	Person responsible for approving certification requests made by the Signatory. RA operators shall also act as Revocation Operators.
Head of Security	Responsible for coordinating, controlling and enforcing the security measures defined by Ivnosys Soluciones' security policies. He/she must be in charge of the aspects related to information security: logical, physical, network, organisational, etc.
Cryptographic operator	Persons responsible for the activation of cryptographic modules for Root and subordinate key management.

5.2.2 Number of people required per task

The following table sets out the number of people required for the execution of the tasks of each trust role in the n of m people rule.

ROLE	NUMBER OF PEOPLE

Internal Auditor	1 of 1 people.
Systems Administrator	1 of 1 people.
RA Operator	1 of multiple persons.
Head of Security	1 of 1 people.
Cryptographic operator	3 of 5 for Root devices 2 of 5 for intermediate key devices

5.2.3 Identification and authentication for each role

Each role is assigned one or more persons, all of whom are appointed by the management. The cryptographic operators will be the custodians of the cryptographic tokens for device management. The rest of the roles will be authenticated by the users and certificates of the Active Directory or the specific IvSign systems (user and password) or the CA (digital certificate), depending on the functions to be performed.

5.2.4 Roles requiring segregation of duties

Incompatibilities between trust roles are detailed below.

ROLE	NUMBER OF PEOPLE
Internal Auditor	Incompatible with any other role.
Systems Administrator	Incompatible with Internal Auditor and Security Officer.
RA Operator	Incompatible with Internal Auditor. An RA operator that has issued a certificate may not revoke the same certificate, unless an exception is made in clause 4.9.3.
Head of Security	Incompatible with Internal Auditor and System Administrator.
Cryptographic operator	Incompatible with Internal Auditor.

5.3 PERSONNEL SECURITY CONTROLS

5.3.1 Requirements for criminal records, qualifications, experience and credentials

The TSP ensures that the personnel designated as RA operators are reliable and, where appropriate, that they are appointed by the delegated body to perform the registration tasks.

For in-house staff, Signaturit will carry out a selection process based on personal interviews with candidates to assess their qualifications and experience, and requires them to undergo role-specific in-house training.

5.3.2 Criminal record verification procedures

Signaturit may request certificates attesting to the absence of a criminal record for its employees in accordance with the provisions of internal procedure **PG002 - Training and Security Procedure**.

5.3.3 Requirements and frequency of training updates

Signaturit draws up an annual Training Plan where staff training needs are detected and planned appropriately.

Specifically, the RA Operator will have taken a preparation course for the performance of the request validation tasks given by Signaturit or Ivnosys Solutions.

5.3.4 Training requirements

For new recruits, the area and product managers, in addition to the specific technical training for their position, must ensure that they are familiar with the Signaturit and/or Ivnosys Soluciones ISMS policy, procedures and requirements, knowing the consequences of a deviation from these specified procedures. A Welcome Manual is available to facilitate this task.

5.3.5 Frequency and sequence of task rotation.

There are no special tasks requiring staff rotation.

5.3.6 Penalties for unauthorised actions

The disciplinary process is specified in the internal procedure **PG002 - Training and Safety Procedure** and is based on the Royal Legislative Decree 2/2015, of 23 October, which approves the revised text of the Workers' Statute Law.

5.3.7 Requirements for independent hiring

Operators of a delegated RA will be personnel under the control and responsibility of the delegated RA organisation and must be authorised by Signaturit to perform the registration tasks and, after receiving the training required for an RA Operator.

5.3.8 Documentation provided to personnel

The one stipulated at a general level in the Signaturit Welcome Manual and the specific one for the job to be carried out (operating manuals, technical or programming procedures, support procedures, etc.).

RA operators receive the manual RA Operation Guide (applications and certificates) and the documentation matrix for the issuance of qualified certificates.

5.4 REGISTRATION AUDIT PROCEDURES

Signaturit Global CA by Signaturit is a Subordinate CA of IvSign Root CA by Ivnosys Soluciones that uses to operate the same technical infrastructure as the IvSign Root CA by Ivnosys Soluciones. Therefore, the procedures defined in the IvSign Root CA CPS apply to it.

Similarly, the IvSign Service has its own procedures according to its PS.

5.5 RECORDS FILING

Signaturit Global CA by Signaturit is a Subordinate CA of IvSign Root CA by Ivnosys Soluciones that uses the same technical infrastructure to operate as the IvSign Root CA by Ivnosys Soluciones. Therefore, the log archiving rules defined in the IvSign Root CA CPS apply to it.

With respect to the IvSign Service, it does not support information files beyond the audit information indicated in the previous point.

However, the record keeping procedures in relation to AR documentation that apply to Signaturit Global CA are set out below.

5.5.1 Type of registered files

Signaturit or its ARs will store directly:

- All data relating to the certificates, including the contracts with the signatories and RA. Data relating to their identification and location.
- Requests for certificates issuance and revocation.
- Type of document submitted in the certificate application.
- Identity of the Registration Authority accepting the certificate request.
- Unique ID number provided by the above document.
- Certification Policies and Practices

Signaturit is responsible for the correct archiving of all this material.

5.5.2 Retention period for filing

Certificates, contracts with the Subjects/Signatories and any information relating to the identification and authentication of the Subject/Signatory shall be retained for at least 15 years from the expiry of the validity of each certificate or from its revocation.

5.5.3 Filing protection

Signaturit's AR archive is electronic. The protection measures are those established in the UNE-ISO/IEC 27001 standard for its entire ISMS.

5.5.4 Procedure for file backup

Signaturit ensures the protection of the archive through a daily backup policy.

5.5.5 Requirements for time-stamping of records

There are no special specifications for the time stamping of the file.

5.5.6 Audit information collection system

Through the systems of the supplier Ivnosys Soluciones.

5.5.7 Procedures to obtain and verify filed information

The management of the archive is the one specified for backups through its supplier Ivnosys Soluciones. Access to the archived information must be requested to the Ivnosys Soluciones systems manager by the interested person or person with sufficient powers of representation of the organisation.

5.6 CHANGE OF KEYS

The change of end-entity keys is performed by carrying out a new issuance process.

The key change of the subordinate CA will be performed before the CA certificate expires in accordance with the procedures established by Ivnosys Solutions. The CA certificate to be updated and its private key will only be used for signing CRLs as long as there are active certificates issued by that CA. A new CA certificate will be generated with a new private key and a CN (common name) different to that of the CA certificate to be replaced.

A CA's certificate shall also be changed when the state of the art cryptographic technology (algorithms, key size, etc.) so requires.

5.7 DISASTER RECOVERY

5.7.1 Incident handling procedures

The treatment of incidents in Signaturit's ISMS is included in specific procedures of the UNE-ISO/IEC 27001 standard certification.

CA incidents will be immediately communicated to Ivnosys Solutions for management and treatment.

5.7.2 IT resources, software and corrupt data

The IvSign Root CA CPS and the IvSign PS shall be followed. In the event that Signaturit detects data problems, this shall be treated as an incident in accordance with the provisions of the previous point.

5.7.3 Proceduresif an entity's private key is compromised

Knowledge of the compromise of an end-entity key by Signaturit or an RA will trigger the process of revocation of the private key and its notification to the holders.

Signaturit will in any case maintain the publication of a final CRL once all CA certificates have been revoked, following the Signaturit/Ivnosys Disaster Recovery Plan.

5.7.4 Capability of business continuity when faced with disasters

Signaturit has a business continuity plan for its ISMS system in accordance with the UNE-ISO/IEC 27001 standard certification.

Additionally, the continuity capacity of the Signaturit Global CA in the event of a disaster is subject to that of Ivnosys Solutions as a CA, which is reflected in risk management, which has a Business Continuity Management System (BCMS) implemented and audited in accordance with the ISO 22301 standard. The scope of the BCMS includes all trusted services of the TSP, including IvSign Root CA.

The BCMS has two main management processes:

- **Continuity Management**, which is triggered by any service continuity incident.
- **Crisis Management**

The **Business Continuity Plan** provides the planning, responsibilities and guidance for Ivnosys Soluciones to be able to provide the continuity of critical services in the face of existing conditions and threats at any given time. Although the severity of an emergency cannot be predicted, this plan seeks to minimise the impact of its consequences on the company's critical operations and human resources.

The **Business Continuity Operating Plan** contains the predetermined continuity and recovery strategies and instructions that Ivnosys Solutions must follow during a crisis to minimise any business impact. The objective is to recover critical processes within an acceptable timeframe.

5.8 CA TERMINATION

Signaturit has a Termiantion Plan, the procedure for which is defined in a specific document. This plan is based on allowing continuity of service as the first option and defines the communication plan to all affected parties (CAs, end users and regulatory body) both in the event that the service is transferred to another provider and if the service is finally suspended.

The Termination Plan guarantees that the CRLs remain available to the degree possible at their original URL and they will always be sent to the supervisory body for their custody and publication as set out in the Electronic Signature Law.

6 TECHNICAL SECURITY CONTROLS

6.1 GENERATION AND INSTALLATION OF KEY PAIRS

6.1.1 Key pair generation

The generation of Signaturit Global CA intermediate keys is performed according to Ivnosys Ceremony Solutions' processes of generation and management of root and subordinate keys on Common Criteria EAL4+ certified HSM equipment in a secure environment.

The generation of the end-entity keys in PKCS#12 software format is carried out prior to download by the holder, using the AR tools provided by Ivnosys Solutions and following the controls established by Ivnosys Solutions and reflected in its own CPS.

The generation of the end-entity key pair in the centralised key management platform is handled by the **IvSign** PS, through a direct integration process from the Ivnosys Solutions key management systems.

6.1.2 Delivery of the private key to the subscriber

The delivery of the private key in software format to the subscriber is done at the time of its generation through an on-line process triggered by the subscriber himself. This process can be carried out after acceptance by an RA operator. After validation, the subscriber will receive an e-mail with the keys that will allow him/her to download his/her certificate in PKCS#12 format.

The delivery of the centralised private key control to its subscriber is carried out in accordance with the **IvSign** PS, through the account generated for this purpose. The private key activation PIN will be delivered to the specified email address of the subscriber.

6.1.3 Delivery of the public key to the certificate subscriber

Under this policy the public key is always delivered together with the private key, at the time of generation and download by the holder, within the PKCS#12 format.

For keys issued in centralised format the public key can be downloaded from the **IvSign** Service control panel.

For certificates issued on Hardware, the public key will be downloaded by the applicant at the time of generating the certificate, once the CSR has been provided (not available in version 1 of this CPS).

6.1.4 Delivery of the CA's public key to users

The Signaturit Global CA public key will be available for download on-line in the corresponding public repository (See point 2.2. Publication of certificate information).

6.1.5 Key length

The key length for the CA is 4,096 bits using a sha256WithRSAEncryption signature algorithm.

The Subject/Signatory's private keys are based on the **RSA** algorithm with a minimum length of **2048** bits.

6.1.6 Public key generation parameters and quality control

The certificate of the Signaturit Global CA and the Signatories follow the RFC 5280 and ETSI EN 319 412 standards.

6.1.7 Key usages

The restricted use of the key is defined in the content of the certificate at the extensions: keyUsage, extendedKeyUsage and basicConstraints, pursuant to the rules established in the standards detailed in the previous point.

6.2 PROTECTION OF THE PRIVATE KEY

As the Signaturit Global CA is generated in Ivnosys Solutions systems as a Subordinate CA, the private key protection procedures and controls are defined in the IvSign Root CA and IvSign PS CPS, as described below.

6.2.1 Cryptographic modules

The cryptographic modules used for the private key management of the IvSign Root CA intermediate CAs are Common Criteria EAL4+ certified.

Signatories' private keys in centralised format are generated in the HSMs of the IvSign systems (in accordance with the IvSign PS).

The private keys of the signatories of qualified signature certificates are generated in HSM devices considered as QSCDs.

6.2.2 Private key control

The private key of the IvSign Root CA is stored and guarded completely off-line, so that it can only be used by means of a key ceremony in a secure environment. Any operation with the root key cryptographic devices requires multi-person control, i.e. the intervention of n persons out of m (3 out of 5 in the case of the root entity cryptographic devices).

The private key of the Signaturit Global CA intermediate CA is used from the CA management application by means of a client licence configured in the application.

The operation of private key generation in the Signaturit Global CA's cryptographic devices requires multi-person control, i.e. the intervention of n persons out of a total of m (2 out of 5 in the case of the intermediate CA's cryptographic devices).

The end-entity private keys in software format (PKCS#12) are generated at the time of download by the holder and protected by a password. This password must be kept by the holder from the moment it is given to them.

The end-entity private keys in centralised format are generated in IvSign HSM devices and guarded with a double encryption: the master key of the cryptographic device and the user's PIN. Only by providing the PIN can the private key be activated, so the holder must maintain control of this PIN.

6.2.3 Safeguarding private keys

The IvSin Root CA's root entity keys are kept in a safe inside the CA's high security environment.

Ivnosys Solutions stores Signaturit Global CA intermediate CA certificates in cryptographic devices located in highly secure environments.

Signatory keys are only held by the PSC in the case of centralised certificates in accordance with the IvSign PS.

6.2.4 Backup private key

The CA's keys are backed up on several devices in high availability and in a contingency centre. In addition, encrypted copies external to the devices are stored in highly secure areas on FIPS 140-2 compliant storage systems and are controlled by 3 out of 5 persons for decryption and restoration.

Signatories' keys held by IvSign are governed by their statement of practice.

6.2.5 Filing private keys

CA keys are archived for a period of 10 years from the last issuance of a certificate for these keys.

The Signatory shall be responsible for the destruction of its keys in software format.

The archiving of centralised keys shall be governed by the IvSign Practice Statement.

6.2.6 Generating private key in cryptographic modules

CA keys are always generated inside the cryptographic modules intended for this purpose.

The centralised keys are generated in the same way in the cryptographic modules of the IvSign system.

6.2.7 Storage of private keys in cryptographic modules

CA keys are stored and used in the cryptographic modules intended for this purpose, and cannot be exported after the initial backups have been made.

6.2.8 Private key activation method

Signatories' keys in software format are activated by entering the key PIN. Each signature application can manage differently the number of times it requests the PIN within the same session or work process.

Centralised keys are activated as specified in the IvSign PS, requiring a login and entry of the activation PIN to perform the signature. The signature software applications integrated with IvSign may manage the number of times the PIN is requested in a single session or work process differently.

Intermediate CA keys are activated exclusively from CA management applications via direct connectivity to cryptographic devices.

Root keys can only be activated by the intervention of 3 persons out of a total of 5.

6.2.9 Private key deactivation method

Signatories' keys in software format are deactivated by the user by deleting them from the application where they have been configured.

Centralised keys are deactivated as specified in the IvSign PS and a login is required for deactivation.

Intermediate CA keys are deactivated by processes controlled by cryptographic operators.

6.2.10 Private key destruction method

Signatories' keys in software format are destroyed by the user by deleting all copies of the software file containing the private key, after deactivation in accordance with the previous point.

Centralised keys are destroyed as specified in the IvSign PS and a login is required for destruction.

Intermediate CA keys are destroyed by processes controlled by cryptographic operators.

6.2.11 Qualification of the cryptographic module

The cryptographic devices used by the CA comply with Common Criteria EAL4+ security standards.

The devices used for centralised qualified signature are qualified devices (QSCD).

6.3 OTHER ASPECTS IN KEY MANAGEMENT

6.3.1 Filing the public key

The filing of the public keys will be carried out by the TSP in the Ivnosys Solutions infrastructure, for a minimum period of 15 years from the expiry of the keys, as long as the technology at any given time allows it.

6.3.2 Usage period for public and private keys

The validity period of the certificate is determined according to the state of the art and cryptographic technology and according to the intended use of the certificate.

Private key must not be used beyond the validity period of the associated public key certificate. Certificates issued to natural or legal persons are valid for a maximum of 60 months.

Public key or its public key certificate can be used as a verification mechanism for data encrypted with the public key outside the temporary scope for validation purposes.

Private key may be used outside the period marked by the corresponding digital certificate, only for the recovery of encrypted data.

6.4 PRIVATE KEY ACTIVATION DATA

This section describes the processes related to the activation data of the end-entity private keys, generated in PKCS#12 format.

For centralised keys stored in the **IvSign CA** Platform, the provisions of its MPS shall apply.

6.4.1 Installation and generation of activation data

The certificate is delivered in a standardised PKCS#12 file protected by a password generated by the management application and delivered to the subject via a link for generation through the mail indicated in the application.

6.4.2 Protection of activation data

The activation data are communicated to the subject via the e-mail address indicated in the request.

6.4.3 Other issues of activation data

There are no other activation data considerations.

6.5 COMPUTER SECURITY CONTROLS

At a general level, the IT security controls of the systems are those used by Ivnosys Soluciones to operate the Signaturit Global CA and the RA of Signaturit Global CA. Signaturit and Ivnosys Soluciones use reliable systems for the provision of certification services and both have carried out IT controls and audits to manage their assets with the level of security required for the management of these systems. In relation to information security, both entities apply their ISMS certified by the UNE-ISO/IEC 27001 standard.

6.5.1 Specific technical IT security requirements

Those established in the ISMS of Signaturit and Ivnosys Solutions, for the CA and RA operation systems of Signaturit Global CA, as well as those established in the PS of IvSign, apply.

6.5.2 Assessment of IT security

The security of systems is reflected by an initial risk analysis such that the security measures implemented are in response to the likelihood and impact of a defined threat group being able to exploit security breaches.

6.6 LIFE CYCLE SECURITY CONTROLS

6.6.1 Development systems controls

The system development systems that support the Signaturit Global CA are the responsibility of Ivnosys Soluciones, which uses commercial CA management software, and therefore does not carry out its own developments for the issuance, renewal and revocation of certificates.

For the **IvSign** centralised key system, owned by Ivnosys Solutions, please refer to its PS.

6.6.2 Security management controls

The security management controls of Signaturit's and Ivnosys Soluciones' ISMS are defined in the Statement of Applicability (SOA) of the UNE-ISO/IEC 27001 standard certification.

Signaturit organises annual training and awareness-raising activities for employees in the field of security.

Signaturit contractually regulates the equivalent security measures for suppliers who collaborate in the provision of the service.

6.6.3 Life cycle security controls

The certificate lifecycle security controls are those applied by Ivnosys Solutions, which has specific instructions within the Physical and Environmental Security procedures for the reuse or safe removal of equipment, where the steps prior to removal and the processes for safe disposal or destruction, among others, of the HSM QSCD devices that store the keys of the centralised certificates are specified.

6.7 NETWORK SECURITY CONTROLS

The applicable network security controls are part of the ISMS of Ivnosys Soluciones and are defined in the Statement of Applicability (SOA) of the UNE-ISO/IEC 27001 standard certification.

6.8 TIME SOURCES

Signaturit uses Ivnosys Solutions Time Stamping services. All Ivnosys Solutions servers are time synchronised with reliable external sources.

7 CERTIFICATE AND CRLS PROFILES

7.1 CERTIFICATE PROFILES

Certificate profiles follow the RFC 5280 standard.

All qualified certificates issued under this policy are in compliance with the X.509 version 3 standard and the different profiles described in EN 319 412.

7.1.1 Version number

X.509 Version 3.

7.1.2 Certificate extensions

Depending on the type of certificate, they are identified in the specific certification profiles.

7.1.3 Object Identifiers (OIDs) of the algorithms

The object identifier of the signature algorithm is 1.2.840.113549.1.1.11 - sha256WithRSAEncryption.

The Subject Public Key Info field (1.2.840.113549.1.1.1) incorporates the rsaEncryption value.

7.1.4 Name format

The naming format follows the guidelines described in this CPS. The exact semantics are described in the specific certification profiles.

7.1.5 Naming constraints

Name restrictions follow the guidelines described in this CPS. Specific restrictions for each type of certificate will be specified in each of the certification profiles.

7.1.6 Object Identifier (OID)of the Certification Policy

The OIDs of the certification policies are detailed in this CPS in point 1.1. General Overview.

7.1.7 Use of the "*Policy Constraints*" extension

Not stipulated in this CPS.

7.1.8 Syntax and semantics of policy qualifiers

Not stipulated in this CPS.

7.1.9 Semantic handling for the "Certificate Policy" critical extension

The "Certificate Policy" extension identifies the policy that defines the practices that Signaturit explicitly associates with the certificate. The policies applied to each type of certificate can be found in point 1.1. General Overview which must be interpreted according to the following table:

PSC	Service	Qualification	Type of certificate	Linking	Type of linkage	Format	Use
1.3.6.1.4.1.50646: Signaturit Soluciones	5: Signaturit Global CA	16: Qualified certificates	1: Electronic signature	1: Citizen		1: Centralised 2: Software 3: Centralised QSCD 4: HSM 5: HW	1: Signature 2: Authentication 3. Encryption
				2: Corporate			
				12: EU Corporate			
				3: Representation	1: General powers		
					2: Public Administration processes		
					3: Special power of attorney		
				4: Civil servant	1: Medium level		
					2: High level		

				5: Public employee with pseudonym			
			6: Electronic seal	2: Corporate			
				4: Public Adminsitrations.	1: Medium level		
					2: High level		
				8: Timestamp			

7.2 CRL PROFILE

CRLs are signed by the CA that issued the certificates.

7.2.1 Version number

The CRLs issued by the CA are version 2.

7.2.2 CRL and extensions

CRLs shall include the field "CRL number".

CRLs shall not include the extension "ExpiredCertsOnCRL".

7.3 OCSP PROFILE

The CA has an OCSP responder certificate. This certificate is used to sign and verify the OCSP service responses on the status of the certificates issued by this CA.

7.3.1 OSCP responder certificate issuance frequency

OCSP responder certificates shall be renewed annually along with the keys thereof, the previous keys shall be deleted according to the procedures established by Signaturit Global CA by trusted personnel of the TSP.

The algorithms to be applied in the generation of the certificate and its key pair will be periodically reviewed and updated if necessary according to the recommendations indicated in the ETSI TS 119 312 standard or equivalent standard.

Currently the key size used is 2048 bits and the signature algorithm sha256WithRSAEncryption.

7.3.2 Version number

OCSP responder certificates are version 3. These certificates are issued by each Signaturit managed CA according to the RFC 6960 standard.

7.3.3 OCSP extensions

OCSP Responder certificates include the following extensions:

- Non-revocation check enabled
- Certification policy
- CRL distribution point

This certificate has the following identification:

Distinguised Name	CN = OCSP Responder Signaturit Global CA OR = SIGNATURIT SOLUTIONS S.L.U. 2.5.4.97 = VATES-B66024167 S = BARCELONA C = EN
OID	1.3.6.1.4.1.50646.5.16.9.7.

8 CONFORMITY AUDIT AND OTHER ASSESSMENTS

Qualified trust services are audited at least biennially (every two years) by a duly accredited Conformity Assessment Body, in application of EU Regulation 910/2014 (eIDAS).

Signaturit's Conformity Assessment Body is **Trust Conformity Assessment Body S.L.**

Additionally, all trust services offered by Signaturit are within the scope of the following quality and security audits:

- Information Security Management System.
    - Renewal every 3 years with annual follow-up audits
    - Auditor: **AENOR Internacional S.A.U.**
    - ISO/IEC 27001 Standard
- Quality Management System.
    - Renewal every 3 years with annual follow-up audits.
    - Auditor: **AENOR Internacional S.A.U.**
    - Standard UNE-EN ISO 9001:2015

8.1.1 Frequency and circumstances of the audit

Signaturit is subject to the following external audits covering the operation of the CA:

- Accreditation of compliance with a Trusted e-Services Management System, in application of EU Regulation 910/2014 (eIDAS).
    - The audit frequency is biennial (at least every two years), with annual follow-up audits.
- Information Security Management System Certificate.
    - Renewal every 3 years with annual follow-up audits.
- Quality Management System Certificate.
    - Renewal every 3 years with annual follow-up audits.

In addition, its infrastructure provider Ivnosys Soluciones, as a Qualified Trust Service Provider, also has eIDAS service compliance accreditations as well as certifications for its Information Security Management System (UNE-ISO/IEC 27001), Quality Management System (UNE-EN-ISO 9001), Business Continuity Management System (UNE-EN ISO 22301) and National Security Scheme Medium Level.

The aforementioned certifications of Signaturit and Ivnosys Soluciones can be consulted at:

https://www.signaturit.com/es/legalidad/

https://www.signaturit.com/es/legalidad-ivnosys/

With these audits Signaturit guarantees that the entire management and security system of the Certification Authority is reviewed at least every 12 months.

8.1.2 Auditor identification

Certification audits are carried out by:

- Trusted Customer Electronic Services Management System, in application of EU Regulation 910/2014 (eIDAS): **Trust Conformity Assessment Body S.L.**
- Information Security Management System: **AENOR Internacional S.A.U.**
- Quality Management System: **AENOR Internacional S.A.U.**

8.1.3 Auditor's relationship with the audited entity

There is no financial or organisational linkage or dependence between the audit firms and Ivnosys Solutions.

8.1.4 Topics covered by the audit

The audits carried out cover the following aspects:

- Electronic Customer Trust Services Management System, in application of EU Regulation 910/2014 (eIDAS):
    - Electronic signature digital certificate issuing service
    - Standards of application: ETSI EN 319 401, ETSI EN 319 411-1, ETSI EN 319 411-2, ETSI EN 319 412-1, ETSI EN 319 412-2, ETSI EN 319 412-5.
- Information Security Management System:
    - Scope: among others, the information systems that support the installation and operation processes of the following trusted service in cloud mode: Management of the life cycle of digital certificates (issuance, validation, maintenance and revocation).
    - Standard of application: UNE-ISO/IEC 27001:2014
- Quality Management System:
    - Scope: Software design, development and implementation activities; User support and corrective, perfective and evolutive software maintenance.
    - Applicable standard: UNE-EN-ISO 9001:2008

8.1.5 Actions taken due to deficiency

All audits have a final audit report where, if applicable, all corrective actions have been taken for minor non-conformities that have led to the granting of certification.

8.1.6 Reporting results

The results of the CSP audit shall be communicated to the regulatory body in accordance with the eIDAS Regulation.

9 OTHER LEGAL AND BUSINESS REQUIREMENTS

9.1 FEES

9.1.1 Certificate issuance and renewal fees

All certificate issuance and renewal fees are subject to prior commercial negotiation. To obtain a commercial proposal, please contact Signaturit's Commercial Department via the contact details indicated at https://www.signaturit.com/es/contacto/.

9.1.2 Certificate access fee

Access to public information on certificates is free of charge.

9.1.3 Fees for access to information on the status of certificates or revoked certificates

Signaturit provides, free of charge, information on the revocation status of certificates through revoked certificate lists (CRL) and the OCSP service.

9.1.4 Other services

Key centralisation services are offered commercially separately from certificate issuance services, in accordance with the commercial offer received by the customer.

9.1.5 Reimbursement policy

Signaturit does not have a specific refund policy and abides by the general regulations in force.

9.2 FINANCIAL LIABILITY

Signaturit, as a Trusted Service Provider, is subject to the national rules on liability set out in the eIDAS Regulation, being liable "for damages caused deliberately or negligently to any natural or legal person due to a breach of the obligations set out".

Signaturit shall be responsible for the services provided to the CAs, and shall be liable to the users of the service and other third parties or users affected by the service in accordance with this CPS.

9.2.1 Insurance coverage

In compliance with current legislation, Signaturit has civil liability insurance covering the provision of the services identified in this PS, to the value of €3,000,000.

9.2.2 Other assets

Not stipulated

9.2.3 Assurance and guarantee for end entities

Included in the Civil Liability Insurance.

9.3 CONFIDENTIALITY

9.3.1 Scope of confidential information

Electronic signature creation data are considered confidential data which may not be disclosed by any of the parties to the extent that they have access to them.

In general, Signaturit shall consider all information that is not expressly classified as public to be confidential. Information declared as confidential shall not be disseminated without the express written consent of the entity or organisation that has granted it the confidential nature of said information, unless there is a legal requirement to do so.

9.3.2 Information outside the scope of confidentiality

The information contained in the certificates and the status of the certificates, as well as the certification policies and the certification practice statement, is not considered confidential information.

9.3.3 Responsibility to protect confidential information

The signatory is responsible for keeping the signature creation data confidential.

Signaturit applies all the necessary security measures described in this CPS to maintain the confidentiality of the information.

The identification information of the requests is collected and stored in Signaturit's certificate management system (outsourced to Ivnosys Solutions) associated in the database to each of the certificate requests.

9.4 PRIVACY POLICY

9.4.1 Privacy Plan

In its risk analysis, Signaturit has drawn up a data impact assessment and has established the necessary security controls in accordance with this analysis within the scope of its Information Security Management System (ISMS).

It has also developed a Privacy Policy in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council 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 (GDPR

- General Data Protection Regulation) and Organic Law 3/2018 of 5 December on the Protection of Personal Data and Guarantee of Digital Rights (LOPDGDD).

With regard to the personal data of Applicants, Subjects/Holders and relations with entities, Signaturit acts as Data Controller in accordance with the RGPD and the LOPDGDD. It has a Register of Personal Data Processing Activities in which the "Certificate Management" processing is included, the purpose of which is to manage applications and certificates issued and to provide the associated certification services.

9.4.2 Information hndled as private

All non-public information is treated as private at the CA level.

9.4.3 Information not considered private

Due to the operation of the certification system itself, the personal data included in the Certificate Directory to check the validity of a given certificate and its consultation by all users, understood as those people who voluntarily trust and make use of Signaturit's certificates and always in accordance with the provisions of the Certification Policy.

9.4.4 Responsibility for the protection of private information

Signaturit treats all personal and private information in accordance with the information security documents established in the UNE-ISO/IEC 27001 standard.

9.4.5 Notice and consent to the use of private information

It is informed that, in order to fulfil the provision of the certification and electronic signature service, the competent Registration Authority (RA) will have access to the data collected in the request for certification services, for the fulfilment of its RA functions.

This information will be noted and accepted by the applicant at the time of entering the certificate data in the application. Similarly, in the Terms and Conditions of Use of the Certificate signed by the subscriber, the subscriber accepts the conditions regarding the use of the personal data included in the certificate.

Furthermore, due to the requirements of the electronic signature legislation, your identification data and the data associated with the issued certificate must be kept for a period of 15 years from the expiry of the certificate. Therefore, by legal imperative, you will not be able to exercise your data protection rights in full.

9.4.6 Disclosure in accordance with a legal or administrative process

Signaturit shall ensure the security of the documentation and data placed in its custody, preventing unauthorised third parties from accessing said information, except when so required by a court order or other competent authority.

9.4.7 Other circumstances of disclosure

Not stipulated.

9.5 INTELLECTUAL PROPERTY

Signaturit holds the intellectual property rights to this CPS and to the electronic certificates it issues, unless otherwise agreed.

9.5.1 CA

SIGNATURIT SOLUTIONS, S.L.U. acts as a Certification Authority, relating a specific public key to a specific person by issuing a Digital Certificate.

9.5.2 RA

The REGISTRATION AUTHORITY is responsible, among other functions, for delivering the Certificate issued in the name of the APPLICANT and verifying the identity of the APPLICANT. All or part of the RA functions may be delegated to a third party entity which shall be constituted, as the case may be, as an External Registration Authority (External RA), and which shall in any case act for the purposes of this CPS as the Registration Authority.

9.5.3 Subscriber

The APPLICANT is a natural person linked to an ENTITY (with or without legal personality) by a relationship of representation, corporate membership or by some type of commercial relationship, possessing a signature creation device, and who assumes the status of OWNER and SIGNATURE within the meaning of the legal framework applicable to the provision of the service.

9.5.4 Relying party

Person who receives an electronic transaction carried out with a certificate issued by Signaturit Global CA and who voluntarily trusts the Certificate issued by the latter.

9.5.5 Other participants

Not stipulated

9.6 REPRESENTATIONS AND GUARANTEES

9.6.1 Of the CA

In accordance with current legislation on the provision of certification services, Signaturit must guarantee compliance with the obligations and procedures described in this CPS and CP and, in this regard, is solely responsible for this, even if it delegates part of the operations to a subcontracted third party.

Signaturit is liable for damages caused to users of its services, whether the Subject or the Relying Party, and to other third parties in accordance with the terms and conditions established in current legislation.

In this regard, Signaturit is solely responsible for issuing certificates and managing them during their life cycle and, if necessary, in the event of certificate revocation. In particular, Signaturit is responsible for:

- The accuracy of all information contained in the certificate

- That the public and private key work together and complementarily, using certified cryptographic devices and mechanisms.
- The correspondence between the certificate requested and the certificate delivered.
- Publish issued certificates in a directory
- Revoking certificates as indicated in this CPS and publishing such revocations in the CRLs
- Publish this CPD and CP and inform those involved in the certification scheme of the changes.
- Protect signature creation data if applicable
- Retain the data relating to the certificates for the legally required period.

Before issuing and delivering the certificate to the subscriber, the CSP informs the subscriber of the terms and conditions relating to the use of the certificate, its price and limitations of use, by means of a subscriber contract (Terms and Conditions of Use) and by means of the PDS document or informative text, both published on its website, so that the participants are aware of the minimum contents of the CA's obligations and those of the other actors, and any changes thereto.

9.6.2 Of the RA

Article 10 of the Trusted Services Act 6/2020 states that: "*Trusted electronic service providers shall assume full liability towards third parties for the actions of persons or other providers to whom they delegate the execution of any or some of the functions necessary for the provision of trusted electronic services, including identity verification actions prior to the issuance of a qualified certificate*".

In this sense, the RAs are also bound by the terms defined in this CPS for the issuance of certificates and, prior to the start of their functions, they must formalise a private Agreement in which they assume a series of obligations and responsibilities towards the CA and towards the Subscribers and Third Parties they trust.

The RA shall be fully responsible for the identification and authentication procedure of Subscribers, Applicants, Subjects or Responsible Parties, for the complete registration of applications and validation of certificates, and for the conservation of the information and documentation accrediting the data included in the certificate and legally required. It shall do so in accordance with the provisions of this CPS or in accordance with another procedure approved by the PSC.

RAs are therefore responsible for the possible consequences of non-compliance with registration duties, and are committed to respecting this CPS, which RAs must keep under control and use as a guide.

In case of a complaint by a Subject, Subscriber or Relying Party, if there is evidence that the cause of the complaint is due to incorrect validation or verification of the data by the RA, the CA may hold the RA liable for the consequences, in accordance with the agreement signed with it.

9.6.3 Of the Applicant, Subject/Holder and Responsible Party

The Applicant as such and in its capacity as future Subject/Holder of the certificate, as well as the party responsible for the electronic seal certificate, undertakes to comply with the provisions of current regulations, and in particular to:

- Provide all information and documentation required by the CA or RA for proper identification,
- Ensure the accuracy and veracity of the information provided.
- Use the certificate in a responsible manner, safeguard the secret keys, passwords or activation pins diligently, taking reasonable precautions to prevent their loss, disclosure, modification or unauthorised use, in order to maintain exclusive control over the use of the certificate.
- Be accountable to the Entity they represent or to which they are linked in the event of unauthorised or incorrect use of the certificate.
- Request the suspension/revocation of the Certificate when any of the cases of suspension and revocation of certificates foreseen in this CPS are fulfilled.
- Immediately notify the CA or RA in the event that it detects that any incorrect or inaccurate information has been included or in the event that, unexpectedly, the information in the Certificate does not correspond to reality or has changed subsequent to its issuance.
- Immediately inform the CA or RA of any situation that may affect the validity of the Certificate, or the security of the keys, and cease its use.
- Do not use the private key or the certificate from the moment it is requested or notified by the CA or RA of the revocation of the certificate, or once the validity period of the certificate has expired.
- Authorise the CA and the RA to process the personal data contained in the certificates, within the framework of the purposes of the telematic relationship and, in any case, to comply with the legal obligations of certificate verification.
- Any other that derives from the content of the specific CPs for each type of Certificate.

9.6.4 Of the Subscriber

In addition to the provisions of current regulations, the Subscriber of a certificate shall be obliged to:

- Accept the Provider's Terms and Conditions
- Inform the RA or CA of any change in the data provided for the issuance of the certificate during its period of validity.
- Inform the RA or the CA as soon as possible of the existence of any cause for revocation.

9.6.5 Of the Relying Party

The Third Party relying on the certificate is obliged to:

- Validate the certificate through the TSL trust anchor and verify that it is a qualified certificate issued by a qualified Signaturit CA.
- Check the status of the certificate by consulting the OCSP service or the CRLs. To check expired certificates, use the OCSP query service.
- Know and submit to the guarantees, limits and responsibilities applicable to the acceptance and use of the certificates on which they rely. In particular, in the case of certificates with the attribute of representation of an Entity based on a special power of attorney or private document with limited powers, the relying Third Party must check the limits of said powers.

9.6.6 Of the Entity

In the case of certificates with a representation attribute or that imply a link between a natural person and an Entity, the Entity shall be obliged to request the CA or RA to revoke the certificate when the natural person is no longer linked to the Entity.

9.7 LIMITATIONS OF LIABILITY

According to current legislation, the liability of Signaturit and the RA does not extend to those cases in which the improper use of the certificate has its origin in conduct attributable to the Subject, and to the Relying Party for:

- Failure to provide adequate information, initially or subsequently as a result of changes in the circumstances reflected in the electronic certificate, where the inaccuracy could not be detected by the certification service provider
- Negligence with regard to the preservation of signature creation data and its confidentiality
- Failure to request the suspension or revocation of the electronic certificate data in case of doubt as to the maintenance of confidentiality
- Having used the signature after the validity period of the electronic certificate has expired.
- Exceed the limits stated in the electronic certificate.
- In conduct attributable to the Relying Party if it acts negligently, i.e. when it fails to check or take into account the restrictions in the certificate as to its possible uses and transaction amount limits; or when it fails to take into account the certificate's validity status.
- Damage caused to the Subject or third parties that he trusts due to the inaccuracy of the data contained in the electronic certificate, if these have been accredited by means of a public document, registered in a public register if this is required.
- Improper or fraudulent use of the certificate in the event that the Subject/Holder and/or the Responsible Party has transferred it or authorised its use in favour of a third party, the Subject/Holder and the Responsible Party being solely responsible for the control of the keys associated with the certificate.

Signaturit and the RAs shall not be liable in any case when faced with any of these circumstances:

- State of War, natural disasters or any other case of Force Majeure.
- For the use of certificates provided that it exceeds the provisions of the current regulations and this CPS and the Certification Policies.
- For the improper or fraudulent use of certificates or CRLs issued by the CA
- For the use of the information contained in the Certificate or in the CRL or OCSP response.
- For the damage caused during the period of verification of the causes for revocation/suspension.

- For the content of digitally signed or encrypted messages or documents.
- For non-recovery of documents encrypted with the Subject's public key.

In relation to the actions or inactions of the Relying Party, Signaturit or the RA shall not be liable if the Relying Party:

- It does not verify the restrictions contained in the certificate or in this CPD and in the CPs with respect to their possible uses.
- Failure to check the expiry date of the certificate indicated in the certificate validity extension or failure to verify the digital signature.

More generally, neither Signaturit nor the RA will be liable for the use of digital certificates in operations that contravene the Certification Policies applicable to each of the Certificates, the CPS or the CA's Contracts with the RAs or with the Subject/Holder and/or the Signatory will be considered improper uses, for the appropriate legal purposes, and the CA will therefore be exempt, in accordance with current legislation, from any liability for this improper use of the certificates by the Signatory or any third party.

Under no circumstances shall Signaturit issue any assessment of the signed content, and the signatory shall therefore assume any liability arising from the content associated with the use of a certificate. Likewise, the signatory shall be held responsible for any liability that may arise from the use of the same outside the limits and conditions of use set out in the Certification Policies applicable to each of the Certificates, the CPS and the CA's contracts with the signatory (subject), as well as any other improper use of the same arising from this section or that may be interpreted as such in accordance with current legislation.

With regard to the publication of personal data in the certificates for the necessary consultations with the parties using them and, given the impossibility of being able to control the subsequent use that users of the system may make of their data, the CA is exonerated from any liability arising from the improper use of such data.

9.8 COMPENATION

The insurance shall cover all amounts that Signaturit must legally pay, up to the contracted limit of cover, as a result of any legal proceedings in which its liability is declared.

When the revocation of a certificate at the request of the CA is unjustified, the CA may compensate those APPLICANTS who request it in writing within three months from the date of revocation. This compensation may not exceed the amount paid by the APPLICANT for obtaining the Certificate.

9.9 TERM AND TEMRINATION

9.9.1 Term

The CPS will enter into force upon publication.

As soon as a new version of the document is published, this CPS will be repealed in all points that have undergone any modification with respect to the previous version.

In general, this CPS will come into force for the subscriber of a certificate on the date of issue of the certificate and will end on the expiry dates, both of which are indicated on the Certificate,

and may be renewed in accordance with the terms set out in this CPS and the corresponding CPs.

9.9.2 Termination

Failure by either party to comply with the provisions contained in this CPS and/or the CPs shall be grounds for termination of the contract for the provision of certification services. In such a case, the non-breaching party shall be entitled to terminate the agreement with immediate effect. Failure by the APPLICANT to comply shall entitle the CA to revoke the Certificate, irrespective of any damages it may claim.

The CA shall have the right to revoke and not renew the Certificate prior to the expiry of its term in the cases provided for in the relevant CP.

The APPLICANT may freely terminate the agreement at any time by giving 30 days' written notice. In no case shall such termination entitle the APPLICANT to a refund of the amounts paid for obtaining the Certificate.

If the exercise of the rights of opposition or cancellation of the data set out in this document hinders the provision of the services covered by this contract, Signaturit shall be authorised to terminate this agreement.

9.9.3 Effects of termination and maintenance of clauses

By virtue of the survival clause, certain rules will continue to apply after the termination of the legal relationship governing the service between the parties. To this effect, the CA ensures that at least the requirements contained in sections 9.6 (Representations and Warranties), 8 (Conformity Audit) and 9.3 (Confidentiality) of this document remain in force after the termination of the service and the general conditions of issue/use.

9.9.4 Notifications and communications between participants

Both the applicant and the Relying party may contact the CA or the RA through the means indicated in this CPS or on the Signaturit website.

The CA may communicate or notify subscribers by any of the means indicated in their certificate application.

9.10 MODIFICATIONS

9.10.1 Modification procedure

This CPS shall be modified when relevant changes occur in the management of any type of certificates subject to it. There shall be at least annual revisions in the event that no changes occur during this time. These revisions will be reflected in the version table at the beginning of the document.

9.10.2 Notification mechanism and deadlines

Amendments shall be communicated to the APPLICANT, where the change has a direct impact on the rights and obligations of the APPLICANT, in accordance with the provisions of the service provision agreement accepted by the applicant at the time of confirmation of the application for a certificate.

9.10.3 Circumstances for change of OID

They are not foreseen.

9.11 CONFLICT RESOLUTION PROCEDURE

In the event of any controversy or dispute arising from these CPS and Terms and Conditions, the parties, waiving any other jurisdiction that may correspond to them, submit to the Spanish Court of Arbitration, unless the claimant is a consumer, for which the Judge or Court corresponding to the consumer's domicile will be competent.

9.12 JURISDICTION

This CPS shall be governed by Spanish and European Union legislation on certification and electronic signatures applicable at all times, and its content shall be interpreted in accordance with such legislation.

9.13 MISCELLANEOUS CLAUSES

9.13.1 Legal framework

Signaturit's Certification Policies (hereinafter CP) and this Certification Practices Statement (hereinafter CPS), together with the terms and conditions accepted at the time of application, constitute the complete agreement that shall regulate the relationship between the parties, internally and with third parties, without prejudice to the provisions of current legislation.

9.13.2 Assignment

Not stipulated.

9.13.3 Separability

Not stipulated.

9.13.4 Compliance

Not stipulated.

9.13.5 Force majeure

Neither the CA nor the RA shall be liable for any failure to perform or delay in the performance of any of the obligations under the CPs if such failure or delay results from or is the consequence of natural disasters, war, state of siege, state of alarm or health emergency or any other force majeure.

9.14 OTHER CLAUSES

Not stipulated.

ANNEX

CERTIFICATES PROFILES POLICIES OF SIGNATURIT GLOBAL CA

1 INTRODUCTION

The following ANNEX lists the specific uses of the different types of certificates issued by Signaturit Global CA.

Each type of certificate references the certification policies that apply to it:

- CA Policy. Identifies the profile within the CA itself
- eIDAS policy. Identifies the policy defined by ETSI EN 319 411 2 "Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates".
- Policy Law 40/2015, as defined in the document "PROFILES OF ELECTRONIC CERTIFICATES" - NIPO: 630-16-298-6 (not available in version 1 of this CPS)

2 CITIZEN'S CERTIFICATE

2.1 POLICY OIDS

- Software
  - 1.3.6.1.4.1.50646.5.16.1.1.2 (Signaturit Global CA)
  - 0.4.0.194112.1.0 (ETSI EN 319 411 2)

2.2 USES

Certificate issued to a natural person that guarantees the identity of the certificate holder.

The use of this certificate is restricted to the holder only, at his/her own risk.

Certificates may be used for electronic signatures and for authentication of the holder.

Centralised and software certificates will generate advanced signatures with qualified certificate.

Certificates centralised in QSCD will generate qualified signatures.

2.3 APPLICANT / HOLDER

This is the natural person identified in the certificate by their name, surname and identity document.

2.4 DOCUMENTATION

The documentation to be submitted to the Registration Authority or an On-Site Verification Point in electronic copy is an identification document as stipulated in the relevant Declaration of Practice. During identification it shall be checked against the original.