Certification Practice Statement

BEWOR

BUSINESSSOFTWARE

General Info

Document control

Safety classification:	Public
Version:	1
Edition date:	20/05/2020
File:	BEWOR_DCP_EN_V1.r2

Formal state

Created by:	Reviewed by:	Approved by:
Name: Albert Borrás Date: 06/05/2020	Name: Patricia Bodelón Date: 20/05/2021	Name: Vicente Serrano Date: 20/05/2021

Version control

Version	Changes	Description of the change	Change author	Change date
1.0	Original	Document create	Albert Borrás	06/05/2020
2.0	Without changes	Annual document review	Patricia Bodelón	20/05/2021

INDEX

1. Introduction

1.1. Presentation

This document declares the Certification Practice of the digital signature of BEWOR.

The issued certificates are the following:

- **Natural Person**
  - Qualified certificate for Natural Person on centralised HSM.
- **Entity Representative**
  - Qualified certificate for Natural Person on centralised HSM.
  - Qualified certificate for Natural Person Representative of Legal Person with the administrations on centralised HSM.
  - Qualified certificate for Natural Person Representative of Entity without Legal Personality with the administrations on centralised HSM.

1.2. Document name and identification

This document is the 'Certification Practice Statement of BEWOR".

1.2.1. Certificates' identifiers

BEWOR has assigned an object identifier (OID) to each certificate policy, for their identification by requests.

Number OID	Type of certificates
	Natural Person
1.3.6.1.4.1.55693.1.1.1	*Qualified certificate for Natural Person on centralised HSM*
	Entity Representative
1.3.6.1.4.1.55693.1.2.1	*Qualified certificate for Natural Person on centralised HSM*
1.3.6.1.4.1.55693.1.3.1	*Qualified certificate for Natural Person Representative of Legal Person with the administrations on centralised HSM*

1.3.6.1.4.1.55693.1.4.1	*Qualified certificate for Natural Person Representative of Entity without Legal Personality with the administrations on centralised HSM*

In case of contradiction between this Certification Practice Statement and other documents of practices and procedures, the established in this Practice Statement shall prevail.

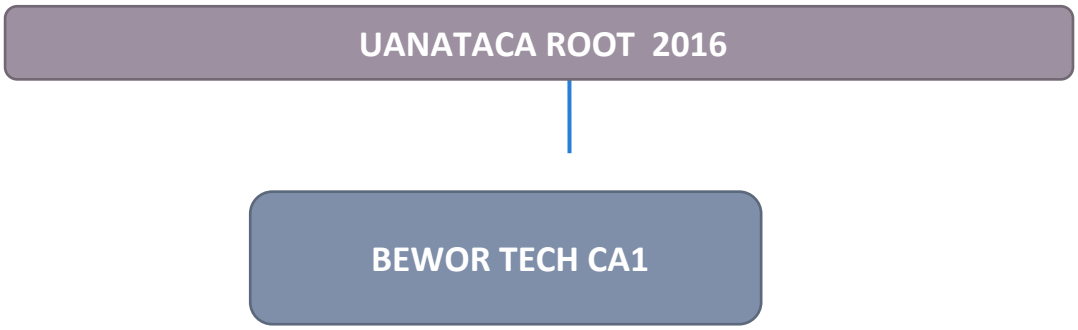
1.3. Participants in the certification services

1.3.1. Certification service provider

The electronic certification service provider is the natural or legal person that issues and manages certificates of end entities, using a Certification Entity, or provides other services relate to the electronic signature.

BEWOR is a relying electronic certification service provider, acting in accordance with Regulation (EU) 910/2014 OF THE EUROPEAN PARLAMENT AND BOARD of 23rd July of 2014 related to the electronic identification and to the relying services for electronic transactions within the domestic market and repealing Directive 1999/93/CE, as well as the technical rules of the ETSI applicable to the issuance and management of qualified certificates, mainly the 319 411-1 and EN 319 411-2, in order to facilitate the legal requirements and international recognition of his services.

To provide certification services, BEWOR has established a hierarchy of certification entities:



1.3.1.1. UANATACA ROOT 2016

This is an entity certification root of the hierarchy that issues certificates to other entities of certification and whose public key certificate has been self-signed.

Identification data:

CN:	UANATACA ROOT 2016
Digital fingerprint:	6d c0 84 50 a9 5c d3 26 62 c0 91 0f 8c 2d ce 23 0d 74 66 ad
Valid from:	Friday, 11th March 2016
Valid until:	Monday, 11th March 2041
RSA key length:	4.096 bits

1.3.1.2. BEWOR TECH CA1

This is an entity certification of the hierarchy that issues certificates to other end entities of certification and whose public key certificate has been self-signed by UANATACA ROOT 2016.

Identification data:

CN:	BEWOR TECH CA1
Digital fingerprint:	8c 62 1d 4d bd 4f 5a 18 19 97 9a d4 bb a7 10 67 c8 54 7f fe
Valid from:	Tuesday, 12 th May 2020
Valid until:	Thursday 12 th May 2033
RSA key length:	4.096 bits

1.3.2. Registry Authority

A Registry authority by BEWOR is the entity in charge of:

- Processing the certificate applications.
- Identify the applicant and verify that complies with the requirements needed for the certificate applications.
- Validating the personal conditions of the signatory of the certificate.
- Managing the key generation and the issuing of the certificate.
- Delivering the certificate to the subscriber or to the means for its generation.
- Custody of the documentation related to the identification and registry of the signers and /or subscribers and management of the life cycle of the certificates.

They will be able to act as RA of BEWOR:

- Any entity authorized by BEWOR.
- BEWOR directly.

BEWOR contractually will formalize the relations between itself and each of the entities that act as Registry Authority of BEWOR.

The entity acting as a Registry Authority by BEWOR will be able to authorize to one or more persons as Trader of the RA to operate with the emission certificates system of BEWOR on behalf of the Registry Authority.

The Registry Authority will be able to delegate the identification functions of the subscribers and /or signers, prior agreement for the delegation of these functions. BEWOR will need to expressly authorize the collaboration agreement.

In addition, the appointed units for this function will be able to be Registry Authorities according to the Practice Declaration Certification, by the certificate subscribers, such as a personal department, as they provide authentic records with regard to the relationship between the signers and the subscriber.

1.3.3. End entities

The end entities are the persons and the organizations receiving the services of the issuance, management and use of digital certificates, for identification and electronic signature.

The end entities of BEWOR of certification services will be the following:

1. Subscribers of the certification service
2. Signers
3. Relying parties

1.3.3.1. Subscribers of the certification services

The subscribers of the certification services are:

- Companies, entities, corporations and organizations that acquire them from BEWOR (directly or through a third party) for its use in its business or organizational corporate level and which have been identified in the certificates.
- Natural persons that acquire the certificates for themselves and they have been identified in the certificates.

The subscriber of the certification services acquires a license to use the certificate, for its own use – electronic seal certificates – or in order to facilitate the certification of the identity of a particular person duly authorized for various actions in the organizational area of the subscriber – electronic signature certificates. In this case, this person appears identified in the certificate.

The subscriber of the relying electronic service, is therefore, the client of the certification services provider, according to the commercial legislation, and has the rights and obligations defined by the certification services provider, which are additional and do not prejudice the rights and obligations of the signers, as it is authorized and regulated in the European technical standards applicable to the issuance of qualified electronic certificates, specially ETSI EN 319 411, sections 5.4.2 y 6.3.4.e).

1.3.3.2. Signers

The signers are natural persons, who possess exclusively the digital signature keys of their identification and/or advance electronic signature or qualified; being typically the employees, legal representatives or volunteers, as well as other persons linked to the subscribers; including Public Administrations employees, to the public employee certificates.

The signers are properly authorized by the subscriber and properly identified in the certificate through their name, last name and their VAT number valid in the jurisdiction, without being possible, in general, the use of pseudonyms.

The private key of a signer cannot be recovered or deducted by the relying electronic services provider, so the natural persons identified in the relevant certificates are the sole responsible for their protection and should consider the implications of losing a private key.

Given the existence of certificates for different use of the electronic signature, such as authentication, the more generic term 'identified natural person in the certificate', is also used, with full respect to the compliance the electronic signature legislation in relation with the signer's rights and obligations.

1.3.3.3. Relying parties

The relying parties are the persons and organizations that receive digital signatures and digital certificates.

To trust certificates, the relying parties must verify them, as it is established in the certification practice statement and in the corresponding instructions available in the web page of the Certification Authority.

1.3.4. Public Key Infrastructure Service Provider

BEWOR and UANATACA, S.A. have signed a contract for the provision of technological services in which UANATACA will provide the public key infrastructure (PKI) that supports the BEWOR trust service. Likewise, UANATACA makes BEWOR available to the technical personnel necessary for the proper performance of the reliable functions of a trusted service provider.

That said, UANATACA is configured as an infrastructure service provider for certification services, it provides its technological services to BEWOR so that it can carry out the services inherent to a trusted service provider, guaranteeing the continuity of services at all times. and in accordance with regulatory requirements.

Similarly, it has been reported that UANATACA is an accredited trusted service provider in accordance with the provisions of European regulation no. 910/2014 of the European Parliament and of the Council, of July 23, 2014, on electronic identification and trust services for transactions. electronics in the internal market and derogation directive 1999/93 / EC (eIDAS regulation).

The UANATACA PKI is subject to annual audits to assess the compliance of qualified trust service providers in accordance with applicable regulations, in accordance with ISO / IEC 17065: 2012, ETSI EN 319 403 V2.2.2., ETSI EN 319 421 v1.1.1, ETSI EN 319 401 v2.1.1, ETSI EN 319 411-2 v 2.1.1., ETSI EN 319 411-1 v 1.1.1., ETSI EN 319 401 v2.1.1, ETSI EN 319 411- 2 2 v 2.1.1 ETSI EN 319 411-1 v 1.1.1, ETSI EN 319 401 v2.1.1.

1.4. Use of certificates

This section lists the requests for which each type of certificate can be used, sets limitations to certain requests and prohibits certain requests of certificates.

1.4.1. Uses permitted for certificates

The permitted used specified in the various fields of the certificate profiles should be taken into consideration, available on the webpage https://bewor.com/proveedor-de-firma.

1.4.1.1. Certificado cualificado de Persona Física en HSM centralizado

This certificate has OID 1.3.6.1.4.1.55693.1.1.1. It is a qualified certificate issued for the advanced electronic signature and authentication, in accordance with the certification statement QCP-n with the OID 0.4.0.194112.1.0, as stated in the certificate. The certificates for natural person issued in centralised HSM, are qualified certificates as stated in Article 28 of the Regulatory (UE) 910/2014 eIDAS.

It guarantees the identity of the subscriber and the indicated person on the certificate and allows the generation of the 'advance electronic signature based on the qualified electronic certificate'.
The certificates can be used for applications like the ones listed below:

a) Authentication in access control systems
b) Signature of secure email
c) Other digital signature requests, in accordance with the agreements between the interested parties or with legal rules applicable in each individual case.

The information of uses in the certificate's profile indicates the following:

The 'key usage' field is activated and therefore it allows us to perform the following functions:

a. Digital Signature for authentication
b. Content commitment for electronic signature
c. Key Encipherment.

1.4.1.2. Qualified certificate for Natural Person Representative for Legal person on centralised HSM

This certificate has OID 1.3.6.1.4.1.55693.1.2.1. It is a qualified certificate issued for the advanced electronic signature and authentication, in accordance with the certification statement QCP-n with the OID 0.4.0.194112.1.0, as stated in the certificate. The certificates for natural person issued in centralised HSM, are qualified certificates as stated in Article 28 of the Regulatory (UE) 910/2014 eIDAS.

It guarantees the identity of the subscriber and the indicated person on the certificate and allows the generation of the 'advance electronic signature based on the qualified electronic certificate'.

On the other hand, the certificates can be used in other requests such as those listed below:

a) Signature of secure email
b) Other electronic signature requests

The information of uses in the certificate's profile indicates the following:

a) The 'key usage' field is activated and therefore it allows us to perform the following functions:
    a. Content commitment for electronic signature

1.4.1.3. Qualified certificate for Natural Person Representative for Legal person with the administrations on centralised HSM

This certificate has the OID 1.3.6.1.4.1.55693.1.3.1. It is a qualified certificate issued for the advance electronic signature and authentication, in accordance with the certification statement QCP-n with the OID 0.4.0.194112.1.0, which it is stated in the certificate.

It is a qualified certificate in accordance with the provisions of article 28 of Regulation (EU) 910/2014 eIDAS, and complies with the provisions of the technical regulations of the European Telecommunications Standards Institute, identified with the reference EN 319 411-2 .

It guarantees the identity of the subscriber and the signatory, and a relationship of legal representation or empowerment between the signatory and an entity, company or organization described in the field "O" (Organization), and allow the generation of the "advanced electronic signature based on qualified electronic certificate".
On the other hand, the certificates can be used in other requests such as those listed below:

a) Authentication in access control systems
b) Signature of secure email
c) Other electronic signature requests

The information of uses in the certificate's profile indicates the following:
The 'key usage' field is activated and therefore it allows us to perform the following functions:

a. Digital Signature for authentication
b. Content commitment for electronic signature
c. Key Encipherment

1.4.1.4. Qualified certificate for natural Person Representative of Entity without Legal Personality with the administrations on centralised HSM

This certificate has the OID 1.3.6.1.4.1.55693.1.4.1 It is a qualified certificate issued for the advance qualified electronic signature and authentication, in accordance with the certification statement QCP-n with the OID 0.4.0.194112.1.0.

It is a qualified certificate in accordance with the provisions of article 28 of Regulation (EU) 910/2014 eIDAS, and complies with the provisions of the technical regulations of the European Telecommunications Standards Institute, identified with the reference EN 319 411-2 .

It guarantees the identity of the subscriber and the signatory, and a relationship of legal representation or empowerment between the signatory and an entity, company or organization described in the field "O" (Organization), and allow the generation of the "advanced electronic signature based on qualified electronic certificate".

On the other hand, this certificate can be used in requests such as those listed below:

a) Authentication in access control systems
b) Signature of secure email
c) Other electronic signature requests

The information of uses in the certificate's profile indicates the following:

The 'key usage' field is activated and therefore it allows us to perform the following functions:

a. Digital Signature for authentication
b. Content commitment for electronic signature
c. Key Encipherment

1.4.2. Limits and forbidden uses of certificates

Certificates are used for their own function and the established purpose, not being able to be used for other functions or other purposes.

Likewise, certificates must be used only in accordance with the applicable law, especially taking into consideration the import and export restrictions prevailing at any given time.

Certificates cannot be used to sign public key certificates of any type, nor Certificate Revocation List (CRL).

The certificates have not been designed, cannot be assigned and its use or resale as control equipment for dangerous situations is not authorised nor for uses that require fail-safe actions, as the operation of nuclear installation, navigation systems or air communications, or weapons control systems, where a failure could lead directly to death, personal injury or severe environmental damage.

There must be taken into account the limits indicated in the various fields of the certificates profiles, visible in the web of BEWOR.

The use of the digital certificates in operations that violate this Certification Practice Statement, the binding legal documents with each certificate, or the contracts with the Registration Authorities or their signers/subscribers, is considered to misuse the legal

purposes, exempting therefore to BEWOR, according to the current legislation, of any liability for this misuse of the certificates made by the signer or any third party.

BEWOR does not have any access to the data on which the use of the certificate can be applied. Therefore, as a result of this technical impossibility to access to the content of the message, BEWOR can't issue any evaluation about the mentioned content, the subscriber, the signer or the person responsible of the custody, is the one who will assume any responsibility arising from the content rigged to the use of a certificate.

Likewise, any responsibility that could result from the use of the custody out of the limits and conditions of use included in this Certification Practice Statement, the binding legal documents with each certificate, or the contracts or agreements with the registration authorities or with their subscribers, and any other misuse thereof derived from this section or may be interpreted as such according to the law, will be attributable to the subscriber, signer or the responsible of it.

1.5. Policy management

1.5.1. Organization that administers the document

Bewor Tech S.L.
P.I. Cortijo del Conde, Calle Pago de Cambea, 14 Nave 7
18015, Granada
España

1.5.2. Contact information of the organisation

Bewor Tech S.L.
P.I. Cortijo del Conde, Calle Pago de Cambea, 14 Nave 7
18015, Granada
España
helpdesk@bewor.com

1.5.3. Document management procedures

The documental and organization system of BEWOR S.L. guarantees, according to the existence and request of the corresponding procedures, the correct maintenance of this document and the specification of the service related to itself.

2. Publication of information and deposit of certificates

2.1. Deposit(s) of certificates

BEWOR has a Deposit of certificates, in which the information related to the certification services is published.

That service is available 24 hours, 7 days per week and, in case of the system failure was under BEWOR's control, it will make its best efforts to ensure that the service is back available within the prescribed time in the section 5.7.4 of this certification practice statement.

2.2. Publication of information of the certification services provider

BEWOR publishes the following information, in its Deposit:

- Issued certificates, when the consent of the natural person identified in the certificate has been obtained.
- Revoked certificates list and other information about the status if the certificates revocation.
- Applicable certificate policies.
- Certification Practice Statement.
- Policy Disclosure Statements - PDS, at least in Spanish and English.

2.3. Frecuencia de publicación

The information of the certification services provides, including the policies and the Certification Practice Statement, is published when available.

The information of the certification services provider, including the policies and change on the Certification Practice Statement shall be governed by the established in section **¡Error! No se encuentra el origen de la referencia.** on this document.

The information of the revocation status of the certificates will be published in accordance with the established in the sections 4.9.9 y 4.9.10 of this Certification Practice Statement.

2.4. Access control

BEWOR does not limit the read access to the information established in the section 2.2, but establishes controls to prevent non-authorized people to add, modify or delete registrations of the Deposit, to protect the integrity and authenticity of the information, especially information about the revocation status.

BEWOR uses reliable systems for the Deposit, in such a way that:

- Only authorized persons could do annotations and modifications.
- The authenticity of the information could be verified.
- The certificates would only be available for consulting if the natural person identified in the certificate induced his consent.
- Any technical change affecting the security requirements could be detected.

3. Identification and authentication

3.1. Initial registration

3.1.1. Type of names

All certificates contain a distinguished name (DN) X.501 in the field Subject including a component Common Name (CN=), relative to the identity of the subscriber and the natural person identified on the certificate, as well as several additional identity information in the field *SubjectAlternativeName.*

The names on the certificates are as follows.

3.1.1.1. Qualified certificate for Natural Person on centralised HSM

Country (C)	State[1]
Organization (O)	Organization to which the signer is bound
Organization Unit (OU)	Organization Unit to which the signer is bound
Organization Identifier	Taxpayer Identification Number of the Organization to which the signer is bound
Title	Title or speciality of the signer
Surname	Signer's Surname
Given Name	Signer's First Name
Serial Number	Identity Card Number / NIE / Passport / or any other identification number recognised by law
Common Name (CN)	Name and surname of the signer

1 The field 'State' corresponds to the state where the contractual relationship take place between the signer and the entity to which it is bound (for being employee, member, partner or other link) , regardless the nationality of the employee.

3.1.1.2. Qualified certificate for Natural Person Representative for Legal person on centralised HSM

Country (C)	State[2]
Organization (O)	Organization to which the signer is bound
Organization Unit (OU)	Organization Unit to which the signer is bound
Organization Identifier	Taxpayer Identification Number of the Organization to which the signer is bound
Title	Title or speciality of the signer
Surname	Signer's Surname
Given Name	Signer's First Name
Serial Number	Identity Card Number / NIE / Passport / or any other identification number recognised by law
Common Name (CN)	Name and surname of the signer

3.1.1.3. Qualified certificate for Natural Person Representative for Legal person with the administrations on centralised HSM

Country (C)	State
Organization (O)	Organization represented by the signer
Organization Unit (OU)	Organization unit to which the signer belongs
Organization Identifier	Tax Identification Number of the Organization which represents the signer
Title	Name of the representation of the signer
Surname	Signer's Surname
Given Name	Signer's First Name
Serial Number	National Identity Card/NIE of the signer
Common Name (CN)	National Identity Card/NIE, first name and surname of the signer and Tax Identification Number of the organisation

2 The field 'State' corresponds to the state where the contractual relationship take place between the signer and the entity to which it is bound (for being employee, member, partner or other link) , regardless the nationality of the employee.

Description	Information about the representation concession of the registration	Información representaci

3.1.1.4. Qualified certificate for natural Person Representative of Entity without Legal Personality with the administrations on centralised HSM

Country (C)	State
Organization (O)	Organization represented by the signer
Organization Unit (OU)	Organization unit to which the signer belongs
Organization Identifier	Tax Identification Number of the Organization which represents the signer
Title	Name of the representation of the signer
Surname	Signer's Surname
Given Name	Signer's First Name
Serial Number	National Identity Card/NIE of the signer
Common Name (CN)	National Identity Card/NIE, first name and surname of the signer and Tax Identification Number of the organisation
Description	Information about the representation concession of the registration

3.1.2. Significado de los nombres

The names in the fields of the certificates *SubjectName* and *SubjectAlternativeName* are understandable in natural language, in accordance with the provisions of the previous section.

3.1.2.1. Emisión de certificados del set de pruebas y certificados de pruebas en general

In case the provided data in the DN or Subject were fictitious (e.g. 'Test Organization', 'Test First Name', Surname1') or expressly stated words indicating its invalidity (e.g. 'TEST' 'EVIDENCE' OR 'INVALID'), the certificate will be considered as legally invalid and therefore with no responsibility for BEWOR. Theses certificates are issued to take interoperability tests and allow the regulatory body its assessment.

3.1.3. Use of anonymous and pseudonymous

Under no circumstances can the pseudonymous be used for identifying an entity, company, organisation or signer. Likewise, under no circumstances can anonymous certificates be issued.

3.1.4. Interpretation of name formats

Name formats will be interpreted in accordance with the law of the country in which the subscriber is established, on its own terms.

The field 'country' or 'state' will be the subscriber's.

The certificates show the relation between a natural person and the legal person, entity or organisation to which is bound, regardless the nationality of the natural person.
The "serial number" field must include the signer's Identity Card Number, NIE, Passport or any other identification number recognised by law.

3.1.5. Uniqueness of names

The names of the subscribers of certificates will be unique, for each certification policy of BEWOR.

It won't be possible to assign a subscriber's name that already has been used, to a different subscriber, situation that, in theory, at first shouldn't happen, thanks to the tax identification number, or equivalent, in the names' scheme.

A subscriber can request more than one certificate whenever the combination of the following existing values in the request was different from a valid certificate:

- Tax Identification Number or other valid legal identifier of the natural person.
- Tax Identification Number or other valid legal identifier of the subscriber.
- Type of Certificate (Description of the certificate field).
- Support of the certificate (QSCD, software, HSM centralized, QSCD centralized)

As an exception, this CPS allows to issue a certificate when there is an overlap with the Tax Identification Number of the subscriber or the signer, Type of certificate, Support of the certificate, with an active certificate, as long as there is a differentiating element between them, in the title and/or Organisational Unit fields.

3.1.6. Resolution of name conflicts

Certificate applicants won't include names in requests that may involve infringement, by the future subscriber, of third party rights.

BEWOR won't be required to first determine that an applicant of certificates has industrial property rights on the name of a certificate request, but at first will proceed to certify it.

Furthermore, it won't act as arbitrator or mediator, or in any other way to resolve any dispute concerning the property of names of persons or organisations, web domains, brands or commercial names.

However, in case of receiving a notification concerning a name conflict, according to the legislation of the subscriber's country, it may take appropriate actions to block or withdraw the certificate issued.

In any case, the certification services provider reserves the right to reject the certification request due to names conflict.

Any controversy or dispute arising out of this document will be solved definitively, by the arbitration law of an arbitrator within the framework of the Spanish Court of Arbitration, in accordance with its Regulation and Statute, to which the administration of the arbitration and the designation of the arbitrator or the arbitral court is entrusted.
The parties state their commitment to comply with the award rendered in the contractual document that formalises the service.

3.2. Initial identity validation

The identity of the subscribers of the certificates is fixed at the time of signing the contract between BEWOR and the subscriber, the moment in which the existence of the subscriber through his identity official document or subsequent documentation as well as the enforcement powers of the person representing are verified. For the verification, public or notarial documentation can be use, or direct consultation to the corresponding public records.

The identity of the natural persons identified in the certificates is validated through the corporative records of the entity, Company or organization of public or private law, subscribers to the certificates. The subscriber will produce a certification of the necessary data, and will send it to BEWOR, through these methods it will enable, for registering the identity of the signers.

3.2.1. Proof of possession of private key

The possession of the private key is demonstrated under the reliable process of delivery and acceptance of the certificate by the subscriber, for seal certificates, and by the signer, for signature certificates

3.2.2. Authentication of organization, company or entity identity through a representative

Natural persons who are capable of acting on behalf of public or private subscribers, will be able to act as representatives of them, as long as there exists a previous situation of legal or voluntary representation between the natural person and the public or private person, that requires their recognition by BEWOR, which will be made through the following face-to-face procedure:

1. The subscriber's representative will meet in person with an authorised representative of BEWOR, where he will have a form of authentication. Alternatively, the subscriber's representative will be able to get the form from BEWOR's web from its previous fulfilment.

2. The representative will fill the form, with the following information and documents:
    - His identification data, as representative:
        - Name and Surname

        - Place and date of birth
        - Document: Representative Tax Identification Number, NIE or any other identification number recognised by law.

    - The identification data of the subscriber to which he is representing:
        - Name or business name.
        - All information existing records, including the data relative to the constitution and legal personality and the extension and validity of the representation faculty of the applicant.
        - Document: Tax Identification Number
        - Document: Public documents that serve to certify the mentioned ends irrefutably and its inscription in the corresponding public registry if required. The mentioned checking can also be done through consultation in the public registry in which the constitution and empowerment documents are enrolled, being able to use the media provided by the mentioned public registries.

    - The data relative to the representation or the capacity for action that holds:
        - The validity of the representation or the ability to act (the start and end date) if applicable.
        - The field and the limits, in its case, of the representation or the capacity of action:
            - TOTAL. Representation or total capacity. This checking will be able to be made through a tele-consultation to the public registry stating the inscribed representation.
            - PARTIAL. Representation or partial capacity. This checking will be able to be made through an authentic electronic copy of the notarial empowerment deed, under the terms of the notarial law.

3. BEWOR's staff will check the identity of the representative through his ID or any other identification number recognised by law with the content of the representation with the documents.

4. BEWOR's staff will verify the provided information as well as deliver a proof of authentication and return the contributed documentation.

5. Alternatively, it will be possible to legitimise by legal process the signature in the form, and be delivered to BEWOR by certified post, in which case steps 3 and 4 above won't be necessary.

The digital certification service provision is formalised through the appropriate contract between BEWOR and the subscriber, duly represented.

3.2.3. Authentication of natural person identity

This section describes the testing methods of the identity of a natural person identify in the certificate.

3.2.3.1. In the certificates

The identity of the natural persons who sign identified in the certificates is validated through a production of its official document of identification. (Identity card, passport or any other identification number recognised by law).

The information of the identification of the natural persons identified in the certificates when the subscriber is an entity with or without legal personality, the information will be validated comparing the information of the request with the registrations of the entity, company or organisation of public or private law to which is bound, ensuring the correctness of the information to be certified.

3.2.3.2. Identity validation

When requesting certificates, the operator or authorised personnel of the Registration Authority of BEWOR validates the requester's identity, in which the natural person will need to show his Identity Card, NIE, Passport or any other identification number recognised by law in the location where the registration is taking place.

There is no need of physical presence to request the certificates when the subscriber is a legal person due to the already proven relationship between the natural person and the

entity, Company or organisation of public or private law to which is bound, as long as no more than five (5) years have passed since the identification. However, before delivering a certificate, the subscriber entity, Company or organisation of public or private law, through their certification responsible, or other designated member, must contrast the identity of the natural person identified in the certificate though this physical presence.

During this proceeding the identity of the natural person identified in the certificate is appropriately confirmed. Therefore, in all cases in which a certificate is issued the identity of the signer is verified in person.

The Registration Authority will verify through the production of documents or through its own sources of information, the remaining data and features that need to be included in the certificate, keeping the supporting information that proves the validity of them.

3.2.3.3. Entail of the natural person

Documentary evidence of the entail of a natural person identified in a certificate with an entity, Company or organisation of public or private law will be proven by the persistence in the internal records (employee contract, commercial contract or records where his position is indicated, or the request as a member of the organisation) of each public or private persons to which is bound.

3.2.4. Subscriber's not verified information

BEWOR does not include any information of the subscriber not verified in the certificates.

3.2.5. Authentication of the identity of a RA and its operators

For the construction of a new Registration Authority, BEWOR performs the necessary checks in order to confirm the existence of the identity or organisation involved. For that purpose, BEWOR will be able to use the production of documents or use its own information sources.

Likewise, BEWOR, directly or through its Registration Authority, verifies and validates the operator's identity of the Registration Authorities, and they send BEWOR the relevant

identification documentation of the new operator, together with its authorisation to act in such capacity.

BEWOR is assured that the operators of the Registration Authority receive the proper training for the performance of their duties, which is verified with a relevant assessment. The Registry Authority previously approved by BEWOR can execute such training and assessment.

For the delivery of services, BEWOR ensures that the operators of the Registration Authority have access to the system via strong authentication with digital certificate.

3.3. Identification and authentication of renewal requests

3.3.1. Validation for certificates routine renewal

Before renewing a certificate, the operator or the authorized personnel of BEWOR's Registration Authority verifies that the information used to verify the identity and the remaining subscriber data and the natural person identified in the certificate remain valid.

The acceptable methods for such verifications are:

- The use of the code 'CRE' or 'ERC' related to the previous certificate, or other methods of personal authentication, that consist in information that only the natural person identified in the certificate knows, and allows in an automatic way the renewal of the certificate, as long as the deadline legally established hasn't exceed.
- The use of the current certificate for its renewal as long as it has not exceeded the deadline legally established for this possibility.

If any information of the subscriber or natural person identified in the certificate has changed, the new information must be properly registered so a complete authentication is done, in accordance with the established in the section 3.2.

3.3.2. Identification and authentication of revocation request

Before generating a certificate to a subscriber whose certificate was renewed, the operator or the authorized personnel of BEWOR's Registration Authority will verify that the information used that day to verify the identity and the rest of the data of the subscriber and the natural person identified in the certificate are still valid, in which case previous section shall apply.

The renewal of the certificates after their revocation will not be possible in the following cases:

- The certificate was revoked by erroneous issuance to a person different than the one identified in the certificate.
- The certificate was revoked by a non-authorised issuance by the natural person identified in the certificate.
- The certificate revoked may contain misleading or fake information.

If any information of the subscriber or natural person identified in the certificate has changed, the new information must be properly registered so a complete authentication is done, in accordance with the established in the section 3.2.

3.4. Identification and authentication of revocation, suspension or reactivation request

BEWOR or an operator or authorised personnel of the Registration Authority authenticate the requests and reports relative to revocation, suspension or reactivation of a certificate verifying that they come from an authorised person.

The identification of the subscribers and/or signers during the process of revocation suspension or reactivation of the certificates can be performed by:

- The subscriber and/or signer:
    - Identifying and authenticating through the Revocation Code (ERC o ERC) via BEWOR's web page in 24x7 schedule.

- Other media, as telephone, e-mail, etc. when there is reasonable assurance of the identity of the applicant for suspension or revocation in the judgement of BEWOR and/or Registration Authorities.

- BEWOR'S registration authorities: they must identify the signer upon a revocation, suspension or reactivation request using the methods they consider appropriate.

When the subscriber would want to initiate a revocation request, and there were doubts for its identification, during office hours, his certificate would go onto suspension status.

4. Certificate life-cycle operational requirements

4.1. Certificate issuance request

4.1.1. Legitimation to apply for the issuance

The requester of the certificate, a natural or legal person, must sign a certification services provision contract with BEWOR.

Likewise, before the issuance and delivery of a certificate, there must exist a request of a certificate either in the same contract, in a specific certificate request form or in the face of the Registration Authority.

When the applicant is a different person than the subscriber, there must be an authorization from the subscriber to allow the applicant to proceed with the request, which is legally implemented by a certificate request form subscribed by that applicant on behalf of the entity, Company or organisation of public or private law.

4.1.2. Registration procedure and responsibilities

BEWOR receives certificates' request, made by persons, entities, Companies or organisations of public or private law.

The requests are implemented by a document in paper or electronic format, individually or in batches, through external databases or interface of *Web Services* whose addressee is BEWOR. When the subscriber of the certificates is filled by an entity, Company or organisation of public or private law that acts as a Registration Authority of BEWOR, the request will be carried out accessing directly to BEWOR's information systems and produce the relevant certificates for the entity, Company or organisation itself or for its members.

The request will go together with the supporting documentation of the identity and other circumstances of the natural person identified in the certificate, in accordance with the established in the section 3.2.3. Also, an address or other data that will allow contacting the natural person identified in the certificate.

4.2. Processing the certification request

4.2.1. Implementation of identification and authentication functions

Once the certificate applicant has been received, BEWOR ensures that the certificates' requests will be completed, precise and duly authorised, before processing them.

If so, BEWOR verifies the information provided, verifying the aspects described in section 3.2

In case of a qualified certificate, the supporting documentation of the approval of the request must be preserved and properly registered with guarantees of security and integrity during 15 years from the expiration of the certificate, even in case of early loss effective for renovation.

4.2.2. Approval or rejection of the request

In case the data is correctly verified, BEWOR should approve the request of the certificate and proceed with its issuance and delivery.

If the verification indicates that the information is not correct, or if it is suspected that it is not correct or it may affect the reputation of the Certification Authority, the Registration Authority or the subscribers, BEWOR will deny the request, or will stop its approval up to having made the additional checks that it considers appropriate.

BEWOR will definitely deny the request in case the additional checks won't help to correct the information to verify.

BEWOR notifies the approval or denial of the request to the applicant.

BEWOR will be able to automate the verification procedures of the information correction that will be in the certificates, and the approval of the requests.

4.2.3. Time to process certificate requests

BEWOR attends to the certificates' requests in order of arrival, in a reasonable time, being possible to specify a guarantee can specify a maximum guarantee in the contract certificate issuance.

Requests remain active until its approval or rejection.

4.3. Certificate issuance

4.3.1. CA actions during certificate issuance

After approving the certification request, the CA proceeds to issue the certificate in a safe way and make it available to the signer for its acceptance.

The established procedures in this section are applicable in case of certification renewal, taking into consideration that the same involves the issuance of a new certificate.

During the process, BEWOR:

- Protects the confidentiality and integrity of the registration data that owns.
- Uses reliable systems and products that are protected against every disturbance and guarantee the technical security and, in its case, cryptographic security of the processes of certification to which they support.
- Generates a pair of keys, through a procedure of generation of certificates bound in a safe way with the procedure of generation of keys.
- Uses a procedure of generation of certificates that links in a safe way the certificate with the registration information, including the certified public key.
- It ensures that the certificate is issued by systems using protection against counterfeiting and guarantees the confidentiality of the keys during the process of generation of the mentioned keys.
- Indicates the date and hour in which a certificate was issued.
- It ensures the exclusive control of the keys by the user, and BEWOR or its Registration Authorities cannot deduce or use them in any way.

4.3.2. Notification to the certificate issuance applicant

BEWOR notifies the issuance of the certificate to the subscriber and/or the natural person identified in the certificate and method for production/download.

4.4. Certificate delivery and acceptance

4.4.1. CA Responsibilities

During this process, the operator or authorised personnel of the BEWOR'S Registration Authority must perform the following actions:

- Definitely confirm the identity of the natural person identified in the certificate, in accordance with the established in the sections **¡Error! No se encuentra el origen de la referencia.** and 3.2.3.
- To have the Trust Services Provision Contract duly signed by the Subscriber.
- Deliver to the natural person identified in the certificate the sheet delivery and acceptance of the certificate with the following minimum contents:
    - Basic information about the use of the certificate, especially including information about the certification services provider and the applicable Certification Practice Statement, as his obligations, faculties and responsibilities.
    - Information about the certificate.
    - Recognition, from the signer, of receiving the certificate and/or the procedures for its creation/download and the acceptance of the mentioned elements.
    - Signer liability regime.
    - Responsibility of the signer.
    - Imputation method exclusive to the signer, of its private key and its certificate activation data, in accordance with the established in the sections 6.2 and 6.4.
    - The date of the act of delivery and acceptance.

  All this information may be included in the Trust Services Provision Contract. In this sense, the delivery and acceptance of the certificate will take place the Subscriber signs the Trust Services Provision Contract.
- To obtain the signature of the person identified in the certificate.

The Registration Authority collaborates in these processes, having to register the previous acts, and preserves the mentioned original ones (delivery and acceptance sheets), referring to BEWOR the electronic copy as well as the original when BEWOR required access to them.

4.4.2. Way in which the certificate is accepted

When the acceptance sheet is delivered, the acceptance of the certificate by the natural person identified in the certificate occurs when signing the delivery and acceptance sheet.

When the generation and delivery of the certificate is carried out through the automated procedure defined by BEWOR, the acceptance of the certificate by the natural person identified in it, it is produced by signing the Trust Services Provision Contract using the certificate itself.

4.4.3. Publication of the certificate

BEWOR publishes the certificate in the Deposit referred in section 2.1, with the proper safety controls and whenever BEWOR had the authorization of the natural person identified in the certificate.

4.5. Key pair and certificate usage

4.5.1. Use by the signer

BEWOR forces him to:

- Provide to BEWOR complete and proper information, in accordance with the requirements of this Certification Practice Statement, especially on the registering procedure.
- Express his consent prior the certificate issuance and delivery.
- Use the certificate in accordance with the established in the section 1.4.

- When the certificate will work in conjunction with a SSCD, recognise its capacity of production of qualified electronic signatures; that is, equivalent to handwritten signatures, as well as other types of electronic signatures and information encryption mechanisms.
- Be especially diligent in the custody his private key, in order to prevent unauthorised uses, in accordance with the established in the sections 6.1, **¡Error! No se encuentra el origen de la referencia.** and 6.4.
- Communicate to BEWOR, Registration Authorities and anyone who believes may trust the certificate, without unjustifiable delays:
    - The loss, theft or potential compromise of his private key.
    - The loss of control over his private key, due to the compromise of the activation data (i.e. PIN) or any other reason.
    - The inaccuracies or changes in the content of the certificate that the subscriber knows or could know.
- Stop using the private key once the period specified in the section 6.3.2 has elapsed.

BEWOR forces the signer to take responsibility to ensure:

- All the information in the certificate provided by the signer is correct.
- The certificate is used exclusively for legal and authorised uses, in accordance with the Certification Practice Statement.
- No unauthorised person has ever had access to the private key of the certificate, and that he is the sole responsible for any damage caused by his infringement of protecting the private key.
- The signer is an end entity and not a certification services provider, and will not use the private key corresponding to the public key listed in the certificate to sign any certificate (or any other format of certified public key), nor Certificate Revocation List, nor certification services provider title, nor any other case.

4.5.2. Use by the subscriber

4.5.2.1. Obligations of the certificate subscriber

BEWOR contractually forces the subscriber to:

- Provide complete and appropriate information to the Certification Authority, in accordance with the requirements of this Certification Practice Statement, especially on the registering procedure.
- Express his consent prior to the certificate issuance and delivery.
- Use the certificate in accordance with the established in the section 1.4.
- Communicate to BEWOR, Registration Authorities and anyone who the subscriber believes may trust the certificate, without unjustifiable delays:
    - The loss, theft or potential compromise of his private key.
    - The loss of control over his private key, due to the compromise of the activation data (i.e. PIN) or any other reason.
    - The inaccuracies or changes in the content of the certificate that the subscriber knows or could know.
    - When there is a loss, alteration, unauthorised use, theft or compromise of the card.
- Communicate to the natural persons identified in the certificate the compliance of the specific obligations of them, and establish mechanisms to guarantee the proper compliance of them.
- Not to monitor, manipulate or perform reverse engineer acts on the technical implantation of the certification services of BEWOR, without previous written permission.
- Not to compromise the safety of the certification services of the certification services provider of BEWOR.

4.5.2.2. Civil liability of the certificate's subscriber

BEWOR contractually forces the subscriber to take responsibility to ensure:

- All the statements in the request are correct.
- All the information provided by the subscriber that is in the certificate is correct.
- The certificate is exclusively used for legal and authorised uses, in accordance with the Certification Practice Statement.
- No unauthorised person has ever had access to the private key of the certificate, and that he is the sole responsible for any damage caused by his infringement of protecting the private key.

- The subscriber is an end entity and not a certification services provider, and will not use the private key corresponding to the public key listed in the certificate to sign any certificate (or any other format of certified public key), nor Certificate Revocation List, nor certification services provider title, nor any other case.

4.5.3. Use by the relying third party in certificates

4.5.3.1. Obligations of the relying third parties in certificates

BEWOR informs the relying third party in certificate of the following obligations he must assume:

- Consulting if the certificate is appropriate for the intending use, in an independent way.
- Verify the validity, suspension or revocation of the issued certificates, for which certificates status information will be used.
- Verify all certificates of the certificates hierarchy, before trusting the digital signature or any of the certificates of the hierarchy.
- Recognise that the verified electronic signatures, produced on a qualified signature creation device (SSCD) have the legal consideration of qualified electronic signatures; that is, equivalent to handwritten signatures, as well as the certificate allows the creation of other types of electronic signatures and encryption mechanisms.
- Remember any limitation on the use of the certificate, regardless of whether in the own certificate or in the relying third party in certificates contract.
- Remember any caution established in a contract or other instrument, regardless of its legal nature.
- Not to monitor, manipulate or perform reverse engineer acts about the technical implementation of the certification services of BEWOR, without previous written permission.
- Not compromise the safety of the certification services of BEWOR.

4.5.3.2. Civil liability of the relying third parties in certificates

BEWOR informs to the relying third party in certificates that he must assume the following responsibilities:

- He has enough information to make an informed decision in order to trust or not the certificate.
- He is the sole responsible for trusting or not the information of the certificate.
- He will be the sole responsible if he breaches his obligations as a third party that trust the certificate.

4.6. Certificate renewal

The certificates renewal requires the renewal of keys, so that must comply with the established in section 4.7.

4.7. Key and certificate renewal

4.7.1. Circumstances for certificate and key renewal

The existing certificates can be renewed through a specific and simplified procedure of request, in order to keep the continuity of the certification service.

There are at least two ways for certificate renewal:

a) Face to face renewal process – it will be carried out the same way as a new certificate issuance.

b) Online renewal process (via internet) – as detail below.

4.7.2. Online renewal process

4.7.2.1. Circumstances for online renewal

The online renewal of the certificate will take place only if the following conditions are executed:

- The Registration Authority and/or BEWOR have access to the online renewal service.
- The certificate that is used for the renewal is valid, in other words, it is not expired, revoked or suspended.

No more than 5 years have passed since the last accreditation of identity with an identification operator when obtaining a certificate.

4.7.2.2. Quién puede solicitar la renovación online de un certificado

4.7.2.3. Approval or rejection of the request

In case the data is correctly verified, BEWOR should approve the request of the certificate and proceed with its issuance and delivery.

BEWOR notifies the approval or denial of the request to the applicant.

BEWOR will be able to automate the verification procedures of the information correction that will be in the certificates, and the approval of the requests.

4.7.2.4. Procedure for online renewal request

The renewal request of a certificate will be carried performed according to the following:

- When the digital certificate of the user is about to expire, BEWOR will be able to send one or more notifications over time, requesting the renewal to the user.
- The signer will connect to the renewal service in BEWOR's webpage and he will proceed with the renewal request.
- The signer will sign his valid certificate renewal.
- Creation of a new pair of keys and generation and import of the certificate taking into account the following constrains:
    - Protects the confidentiality and integrity of the registration data that owns.
    - Uses reliable systems and products that are protected against every disturbance and guarantee the technical security and, in its case, cryptographic security of the processes of certification to which they support.
    - Generates a pair of keys, through a procedure of generation of certificates bound in a safe way with the procedure of generation of keys.
    - Uses a procedure of generation of certificates that links in a safe way the certificate with the registration information, including the certified public key.

- It ensures that the certificate is issued by systems using protection against counterfeiting and guarantees the confidentiality of the keys during the process of generation of the mentioned keys.
- Indicates the date and hour in which a certificate was issued.
- It ensures the exclusive control of the keys by the user, and BEWOR or its Registration Authorities cannot deduce or use them in any way.

4.7.2.5. Notification of the renewed certificate issuance

BEWOR notifies the certificate issuance to the subscriber and the natural person identified in the certificate.

4.7.2.6. Way in which the certificate is accepted

The acceptance of the certificate occurs when signing the renewal electronically.

.

4.7.2.7. Publication of the certificate

BEWOR publishes the renewed certificate in the Deposit to which refers in the section 2.1, with the proper safety controls.

4.7.2.8. Notification of certificate issuance to third parties

BEWOR does not make any notification of the issuance to third entities.

4.8. Certificate modification

The modification of certificates, except the modification of the certified public key, which is considered renewal, will be treated as a new issue of certificate applied as described in sections 4.1, 4.2, 4.3 y 4.4.

4.9. Revocation, suspension or reactivation of certificates

The revocation of a certificate means the definitive withdrawal of the certificate and it is irrevocable.

The suspension (or temporal revocation) of a certificate means the temporal withdrawal of it and it is reversible. Only end entity certificates will be able to be stopped.

The reactivation of a certificate is the transition from a hold status to an active state.

4.9.1. Causes of certificate revocation

BEWOR revokes a certificate when any of the following causes occur:

1) Circumstances affecting the information contained in the certificate:
   a) Modification of any of the data contained in the certificate, after the corresponding issue of the certificate including amendments.
   b) Discovery that any of the data contained in the certificate application is incorrect.
   c) Discovery that any of the data contained in the certificate is incorrect.

2) Circumstances affecting the security of the key or certificate:
   a) Compromise of the private key, infrastructure or systems certification service provider that issued the certificate, provided that it affects the reliability of the certificates issued from that incident.
   b) Infringement, by BEWOR, of the requirements of the certificate management procedures established in this Certification Practice Statement.
   c) Commitment or suspected compromise of the security key or certificate issued.

d) Unauthorised access or use, by a third party private key corresponding to the public key contained in the certificate.

e) Irregular use of the certificate by the natural person identified in the certificate or lack of diligence in the custody of the private key.

3) Circumstances affecting the subscriber or the natural person identified in the certificate:

a) Completion of the legal relationship between BEWOR provision of services and the subscriber.

b) Modification or termination of the underlying legal relationship or what caused the issuance of the certificate to the natural person identified in the certificate.

c) Infringement by the certificate applicant of the present requirements for the application thereof.

d) Violation by the subscriber or by the person identified in the certificate, of their obligations, responsibility and guarantees established in the relevant legal document.

e) Incapacity or death of key owner.

f) The termination of the legal certificate underwriter _ and authorisation to the holder by the subscriber key or termination of the relationship between subscriber and identified in the certificate.

g) Request by the subscriber for certificate revocation in accordance with the provisions of section 3.4.

4) Other circumstances:

a) Termination of Certification Service Certification Entity BEWOR.

b) The use of the certificate that is harmful and continued to BEWOR. In this case, it is considered that a use is harmful in terms of the following criteria:

- The nature and number of complaints received.
- The identity of the entities filing complaints.
- The relevant legislation in force at all times.
- The response of the subscriber or of the person identified in the certificate to complaints received.

4.9.2. Reasons for suspension of certificates

BEWOR certificates may be suspended from the following causes:

- When so requested by the subscriber or the person identified in the certificate.
- When the documentation required in the request for revocation is sufficient but cannot reasonably identify the subscriber or the person identified in the certificate.
- The lack of use of the certificate for an extended period of time, previously known.
- If the key is suspected to have been compromised until it is confirmed. In this case, BEWOR will have to make sure that the certificate is not suspended for longer than necessary to confirm their commitment.

4.9.3. Reason for reactivation of certificates

BEWOR certificates may be reactivated from the following causes:

- When the certificate is in suspended status.
- When so requested by the subscriber or the natural person identified in the certificate.

4.9.4. Who can request the revocation, suspension or reactivation of a certificate

The certificate may be requested to be revoked, suspended or reactivated by:

- The person identified in the certificate.
- The subscriber of the certificate through a responsible certification service.

4.9.5. Procedimientos de solicitud de revocación, suspensión o reactivación

The entity required to revoke, suspend or reactivate a certificate must apply to BEWOR or the Registration Authority of the subscriber or doing it himself via the online service available in the BEWOR's website. The revocation, suspension or reactivation request shall include the following information:

- Date of application for the revocation, suspension or reactivation.
- Identity of the Subscriber.

- Name and title of the person requesting the revocation, suspension or reactivation.
- Contact information for the person requesting the revocation, suspension or reactivation.
- Detailed reason for the revocation.

The application must be authenticated by BEWOR, in accordance with the requirements of section 3.4 of this policy, prior to the revocation, suspension or reactivation.

The revocation, suspension or reactivation service can be found in the website at:: https://bewor.com/proveedor-de-firma.

If the recipient of a request for revocation, suspension or reactivation by a natural person identified in the certificate is outside the subscribing entity, once authenticated the application must submit a request to that effect to BEWOR.

The revocation, suspension or reactivation request will be processed upon receipt, and inform the subscriber and, where appropriate, physical person identified in the certificate about the change of status of the certificate.

Both, the revocation, suspension or reactivation management service as consultation service are considered critical services and thus contained in the Plan contingency and business continuity planning of BEWOR.

4.9.6. Temporary revocation, suspension or reactivation application

Revocation, suspension or reactivation requests shall be sent immediately when knowledge of the cause of revocation is known.

4.9.7. Temporary period of revocation, suspension or reactivation application processing

The revocation, suspension or reactivation will occur immediately when received. If it takes place with an operator, it will be executed within the regular hours of operation

BEWOR or the Registration Authority. If it is carried out via the online service, it will happen immediately.

4.9.8. Obligation to consult certificate revocation or suspension information

Third parties should check the status of those certificates in which they wish to rely.

A method by which you can check the certificate status is by consulting the latest Certificate Revocation List issued by the Certification of BEWOR.

The Certificate Revocation Lists are published in the Deposit of the Entity Certification, as well as the following web addresses indicated in certificates:

- http://crl1.uanataca.com/public/pki/crl/bewor.crl
- http://crl2.uanataca.com/public/pki/crl/bewor.crl

The status of the certificate validity can also be checked by the OCSP protocol.

- http://ocsp1.uanataca.com/public/pki/ocsp/
- http://ocsp2.uanataca.com/public/pki/ocsp/

4.9.9. Frequency of issuance of certificate revocation lists (CRLs)

BEWOR issues an LRC at least every 24 hours.

The LRC indicates the scheduled time of issuance of a new LRC, although it may issue an LRC before the deadline stated in the previous LRC, to reflect revocations.

The LRC is obliged to maintain the revoked or suspended certificate until it expires.

4.9.10. Maximum period of publication of CRLs

The CRLs are published in the Deposit within a reasonable period immediately after their generation, which in any case is no more than a few minutes.

4.9.11. Availability of the service checking in line with the state of the certificates

Alternatively, third parties who rely on certificates may consult BEWOR deposit certificates, which is available 24 hours 7 days a week on the web:

- *https://bewor.com/wp-content/uploads/subordinate.crt*

Para comprobar la última CRL emitida en cada CA se debe descargar:

- *Certification Authority (CA) ROOT (UANATACA ROOT 2016):*
- *http://crl1.uanataca.com/public/pki/crl/arl_uanataca.crl*
- *http://crl2.uanataca.com/public/pki/crl/arl_uanataca.crl*

- *Certification Authority (CA) Intermediate 1 (BEWOR TECH CA1):*
  - *http://crl1.uanataca.com/public/pki/crl/bewor.crl*
  - *http://crl2.uanataca.com/public/pki/crl/bewor.crl*

In case of failure of systems checking certificate status for reasons beyond the control of BEWOR, it must make its best efforts to ensure that this service remains inactive for the minimum possible time, which may not exceed one day.

BEWOR provides information to third parties who rely on certificates on the operation of the service certificate status information.

4.9.12. Obligation to check the consultation certificate status service

It is mandatory to check the status of certificates before relying on them.

4.9.13. Special requirements in case of compromise of the private key

The compromise of the private key BEWOR is notified to all participants in certification services, as far as possible, by posting this in the website BEWOR and, if deemed necessary, in other media, even on paper.

4.9.14. Maximum period of suspension of digital certificate

The maximum suspension of a digital certificate is indefinite until its date of expiry.

4.10. Completion of the subscription

After the period of validity of the certificate, the service subscription ends.

As an exception, the subscriber can maintain the existing service, requesting certificate renewal, in time determined by this Certification Practice Statement.

BEWOR can officially issue a new certificate, while subscribers maintain that state.

4.11. Deposit and recovery of keys

4.11.1. Policies and practices of deposit and key recovery

BEWOR does not provide deposit services and key recovery.

4.11.2. Policy and practices of encapsulation and recovery of key session

No stipulation.

5. Physical security controls, management and operations

5.1. Physical security controls

BEWOR has established physical and environmental security controls to protect the resources of the facilities where the systems, the systems themselves and the equipment used for operations of the provision of relying electronic services.

Specifically, the BEWOR's security policy applicable to the relying electronic services has established requirements for the following contingencies:

- Physical access controls.
- Protection against natural disasters.
- Protective measures against fires.
- Failure of the support systems (electronic energy, telecommunications, etc.)
- Collapse of the building.
- Flooding.
- Antitheft protection.
- Unauthorized removal of equipment, information, media and applications relating to components used for the services of the service provider certification.

These measures are applicable to installations where the certificates are produced under the full responsibility of BEWOR, which lends from its both mainstream and, where appropriate, operating in contingency high security installations that are properly audited periodically.

Facilities include preventive and corrective maintenance systems with assistance 24/7 all year round with assistance in the following 24 hours notice.

5.1.1. Location and construction of facilities

Physical protection is achieved by creating clearly defined security perimeters around services. The quality and strength of building materials facility ensures adequate levels of

protection against intrusion by brute force and located in an area of low risk of disasters and allows quick access.

The room where the cryptographic operations are performed in the Data Processing Centre has redundancy in its infrastructure, as well as several alternative sources of power and cooling in an emergency.

BEWOR has facilities to physically protect the provision of services approval of applications for certificates and revocation management, compromise caused by unauthorised access to systems or data access and disclosure thereof.

5.1.2. Physical access

BEWOR has three levels of physical security (building entrance where the CPD is found, access to the room of the CPD and access to the rack) for service of protecting the certificate generation, and must be accessed from the lower to the upper levels.

Physical access to the premises of BEWOR, where certification is processed, is limited and protected by a combination of physical and procedural measures are carried out as such:

- Limited to expressly authorised persons, with identification at the time of access and registration thereof, including filming by CCTV.
- Access to the rooms is done with ID card readers and managed by a computer system that keeps a log of inputs and outputs automatically.
- To access the rack where the cryptographic processes are located, prior authorisation from BEWOR administrators hosting service is necessary to have the key to open the cage.

5.1.3. Electrical power and air conditioning

BEWOR facilities have current-stabilising equipment and power system doubled with generator equipment.

The rooms housing IT equipment have temperature control systems with air conditioners.

5.1.4. Exposure to water

The facilities are located in an area of low risk of flooding.

The rooms where computers are housed have a moisture detection system.

5.1.5. Fire prevention and protection

The facilities and assets of BEWOR have automatic detection and fire fighting systems.

5.1.6. Backup storage

Only authorised individuals have access to support storage.

The most highly classified information is stored in a safe offsite Data Processing Centre.

5.1.7. Waste management

The elimination of media, both paper and magnetic, is made by mechanisms that guarantee the impossibility of retrieving information.

In the case of magnetic media, it proceeds to formatting, permanent deletion, or physical destruction of the support. For paper documents, paper shredders or specially arranged bins for later destruction are used, under supervision.

5.1.8. Offsite backup

BEWOR uses a secure external storage for the safekeeping of documents, magnetic and electronic devices that are independent of the operations centre.

5.2. Procedure controls

BEWOR guarantees that its systems are operated safely, for which it has establish and implemented procedures for the functions which affect the supply of its services.

The staff of BEWOR runs the administrative and management procedures according to the security policy procedures.

5.2.1. Reliable features

BEWOR has identified, according with its security policy, the following reliable functions and roles

- **Internal Auditor**: Responsible for compliance with operating procedures. This is an external person to the Department of Information Systems. The tasks of Internal Auditor are incompatible in time with tasks and incompatible with Certification Systems. These functions will be subordinate to the head of operations, reporting both this technical direction.
- **System Administrator**: Responsible for the proper functioning of hardware and software support platform certification
- **Certification Authority Administrator**: Responsible for the actions to be executed with the cryptographic material, or performing any function involving the activation of private keys of certification authorities described in this document, or any of its elements.
- **Certification Authority Operator**: Necessary to be responsible, in conjunction with CA Manager, of the custody of material activation of cryptographic keys, and responsibility for backup operations and maintenance of AC.
- **Register Administrator**: Person responsible for approving the certification requests made by the subscriber and issuing digital certificates.
- **Revocation officer**: Person responsible for making the changes in the status of a certificate, mainly proceed with the suspension and revocation of the same.
- **Security Manager**: Responsible for coordinating, monitoring and enforcing security measures as defined by the security policies of BEWOR. This individual should be responsible for aspects related to information security: logic, physics, networking, organization, etc.

Persons holding previous posts are subject to procedures of investigation and specific control. Additionally, BEWOR applies policy criteria for the segregation of duties, as preventive measure to fraudulent activities.

5.2.2. Number of individuals per task

BEWOR guarantees at least two people to perform tasks related to the generation, recovery and back up of the private key of the Certification Authorities. Same criteria applies to the implementation of issuance tasks and activation of the certificates and private keys of the Certification Authorities and in general in handling the device custody of the keys of the Authority root and intermediate certification.

5.2.3. Indentification and authentication for each role

The individuals assigned for each role are identified by the internal auditor will ensure that each person performs the operations for which they are assigned.

Each person only controls the assets required for its role, ensuring that no person access unallocated resources.

Access to resources is performed depending on the asset through cryptographic cards and activation codes.

5.2.4. Roles requiring separation of tasks

The following tasks are performed by at least two people:

- The tasks of the Auditor role will be incompatible with the operation and management of systems, and in general, with those roles related to the direct provision of relying electronic services.
- Issuance and revocation of certificates will be incompatible tasks with the Management and systems operation.
- The management and systems operation and the Certification Authorities will be mutually incompatible.

5.2.5. PKI management system

The PKI system is composed of the following modules:

- Component/module for Subordinate Certificate Authority management.
- Component/module for Registration Authority management.

- Component/module for solicitation management
- Component/module for key management (HSM)
- Component/module for databases
- Component/module for CRL management.

Component/module for OCSP service management.

5.3. Personnel controls

5.3.1. History, qualification, experience and authorisation requirements

All staff is qualified and has been properly instructed to perform operations that they have been assigned.
Staff in positions of trust has no personal interests that conflict with the development of the role that has been entrusted.

BEWOR ensures that personnel record is reliable for registration tasks. The Registration Manager has completed a course of preparation for the tasks of validation requests.

In general, BEWOR withdraws an employee from their duties when knowledge of the existence of the commission of any criminal act that could affect the performance of its functions.

BEWOR does not assign to a reliable site management a person who is not suitable for the position, especially for having been convicted of a crime or minor affecting their suitability for the position. For this reason, a previous investigation, **to the extent permitted by applicable law**, on the following is done:

- Studies, including alleged degree.
- Previous work up to five years, including professional references.
- Professional references.

In any case, the Registration Authorities will be able to establish checking procedures of different backgrounds, always preserving BEWOR's policies, who remains responsible for the actions of the persons who authorise the operations.

5.3.2. Procedures of history investigation

BEWOR, before hiring a person or before that person has access to the job, performs the following checks:

- References of the past years jobs
- Professional references
- Studies, including qualifications

BEWOR obtains the unequivocal consent of the affected to such previous research, and processes and protects all his personal data in accordance with the regulations in force regarding the protection of personal data, reflected in the General Data Protection Regulation (EU) 2016/679 and in general any applicable national regulations.

All checks are made up to be allowed by the applicable law. The reasons that may lead the candidate rejection of a job are the followings:

- Falsehoods on the job application, done by the candidate.
- Very negative professional references or not very reliable.

5.3.3. Training requirements

BEWOR trains the staff in reliable and management jobs, until they reach the required qualification, keeping reports of the training.

Training programs are updated and improved periodically and they are updated and improved periodically.

Training includes, at least, the following contents:

- Principles and mechanisms of security of the certification hierarchy, and the user environment of the person to train.
- Tasks the person must do.
- Policies and security procedures of BEWOR. Use and operation of machinery and installed applications.
- Management and processing of incidents and security commitments.
- Procedures of business continuity and emergency.
- Process management and security regarding the processing of personal data.

5.3.4. Retraining frequency and requirements

BEWOR updates the staff training in accordance with the needs, and with enough frequency to comply their functions in a competent and satisfactory way, especially when doing the substantial modifications in the certification tasks.

5.3.5. Job rotation frequency and sequence

Not applicable.

5.3.6. Sections and unauthorized actions

BEWOR has a disciplinary system, to debug the responsibilities arising from unauthorised actions, appropriate to the applicable labour legislation.

Disciplinary actions include suspension and loss of employment of the person responsible for the harmful action, proportionate to the gravity of the unauthorised action.

5.3.7. Professionals contracting requirements

The staff hired to perform reliable tasks sign a previous confidentially agreement and the operational requirements used by BEWOR. Any action that may compromise the security of the accepted processes could, once evaluated, lead to the termination of the employment contract.

In case all or part of the certification services were performed by a third party, the previsions and controls performed in this section, or other parts of the Certification Practice Statement, will be applied and complied by the third party who performs the operation functions of the certification services, notwithstanding, the certification authority will be responsible in any case for the effective implementation. These aspects are concretised in the legal instrument used to arrange the certification services provision by a third party different tan BEWOR.

5.3.8. Documentation supplied to personnel

The certification services provider will provide the documentation strictly needed by the staff at any moment, to perform their job in a competent and satisfactory form.

5.4. Security audit procedures

5.4.1. Types of recorded events

BEWOR produces and safely register, at least, of the following events related to the entity security:

- Booting and shutting down of systems.
- Attempts to create, delete, set passwords or change privileges.
- Attempts to login and logout.
- Unauthorised attempts to enter the CA network.
- Unauthorised attempts to access system files.
- Physical access to logs.
- System configuration maintenance and changes.
- Records of the CA applications.
- Booting and shutting down of CA application.
- Changes of the CA and/or keys details.
- Changes in certificate issuing policies.
- Generation of own keys.
- Creation and revocation of certificates.
- Records of destruction of materials containing key information or activation data.
- Events related to the certificate's lifecycle of the cryptographic module, as lobby, use and uninstalling of it.
- Generation keys ceremony and keys management databases.
- Physical access records.
- System configuration maintenance and changes.
- Staff changes.
- Commitments and disagreements reports.
- Records of destruction of materials containing key information, activation data or personal information of the subscriber, in case of individuals certificates, or

the natural person identified in the certificate, in case of organisation certificates.

- Possession of activation information for operations with the private key of the certification Authority.
- Complete reports of the physical intrusion attempts in the infrastructures that support the certificates issuance and management.

Log entries include the following elements:

- Login date and time.
- Serial number or entry sequence, in the automatic records.
- Identity of the entity entering in the register.
- Type of entrance.

5.4.2. Frequency of processing audit logs

BEWOR reviews its logs when a system alert motivated by the existence of any incident occurs.

Processing audit logs is a review of the records including the verification that confirm they have not been tampered, a brief inspection of all log entries and a deeper investigation of any alert or irregularities in the logs. The actions from the audit review are documented.

BEWOR keeps a system that guarantees:

- Enough space for logs storage.
- Logs files are not rewritten.
- Information held includes, at least: type of event, date and time, user running the event and result of the operation.
- Logs files will be held in structured files susceptible to incorporate into a DB for further exploration.

5.4.3. Period of retention of audit logs

BEWOR holds the logs information for a period of between 1 and 15 years, depending on the type of information recorded.

5.4.4. Audit logs protection

The systems logs:

- Are protected from manipulation by signing the files that contain them.
- Are stored in fireproof devices.
- Availability is protected through its storage in facilities out of the centre where the CA is located.

Access to logs files is reserved only to authorised persons. Also, devices are handled at all times by authorised personnel.

There is an internal procedure where management processes devices containing the data of the audit logs are detailed.

5.4.5. Audit log backup procedures

BEWOR has a proper backup procedure so that, in case of loss or destruction of relevant files, were available in a short period of time the corresponding logs backup.

BEWOR has implemented a secure backup procedure of audit logs, making a copy of all logs weekly in an external source. Additionally, a copy is held in a custody external centre.

5.4.6. Location of the audit logs storage system

The information of the audit events is collected internally and in an automated way by the operating system, network communications and software certificate management, in addition to the data generated manually, will be stored by the authorised personnel. All this composes the storage system of audit logs.

5.4.7. Notification of the audit event to the subect that caused the event

When the log audit accumulation system records an event, it is not necessary to send a notification to the individual, organisation, device or application that caused the event.

5.4.8. Vulnerabily analysis

The audit processes of BEWOR cover vulnerability analysis.

Vulnerability analysis must be run, reviewed and revised by an examination of these monitored events. This analysis must be run daily, monthly and annually in accordance with the internal procedure intended for this purpose.

Audit data systems are stored in order to be used in the investigation of any incident and to locate vulnerabilities.

5.5. Information files

BEWOR guarantees that all information relating to the certificates is held for an appropriate period of time as established in section 5.5.2 of this policy.

5.5.1. Types of records archived

The following documents involved in the life cycle of the certificate are stored by BEWOR (or registration authorities):

- All audit data system.
- All data relating to certificates, including contracts with the signers and the data relating to their certification and location.
- Requests of issuance and revocation of certificates.
- Type of document presented in the certificate request.
- Identity of the Registration Authority that accepts the certificate request.
- Unique identification number provided by the previous document.
- All certificates issued or published.
- CRLs issued or logs of the status of the generated certificates.
- The history of generated keys.
- Communications between the elements of the PKI.
- Policies and Practices Certification.
- All audit data identified in section 5.4.
- Information of requests certification.
- Documentation provided to justify the certification requests.
- Life cycle certificate information.

BEWOR and/or the Registration Authorities accordingly are responsible for the correct file of all this material.

5.5.2. Retention period for the files

BEWOR saves the mentioned logs above for at least 15 years, or the period defined in the current law.

5.5.3. Protection of the file

BEWOR protects the file so only the duly authorised persons can access to it. The file is protected against visualisation, modification erased or any other manipulation through its storage in a reliable system.

BEWOR ensures proper protection of the files by assigning qualified personnel for its treatment and its storage in secure fireproof boxes and external facilities.

5.5.4. File backup procedures

BEWOR has an external storage centre to ensure the availability of the file backups of electronic files. The physical documents are stored in safe places restricted to authorised personnel.

BEWOR, at least, makes incremental daily backups of support of all its electronic documents and makes weekly full backups for data recovery cases.

In addition, BEWOR (or the organisations that make the registration functions) keeps a copy of the paper documents in a safe place different from the own Certification Authority.

5.5.5. Requirements of timestamping

Records are dated with a reliable source via NTP.

There is no need to sign this information digitally.

5.5.6. Location of the file system

BEWOR has a centralised system of gathering information of the activity of the equipment involved in the certificate management service.

5.5.7. Procedures to obtain and verify file information

BEWOR has a procedure where describes the process to verify that the stored information is correct and reachable. BEWOR provides the information and means of verification to the auditor.

5.6. Keys renewal

The CA keys will be changed before the use of the private key expires. The former CA and its private key will only be used for signing CRLs while there are active certificates issued by that CA. A new CA will be generated with a new private key and a new DN. The key change of the subscriber is done by a new issuing process.

Alternatively, in the case of the subordinated Certification Authorities, you will be able to renew the certificate with or without key change, not applying the procedure described earlier.

5.7. Compromised key and recovery of disaster

5.7.1. Management procedures of incidents and commitments

BEWOR has developed security policies and business continuity, which allows the management and backup of the systems in case of compromise or disaster of its operations, ensuring critical services of revocation and publication of the condition of the certificates.

5.7.2. Resources, applications or data corruption

When resources, applications or data corruption events happen, the incidences will be communicated to security, and the proper management procedures will begin, which contemplate scaling, investigation and response to the incident. Procedures of commitment of the keys or disaster recovery of BEWOR will begin, if necessary.

5.7.3. Compromised private key of the entity

In case of suspicion or knowledge of the commitment of BEWOR, key commitment procedures will be activated in accordance to the security policies, incident management and business continuity, which allow the recovery of the critical systems, and if necessary in an alternative data center.

5.7.4. Business continuity capabilities after a disaster

BEWOR will restore critical services (suspension and revocation, and publication of the information of the certificates status) in accordance with the contingency and business continuity plan restoring the normal operation of the previous services within 24 hours of the disaster.

BEWOR has an alternative centre for the operation of certification schemes described in the business continuity plan, if necessary.

5.8. Service termination

BEWOR ensures that potential disruptions to subscribers and third parties are minimal due to the cessation of the certified services provider and, specially, ensures a continuous maintenance of the records required to provide certified evidence for civil or criminal investigation, by transfer to a notary deposit.

Before the services cessation, BEWOR develops a termination plan, with the following provisions:

- To provide the necessary funds (by civil liability insurance) to continue the completion of revocation activities.
- To inform all Signers/Subscribers, relying third parties and other CA's with which it has agreements or another type of relation of the cessation with a minimum of 6 months.
- To revoke any authorisation to outsourced entities to act on behalf of the CA in the process of certificates issuance.
- To transfer its obligations regarding the maintenance of the registry information and logs for the period of time indicated to subscribers and users.

- To destroy or disable for use the private keys of the CA.
- To keep active the certificates and verification system to extinction and revocation of all certificates issued.
- To run all necessary tasks to transfer the maintenance obligations of registration information and the files of events log during the respective time periods indicated to the subscriber and relying third parties in certificates.
- To communicate the Ministry of Energy, Tourism, and Digital Agenda, no later than 2 months before, the cessation of activity and destination of the certificates specifying if the management is transferred and to whom or if the validity will be extinguished.
- To communicate, also to the Ministry of Energy, Tourism and Digital Agenda, the opening of any bankruptcy process against BEWOR, as well as any other relevant circumstance that can prevent the continuation of activity.

6. Technical security controls

BEWOR uses reliable systems and products, protected against any alteration and guarantee the technical and cryptographic security of the certification, which are used as support.

6.1. Generation and installation of the pair of keys

6.1.1. Generation of the pair of keys

The certification authority root "UANATACA ROOT 2016" in accordance with the ceremony procedures of BEWOR creates the pair of keys of the intermediate Certification Authority "BEWOR TECH CA1 2016", within the high security perimeter addressee to this area.

The activities performed during the keys generation ceremony have been registered, dated and signed for all the individuals participating in it, with the presence of an Auditor CISA. Such records are guarded to the effects of audit and follow-up during an appropriate period determined by BEWOR.

For the certification authorities root and intermediate key generation, devices with the certification FIPS 140-2 level 3 and Common Criteria EAL4+ are used.

UANATACA ROOT 2016	4.096 bits	25 years
BEWOR TECH CA1 2016	4.096 bits	13 years
- Final entity certificates	2.048 bits	Up to 5 years

The PKI Disclosure Statement (PDS) of all the electronic certificate profiles indicated in this document, are accessible under the link: https://bewor.com/proveedor-de-firma

6.1.1.1. Generation of the signer pair of keys

The signer can create the signer keys through hardware and/or software devices authorized by BEWOR. The keys that have not being created on a SSCD will be created by the signer. BEWOR never creates a key outside of a SSCD to be sent to the signer.

The keys are created using public key algorithm RSA, with a minimum length of 2048 bits.

6.1.2. Sending the private key to the signer

In certificates, the private key of the qualified signature creation device is created and stored, properly protected, in the interior of such a qualified device.

In the software certificate the private key of the signer is created and stored in the computer system that this signer uses when requesting the certification so the sending of the private key does not exist, ensuring the exclusive control of the key by the user.

In certificates HSM centralized and QSCD centralized, the private key of the signer is created in a private area of the signer on a distant HSM. The signatory enters the login information to the private key, and it is not stored, or susceptible to powers of deduction or interception by the generation system and remote custody. The private key is not sent to the signer, in other words, never leaves the security environment that guarantees the exclusive control of the private key by the signer.

6.1.3. Sending of the public key to the certificate issuer

The method of remission of the public key to the relying electronic certification services provider is PKCS#10, other equivalent cryptographic test or any other method approved by BEWOR.

6.1.4. Public key distribution of the certification services provider

BEWOR's keys are communicated to third parties who trust in certificates, ensuring the integrity of the key and authenticating its origin, through its publication in the Deposit.

Users can access to the Deposit to obtain the public keys, and additionally, in applications S/MIME, the data message may contain a chain of certificates, which are distributed to the users in this way.

The certificate of the CA root and subordinated will be available on the BEWOR web page.

6.1.5. Key sizes

- The length of the Certification Authority root keys is 4096 bits.
- The length of the Certification Authority subordinated keys is 4096 bits.
- The length of the end Entity Certificates keys are 2048 bits.

6.1.6. Generation of public key parameters

The CA Root, CA subordinated and the subscriber certificates public key are encrypted in accordance with RFC 5280.

6.1.7. Quality check of the public key parameters

- Module Length= 4096 bits
- Algorithm of keys generation: rsagen1
- Cryptographic functions of Summary: SHA256.

6.1.8. Key generation in IT applications or in equipment goods

All keys are generated in equipment goods, in accordance with the indicated in section 6.1.1.

6.1.9. Key usage purposes

Key usage for the CA certificates is exclusively for signing certificates and CRLs.

Key usage for the end entity is exclusively for the digital signature, non-repudiation and data encryption.

6.2. Private key protection

6.2.1. Cryptographic modules standards

In relation to the modules that manage the keys of BEWOR and the subscribers of the electronic signature certificates, the required level by the standards indicated in the above sections is ensured.

6.2.2. Private key multi-person (n of m) control

A multi-person control is required for activating the private key of the AC. In case of this Certification Practice Statement, in detail there is a policy of **3 of 6** persons for the keys activation.

Cryptographic devices are physically protected, as determined in this document.

6.2.3. Private key deposit

BEWOR doesn't store usable copies by proper means of the private key of the signers.

6.2.4. Private key backup

BEWOR makes backup copy of the CA private key that makes their recovery in case of disaster, loss or deterioration thereof. Both generation of the copy and the recovery thereof need at least two people participation.

These recovery files are stored in fireproof cabinets and in the external custody centre.

Keys generated on software device: BEWOR cannot make keys backups, since no longer have access to them. The signer may make a backup.
Keys generated on HSM centralized and QSCD centralized: Only it is possible to make backups of an encrypted blob with Security World key of the HSM used and it is impossible to decrypt it without the use of the credentials that only the owner of the certificate knows.

6.2.5. Private key storage

The CA private keys are archived for a period of **10 years** after the issuance of the last certificate. They will be stored in secure fireproof files and in the external custody centre. At least the collaboration of two people will be needed to recover the CA private key in the initial cryptographic device.

The subscriber can store the private key during the time he thinks appropriate, just in case of encrypted certificates. In this case BEWOR also keep a copy of the private key associated to the encrypted certificate.

BEWOR does not generate or archive certificate keys, issued on software.

6.2.6. Private key transfer into a cryptographic module

Private keys are directly generated in the cryptographic modules of production of BEWOR.

6.2.7. Method of activating the private key

The Certification Authority private keys are encrypted stored in the cryptographic modules of BEWOR production.

6.2.8. Method of deactivating the private key

BEWOR private key is activated by the running of the corresponding safe boot procedure of the cryptographic module, by the indicated persons in section 6.2.2.

The CA keys are activated by a process m of n (3 of 6).
The activation of the private keys of the Intermediate CA is managed with the same process of m of n of the CA keys.

6.2.9. Method of destroying the private key

For deactivation of BEWOR private key, the same steps outlined in the corresponding manual of the cryptographic equipment are followed.

6.2.10. Cryptographic modules clasification

Before destroying the keys, a revocation of the certificate of the public keys associated with them will be issued.

Devices that have stored any part of BEWOR private keys are physically destroyed or reset to low level. For disposal, the same steps outlined in the corresponding manual of the cryptographic equipment are followed.

Finally, the backups will be destroyed in a safety way.

The signer keys on software may be destroyed by deleting them following the instructions of the application.

The signer keys in hardware may be destroyed by a special computer application at the offices of the RA or BEWOR.

6.3. Other aspects of key pair management

6.3.1. Public key file

BEWOR archives its public keys routinely, according to the established in section **¡Error! No se encuentra el origen de la referencia.** of this document.

6.3.2. Public and private key usage periods

Periods of use of the keys are determined by the duration of the certificate, after which they cannot continue to be used.

As an exception, the private key of decryption can continue being used even after the expiration of the certificate.

6.4. Activation data

6.4.1. Activation data generation and instalation

Activation data of the devices that protect BEWOR private keys are generated in accordance with the established in section 6.2.2 and key procedures ceremony.

The creation and distribution of such devices is recorded.

Likewise, BEWOR generates the activation data in a safe way.

6.4.2. Activation data protection

Activation data devices that protect the private keys of the Certification Authority root and subordinated, are protected by the holders of cards managers of the cryptographic modules, as stated in the document of the keys ceremony.

The certificate signer is responsible for protecting his private key, with a password as complete and complex as possible. The signer must remember the password(s).

6.5. Computer security controls

BEWOR uses reliable systems to provide certification services. BEWOR has made controls and computer audits to establish its proper computer activity management with the level of security required in the system management of electronic certification.

Regarding the information security, BEWOR applies the certification scheme controls on management systems ISO 27001.

Used equipment's are initially configured with appropriate security profiles of BEWOR staff system, in the following aspects:

- Setting up the operating system.
- Setting up the application security.

- Correct sizing of the system.
- User and permissions settings.
- Setting event Log.
- Backup and recovery plan.
- Antivirus settings.
- Requirements of network traffic.

6.5.1. Specific computer security technical requirements

Each BEWOR server includes the following functionalities:

- Access control of the subordinate CA services and privilege management.
- Imposition of separation of duties for managing privileges.
- Identification and authentication of roles associated to identities.
- Archive of the subscriber and subordinate CA history and audit data.
- Audit events related to security.
- Self-diagnosis of safety related with the subordinate CA services.
- Recovery mechanisms of keys and subordinate CA system.

The stated functionalities are performed through a combination of operating system, PKI software, physical protection and procedures.

6.5.2. Computer security rating

The CA and RA applications used by BEWOR are reliable.

6.6. Life cycle technical controls

6.6.1. System development controls

The applications are developed and implemented by BEWOR in accordance with the development and change control standards.

The applications have methods for verifying the integrity and authenticity, as well as the correction of the version to use.

6.6.2. Security management controls

BEWOR develops the precise activities for training and employee awareness of security. The materials used for training and descriptive documents processes are updates after approval by a group for security management. An annual training plan is used.

BEWOR requires by contract security measures equivalent to any external provider involved in the certification tasks of the relying electronic service.

6.6.2.1. Classification and management of information and goods

BEWOR supports an inventory of assets and documentation and a procedure for the management of this material to guarantee its use.

BEWOR security policy details the procedures of information management where it is classified according to its level of confidentiality.

The documents are classified into three levels: UNCLASSIFIED, INTERNAL USE and CONFIDENTIAL.

6.6.2.2. Management operations

BEWOR has an appropriate process management and incident response, by implementing a warning system and the generation of periodic reports.

In BEWOR security document the incident management process is developed in detail.

BEWOR has documented all the procedure relative to the roles and responsibilities of the staff involved in the control and manipulation of elements contained in the certification process.

6.6.2.3. Treatment of supports and safety

All supports are treated safely in accordance with the requirements of the classification of information. The supports that contain sensitive information are destroyed safely if they are not going to be required again.

Planning system

BEWOR Systems department keeps track of the capabilities of the equipment. In conjunction with the implementation of resources control each system can provide a possible downsizing.

Reports of incidents and response

BEWOR has a procedure for follow-up of incidents and its resolution, where the answers and an economic evaluation are registered, which supposes the resolution of the incident.

Operational procedures and responsibilities

BEWOR defines activities assigned to persons with a role of trust, other than those responsible for performing daily operations that do not have character of confidentiality.

6.6.2.4. Access system management

BEWOR makes all efforts that are reasonable available to confirm that the system access is limited to authorised persons.

In particular:

CA General

- Controls based on firewalls, antivirus and IDS high availability are available.
- Sensitive data is protected by cryptographic techniques or controls with strong identification.
- BEWOR has a documented procedure for managing the users' authorisations and cancellations and access policy, detailed in its policy of security.

- BEWOR has procedures to ensure that operations are performed in accordance with policy roles.
- Each person has associated a role to perform the certification operations.
- BEWOR staff is responsible for its actions by the confidentiality agreement signed with the Company.

Certificate generation

Authentication for Issuance process is performed through a system of m of n operators for activating BEWOR private key.

Revocation management

Revocation will be performed by strong authentication to the applications of an authorised administrator. Logs systems will generate the tests that guarantee non-repudiation of the action taken by BEWOR administrator.

Revocation status

The application for the status of the revocation offers access control based on the authentication with certificates or dual factor identification to avoid the attempt to change of the status information of the revocation.

6.6.2.5. Life cycle management of cryptographic hardware

BEWOR ensures that the cryptographic hardware used for signing certificates is not handled during its transport by inspecting the delivered material.

The cryptographic hardware moves on prepared supports to prevent any manipulation.

BEWOR records all relevant device information to add to the catalogue of assets.

The use of cryptographic hardware for signature certificates requires the use of at least two trusted employees.

BEWOR makes periodic tests to ensure the correct functionality of the device.

Only reliable personnel manipulate the cryptographic hardware device.

BEWOR signature private key stored in the cryptographic hardware will be erased once the device is removed.
BEWOR system configuration, as well as its modifications and updates are documented and controlled.

Changes or updates are authorised by the security officer and they are reflected in the corresponding team's working minutes. At least, two reliable persons perform these settings.

6.7. Network security controls

BEWOR protects the physical access to network management devices and has an architecture that directs the traffic generated based on its features of security, creating clearly defined network sections. This division is performed with firewalls.

Confidential information is transferred through unsecured networks; it is performed in an encrypted way using SSL protocols or VPN system with dual factor authentication.

6.8. Engineering controls of cryptographic modules

Cryptographic modules are subject to engineering controls provided in the standards indicated along this section.

The key generation algorithms used are commonly accepted for the use of the key to which they are intended.

All cryptographic operations of BEWOR are performed in modules with FIPS 140-2 level 3 certification.

6.9. Time sources

BEWOR has a procedure of time synchronisation coordinated via NTP, that has access to two independent services:

The first synchronisation is a service based on GPS antennas and receivers that allow a level of trust of STRATUM 1 (with two high availability systems)
The second one has a complementary synchronisation, via NTP, with the Spanish Royal Institute and Observatory of the Navy (ROA).

6.10. Change of the Status of a Secure Signature Creation Device (SSCD)

In the case of modification of the certification status of the secire signature creation devices (SSCD), the following procedure will be followed:
1. A list of several certified SSCDs is available, as well as a close relationship with suppliers of such devices, in order to guarantee alternatives to possible loss of status of QSCD device certification.
2. In the event of the end of the period of validity or loss of the certification, said SSCDs will not be used for the issuance of new digital certificates, either for new issues or eventually for possible renewals.
3. You will immediately proceed to switch to SSCD devices with valid certification.
4. In the event that a SSCD device has been shown to never have been, due to counterfeiting or any other type of fraud, we will immediately notify your customers and the regulatory body, revoke the digital certificates issued on these devices and replace them. issuing them in valid SSCDs.

7. Certificates profiles and CRLs

7.1. Certificate profile

All qualified certificates issued under this policy comply the X.509 standard version 3, RFC 3739 and ETSI 101 862 “Qualified Certificate Profile”. The documentation relating to the profiles of the policy EN 319 412 can be requested to BEWOR.

7.1.1. Version number

BEWOR issues certificates X.509 Version 3

7.1.2. Extensiones del certificado

Certificates extensions are detailed in the profiles documents, which are accessible from BEWOR’S web https://bewor.com/proveedor-de-firma.

In this way, it is allowed to keep more stable versions of the Certification Practice Statement and decouple them from frequent adjustments in the profiles.

7.1.3. Object identifier (OID) of the algorithms

The object identifier of the signature algorithm is:

- 1.2.840.113549.1.1.11 sha256WithRSAEncryption

The object identifier of the public key algorithm is:

- 1.2.840.113549.1.1.1 rsaEncryption

7.1.4. Names format

Certificates must contain the required information for its use, as determined by the appropriate policy.

7.1.5. Names restriction

Names contained in the certificates are restricted as “Distinguished Names” X.500, which are unique and not ambiguous.

7.1.6. Object identifiers (OID) of certificates types

All certificates include an identifier of the certificates policy under which they have been issued, in accordance with the indicated structure in section 1.2.1

7.2. CRL profile

7.2.1. Version number

CRLs issued by BEWOR are from version 2.

7.2.2. OCSP profile

According to standard IETF RFC 6960.

8. Compliance audit

BEWOR has communicated the beginning of its activity as certification services provider by the Ministry of Industry and when the authority deems necessary it is subjected to check controls.

8.1. Frequency of compliance audit

BEWOR conducts a compliance audit annually, in addition to internal audits carried out at its own discretion or at any time, due to a suspected breach of any security measure.

8.2. Identification and qualification of the auditor

An external independent audit signature performs the audits, demonstrating technical competence and experience in computer security, information systems security and compliance audits of public key certification services and related elements.

8.3. Auditor relationship to audited entity

Audit firms are of renowned prestige, with specialised departments in conducting IT audits, so there is no conflict of interest that could undermine its performance in relation to BEWOR.

8.4. Topics covered by audit

The audit verifies with reference to BEWOR that:

a) The entity has a management system, which ensures the quality of service.
b) The entity complies with the requirements of the Certification Practice Statement and other documentation related to the issuance of the various digital certificates.

c) The Certification Practice Statement and other related legal documentation comply with the agreed with BEWOR and the established in the current regulation.
d) The entity properly manages its information systems.

Specially, the topics covered by audit are as follows:

a) CA, RA's and related elements processes.
b) Information systems.
c) Protection of the data processing centre.
d) Documents.

8.5. Actions taken as a result of lack of conformity

Once the management has received the auditor's compliance report, the deficiencies found are analysed with the audit entity. This report also develops and implements the corrective policies that tackle these deficiencies.

If BEWOR is unable to develop and/or implement the corrective measures or if the deficiencies found suppose an immediate threat to the system security or integrity, shall immediately inform to the Security Committee of BEWOR which can perform the following actions:

- Cease operation temporarily.
- Revoke the CA key and regenerate the infrastructure.
- Terminate the CA service.
- Other complementary actions needed.

8.6. Treatment of audit reports

Audit reports results are delivered to the Security Committee of BEWOR within a maximum period of 15 days after completion of the audit.

9. Business and legal requirements

9.1. Fees

9.1.1. Certificate issuance or renewal fees

BEWOR can establish a certificate issuance or renewal fee and when appropriate the subscribers will be informed in due course.

9.1.2. Certificate access fees

BEWOR hasn't established any fee for certificates access.

9.1.3. Certificate status information access fees

BEWOR hasn't established any fee for certificates status information access.

9.1.4. Fees for other services

Not stipulated.

9.1.5. Reund policy

Not stipulated.

9.2. Financial capacity

BEWOR has enough economic resources to keep its operations, to comply with its obligations and to confront the risk of liability for claim and damages, as established in ETSI EN 319 401-1 7.12 c), in relation to the management of the services finalisation and termination plan.

9.2.1. Insurance coverage

BEWOR has warranty coverage of its civil liability, with an insurance of professional civil liability that complies with the current regulation applicable.

9.2.2. Other assets

Not stipulated.

9.2.3. Insurance coverage for subscribers and relaying third parties in certificates

BEWOR has a warranty coverage of its civil liability, with an insurance of professional civil liability, for relying electronic services, with the minimum insured of 3,000,000 Euros.

9.3. Confidentiality

9.3.1. Confidential information

BEWOR keeps in confidence the following information:

- Certificates request, approved or rejected, and all other personal information obtained for issuance and maintenance of certificates, except the information indicated in next section.
- Private keys generated and/or stored by the certification services provider.
- Transaction record, including full records and audit records of the transactions.
- Internal and external transactions records created and/or kept by the Certification Authority and its auditors.
- Business continuity and emergency plans.
- Security plans.
- Documentation of operations, archiving, motorisation and other analogous.
- All other information identified as 'Confidential'.

9.3.2. Non confidential information

The following information is considered non-confidential:

- Certificates issued or in the process of issuance.

- Linking the subscriber to a certificate issued by the Certification Authority.
- Name and surname of the natural person identified on the certificate, as well as any other circumstance or personal information of the holder, in the event that it is important according to the purpose of the certificate.
- Email of the natural person identified on the certificate, or email assigned to the subscriber, in case it is important according to the purpose of the certificate.
- Economic uses and limits outlined in the certificate.
- Validity period of the certificate, as well as date of issue and expire date of the certificate.
- Serial number of the certificate.
- The different status or conditions of the certificate and starting date for each, specifically: pending of generation and/or delivery, valid, revoked, suspended or expired and the reason that caused the change of status.
- The Certificate Revocation Lists (CRLs), and the remaining revocation status information.
- The information contained in the certificates deposits.
- Any other information not indicated in the previous section.

9.3.3. Information disclosure of suspension and revocation

See previous section.

9.3.4. Legal disclosure of information

BEWOR only discloses the confidential information in the cases legally foreseen.

Specifically, records that support the reliability of the data contained in the certificate will be disclosed if required to prove the evidence of the certification in legal proceedings, even without the consent of the certificate subscriber.

BEWOR will indicate these circumstances in the privacy policy under section 9.4.

9.3.5. Information disclosure on request of the owner

BEWOR includes under privacy policy Section 9.4, requirements to allow the disclosure of subscriber information and, when appropriate, of the natural person identified on the certificate directly allocated or to third parties.

9.3.6. Other information disclosure circumstances

Not stipulated.

9.4. Personal data protection

BEWOR is compliance with current regulations on the protection of personal data, as reflected in the General Data Protection Regulation No. 2016/679 and in general any applicable national regulations.

In compliance with, BEWOR has documented in this Certification Practice Statement the security and organizational aspects and procedures, in order to guarantee that all the personal data to which it has access are protected against its loss, destruction, damage, forgery and illegal or unauthorized processing.

The following is a detail of all the necessary information regarding the processing of personal data made by BEWOR:

Responsable del tratamiento
Bewor Tech S.L.
NIF: B19603968
Dirección: P.I. Cortijo del Conde, Calle Pago de Cambea, 14 Nave 7 18015-Granada
Correo electrónico: helpdesk@bewor.com

Purposes of data processing
BEWOR has the duty to inform users that all their personal data provided are treated for the following purposes:

- Provision of Electronic Trust Services. The data is collected through the appropriate contract and is processed with the purpose of carrying out the electronic services requested and contracted by the users, all based on the provisions of this Certification Practice Statements.
- Address inquiries and requests. The data is collected through the contact form available on the website and will be used exclusively to manage the queries and requests received.

BEWOR informa que los datos personales facilitados únicamente se tratarán para las finalidades anteriormente descritas y no serán tratados de manera incompatible con las mismas.

Lawfulness of processing

In accordance with the indicated data purposes, the legal basis for the treatment of personal data of users is:

- The legitimation of the data processing for the provision of electronic trust services is the execution of the contract for the services requested, where the user is part of it.
- The legitimacy of the data processing to attend to inquiries and requests is based on the consent of the interested party, who gives it expressly and unequivocally, through positive action and prior to sending, upon accepting the conditions and the privacy policy. Such consent can be withdrawn at any time by sending an email to helpdesk@bewor.com.

Processed data and conservation

The categories of personal data processed by BEWOR, including but not limited to, include identifying data (name, surname and identity) and contact information (postal address, email and telephone).

Personal data will be kept as long as they are necessary to respond to inquiries and requests, until the end of the contractual relationship and subsequently, during the legally required periods according to each case, as defined in this Certification Practice Statement.

Data transfer

Personal data will not be transferred to third parties without legal obligation, nor will international transfers be made.

User rights

- Confirmation. All users have the right to obtain confirmation on whether BEWOR is processing personal data concerning them.
- Access and rectification. Users have the right to access all their personal data, as well as request the rectification of those that are inaccurate or erroneous.
- Suppression / cancellation. Users may request the deletion / cancellation of data when, among other reasons, these are not necessary for the purposes for which they were collected.
- Limitation and opposition. The user may request the limitation of the treatment so that their personal data is not applied in the corresponding operations. In certain circumstances and for reasons related to their particular situation, the user may object to the data processing, being BEWOR obliged to stop treating them, except for compelling legitimate reasons, or the exercise or defense of possible claims.
- Portability Interested parties may request that their personal data be sent to them or else be transmitted to another person in charge, in a structured electronic format and of habitual use.

To exercise their rights, users can send a request to the e-mail address helpdesk@bewor.com or send a letter to the address indicated in the information section of the person responsible for processing. In this petition, they must attach a copy of their identity document and clearly indicate which right they wish to exercise.

9.5. Intellectual property rights

9.5.1. Property of certificates and revocation information

BEWOR is the only one that has intellectual property rights on the certificates that issues, without any prejudice of the rights of the subscribers, key holders and third parties, to which it grants non exclusive license to reproduce and distribute certificates, free of charge, as long as the reproduction is full and does not alter any element of the certificate, and is necessary in relation with digital signatures and/or encryption systems within the scope of the certificate use, and according to the documentation that links them.

In addition, certificates issued by BEWOR have a legal notice concerning their ownership.

The same rules are applicable to the use of the information of certificates revocation.

9.5.2. Property of the Certification Practice Statement

BEWOR is the only one that has intellectual property rights of this Certification Practice Statement.

9.5.3. Property of information relating to names

The subscriber and, where appropriate, the natural person identified on the certificate, preserves all rights on the brand, product or trade name included on the certificate.

The subscriber owns the distinguished name of the certificate, consisting of the information specified in section 3.1.1.

9.5.4. Property of keys

The subscribers of the certificates are the owners of the key pair.

When a key is divided in parts, all parts of the key are property of the owner of the key.

9.6. Obligations and civil liability

9.6.1. BEWOR obligations

BEWOR guarantees, under full responsibility that complies with all requirements established in the Certification Practice Statement, and it is responsible for ensuring compliance with the procedures described, according to the instructions contained in this document.

BEWOR provides relying electronic services in accordance with this Certification Practice Statement.

Previous issuance and delivery of the certificate to the subscriber, BEWOR informs the subscriber of the terms and conditions related to the use of the certificate, price and use limitations, through a subscriber contract that includes by reference the disclosure texts (PDS) of each of the acquired certificates.

The disclosure text document, also known as PDS[3], meets the content of Annex A of ETSI EN 319 411-1 v1.1.1 (2016-02) this document can be transmitted by electronic media, using a sustainable communication method, and in accessible language.

BEWOR binds subscribers, key holders and third parties that trust in certificates through the disclosure text or PDS, in written and understandable language, with the minimum following contents:

- Requirements to comply with the provisions of sections 4.5.3, **¡Error! No se encuentra el origen de la referencia.**, **¡Error! No se encuentra el origen de la referencia.**, 9.6.8, 9.6.9 y **¡Error! No se encuentra el origen de la referencia.**.
- Requirements to comply with the provisions of sections 4.5.3, **¡Error! No se encuentra el origen de la referencia.**, **¡Error! No se encuentra el origen de la referencia.**, 9.6.8, 9.6.9 and **¡Error! No se encuentra el origen de la referencia.**.
- Indication of the applicable policy, indicating that the certificates are not issued to the public.

3 “PKI Disclosure Statement”.

- Demonstration of the information contained in the certificate is accurate, unless notification against the subscriber.
- Consent for the publication of the certificate in the deposit and third party access.
- Consent for storing information used for the subscriber registration and the termination of such information to third parties, in case of termination of operations of the Certification Authority without revocation of valid certificates.
- Limits of use of the certificate, including those established in section 1.4.2.
- Information about how to validate a certificate, including the requirement to check the certificate status and the conditions under which it can reasonably trust the certificate, which applies when the subscriber acts as a relying third party in the certificate.
- The way in which the liability of the Certification Authority is guaranteed.
- Limitations of liability, including the uses for which the Certification Authority accepts or excludes its liability.
- Certificates request information file period.
- Audit registry file period.
- Applicable procedures of dispute settlement.
- Applicable Law and competent jurisdiction.
- If the Certification Authority has been declared in conformity with the certification policy, where appropriate, according to which system.

9.6.2. Guarantees offered to subscribers and relying third parties in certificates

BEWOR establishes and rejects guarantees and applicable disclaimers in the documentation that connects the subscribers and relying third parties in certificates.

BEWOR guarantees the subscriber, at least:

- Not factual errors in the information in the certificates, known or made by the Certification Authority.
- Not factual errors in the information in the certificates, due to lack of due diligence of the certificate request or to its creation.
- The certificates comply with all the material requirements established in the Certification Practice Statement.

- Revocation services and the use of the Deposit comply with all material requirements established in the Certification Practice Statement.

BEWOR guarantees the third party that trusts in the certificate, at least:

- The information contained or incorporated by reference in the certificate is accurate, except when the opposite is indicated.
- In case of certificates published in the Deposit, that the certificate has been issued to the identified subscriber and the certificate has been accepted, in accordance with section 4.4.
- The approval of the certificate request and in the certificate issuance all the material requirement established in the Certification Practice Statement has been accomplished.
- Speed and assurance with the services provision, especially with revocation services and Deposit.

In addition, BEWOR guarantees the subscriber and the relying third party in the certificate:

- The certificate has the information that a qualified certificate must have, in accordance with Article 11 of the Regulation 59/2003, 19th December.
- Confidentiality is preserved during the process if private keys are generated by the subscriber or, where appropriate, the natural person identified on the certificate.
- The responsibility of the Certification Authority, with the limits established.

9.6.3. Rejection of other guarantees

BEWOR rejects any other guarantee that is not enforceable under the laws, except the ones covered in section 9.6.2.

9.6.4. Limitation of liability

BEWOR limits its responsibility to the issuance and management of certificates and key pair of subscribers supplied by the Certification Authority.

9.6.5. Indemnity clauses

9.6.5.1. Subscriber indemnity clause

BEWOR includes in the contract with the subscriber, a clause whereby the subscriber agrees to indemnify the Certification Authority of any damage from any action or omission that results in liability, damage or loss, expenses of any kind, including judicial and legal representation that may be incurred by the publication and use of the certificate, when occurs any of the following causes:

- Falsehood or inaccurate statements committed by the certificate user.
- Certificate user error when administering enrolment request data. If there was fraud or negligence in the action or omission regarding the Certification Authority or any relying person in the certificate.
- Private key protection negligence, when using a relying system or when keeping the necessary precautions to avoid its compromise, loss, disclosure, modification or the unauthorised use.
- Use of a name (including names, email address and domain names), or other certificate information that infringes intellectual or third party industrial property of others by the subscriber.

9.6.5.2. Relying third person in the certificate indemnity clause

BEWOR includes in the disclosure text or PDS, a clause whereby the relying third party in the certificate agrees to indemnify the Certification Authority of any damage from any action or omission that results in liability, damage or loss, expenses of any kind, including court and legal representation that may be incurred by the publication and use of the certificate, when any of the following causes occurs:

- Breach of the obligations of the relying third party in the certificate.
- Reckless trust in a certificate, along with the circumstances.
- Lack of checking of the certificate status, to determine that it is not suspended or revoked.

9.6.6. Fortuitous event and force majeure

BEWOR includes in the disclosure text or PDS, clauses that limit its responsibility in fortuitous event or force majeure.

9.6.7. Applicable law

BEWOR establishes, in the subscriber contract and in the disclosure text or PDS, that the applicable law of services provision, including the policy and practices of certification, is the Spanish Law.

9.6.8. Severability, survival, entire agreement and notification clauses

BEWOR establishes, in the subscriber's contract and in the disclosure text or PDS, the severability, survival, entire agreement and notification clauses:

- Under the severability clause, the invalidity of a clause will not affect the rest of the contract.
- Under the survival clause, certain rules will remain in force after the completion of the regulatory service of the legal relationship between the parties. For this purpose, the Certification Authority ensures that the requirements of sections 9.6.1 (Obligations and liability), 8 (Compliance audit) and 9.3 (Confidentiality), remain in force after the termination of the service and the general conditions of issuance/use.
- Under the entire agreement clause it is understood that the regulatory legal service contains the full will and all agreements between the parties.
- Under the notification clause, it will be established the procedure by which the parties mutually report incidents.

9.6.9. Competent jurisdiction clause

BEWOR establishes, in the subscriber's contract and in the disclosure text or PDS, a jurisdiction clause, indicating that the international jurisdiction corresponds to the Spanish judges.

The territorial and functional jurisdiction shall be determined under the regulations of international private law and procedural law that may be applied.

9.6.10. Resolution of conflicts

BEWOR establishes, in the subscriber's contract, and in the disclosure text or PDS, mediation and resolution procedures of applicable disputes.

10. Annex I - Acronyms

EBA	European Banking Authority
CA	Certification Authority.
RA	Registration Authority
CP	Certificate Policy
CPS	Certification Practice Statement.
CRL	Certificate Revocation List.
CSR	Certificate Signing Request.
DES	Data Encryption Standard.
DN	Distinguished Name.
DSA	Digital Signature Algorithm.
SSCD	Secure Signature Creation Device.
FIPS	Federal Information Processing Standard Publication
ISO	International Organization for Standardisation.
LDAP	Lightweight Directory Access Protocol.
OCSP	On-line Certificate Status Protocol.
OID	Object Identifier.
PA	Policy Authority.
PIN	Personal Identification Number.
PKI	Public Key Infrastructure.
RSA	Rivest-Shimar-Adleman.
SHA	Secure Hash Algorithm.
SSL	Secure Sockets Layer
TCP/IP	Transmission Control. Protocol/Internet Protocol