ORGANIZACIÓN MÉDICA COLEGIAL DE ESPAÑA
CONSEJO GENERAL DE COLEGIOS OFICIALES DE MEDICOS

Plaza de las Cortes,11
28014 Madrid
Tel. +34 914 317 780
cgcom@cgcom.es
www.cgcom.es

PKI DISSEMINATION STATEMENT - PDS

1. GENERAL INFORMATION

Formal state		
Prepared by:	**Review by:**	**Approved by:**
Name: AC Date: 21-03-2022	Name: ASTREA Date: 22-03-2022	Name: CP Date: 23-03-2022

Control version				
Version	**Changed parts**	**Description of the changed parts**	**Author**	**Date**
2.0	Original		VH	10-01-2020
2.1		Adaptation to the Spanish Law Ley 6/2020	Astrea	12-05-2021
2.2	2.1.3, 2.2.1, 2.3	Profile updates Minor corrections	Astrea	23-03-2022
2.3		Annual review	Astrea	10-05-2023

Index

1. Contact information

1.1. Responsible organization

The Certification Entity of the “Consejo General de Médicos de Colegios Oficiales de Médicos”, hereinafter referred to as "AC-CGCOM", is an initiative of:

CONSEJO GENERAL DE COLEGIOS OFICIALES DE MÉDICOS

PLAZA DE LAS CORTES, 11- 28014 MADRID

PHONE: 91 431 77 80 / FAX: 91 576 43 88

1.2. Organization that administrates the document

COMISIÓN PERMANENTE DEL CONSEJO GENERAL DE COLEGIOS OFICIALES DE MÉDICOS

PLAZA DE LAS CORTES, 11- 28014 MADRID

PHONE: 91 431 77 80 / FAX: 91 576 43 88

1.3. Contact person

CONSEJO GENERAL DE COLEGIOS OFICIALES DE MÉDICOS

PLAZA DE LAS CORTES, 11- 28014 MADRID

PHONE: 91 431 77 80 / FAX: 91 576 43 88

1.4. Contact for revocation processes

For revocation processes, contact to:

CONSEJO GENERAL DE COLEGIOS OFICIALES DE MÉDICOS

· UNIDAD TECNOLÓGICA ·

PLAZA DE LAS CORTES, 11- 28014 MADRID

TELÉFONO: 91 431 77 80 / FAX: 91 576 43 88

2. Types and certificate purposes

2.1. Qualified certificates for natural person

These certificates are qualified certificates in accordance with Article 28 and Annex I of Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014 and comply with the provisions of the technical regulation identified with the reference ETSI EN 319 411-2.

2.1.1. Hardware certificates

Hardware certificates work with a qualified signature creation device, in accordance with Annex II of Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014

2.1.2. Cloud certificates

These certificates are managed centrally.

These certificates work with a qualified signature creation device, in accordance with Annex II of Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014.

These certificates guarantee the identity of the subscriber, and the person included in the certificate, and allow the generation of the **qualified electronic signature** based on qualified electronic certificates”.

2.1.3. Software certificates

These certificates are managed on a user local environment.

These certificates does not work with a qualified signature creation device.

These certificates guarantee the identity of the subscriber, and the person identified in the certificate.

2.1.4. Certificates for identification usage

Certificates for identification usage grants the identity of the subscriber and the signatory.

2.1.5. Certificates for signing usage

Certificates for signing usage allow the generation of the "qualified electronic signature"; that is, the advanced electronic signature that is based on a qualified certificate and that has been generated using a qualified device, for which, in accordance with the provisions of Article 25.2 of Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014, it shall have a legal effect equivalent to that of a handwritten signature.

2.1.6. Certificates for encryption usage

Certificates for encryption usage may be used to encrypt own documents or to receive confidential documents, in any format, protected by encryption using:

a) The public key belonging to the person identified in the certificate.
b) An encryption session key, symmetric, encrypted with the public key of the person identified in the certificate.

In any case, the private key shall be used to decrypt the message, warning the subscriber of the certificate and the person indicated in the certificate that a lost key shall not be recovered under no circumstance, so that **CGCOM shall not be liable for any loss of encrypted information that cannot be recovered in cases of loss of certificates or keys**.

2.1.7. Collegiate doctor certificates

These certificates are issued to collegiate doctors within the corporative scope of the subscriber college. These certificates are not issued to the general public under no circumstances. The collegiate doctor is considerate to be the signatory.

Likewise, these certificates guarantee the status of collegiate, given the mandatory intervention of the college in the procedure for issuing the certificate, acting as a registration entity or as a guarantor of the information.

2.1.8. Natural person representing legal entity certificates

These certificates guarantee the identity of the subscriber and the signatory, indicate a relationship of legal representation or general power of attorney between the signatory and an entity, college of doctors or medical organisation described in field "O" (Organisation)

Likewise, they also include a statement regarding the category of the signatory, which has been verified before issuing the certificate, and is correct. It is necessary to note that this indication is not, by itself, sufficient to determine the powers that the signatory has to sign, if applicable, on behalf of the certification service subscriber; therefore, the user part shall verify the signature faculties and powers of the signatory though means other than a certificate, such as the CGCOM validation service.

2.1.9. Natural person linked to an organization certificates

These certificates are issued to a natural person linked within the corporative scope of the subscriber college or the legal person within the medical scope. This natural person is considerate to be the signatory and, therefore, the holder of the corresponding card and the complementary software.

2.2. Qualified electronic seal certificates

These certificates are qualified certificates in accordance with Article 38 and Annex III of Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014 and comply with the provisions of the technical regulation identified with the reference ETSI EN 319 411-2.

2.2.1. Cloud qualified electronic seal certificates

Electronic seal certificates allow the generation of the "**qualified electronic seal**"; that is, the **advanced electronic** seal that is based on a qualified seal certificate and that has been generated using a qualified device.

2.2.1. Software Qualified seal certificate

These certificates are managed on a seal creator local environment.

These certificates do not work with qualified signature creation device.

These certificates are issued to Doctors Colleges and to legal person within the medical scope. These certificates are not issued to the general public under no circumstances.

2.3. Types of certificates

Type	Media	Usage	OID
Collegiate Doctor	Card	Authentication	• 1.3.6.1.4.1.26852.1.1.1.1 • 0.4.0.2042.1.2
		Signature	• 1.3.6.1.4.1.26852.1.1.1.2 • 0.4.0.194112.1.2
		Encryption	• 1.3.6.1.4.1.26852.1.1.1.3
	Centralised on CLOUD	Authentication, Signature	• 1.3.6.1.4.1.26852.1.1.1.4 • 0.4.0.194112.1.2
	Software	Authentication, Signature	• 1.3.6.1.4.1.26852.1.1.1.5 • 0.4.0.194112.1.0

Type	Media	Usage	OID
Natural personal linked	Card	Authentication	• 1.3.6.1.4.1.26852.1.1.2.1 • 0.4.0.2042.1.2
		Signature	• 1.3.6.1.4.1.26852.1.1.2.2 • 0.4.0.194112.1.2
		Encryption	• 1.3.6.1.4.1.26852.1.1.2.3

	Centralised on CLOUD	Authentication, Signature	• 1.3.6.1.4.1.26852.1.1.6 • 0.4.0.194112.1.2
	Software	Authentication, Signature	• 1.3.6.1.4.1.26852.1.1.2.5 • 0.4.0.194112.1.0

Type	Media	Usage	OID
Natural personal representing a legal person	Card	Authentication	• 1.3.6.1.4.1.26852.1.1.11.1 • 0.4.0.2042.1.2 • 2.16.724.1.3.5.8
		Signature	• 1.3.6.1.4.1.26852.1.1.11.2 • 0.4.0.194112.1.2 • 2.16.724.1.3.5.8
		Encryption	• 1.3.6.1.4.1.26852.1.1.11.3 • 2.16.724.1.3.5.8
	Centralised on CLOUD	Authentication, Signature	• 1.3.6.1.4.1.26852.1.1.12 • 0.4.0.194112.1.2 • 2.16.724.1.3.5.8
	Software	Authentication, Signature	• 1.3.6.1.4.1.26852.1.1.11.5 • 0.4.0.194112.1.0 • 2.16.724.1.3.5.8

Type	Media	Usage	OID
Legal person electronic seal	Centralised on CLOUD	Authentication, Signature	• 1.3.6.1.4.1.26852.1.1.10.2 • 0.4.0.194112.1.3
	Software	Authentication, Signature	• 1.3.6.1.4.1.26852.1.1.10.5 • 0.4.0.194112.1.1

2.4. Issuing certification body

The certificates indicated are issued by the CGCOM Certificacion Authorithy (AC-CGCOM), identified by the data indicated above.

The AC-CGCOM outsources the certificate production service on Vintegris, as its technical provider, which always performs its services following the AC-CGCOM indications.

2.5. Certificate validation

The lists of revoked certificates and OCSP services can be found on the AC-CGCOM website and at the URLs indicated in each of the certificates.

3. Limits on the use of the certificate

3.1. Limits on use for signatories

The signatory and the seal creator shall use the certificate certification service provided by the AC-CGCOM exclusively for the uses authorised in the contract signed between the AC-CGCOM and the Doctor College or the subscriber legal person, and which are reproduced below.

Likewise, the signatory and the seal creator undertakes to use the digital certification service in accordance with the instructions, manuals or procedures provided by the AC-CGCOM.

The signatory and the seal creator shall comply with any laws and regulations that may affect its right to use the cryptographic tools it employs.

The signatory and the seal creator shall not take any measures to inspect, alter or reverse engineer AC-CGCOM's digital certification services, without prior express permission.

3.2. Limits on use for verifiers

The certificates are used for their own function and established purpose, without being able to be used for other functions and for other purposes.

Similarly, certificates shall be used only in accordance with the applicable law, especially taking into account the import and export restrictions in place at any given time.

Certificates shall not be used to sign requests for the issuance, renewal, suspension or revocation of certificates, or to sign public key certificates of any kind, or to sign certificate revocation lists (CRLs).

The certificates have not been designed, may not be used and are not authorised for use or resale as hazardous situation control equipment or for uses requiring fail-safe action, such as the operation of nuclear facilities, air navigation or communication systems, or weapons control systems, where failure could directly lead to death, personal injury or severe environmental damage.

The limits indicated in the various fields of the certificate profiles, visible on CGCOM's website (https://psc.cgcom.es /), shall be taken into account.

The use of the digital certificates in operations that contravene this text of disclosure (PDS), or the contracts with the subscribers, is considered to be an improper use for the appropriate legal purposes, and therefore the AC-CGCOM is exempt, according to the legislation in force, from any responsibility for this improper use of the certificates by the signatory or any third party.

The AC-CGCOM does not have access to the data on which the use of a certificate may be applied. Therefore, and as a consequence of this technical impossibility to access the content of the message, it is not possible for the AC-CGCOM to make any assessment of such content. The subscriber, the signatory or the person responsible for the custody, assumes any responsibility arising from the content associated with the use of a certificate.

Likewise, the subscriber, the signatory will be responsible for any responsibility that could be derived from the use of the same outside the limits and conditions of use included in this text of disclosure, or in the contracts with the subscribers, as well as for any other improper use of the same derived from this section or that could be interpreted as such according to the legislation in force.

4. Subscribers' obligations

4.1. Key generation

For Card Certificates, the subscriber authorizes the signatory to generate the keys, private and public, within a Qualified Signature Creation Device, and requests on the signatory's behalf the issuance of the certificate to the AC-CGCOM.

For CLOUD certificates, the subscriber authorizes the signatory to generate the keys, private and public, and requests, on signatory's behalf, the issuance of the certificate to the AC-CGCOM.

For electronic seal certificates, the subscriber authorizes the AC-CGCOM to generate the keys, private and public, to be used by the seal creator, and requests on his behalf the issuance of the electronic seal certificate.

4.2. Certificate application

The subscriber undertakes to apply for the certificates in accordance with the procedure and, if necessary, the technical components supplied by the AC-CGCOM, in accordance with the provisions of the Certification Pratice Statement (DPC) and the AC-CGCOM's operational documentation.

4.3. Veracity of the information

The subscriber is responsible for ensuring that all information included in his certificate application is accurate, complete for the purpose of the certificate and up-to-date at all times.

The subscriber shall immediately inform the AC-CGCOM of any inaccuracies detected in the certificate once it has been issued, and of the changes that occur in the information provided and/or recorded for the issuance of the certificate.

4.4. Custody obligations

The subscriber undertakes to custody all the information generated in its activity as a registry entity.

5. Obligations of the signatories and seal creators

5.1. Custody obligations

The signatory or the seal creator undertakes to custody the personal identification code or any technical support provided by the AC-CGCOM, the private keys and, if necessary, the specifications owned by the AC-CGCOM that are supplied to him.

In case of loss or theft of the certificate's private key, or in case the subscriber suspects that the private key has lost its reliability for any reason, such circumstances shall be immediately notified by, or through, the subscriber to the AC-CGCOM.

5.2. Obligations of correct use

The signatory or the seal creator shall use the certificate certification service provided by the AC-CGCOM, exclusively for the uses authorised in the DPC and in any other instruction, manual or procedure provided to the subscriber.

The signatory or the seal creator shall comply with any laws and regulations that may affect his right to use the cryptographic tools employed.

The signatory or the seal creator shall not take measures to inspect, alter or decompile the digital certification services provided.

The signatory or the seal creator shall stop using the private key in case of compromise of said key, revocation, or compromise of the CA keys.

The signatory or the seal creator shall acknowledge:

a) That when he is using any certificate, and as long as the certificate has not expired or been suspended or revoked, he will have accepted that certificate and will be operational.

b) That he does not act as a certification body and, therefore, is obliged not to use the private keys corresponding to the public keys contained in the certificates for the purpose of signing any certificate.

5.3. Prohibited transactions

The signatory or the seal creator agrees not to use his private keys, certificates, cards, or any other technical support provided by the AC-CGCOM in the performance of any transaction prohibited by applicable law.

The digital certification services provided by the AC-CGCOM have not been designed nor do they allow their use or resale as equipment to control dangerous situations, or for uses that require error-proofing, such as the operation of nuclear facilities, air navigation or communication systems, air traffic control systems or weapons control systems, where an error could directly cause death, physical damage or serious environmental damage.

6. Obligations of verifiers

6.1. Informed decision

The AC-CGCOM informs the verifier that it has access to sufficient information to make an informed decision when verifying a certificate and to rely on the information contained in the certificate.

In addition, the verifier shall acknowledge that the use of the AC-CGCOM Registry and Certificate Revocation Lists (hereinafter referred to as "CRLs" or "CRLs") is governed by the AC-CGCOM's DPC and shall undertake to comply with the technical, operational and security requirements described in the said DPC.

6.2. Requeriments for the verification of electronic signatures

The verification of the electronic signature of the certificate is essential to determine that the public key contained in the certificate corresponds to the signatory, and that the corresponding private key allows the decryption of the message.

The check will normally be performed automatically by the verifier's software and, in any case, in accordance with the DPC, with the following requirements:

- It is necessary to use the appropriate software for the verification of a digital signature with the algorithms and key lengths authorised in the certificate and/or to execute any other cryptographic operation, and to establish the chain of certificates on which the electronic signature to be verified is based, since the electronic signature is verified using this chain of certificates.

- It is necessary to ensure that the chain of certificates identified is the most appropriate for the electronic signature being verified, since an electronic signature can be based on more than one chain of certificates, and it is up to the verifier to ensure that the most appropriate chain is used to verify it.

- It is necessary to check the revocation status of the certificates in the chain with the information supplied to the AC-CGCOM Registry (with LRCs, for example) to determine the validity of all the certificates in the chain of certificates, since an electronic signature can only be considered correctly verified if each and every one of the certificates in the chain is correct and in force.

- It is necessary to ensure that all the certificates in the chain authorise the use of the private key by the subscriber of the certificate and the signatory, since there is a possibility that some of the certificates may include usage limits that prevent the electronic signature being verified from being trusted. Each certificate in the chain has an indicator that refers to the applicable conditions of use, for review by the verifiers.

- It is necessary to technically verify the signature of all the certificates in the chain before relying on the certificate used by the signatory.

To encrypt a message or document by a person, **when this functionality is available**, the recipient's own public key shall be used. Said public key can be obtained from its certificate.

Therefore, it is necessary to verify this certificate before proceeding with encryption.

6.3. Reliance on an unverified certificate

When this functionality is available, it is prohibited to encrypt messages for a recipient without having successfully verified its certificate.

If the verifier relies on an unverified certificate, he or she will assume all risks arising from this action.

6.4. Effect of verification

By virtue of the correct verification of the certificates, in accordance with this dissemination text (PDS), the verifier shall rely on the identification and, where appropriate, on the public key of the signatory, within the corresponding limitations of use, to generate encrypted messages.

6.5. Correct use and prohibited activities

The verifier agrees not to use any certificate status information or any other information provided by the AC-CGCOM, in the performance of any transaction prohibited by the law applicable to such transaction.

The verifier undertakes not to inspect, interfere with or reverse engineer the technical implementation of the AC-CGCOM's public certification services without prior written consent.

In addition, the verifier undertakes not to intentionally compromise the safety of the AC-CGCOM's public certification services.

The digital certification services provided by the AC-CGCOM have not been designed nor do they allow the use or resale, as control equipment for dangerous situations or for uses that require error-proofing, such as the operation of nuclear facilities, air navigation or communication systems, air traffic control systems, or weapons control systems, where an error could cause death, physical damage or serious environmental damage.

6.6. Indemnity clause

The third party who relies on the certificate undertakes to hold the AC-CGCOM harmless from any damage arising from any action or omission resulting in liability, damage or loss, expense of any kind, including legal fees and representation incurred, by the publication and use of the certificate, when any of the following causes are present:

- Failure to comply with the obligations of the third party relying on the certificate.
- Reckless confidence in a certificate, depending on the circumstances.
- Failure to check the status of a certificate, to determine that it is not suspended or revoked

The AC-CGCOM shall not be liable for the damages and losses caused, in the terms indicated in article 11 of the Spanish *Law 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.*

7. AC-CGCOM's obligations

7.1. Related to the provision of the digital certification service

The AC- CGCOM undertakes to:

a) Issue, deliver, administer, suspend, revoke and renew certificates, in accordance with the instructions provided by the subscriber, in the cases and for the reasons described in the AC-CGCOM's DPC.

b) Carry out the services with the appropriate technical and material means, and with personnel who fulfil the conditions of qualification and experience established in the DPC.

c) Comply with the quality levels of the service, in accordance with the provisions of the DPC, in the technical, operational and safety aspects.

d) Notify the subscriber, prior to the expiry date of the certificates, of the possibility of renewing or revoking them, when these circumstances occur.

e) Communicate to third parties who request it, the status of the certificates, in accordance with what is established in the CPS for the different certificate verification services.

7.2. Related to the registry checks

The AC-CGCOM undertakes to issue certificates on the basis of the data supplied by the subscriber and may, therefore, carry out any checks it deems appropriate regarding the identity and other personal and complementary information of the subscribers and, where appropriate, of the signatories.

These verifications may include the documentary justification provided by the signatory through the subscriber, if the AC-CGCOM considers it necessary, and any other relevant document and information provided by the subscriber and/or the signatory.

In the event that the AC-CGCOM detects errors in the data to be included in the certificates or that justify these data, it may make the changes it considers necessary before issuing the certificate or suspend the issuing process and manage the corresponding incident with the subscriber. In the event that the AC-CGCOM corrects the data without first managing the corresponding incident with the subscriber, it must notify the certified data to the subscriber.

The AC-CGCOM reserves the right not to issue the certificate, when it considers that the documentary justification is insufficient for the correct identification and authentication of the subscriber and/or signatory.

8. Limited warranties and disclaimer of warranties

8.1. AC-CGCOM guarantee for digital certification services

The AC-CGCOM guarantees the subscriber:

- That there are no factual errors in the information contained in the certificates, known or made by the Certification Body.
- That there are no errors of fact in the information contained in the certificates, due to a lack of due diligence in the management of the certificate application or in the creation of the certificate.

- That the certificates comply with all the material requirements established in the DPC.
- That the revocation services and the use of the deposit comply with all the material requirements set out in the DPC.

The AC-CGCOM guarantees the third party that it has confidence in the certificate:

- That the information contained or incorporated by reference in the certificate is correct, except where otherwise stated.
- In the case of certificates published in the repository, that the certificate has been issued to the subscriber and signatory identified therein and that the certificate has been accepted.
- That in approving the application for the certificate and in issuing the certificate all the material requirements established in the DPC have been fulfilled.
- Speed and security in the provision of services, especially revocation and deposit services.
-

In addition, the AC-CGCOM guarantees the subscriber and the relying parties:

- That the certificate contains the information that a qualified certificate must contain, in accordance with Annex I to Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.
- That, in the event that it generates the private keys of the subscriber or, if applicable, the natural person identified in the certificate, its confidentiality is maintained during the process.
- The responsibility of the Certification Body, with the limits established. The AC-CGCOM shall not be liable in any case for unforeseen circumstances or in cases of force majeure.
- The private key of the certification entity used to issue certificates has not been compromised, unless otherwise communicated by the AC-CGCOM through the Certification Registry, according to the DPC.
- It has not originated or introduced false or erroneous statements in the information of any certificate, nor has it failed to include necessary information provided by the subscriber and validated by the AC-CGCOM, at the time the certificate is issued.
- All the certificates comply with the content and the formal requirements within the DPC, including all the legal requeriments in force and applicable.
- It is bound by the operational and security procedures described in the DPC.

8.2. Exclusión de la guarantee

The AC-CGCOM rejects any guarantee other than the above that is not legally enforceable.

Specifically, the AC-CGCOM does not guarantee any software used by any person to sign, verify signatures, encrypt, decrypt, or otherwise use any digital certificate issued by the AC-CGCOM, except where a written statement to the contrary exists.

9. Applicable agreements and DPC

9.1. Applicable agreements

The agreements applicable to the certificates are as follows:

- Certification services contract, which regulates the relationship between the AC-CGCOM and the College, Autonomic Health Services or legal person subscribing to the certificates.

- General conditions of service incorporated in the text of the certificate or PDS.

- DPC, which regulate the issue and use of the certificates.

9.2. Certification Practices Statement (DPC)

The AC-CGCOM’s certification services are technically and operationally regulated by the AC-CGCOM’s DPC, by its subsequent updates, as well as by complementary documentation.

The DPC and the transaction documentation are periodically amended in the Registry and can be consulted on the website: https://psc.cgcom.es

9.3. Certification policy

The AC-CGCOM has a certification policy that specifies the technical, legal and operational requeriments, as well as certificate requirements. This policy is available to the community of users who request it.

10. Rules of trust for long-lasting firms

The AC-CGCOM informs certificate applicants that it does not offer a service that guarantees the reliability of the electronic signature of a document over time.

For the reliability of the electronic signature of a document over time, the AC-CGCOM recommends the use of the standards indicated in section IV.3 of the NTI Policy for Electronic Signature and Seal and Administration Certificates (Resolution of 27 October 2016, of the Secretary of State for Public Administrations)

11. Intimacy policy

The AC-CGCOM cannot disclose or be compelled to disclose any confidential information regarding certificates without a specific prior request from

a) The person in respect of whom the AC-CGCOM has a duty to keep the information confidential, or
b) A judicial, administrative or any other order provided for in the legislation in force.

However, the subscriber accepts that certain information, personal and other, provided in the application for certificates, will be included in their certificates and in the mechanism for checking the status of the certificates, and that the information mentioned is not confidential, as required by law.

The AC-CGCOM does not pass on the data provided specifically for the provision of the certification service to any person.

The processing of said data for the provision of the AC-CGCOM certification service by the technical provider, among others, by way of example but not limitation, occurs within the framework of a processing order (where the AC-CGCOM is responsible for the processing of personal data and the technical provider is in charge of their processing) referred to in article 28 of the REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of April 7, 0 6 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (GDPR), and article 33 of the Spanish Organic Law 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD) and by virtue of it is in accordance with the requirements of the GDPR and the LOPDGDD, and guarantees the protection of the rights of the interested party.

12. Privacy policy

The AC-CGCOM has a privacy policy in section 9.4 of the DPC, and specific privacy regulations regarding the registration process, the confidentiality of the registration, the protection of access to personal information, and the consent of the user.

Likewise, the AC-CGCOM keeps the information related to the services provided in accordance with article 24.2.h) of Regulation (EU) 910/2014 of the European Parliament and of the Council, of 23 July 2014, for at least 15 years from the extinction of the certificate or the termination of the service provided.

13. Refund policy

The AC-CGCOM will not refund the cost of the certification service under any circumstances.

14. Applicable, law and competent jurisdiction

Relations with the AC-CGCOM will be governed by the Spanish law on trustworthy services in force at any given time, as well as by civil and commercial legislation insofar as it is applicable.

The competent jurisdiction is that indicated in Law 1/2000, of 7 January, on Civil Procedure.

In case of disagreement between the parties, the parties will try to reach an amicable resolution beforehand. To this end, the parties must send a communication to the AC-CGCOM by any means that leaves a record to the contact address indicated under the point 1. this PDS.

If the parties do not reach an agreement on this matter, either party may submit the dispute to civil jurisdiction, subject to the Courts of the AC-CGCOM's registered office.

15. Accreditations and quality seals

The AC-CGCOM is included in the Spanish providers Trusted List (TSL):

https://sedediatid.mineco.gob.es/Prestadores/Paginas/Inicio.aspx

The AC-CGCOM has "eIDAS-compliant" certification for the following services:

- Service for issuing qualified electronic signature certificates
  - Collegiate Doctor Certificates;
  - Natural person linked Certificates;
  - Natural person representing a legal person Certificates.
- Service for issuing qualified electronic certificates with electronic stamp
  - Legal person electronic seal Certificates.

16. Link to the list of providers

The AC-CGCOM is a qualified provider of certification services, so it forms part of the List of Qualified Providers (TSL) maintained by the national supervisor, that can be obtained at the following address:

https://sedeaplicaciones.minetur.gob.es/Prestadores/

The AC-CGCOM is included in the "Trust List" of the European Union as a Qualified Provider of trusted electronic services:

https://webgate.ec.europa.eu/tl-browser/#/tl/ES/19

17. Severability of clauses, survival, full agreement and notification

The clauses in this disclosure text are independent of each other, which is why if any clause is considered invalid or inapplicable, the rest of the clauses in the PDS will continue to apply, unless the parties expressly agree otherwise.
The requirements contained in sections 9.6 (Obligations), 9.8 (Responsibility), 8 (Compliance Audit) and 9.3 (Confidentiality) of the AC-CGCOM Certification Practice Statement shall continue to apply after termination of service.

This text contains the complete will and all the agreements between the parties.

The parties will notify each other of events through a send-to-address procedure to the address certificacion@cgcom.es