OMC 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 DISCLOSURE STATEMENT - PDS

This document contains information that must be understood in relation to the certification service of the Organización Médica Colegial de España.

This document follows the structure defined in Appendix A of the ETSI EN 319 411-1 standard, in accordance with the indications of section 4.3.4 of the ETSI EN 319 412-5 standard.

Under no circumstances does this document develop, expand or modify the Declaration on Certification Practices of the EC-OMC.

Version Control

Version	Parts changed	Description of change	Author of change	Date of change
1.0	Original	Creation of document	ASTREA	22/06/2017
1.1	Section 1.1	Modification responsible	ASTREA	11/02/2019
	Section 10	Modification on long-term signature		
	Section 15	Modification on accreditation		
	Section 16	Creation section on TL link		
	Section 11	Regulation amendment		
1.2	Section 11	Regulation updates	ASTREA	29/03/2019
1.3	Section 2.1; 2.3; 9.1; 15		ASTREA	25/07/2019

1. Contact Information

1.1. Responsible organisation

The Certification Body of the Organización Médica Colegial (Spanish Collegiate Medical Association), hereinafter the “EC-OMC”, is an initiative of:

CONSEJO GENERAL DE COLEGIOS OFICIALES DE MÉDICOS DE ESPAÑA –Organización Médica Colegial

Plaza de las Cortes, 11- 28014 Madrid

Telephone: (+34) 91 431 77 80 / Fax: (+34) 91 576 43

1.2. Organisation that administers the document

Comisión Permanente del CONSEJO GENERAL DE COLEGIOS OFICIALES DE MÉDICOS DE ESPAÑA

Plaza de las Cortes, 11- 28014 Madrid

Teléfono: 91 431 77 80 / Fax: 91 576 43 88

1.3. Contact person

For any consultations, please contact:

CONSEJO GENERAL DE COLEGIOS OFICIALES DE MÉDICOS DE ESPAÑA –Organización Médica Colegial

Plaza de las Cortes, 11- 28014 Madrid

Telephone: (+34) 91 431 77 80 / Fax: (+34) 91 576 43

1.4. Contact for revocation processes

For revocation processes, please contact:

CONSEJO GENERAL DE COLEGIOS OFICIALES DE MÉDICOS DE ESPAÑA –ORGANIZACIÓN MÉDICA COLEGIAL

· UNIDAD TECNOLÓGICA ·

PLAZA DE LAS CORTES, 11- 28014 MADRID

TELEPHONE: (+34) 91 431 77 80 / FAX: (+34) 91 576 43 88

2. Type and Purpose of Certification

2.1. Natural person qualified certificates

These certificates are qualified in accordance with article 28 and with Appendix I of Regulation (EU) 910/2014 of the European Parliament and of the Council, of 23 July 2014, and in compliance with the provisions established in technical regulations identified with the reference ETSI EN 319 411-2.

2.1.1 Card certificates

Certificates that use a card and work with a qualified electronic signature creation device, in accordance with Appendix II of Regulation (EU) 910/2014 of the European Parliament and of the Council, of 23 July 2014.

2.1.2 Certificates for identification

Certificates with the function of identification, guaranteeing the identity of the subscriber and the signatory.

2.1.3 Advanced signature certificates

Certificates with a signature function, enabling the generation of the “advanced electronic signature” that is based on a qualified certificate and which are used on software.

2.1.4 Certificates for qualified signature

Certificates with a signature function, enabling the generation of the “qualified electronic signature”; in other words, the advanced electronic signature that is based on a qualified certificate **when it has been generated** using a qualified device, for which reason, in accordance with the article 25.2 of Regulation (EU) 910/2014 of the European Parliament and of the Council, of 23 July 2014, it will have a legal effect equivalent to a handwritten signature.

2.1.5 Certificates for encryption

Certificates with the function of encryption can be used to encrypt documents or to receive confidential documents in any format, and are protected via encryption, using:

a) The public key of the individual indicated on the certificate.
b) A symmetric session key encrypted with the public key of the person indicated on the certificate.

In any case, the private key must be used to decrypt the message, warning the subscriber of the certificate and the individual indicated on the certificate that in no case may a lost key be recovered, such that **the OMC will not be liable for any loss of encrypted information that cannot be recovered in cases where certificates or keys are lost**.

2.1.6 Licensed doctor certificates

Certificates are issued to licensed doctors from the corporate scope of the subscribing association and are not issued to the public under any circumstances. The licensed doctor is considered the signatory.

Furthermore, they guarantee the status of licensed doctor, given the obligatory involvement of the association in the process of issuing the certificate, acting as the registration body or as guarantor of the information.

2.1.7 Administrative staff certificates

Certificates are issued to administrative staff members from the corporate scope of the subscribing association and are not issued to the public under any circumstance. This person is considered the signatory.

2.1.8 Legal entity representative certificates

These certificates guarantee the identity of the subscriber and the signatory, and a relationship of legal representation or power of attorney between the signatory and an entity, medical association or organisation in the health sector, described in the "O" section (Organization).

Furthermore, they include a declaration related to the category of the signatory, which will have been checked before issuance of the certificate and which is correct. Note that this indication alone is insufficient to determine the powers that the signatory has to sign, if applicable, in the name of the subscriber of the certification service; therefore, the user must check the signing powers and authorities of the signatory via other means, different to the certificate, such as via the validation service of the OMC.

2.1.9 Collegiate body certificates

These certificates are issued to licensed doctors as collegiate bodies in the corporate scope of the subscribing association and are not issued to the public under any circumstances. This body is considered the signatory.

Furthermore, they include a declaration related to the category or role in the body of the signatory, which will have been checked before issuance of the certificate and which is correct.

2.2. Qualified electronic stamp certificates

These certificates are qualified in accordance with article 38 and with Appendix III of Regulation (EU) 910/2014 of the European Parliament and of the Council, of 23 July 2014, and in compliance with the provisions established in technical regulations identified with the reference ETSI EN 319 411-2.

2.2.1 Stamp certificates on qualified device

Stamp certificates that function with a qualified electronic signature creation device, in accordance with Appendix II of Regulation (EU) 910/2014 of the European Parliament and of the Council, of 23 July 2014.

2.2.2 Stamp certificates for identification

Certificates with the function of identification, guaranteeing the identity of the subscriber and, if applicable, the person who manages them.

2.2.3 Advanced stamp certificates

Certificates with a signature function, enabling the generation of the “advanced electronic stamp” that is based on a qualified certificate and which are used on software.

2.2.4 Qualified stamp certificates

Certificates with a signature function, enabling the generation of the “qualified electronic stamp”; in other words, the advanced electronic stamp that is based on a qualified certificate **when it has been generated** using a qualified device, for which reason, in accordance with article 35.2 of Regulation (EU) 910/2014 of the European Parliament and of the Council, of 23 July 2014, it will enjoy the presumption of the integrity of the data and of the correction of the origin of the data to which the qualified electronic stamp is linked.

2.2.5 Stamp certificates for encryption

Stamp certificates with the function of encryption can be used to encrypt documents or receive confidential documents.

The OMC will not be liable for any loss of encrypted information that cannot be recovered in cases where certificates or keys are lost.

2.3. Types of certificates

Type of Certificate	Storage Device	Uses	OID
Licensed Doctor	Card	Authentication	• 1.3.6.1.4.1.26852.1.1.1.1

Type of Certificate	Storage Device	Uses	OID
			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
	Software	Authentication, Signature and Encryption	1.3.6.1.4.1.26852.1.1.7 0.4.0.194112.1.0
Administrative Staff	Card	Authentication	1.3.6.1.4.1.26852.1.1.2.1 0.4.0.194112.1.2
		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
	Software	Authentication, Signature and Encryption	1.3.6.1.4.1.26852.1.1.6 0.4.0.194112.1.0
Collegiate Body	Card	Authentication	1.3.6.1.4.1.26852.1.1.4.1 0.4.0.2042.1.2
		Signature	1.3.6.1.4.1.26852.1.1.4.2 0.4.0.194112.1.2
		Encryption	1.3.6.1.4.1.26852.1.1.4.3
	Software	Authentication, Signature and Encryption	1.3.6.1.4.1.26852.1.1.8 0.4.0.194112.1.0
Legal Representative	Card	Authentication	1.3.6.1.4.1.26852.1.1.11.1 0.4.0.194112.1.2 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
	Software	Authentication, Signature and Encryption	1.3.6.1.4.1.26852.1.1.12 0.4.0.194112.1.0 2.16.724.1.3.5.8

Type of Certificate	Storage Device	Uses	OID
Legal Entity Electronic Stamp	Qualified signature creation device	Authentication, Signature and Encryption	• 1.3.6.1.4.1.26852.1.1.10.1 • 0.4.0.194112.1.3
	Software	Authentication, Signature and Encryption	• 1.3.6.1.4.1.26852.1.1.10.2 • 0.4.0.194112.1.1

2.4. Certification issuing body

These certificates are issued by the EC-OMC, identified via the data indicated previously.

The EC-OMC outsources certificate production services to Camerfirma, which always acts following the indications of the EC-OMC.

2.5. Validation of certificates

The lists of revoked certificates and OCSP services are found on the website of the EC-OMC and on the URLs indicated on each certificate.

3. Limits of Use of the Certificate

3.1. Limits of use aimed at signatories

The signatory and the stamp creator must use the certification service provided by the EC-OMC exclusively for the uses authorised in the agreement signed between the Consejo General de Colegios Oficiales de Médicos (General Council of Official Medical Associations - hereinafter the “CGCOM”) and the subscribing associate or legal entity, and that are subsequently reproduced.

Furthermore, the signatory and stamp creator undertake to use the digital certification service in accordance with the instructions, manuals or procedures supplied by the EC-OMC.

The signatory and stamp creator must comply with any law or regulation that may affect their right to use the cryptography tools they employ.

The signatory and the stamp creator may not adopt inspection, alteration or reverse engineering measures for the digital certification services of the EC-OMC without express permission having been granted in advance.

3.2. Limits of use aimed at verifiers

Certificates are used for their own function and established purpose and they may not be used for other functions or purposes.

Likewise, certificates must only be used in accordance with applicable legislation, especially considering the importation and exportation restrictions in force at any given time.

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

Certificates are not designed for, nor may they be used for, nor is their use or re-sale as control equipment for hazardous situations authorised, nor are they permitted or designed for uses that require fail-safe actions, such as the operation of nuclear facilities, air communications or navigation systems, or armament control systems, where a failure may directly lead to death, personal injury or serious environmental damage.

The limits indicated in the different fields of the certificate profiles, which can be viewed on the website of the EC-OMC (https://certificacion.cgcom.es), must be considered.

Use of digital certificates in operations that contravene this PKI Disclosure Statement (hereinafter "PDS"), or contracts with subscribers, will be considered undue use for the corresponding legal effects, therefore exempting the EC-OMC, based on current legislation, from any liability for said undue use of certificates performed by the signatory or any third party.

The EC-OMC does not have access to the data to which the use of a certificate may be applied. Thus, and as a consequence of this technical impossibility of accessing the content of the message, the EC-OMC cannot issue an evaluation on said content, with the subscriber, signatory or person responsible for its safeguarding therefore assuming any liability derived from the content linked to the use of a certificate.

Moreover, any liability that may be derived from the use of the certificate beyond the limits and terms and conditions of use gathered in this PDS, or in contracts with subscribers, will be attributable to the subscriber or signatory, as will any other undue use of the certificate derived from this section or that may be interpreted as such based on current legislation.

4. Obligations of Subscribers

4.1. Generation of keys

In card certificates the subscriber authorises the signatory to generate their private and public keys within a qualified electronic signature creation device and requests, in the name of the signatory, the issue of the certificate from the EC-OMC.

In software certificates the subscriber authorises the signatory to generate their private and public keys and requests, in the name of the signatory, the issue of the certificate from the EC-OMC.

In electronic stamp certificates the subscriber authorises the EC-OMC to generate private and public keys for their use by the stamp creators, and requests in its name the issue of the electronic stamp certificate.

4.2. Certificate request

The subscriber undertakes to make certificate requests in accordance with the procedure and, if necessary, the technical components supplied by the EC-OMC, in compliance with the provisions established in the Declaration of Certification Practices (hereinafter “DCP”) and in the operations documentation of the EC-OMC.

4.3. Veracity of information

The subscriber is responsible for ensuring all the information included in their certificate request is exact, complete for the purpose of the certificate, and updated at all times.

The subscriber must immediately inform the EC-OMC of any inaccuracy detected in the certificate once it has been issued, as well as the changes that occur to the information supplied and/or registered for the issue of the certificate.

4.4. Obligations of safe-keeping

The subscriber undertakes to safeguard all the information they generate in their activity as a registration body.

5. Obligations of Signatories and Stamp Creators

5.1. Obligations of safe-keeping

The signatory or stamp creator undertakes to safeguard the personal identification code, private keys, card (when one exists) or any other technical storage format delivered by the EC-OMC and, if necessary, the specifications owned by the EC-OMC that are supplied to them.

If the private key of the certificate is lost or stolen, or if the subscriber suspects that the private key has lost reliability for any reason, the EC-OMC must be informed immediately of said circumstances directly or via the subscriber.

5.2. Obligations of correct use

The signatory or stamp creator must use the certification service provided by the EC-OMC exclusively for the uses authorised in the DCP and in any other instruction, manual or procedure supplied to the subscriber.

The signatory or stamp creator must comply with any law or regulation that may affect their right to use the cryptography tools employed.

The signatory or stamp creator may not adopt inspection, alteration or de-compilation measures for the digital certification services provided.

The signatory or stamp creator must cease to employ the private key if said key becomes compromised, is revoked, or keys of the certification authority are compromised.

The signatory or stamp creator recognises:

a) When they use any certificate, and while the certificate has not expired or been suspended or revoked, they will have accepted said certificate and it will be operational.

b) They do not act as a certification body and, therefore, undertake not to use the private keys corresponding to the public keys contained in certificates for the purpose of signing any certificate.

5.3. Prohibited transactions

The signatory or stamp creator undertake to refrain from using their private keys, certificates, cards or any other technical storage format delivered by the EC-OMC in the execution of any transaction prohibited by applicable law.

The digital certification services provided by the EC-OMC have not been designed for, nor is their use or re-sale as control equipment for hazardous situations permitted, nor are they permitted or designed for uses that require fail-safe actions, such as the operation of nuclear facilities, air communications or navigation systems, air traffic control systems or armament control systems, where an error may directly lead to death, personal injury or serious environmental damage.

6. Obligations of Verifiers

6.1. Informed decision

The EC-OMC informs the verifier that they have access to sufficient information to make an informed decision when verifying a certificate and trusting in the information contained in said certificate.

Additionally, the verifier will recognise that use of the Certificate Register and Certificate Revocation Lists (hereinafter “CRLs”) of the EC-OMC is governed by the DCP of the EC-OMC and they will undertake to comply with the technical, operational and security requirements described in said DCP.

6.2. Electronic signature verification requirements

Checking the electronic signature of the certificate is essential to determine that the public key contained in the certificate corresponds to the subscriber and that the corresponding private key enables the message to be decrypted.

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

- Appropriate software must be used to verify a digital signature with the algorithms and key lengths authorised in the certificate and/or perform any other cryptographic operation and establish the certificate chain on which the electronic signature to be verified is based, given that the electronic signature is verified using this certificate chain.
- The certificate chain identified must be the most appropriate for the electronic signature being verified, as an electronic signature can be based on more than one certificate chain, and the verifier must make the decision to ensure the use of the most suitable chain to verify it.
- The revocation status of the certificates in the chain must be checked with the information supplied to the Register of the EC-OMC (with CRLs, for example) to determine the validity of all the certificates in the certificate chain, as an electronic signature may only be considered correctly verified if each and every one of the certificates in the chain are correct and valid.
- All certificates in the chain must authorise the use of the private key by the subscriber of the certificate and the signatory, as some of the certificates may include limits of use that mean the electronic signature that is being verified may not be trusted. Each certificate in the chain has an indicator that refers to the applicable terms and conditions of use for their review by verifiers.
- The signature of all certificates in the chain must be verified technically before trusting in the certificate used by the signatory.

In order to proceed to encrypt a message or document created by a person, when they have this function, the public key of the recipient must be used. This public key can be obtained from their certificate.

Therefore, this certificate must be verified before proceeding with encryption.

6.3. Trusting an unverified certificate

When this function exists, it is prohibited to encrypt messages to a recipient without having successfully verified their certificate.

If the verifier trusts in an unverified certificate, they will assume all risks derived from this action.

6.4. Effect of verification

Pursuant to the correct verification of these certificates, in compliance with this PDS, the verifier may trust in the identification and, if applicable, public key of the signatory, within the corresponding limitations of use, to generate encrypted messages.

6.5. Correct use and prohibited activities

The verifier undertakes to refrain from using any type of information regarding the status of certificates or information of any other kind that has been supplied by the EC-OMC in the execution of any transaction prohibited by legislation applicable to said transaction.

The verifier undertakes to refrain from inspecting, interfering or performing reverse engineering on the technical implementation of the EC-OMC’s public services of certification without being first granted written consent.

In addition, the verifier undertakes to refrain from intentionally compromising the security of the EC-OMC’s public services of certification.

The digital certification services provided by the EC-OMC have not been designed for, nor is their use or re-sale as control equipment for hazardous situations permitted, nor are they permitted or designed for uses that require fail-safe actions, such as the operation of nuclear facilities, air communications or navigation systems, air traffic control systems or armament control systems, where an error may directly lead to death, personal injury or serious environmental damage.

6.6. Indemnity clause

Any third party trusting in the certificate undertakes to maintain the EC-OMC harmless from all damage stemming from any action or omission that results in liability, damage or loss, or expenses of any kind, including legal representation and counsel, that may arise due to the publication and use of the certificate when any of the following causes occurs:

- Failure of the third party trusting in the certificate to comply with their obligations.
- Reckless trust in a certificate, under the circumstances.
- Failure to check the status of a certificate to determine whether or not it has been suspended or revoked.

7. Obligations of the EC-OMC

7.1. Regarding the provision of the digital certification service

The EC-OMC undertakes to:

a) Issue, deliver, administer, suspend, revoke and renew certificates, in accordance with the instructions supplied by the subscriber, in the cases and for the reasons described in the DCP of the EC-OMC.

b) Perform the services with suitable technical means and materials, and with staff who comply with the qualification and experience conditions established in the DCP.

c) Comply with the quality levels for the service, in compliance with the provisions established in the DCP regarding the technical, operational and security aspects.

d) Notify the subscriber before the expiry date of certificates of the possibility of renewing them, in addition to the suspension, increasing of suspension, or revocation of certificates, when these circumstances occur.

e) Inform the third parties who request knowledge of the status of certificates, in accordance with the provisions established in the DCP for the different certificate verification services.

7.2. Regarding register checks

The EC-OMC undertakes to issue certificates based on the data supplied by the subscriber, meaning it may perform the checks it considers necessary in relation to the identity and other personal and complementary information of subscribers and, when applicable, of signatories.

These checks may include the documented justification supplied by the signatory via the subscriber, if the EC-OMC deems it necessary, and any other relevant document or information supplied by the subscriber and/or signatory.

If the EC-OMC were to detect errors in the data that must be included in certificates or that justifies this data, it may make the changes it considers necessary before issuing the certificate, or suspend the issue process and manage the corresponding incident with the subscriber. If the EC-OMC were to correct the data without prior management of the corresponding incident with the subscriber, it must inform the subscriber of the data that is finally certified.

The EC-OMC reserves the right not to issue the certificate when it considers that the documented justification is insufficient for the correct identification and authentication of the subscriber and/or signatory.

The aforementioned obligations will remain suspended in cases in which the subscriber acts as registration authority and has the technical elements corresponding to the generation of keys, issue of certificates and recording of corporate signature devices.

8. Limited Guarantee and Guarantee Disclaimer

8.1. EC-OMC guarantee for the digital certification services

The EC-OMC guarantees the subscriber:

- There are no factual errors in the information contained in the certificates, of which the EC-OMC is aware or which it has made.
- There are no factual errors in the information contained in the certificates due to a lack of due diligence in the management of the certificate request or in the creation of the certificate.
- The certificates comply with all material requirements established in the DCP.
- The revocation services and use of the store comply with all material requirements established in the DCP.

The EC-OMC guarantees the third party trusting in the certificate:

- The information contained or incorporated by reference in the certificate is correct, unless indicated otherwise.
- In the case of certificates published in the Store, the certificate has been issued to the subscriber and signatory identified in it and the certificate has been accepted.
- In approval of the certificate request and in the issue of the certificate all material requirements established in the DCP have been met.
- Speed and security in the provision of services, especially revocation and Store services.

Additionally, the EC-OMC guarantees the subscriber and third party trusting in the certificate:

- The certificate contains the information a qualified certificate must contain, in accordance with Appendix I of Regulation (EU) 910/2014.

- If it generates the private keys of the subscriber or, if applicable, the individual identified in the certificate, their confidentiality is maintained throughout the process.
- The liability of the EC-OMC, with the established limits. In no case will the EC-OMC be liable for acts of God or force majeure.
- The private key of the EC-OMC used to issue certificates has not been compromised, unless the EC-OMC communicates otherwise via the Certification Register, in accordance with the DCP.
- False or erroneous declarations have not been used or entered in the information of any certificate, nor has necessary information provided by the subscriber and validated by the EC-OMC been omitted when the certificate was issued.
- All certificates comply with the formal and content requirements of the DCP, including all applicable legal requirements in force.
- It remains associated by the operational and security procedures described in the DCP.

8.2. Guarantee disclaimer

The EC-OMC rejects any other guarantee different to the aforementioned that is not legally enforceable.

Specifically, the EC-OMC does not guarantee any software used by anyone to sign, verify signatures, encrypt, decrypt or use in another manner any digital certificate issued by the EC-OMC, except in cases when a written declaration stating otherwise exists.

9. Applicable Agreements and DCP

9.1. Applicable agreements

The agreements applicable to these certificates are as follows:

- Collaboration agreement for certification services, which regulates the relationship between the EC-OMC and the subscribing Association, or a health care system legal entity that subscribes the certificates.
- General Terms and Conditions of Service included in this PDS.
- DCP, which regulates the issue and use of certificates.

9.2. Certification Practice Statement (CPS)

The EC-OMC's certification services are technically and operationally regulated by the EC-OMC's CPS and the subcontracted Camerfirma's CPS as technical provider, by their subsequent updates, and by complementary documentation.

The CPS and operational documentation are modified periodically in the Register and they may be consulted on the following webpage: http://www.cgcom.es/registro.

9.3. Certification policy

The EC-OMC has a Certification Policy that details the technical, legal and operational requirements, as well as certificate regulations, which is available to users who so request it.

10. Rules of Trust for Long-Term Signatures

The EC-OMC hereby informs the certificates applicant that it does not offer a service that guarantees the reliability of the long-term electronic signature within a document.

The EC-OMC recommends, for the reliability of the long-term electronic signature of a document, the use of the rules for trusting in long-term signatures, as in section IV.3 of the NTI of the "Application Guide of the Technical Standard of Interoperability of Electronic Signature Policy."

11. Confidentiality Policy

The EC-OMC may not disclose nor may it be obliged to disclose any confidential information related to certificates without a prior specific request having been made, detailing:

- the person regarding whom the EC-OMC has the duty to keep information confidential
- a court or administrative order, or order of any other kind considered in current legislation

However, the subscriber accepts that certain information, whether it is personal or of another nature, provided in the certificate request will be included in their certificates and in the status checking mechanism for certificates, and that said information will not be considered confidential, as required by law.

The EC-OMC does not cede the data supplied specifically for the provision of the certification service to anyone.

The processing of the said data by third parties for a service provision to the EC-OMC, among others, including but not limited to, the certification service provided by Camerfirma occurs within the framework of a data treatment request to which Article 28 of the REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), and Article 33 of the Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD) refers and by virtue of this, it complies with the requirements of the GDPR and the LOPDGDD, and guarantees the protection of the interested party rights.

12. Privacy Policy

The EC-OMC has a Privacy Policy in section 9.4 of the DCP, and specific privacy regulations in relation to the registration process, the confidentiality of registration, access protection to personal information, and user consent.
Furthermore, the documentation justifying approval of the request must be kept and duly registered, with guarantees of security and integrity for 15 years from the expiry of the certificate, even in any case of early loss of validity due to revocation.

13. Refund Policy

The EC-OMC will not refund the cost of the certification service under any circumstances.

14. Applicable Legislation, Corresponding Jurisdiction and Claims and Disputes System

Spanish law regarding trust services in force at any given time, as well as civil and commercial law, where applicable, will rule the EC-OMC's relationships.

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

In the event of disagreement between the parties, the parties will first try to reach an amicable resolution. For this purpose, the parties must send a communication to the EC-OMC using any means that leaves a record of said communication to the contact address indicated in point 1 of this PDS.

If the parties fail to reach an agreement, either of them may submit the dispute to civil jurisdiction, subject to the Courts of the registered address of the EC-OMC.

15. Accreditations

The EC-OMC has, with regard to the shipping of certificates, AC CAMERFIRMA accreditations available on the following website:

https://www.camerfirma.com/camerfirma/acreditaciones/

The EC-OMC has the "eIDAS-compliant" certification available for the following services:

1. Issuance service of electronic signature qualified electronic certificates

   a) Corporate licensed doctor certificates

   b) Corporate collegiate body certificates

   c) Corporate administrative staff certificates

   d) Corporate legal person representative certificates

2. Issuance service of electronic seal qualified electronic certificates

   e) Legal person electronic seal certificates

16. Trusted List link

The EC-OMC is a qualified certification service provider; therefore it forms a part of the Trusted Service List (TSL) as a qualified provider. The national supervisor keeps the TSL, that is hosted on the following website:

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

The EC-OMC is included in the European Union Trusted List as a qualified trusted electronic services provider:

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

17. Divisibility of the Clauses, Survival, Entire Agreement and Notification

The clauses in this PDS are independent of each other, for which reason if any clause is considered void or not applicable, all other clauses will continue to be applicable, except when express agreement between the parties stating otherwise exists.

The requirements contained in the sections “Obligations and Liability”, “Compliance Audit” and “Confidentiality” of the DCP of the EC-OMC will continue to be valid following the termination of the service.

This text contains the full wishes and all agreements between the parties.

The parties will mutually notify one another of events via a procedure of sending communications to the email address certificacion@cgcom.es.