INFORMATIVE TEXT

APPLYING TO

CORPORATE CERTIFICATES OF REGISTERED BODY

This document contains the essential information to be known, before applying for the certificate, with regard to the certification service of the Organización Médica Colegial.

1. Contact information

1.1. Responsible organisation

The Certification Entity of the "Organización Médica Colegial", hereinafter "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: 91 431 77 80 / FAX: 91 576 43 88

1.2. Contact person

For any queries, please contact:

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

PLAZA DE LAS CORTES, 11- 28014 MADRID

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

2. Type and purpose of the corporate certificate of registered body

This document covers the following certificates:

NAME OF CERTIFICATE	OBJECT IDENTIFIER (OID) NUMBER	FUNCTIONS
Certificates of registered body on card	1.3.6.1.4.1.26852.1.1.4	Identification, signature and encipherment
Certificates of registered body on card (I)	1.3.6.1.4.1.26852.1.1.4.1	Identification
Certificates of registered body on card (F)	1.3.6.1.4.1.26852.1.1.4.2	Signature
Certificates of registered body on card (C)	1.3.6.1.4.1.26852.1.1.4.3	Encipherment

The corporate certificates of registered body are certificates qualified in accordance with the provisions set out in article 11.1, with the contents prescribed in article 11.2 and issued in compliance with the obligations of articles 12, 13, and 17 to 20 of Law 59/2003, of 19 December, on electronic signature.

Corporate certificates of registered body work with secure device for creating electronic signature, in accordance with article 24.3 of Law 59/2003, of 19 December, and they comply with the provisions laid down in the technical standards of the European Telecommunications Standards Institute, identified with reference TS 101 456.

The certificates are issued to registered bodies in the corporate scope of the subscriber association, and in no event are they issued to the public. This body is considered the owner of the respective keys and of the card and complementary software.

2.1. Certificate of registered body on card for identification, signature and encipherment.

This certificate has OID 1.3.6.1.4.1.26852.1.1.4.

The corporate certificates of registered body (identification, signature and encipherment) guarantee the identity of the subscriber and owner of the private identification key and signature, and permit the "qualified electronic signature" to be generated; in other words, the advanced electronic signature which is based on a qualified certificate and which has been generated using a secure device, for which, as set out in article 3 of Law 59/2003, of 19 December, it has a status equal to the written signature, for legal effects, without having to fulfil any other additional requirement.

They likewise include a declaration concerning the category and organic office of the owner of keys, that they have been verified before issuing the certificate, and are correct. It should be pointed out that this indication is not, in itself, enough to determine the powers which the owner of keys has in order to sign on behalf of the

subscriber; consequently the user of the certificate will have to verify the signature authorities and powers of the owner by other different means to the certificate, for example the OMC validation service.

On the other hand, the corporate certificates of registered body (identification, signature and encipherment) may be used in applications that do not require electronic signature equivalent to written signature, but only the identification of the owner of the keys, in the name of the subscriber, such as the applications which are indicated below:

a) Authentication in access control systems.
b) Secure electronic mail signature.
c) Other digital signature applications.

The electronic signature generated in the use of these applications will have the effects determined in the regulatory standards of the application, which may declare the equivalence with the written signature or only the identification effect, because this signature, at least, will have been produced with the secure device.

Lastly, the corporate certificates of registered body (identification, signature and encipherment) may be used to encipher own documents or to receive confidential documents, in any format, protected by the encipherment of the document using:

a) The public key of the owner of keys indicated in the certificate.
b) An encipherment key to session, symmetric, enciphered with the public key of the key owner indicated in the certificate.

In all events, the owner of the key shall use his private key to decipher the message, warning the subscriber of the certificate and the owner of the key that in no event can a lost key be recovered, so that the CGCOM will not respond for any loss of enciphered information that cannot be recovered in cases of loss of certificates or keys.

2.2. Certificates of registered body on card for identification

This certificate has OID 1.3.6.1.4.1.26852.1.1.1.4.

The corporate certificates of registered body (identification) guarantee the identity of the subscriber and owner of the private identification key.

2.3. Certificates of registered body on card for signature

This certificate has OID 1.3.6.1.4.1.26852.1.1.4.2.

The corporate certificates of registered body (signature) guarantee the "qualified electronic signature" to be generated; in other words, the advanced electronic signature which is based on a qualified certificate and which has been generated using a secure device, which, as set out in article 3 of Law 59/2003, of 19 December, will have a status equal to the electronic signature, for legal effects, without having to fulfil any other additional requirement.

They likewise include a declaration concerning the category and organic office of the owner of keys, that they have been verified before issuing the certificate, and are correct. It should be pointed out that this indication is not, in itself, enough to determine the powers which the owner of keys has in order to sign on behalf of the subscriber; consequently the user of the certificate will have to verify the signature authorities and powers of the owner by other different means to the certificate, for example the OMC validation service.

On the other hand, the corporate certificates of registered body (signature) may be used in applications that do not require electronic signature equivalent to written signature, such as the applications which are indicated below:

a) Secure electronic mail signature.
b) Other digital signature applications.

The electronic signature generated in the use of these applications will have the effects determined in the regulatory standards of the application, which may declare the equivalence with the written signature or only the identification effect, because this signature, at least, will have been produced with the secure device.

2.4. Certificates of registered body on card for encipherment

This certificate has OID 1.3.6.1.4.1.26852.1.1.4.3.

The encipherment certificates may be used to encipher own documents or to receive confidential documents, in any format, protected by the encipherment of the document using:

a) The public key of the owner of keys indicated in the certificate.

b) An encipherment key to session, symmetric, enciphered with the public key of the key owner indicated in the certificate.

In all events, the owner of the key shall use his private key to decipher the message, warning the subscriber of the certificate and the owner of the key that in no event can a lost key be recovered, so that the CGCOM will not respond for any loss of enciphered information that cannot be recovered in cases of loss of certificates or keys.

2.5. Issuer Certification Entity

The corporate certificates of registered body are issued by the OMC Certification Entity (EC-OMC), identified by means of the above-mentioned data.

The EC-OMC subcontracts Symantec for the production services of certificates, which always works following the indications of the EC-OMC.

3. Limits of use of the certificate

3.1. Limits of use addressed at the subscribers

The subscriber must use the certification service of corporate certificates of registered body provided by the EC-OMC exclusively for the uses authorised in the agreement signed by OMC and Colegio de Médicos, and which are reproduced later (section “obligations of the subscribers”).

The subscriber furthermore undertakes to use the digital certification service in accordance with the instructions, manuals or procedures supplied by the EC-OMC.

The subscriber shall comply with any law and regulation that might affect its right of use of the cryptographic tools that it employs.

The subscriber shall not adopt inspection, alteration or inverse engineering measures of the digital certification services of the EC-OMC, without prior express permission.

3.2. Limits of use addressed at the verifiers

The verifier must use the certification service of corporate certificates of registered body, and the respective information service provided by the EC-OMC, exclusively for the uses authorised in the document on general conditions of use of the corporate certificate of registered body, and which are reproduced below (section “obligations of the verifiers”).

The verifier furthermore undertakes to use the digital certification service in accordance with the instructions, manuals or procedures supplied by the EC-OMC.

The verifier shall comply with any law and regulation that might affect its right of use of the cryptographic tools employed.

The verifier shall not adopt inspection, alteration or inverse engineering measures of the digital certification services of the EC-OMC, without prior express permission.

4. Obligations of the subscribers

4.1. Generation of keys

The subscriber authorises the EC-OMC to generate its own private and public key, for the identification and electronic signature within a secure device for creating electronic signature (the card received by the owner of keys), and requests the issue of the corporate certificate for the registered body.

4.2. Request for certificates

The subscriber undertakes to make the requests for corporate certificates of registered body in accordance with the procedure and, if necessary, the technical components supplied by the EC-OMC, pursuant with the provisions set out in the DPC and in the documentation on operations of the EC-OMC.

4.3. Truthfulness of information

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

The subscriber shall immediately inform the EC-OMC of any inaccuracy detected in the certificate after it has been issued, and also about any changes that are made in the information provided and/or registered for the issue of the certificate.

4.4. Custody obligations

The subscriber undertakes to assume the custody of the personal identification code, the card or any other technical support supplied by the EC-OMC, the private keys and, if necessary, the specifications which are the property of the EC-OMC which he is supplied, and also any information generated in his activity as registration entity.

In the event of loss or theft of the private key of the certificate, or if the subscriber suspects that the private key is no longer trustworthy for any reason, these circumstances must be immediately reported to the EC-OMC.

4.5. Obligations of correct use

The subscriber shall use the certification service of corporate certificates of registered body provided by the EC-OMC, exclusively for the uses authorised in the DPC and in any other instruction, manual or procedure supplied to the subscriber.

The subscriber shall comply with any law and regulation that might affect its right of use of the cryptographic tools employed.

The subscriber shall not adopt inspection, alteration or decompiling measures of the digital certification services provided.

The subscriber shall acknowledge:

a) That when he uses any certificate, and until the expiry of the certificate, or its suspension or revoke, he has accepted that certificate and it is operational.

b) That he does not act as certification entity and consequently, he undertakes not to use the private keys corresponding to the public keys contained in the certificates for the purpose of signing any certificate.

4.6. Forbidden transactions

The subscriber undertakes not to use his private keys, the certificates, the cards or any other technical support delivered by the EC-OMC in the performance of any transaction forbidden in the applicable law.

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

5. Obligations of the verifiers

5.1. Informed decision

The EC-OMC informs the verifier that he has access to sufficient information to adopt an informed decision at the time of verifying a certificate and trusting the information contained in the certificate.

In addition, the verifier will acknowledge that the use of the Register and the Lists of Revoked Certificates (hereinafter, "the LRCs" or "the CRLs) of the OMC, are ruled by the DPC of the EC-OMC and he will undertake to comply with the technical, operational and security requirements described in that DPC.

5.2. Verification requirements of the electronic signature

Before ciphering a message or document by an individual, the recipient's specific public key must be used. That public key can be obtained from his corporate certificate of registered body.

This certificate must therefore be verified before being ciphered.

The verification of 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 respective private key permits the deciphering of the message.

The verification will normally be executed automatically by the verifier's software and, in all events, in accordance with the DPC, with the following requirements:

- The suitable software must be used to verify a digital signature with the algorithms and lengths of keys authorised in the certificate and/or to execute any other cryptographic operation, and establish the chain of certificates on which the electronic signature to be verified is based, because the electronic signature is verified using this chain of certificates.
- It must be ensured that the chain of certificates identified is the most suitable for the electronic signature that is verified, because an electronic signature may be based on more than one chain of certificates, and it is up to the verifier to ensure that the most suitable chain is used in order to verify it.
- The revoke state of the certificates of the chain must be verified with the information supplied to the EC-OMC Register (with LRCs, for example) to determine the validity of all the certificates of the chain of certificates, because an electronic signature can only be considered correctly verified if each and every one of the certificates in the chain are correct and valid.
- It must be ensured that all certificates in the chain authorise the use of the private key for the certificate subscriber and the key owner, because of the possibility that any of the certificates may include limits in use that impede trusting the electronic signature that is verified. Each certificate in the chain has an indicator which refers to the applicable terms of use, for their review by the verifiers.
- The signature of all the certificates in the chain must be technically verified before trusting the certificate used by the signatory.

5.3. Trust in a non-verified signature

It is forbidden to cipher messages or documents by an addressee without having successfully verified his certificate.

If the verifier trusts a non-verified certificate, he will assume all the risks arising from this action.

5.4. Effect of the verification

By reason of the correct verification of corporate certificates of registered body, in accordance with these terms of use, the verifier may trust the identification and, if applicable, the public key of the key owner, within the respective limitations of use.

5.5. Correct use and forbidden activities

The verifier undertakes not to use any kind of information on state of the certificates or of any other class that has been supplied by the EC-OMC, in performing any transaction prohibited by the applicable law on that transaction.

The verifier undertakes not to inspect, interfere, or carry out inverse engineering in the technical implementation of the public certification services of the EC-OMC, without the previous written consent.

In addition, the verifier undertakes not to intentionally compromise the security of the public certification services of the EC-OMC.

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

6. Limited guarantees and rejection of guarantees

6.1. Guarantee of the EC-OMC for the digital certification services

The EC-OMC guarantees that:

a) The private key of the certification entity used to issue certificates has not been committed, unless the EC-OMC has not notified otherwise by the certification Register, in accordance with the DPC.

b) No false or erroneous declarations have been introduced in the information of any certificate, nor has necessary information provided by the subscriber and validated by the EC-OMC, not been included at the time of issue of the certificate.

c) All the certificates comply with the formal requirements and contents of the DPC, including all the legal requirements in force and applicable.

d) It is entailed by the operational and security procedures described in the DPC.

6.2. Exclusion from the guarantee

The EC-OMC does not guarantee any software used by any person for signing, for verifying signatures, ciphering, deciphering, or using any digital certificate in any other form, issued by the EC-OMC, except in the cases in which there is a written declaration to the contrary.

7. Applicable agreements and DPC

7.1. Applicable agreements

The following agreements apply to the corporate certificate of registered body:

- Collaboration agreement of certification services, which regulates the relation between the EC-OMC and the subscriber medical association of the certificates.
- General Terms of use, which regulate the relation between the EC-OMC and the individuals or legal entities that use the certificates, also called "verifiers".

7.2. Declaration of certification practices

The certification services of the EC-OMC are technically and operationally regulated by the Declarations of certification practices of the EC-OMC and of Symantec, by their subsequent updates, and also by complementary documentation.

The DPC and the documentation of operations is modified periodically at the Register and may be consulted on the Internet site: http://www.cgcom.es/registro.

7.3. Certification policy

The EC-OMC has a certification policy which provides details of the technical, legal and operational requirements and also the regulation of the corporate certificate of registered doctor, which is available to the users' community upon request.

8. Rules of trust for long-life signatures

Point b.2 of article 18 of Law 59/2003, of 19 December, on electronic signature refers to the obligation of the certification entities to inform applicants about the mechanisms to guarantee the reliability of the electronic signature of a document in time.

The EC-OMC informs the applicants of the corporate certificates of registered body that it does not offer a service that guarantees the trustworthiness of the electronic signature of a document throughout time

For the trustworthiness of the electronic signature of a document throughout time, the EC-OMC recommends the use of the standards indicated in section 7.3 (rules of trustworthiness for long-life signatures) of the Application Guide of the Technical Standard on Inter-operability "Electronic Signature Policy and certificates of the Administration".

The general considerations for the rules of trustworthiness of long-life signatures are set out in sub-item IV.3 of the NTI on electronic signature:

IV.3 Rules of trust for long-life signatures

1. *In the case of long-life signatures, the signatory or the verifier of the signature will include a time stamp that permits it to be guaranteed that the certificate was valid at the time when the signature was made. In the event that it is included by the signatory, it may be made after the precaution term or grace period has elapsed.*
2. *To convert an electronic signature into a long-life electronic signature:*
   a) *The electronic signature produced or verified will be verified, validating the integrity of the signature, the compliance of standards XAdES, CAdES or PAdES and the references.*
   b) *A process of completing the electronic signature will be made which will consist of obtaining and storing the references to:*
      I. *Certificates: including the certificates of the signatory and of the certification chain.*
      II. *Information about the state of the certificates, CRLs or the OCSP responses.*
   c) *Applying the stamping to the references to the certificates and information on state.*
3. *To incorporate the signature of the complete validation information, validation will be used by CRLs or OCSP.*
4. *The signature policies will contemplate the definition of formats and considerations of use of long-life signatures according to the specific needs of their scope of application and the specific applicable standards.*

8.1. XAdES format

Within the XAdES signature format, the XAdES-C extended format includes two non-signed properties:

I. *CompleteCertificateRefs: contains references to all the certificates of the trust chain needed for verifying the signature, except the signatory certificate.*
II. *CompleteRevocationRefs: contains references to the CRLs and/or OCSP responses used in the verification of certificates.*

If this validation information is to be included in the signature, it is recommended using the XAdES-X format, which adds a time stamp to the above information.

Apart from the information included in XAdES-X, the XAdES-XL format includes two new unsigned properties: CertificateValues y RevocationValues which include:

I. *References to the validation information.*
II. *Complete trust chain.*
III. *CRL or OCSP response obtained in the validation.*

If this validation information is to be included in the signature, it is recommended using the XADES-A format, which adds a time stamp to the above information. In this case it is recommended using validation by OCSP, because with this method the properties CertificateValues and RevocationValues have a smaller size.

8.2. CAdES format

Within the CAdES signature format, the CAdES-C extended format includes two attributes:

I. *Complete-certificate-references: contains references to all the certificates in the trust chain needed to verify the signature.*
II. *Complete-revocation-references: contains references to the CRLs and/or OCSP responses used in the signature verification.*

The CAdES-X Long format, in addition to the information included in CAdES-C, includes two new attributes certificate-values and revocation-values which include:

I. *References to the validation information.*
II. *Complete trust chain.*
III. *CRL or OCSP response obtained in the validation.*

If this validation information is to be included in the signature, the validation by OCSP favours obtaining a smaller size in the certificate-values properties and revocationvalues .

It is consequently recommended using the following formats, depending on the type of validation.

I. *If the validation is made by OCSP consultation: the CAdES-X Long type 1 or CAdES-X Long type 2 formats, which add a time stamp to the information included in a CAdES-X Long signature. In this case, the attributes certificatevalues and revocation-values are included because the response to an OCSP enquiry does not occupy much space.*

II. *If the validation cannot be made by OCSP and it is carried out by consulting a CRL: the CAdES-X type 1 or CAdES-X type 2 formats, that include a time stamp in the information included in a CAdES-C signature, namely, the references to the consulted CRL and the certificates of the trust chain. It is not recommended including the certificate-values and revocation-values attributes because they may be very voluminous.*

If the time stamp added to build the long-life signature is about to expire, the CAdES-X Long type 1 or CAdES-X Long type 2 may be transformed into a CAdES-A signature, adding a file time stamp to the above signature.

8.3. PAdES format

In the case of PAdES format, the use of the PAdES-Long Term format would be recommended.

As in the above cases, it is recommended using validation by OCSP, because the size of the validation information to be added is smaller.

Also, a time stamp could be added that would include that validation information, because the validity of the resulting signature is determined by the duration of the time stamp that is added to the long-life signature.

9. Intimacy policy

The EC-OMC cannot disclose or be obliged to disclose any confidential information regarding certificates without a specific previous request which comes from:

a) the person in respect of whom the EC-OMC has the duty to keep the information confidential, or

b) a court order, administrative order or any other foreseen in valid law.

The subscriber however accepts that certain personal information and of any other class, provided in the application for certificates, will be included in its certificates and in the mechanism for verifying the state of the certificates, and that the mentioned information will not be confidential, by legal imperative.

The EC-OMC does not assign anyone the data specifically delivered for providing the certification service.

The notification of those data to the collaborators of EC-OMC in providing the certification and registration services (in particular, Symantec.) is produced in the framework of a processing manager agreement, in the terms of the valid LOPD, and consequently is not considered an assignment.

10. Reimbursement policy

In no event shall the EC-OMC reimburse the cost of the certification service.

11. Applicable law and competent jurisdiction

The relations with the EC-OMC will be ruled by Spanish law and specifically by Law 59/2003, of 19 December, on electronic signature, and also by the applicable civil and mercantile law.

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

12. Accreditations and quality stamps

The EC-OMC has documentation evidencing the fulfilment of the following audits:

- WebTrust for Certification Authorities, applicable to the VeriSign data processing Centre.
- Procedures of the voluntary technical specification ETSI TS 101 456.