Certificate Profiles of the Certification Entity

Organización Médica Colegial de España

1. General information

1.1 Documentation Control

Project:	**Documentation on practices of the Certification Entity**
Target entity:	**Organización Médica Colegial de España**
Version:	**3.6**
Date of publication:	**26/06/2013**
File:	**Perfiles_CGCOM_v3r6-def**
Format:	**Word 97-2003**
Authors:	**Astrea**

1.2 Formal State

Prepared by:	**Reviewed by:**	**Approved by:**
Name: Astrea Date: **26/06/2013**	Name: OMC Date:	Name: OMC Date:

1.3 Control of versions

Version	Parts that change	Description of the change	Change in Author	Date of the change
1.0	All	Original	Astrea	18/07/2006
2.0	Profiles	OMC review	Astrea	09/08/2006
2.1	Profiles	VeriSign Review	Astrea	19/09/2006
2.2	Profiles	OIDs policy correction	Astrea	25/09/2006
3.0	Profiles	Addition external profiles	Astrea	15/12/2009
3.1	External profile	Addition Pol. Cert.	Astrea	22/03/2011
3.2	Software profile and others	. Addition Legal Entity Profile on software . Improvements in field Qualified Certificate Statements of all profiles	Astrea	13/07/2011
3.3	Profiles	. Alignment with contents of the different certificates issued. . The Issuer Alternative Name is extended	Astrea	18/01/2012
3.4	Profiles	OCSP information included	Astrea	13/07/2012
	External profile	Modification in Title of the Subject.	Astrea	13/07/2012
3.5 3.6	New profiles	. Change of name in the association certificate to that of legal entity. . The encipherment certificates are added. . New types of certificate are added for separate identification and signature. . Certificate profile is added in software for administrative personnel	Astrea	07/06/2013

1.4 References

- VeriSign Trust Network certification policy.
- Certification policy of the Organización Médica Colegial de España.
- Order HAC/1181/2003, of 12 May, establishing specific rules for the use of electronic signature in tax relations by electronic, IT and telematic means with the Tax Administration State Agency. (Official State Gazette [B.O.E.] 15-05-2003)
- Schema of identification and electronic signature of Public Administrations. Block I: Profiles of electronic certificates (v1.7.3) CertiCA

2. Table of Contents

3. Overview

3.1 Typology of certificates to be issued

The certification policy of the Organización Médica Colegial determines the possibility of issuing the following types of certificates:

a) Certificates of signature and certificates of encipherment

Regarding the use, there are two types of certificates:

1) Qualified certificates of electronic signature, which are used as basis of the advanced electronic signature, and in combination with a secure device for creating signature. They may also be used for signing authentication messages (confirmation of identity), as well as for signing other classes of messages.

2) Ordinary encipherment certificates, which are used to produce or to receive ciphered messages and documents.

b) Corporate certificates and external certificates

Certificates of final entity may be corporate certificates or external certificates:

1) The corporate certificates are characterised by the fact that the subscriber belongs to one of the entities that form the Organización Médica Colegial. The corporate certificates are always for group.

2) The external certificates are all the other certificates. A complete registration of the data to be certified must be made.

Only external certificates are issued, except when necessary, for example in the case of doctors, whether or not registered, of a regional health service. External certificates may be individual or group:

a) Individual external certificates, characterised by the fact that the person identified in the certificate acts in his/her own name and representation (in this case the subscriber or holder of the certificate)

b) External group certificates, in which the person identified in the certificate acts within the organisational scope of a legal entity (which will be the subscriber or holder of the certificate). For example, certificates issued to doctors, whether or not registered, assigned to a regional health service will be external group certificates, where the subscriber will be that regional health service.

External group certificates issued to a registered doctor assigned to a regional health service may be included in the professional card which the Association issues to the registered doctor, in which case the card will include two certificates.

Likewise, the external group certificate may be issued by remote means with authentication based on the registered doctor's qualified electronic signature.

c) Certificates of registered doctor and certificates of administrative personnel

Corporate certificates may be issued to registered doctors or to administrative personnel:

1) Certificates of registered doctor, issued with the intervention of their Medical Association, in its status as registrar with the exclusive capacity of certifying the status of "registered doctor" of a person identified in the certificate.

2) Certificates of administrative personnel of the entities that form the Organización Médica Colegial.

d) Certificates of individual and certificates of legal entity

Certificates may be issued to individuals or to legal entities:

1) Certificates of individual, who acts as signatory, should take into account their empowerments and capacities of action, whether or not indicated in the certificate, before trusting the signature.

2) Certificates of legal entity, to which the signed documents are attributed, as signatory, without having to consider the empowerments or capacities of action of the person who has custody of the electronic signature certificate.

3.2 Effective profiles to be implemented

This document contains the profiles of certificates to be issued by the Certification Entity of the Organización Médica Colegial del España, with the following considerations:

- It has been considered appropriate to unify the electronic signature and encipherment certificates, since in no event are encipherment private key recovery services going to be provided, owing to the sensitiveness of health information.
- Five corporate certificate profiles are defined: three profiles correspond to certificates of individuals (registered doctor, organic and administrative personnel), one to the legal entity certificate (professional association) on card and one to the legal entity certificate (professional association) on software.
- A single group external certificate profile is defined, for registered or non-registered doctors assigned to a regional health service.
- As from 2013, new profiles of certificates appear on card to separate the functions of signature, identification and encipherment, in different certificates.

The certificates are issued based on the class 2 policy of the VeriSign Trust Network, which should be indicated as second certification policy, on the actual certificates.

The certificates will be issued on cryptographic card and will be considered secure signature creation device, and will last for a maximum of three years, with annual re-authentication of the key owners, by organisational procedures, with the exception of the certificate on legal entity software.

The object identifier (OID) of OMC is 1.3.6.1.4.1.26852

4. Corporate Certificates

4.1 Corporate certificate of registered doctor (individual) for identification, signature and encrypting

Field	Contents	Compulsory	Critical
1. Basic structure			
1.1. Version	"2"[1]	Yes	
1.2. Serial Number	Established automatically[2]	Yes	
1.3. Signature Algorithm	SHA-1 with RSA Signature	Yes	
1.4. Issuer Distinguished Name		Yes	
1.4.1. Country (C)	"ES"	Yes	
1.4.2. Organization (O)	"Organizacion Medica Colegial"[3]	Yes	
1.4.3. Organizational Unit (OU)	"Certification Entity" [4]	Yes	
1.4.4. Organizational Unit (OU)	"Class 2 Managed PKI Individual Subscriber CA"	Yes	
1.4.5. Organizational Unit (OU)	"VeriSign Trust Network"	Yes	
1.4.6. Common Name (CN)	"OMC"	Yes	
1.5. Validity	3 years.	Yes	
1.5.1. Not Before	Start date of validity	Yes	
1.5.2. Not After	Date of expiry	Yes	
1.6. Subject		Yes	
1.6.1. Country (C)	"ES"[5]	Yes	

[1] The literal "2" corresponds to version 3.

[2] It should not exceed 32 hexadecimal characters in hexadecimal notation.

[3] The text is included without accents.

[4] The text is included without accents.

Field	Contents	Compulsory	Critical
1.6.2. Organization (O)	Professional association	Yes	
1.6.3. Organizational Unit (OU)	"Conditions of use at https://www.cgcom.es/CertCol (c)06"	Yes	
1.6.4. Organizational Unit (OU)	"Use is subject to terms at https://www.verisign.com/rpa (c)99"	Yes	
1.6.5. Surname	Surnames	Yes	
1.6.6. Given Name	Given name	Yes	
1.6.7. Title	"Registered doctor"	Yes	
1.6.8. Serial Number	National ID Document (DNI)/ Foreigner's ID Number (NIE)[6]	Yes	
1.6.9. Common Name (CN)	"(Registered Doctor)" + Given name and surnames + "-" + Registered Doctor's number	Yes	
1.6.10. Email (E)	E-mail Address	Yes	
1.7. Subject Public Key Info	2048-Bit Public key encoded in accordance with RFC2459 & PKCS#1	Yes	
2. Extensions			
2.1. Authority Key Identifier	Present	Yes	
2.1.1. Authority Key Identifier			
2.1.2. AuthorityCertIssuer			
2.1.3. AuthorityCertSerialNum			

[5] The field "country" will always be Spain, since the certificate shows the relation between a registered doctor and a Spanish professional association, regardless of the nationality of the registered doctor. This arises from the corporate nature of the certificate, whose subscriber is the association, and the registered doctor, the person authorised for its use.

[6] The field "serial number" should include the National ID Document (DNI) or the Foreigner's ID Number (NIE) of the registered doctor, in order to admit the certificate for performing formalities with the Spanish Administrations.

Field	Contents	Compulsory	Critical
ber			
2.2. Subject Key Identifier	Present	Yes	
2.3. Key Usage		Yes	Yes
2.3.1. Digital Signature	Selected. “1”	Yes	
2.3.2. Non Repudiation	Selected. “1”	Yes	
2.3.3. Key Encipherment	Selected. “1”	Yes	
2.3.4. Data Encipherment	Selected. “1”	Yes	
2.3.5. Key Agreement	Not selected. “0”		
2.3.6. Key Certificate Signature	Not selected. “0”		
2.3.7. CRL Signature	Not selected. “0”		
2.4. Qualified Certificate Statements		Yes	
2.4.1. qCCompliance (0.4.0.1862.1.1)		Yes	
2.4.2. QcEuRetentionPeriod (0.4.0.1862.1.3)	15	Yes	
2.4.3. QcSSCD (0.4.0.1862.1.4)		Yes	
2.5. Certificate Policies		Yes	
2.5.1. Policy Identifier	1.3.6.1.4.1.26852.1.1.1	Yes	
2.5.2. Policy Qualifier ID		Yes	
2.5.2.1. CPS Pointer	“https://www.cgcom.es/CertCol”	Yes	
2.5.2.2. User Notice	“Corporate certificate of qualified electronic signature and registered doctor encipherment. “Conditions of use on https://www.cgcom.es/CertCol”	Yes	
2.5.3. Policy Identifier	OID of class 2 policy of VeriSign	Yes	
2.5.4. Policy Qualifier ID		Yes	

Field	Contents	Compulsory	Critical
2.5.4.1. CPS Pointer	Reference to VeriSign RPA	Yes	
2.5.4.2. User Notice	Notice of VeriSign user	Yes	
2.6. Subject Alternative Names		Yes	
2.6.1. rfc822Name	Corporate e-mail of registered doctor[7]	Yes	
2.6.2. directoryName[8]		Yes	
2.6.2.1. CGCOM.2.1	IdAssociation	Yes	
2.6.2.2. CGCOM.2.2	Professional association	Yes	
2.6.2.3. CGCOM.2.3	IdAssociation	Yes	
2.6.2.4. CGCOM.2.4	Given name and surname of registered doctor	Yes	
2.7. Issuer Alternative Name		Yes	
2.7.1. rfc822Name	"certificacion@cgcom.es"	Yes	
2.7.2. directoryName		Yes	
2.7.2.1. Organization (O)	"Consejo General de Colegios de Medicos"	Yes	
2.7.2.2. SerialNumber	"Q2866017C"	Yes	
2.7.2.3. Location (L)	"Plaza de las Cortes 11"	Yes	
2.7.2.4. Postal Code	"28014"	Yes	
2.7.2.5. State Or Province Name	"Madrid"	Yes	
2.7.2.6. Country (C)	ES	Yes	
2.8. Extended Key Usage		Yes	
2.8.1. emailProtection	Present	Yes	

[7] This field contains the corporate e-mail address of the registered doctor, for notification purposes.

[8] This field links with the CGCOM re-certification and validation system, permitting the efficient recovery of additional information. Certain information is included, although this may be redundant, in order to have complete information about the user in a single consultation against the certificate.

Field	Contents	Compulsory	Critical
2.8.2. clientAuth	Present	Yes	
2.9. cRLDistributionPoint		Yes	
2.9.1. distributionPoint	"http://crl1.cgcom.es/crl/ec-cgcom.crl"	Yes	
2.9.2. distributionPoint	"http://crl2.cgcom.es/crl/ec-cgcom.crl"	Yes	
2.10. Authority Info Access		Yes	
2.10.1. Access Method		Yes	
2.10.2. Access Location	http://pki-ocsp.verisign.com	Yes	
2.11. NetscapeCertType	"SSL client", "S/MIME"	Yes	
2.12. Subject Directory Attributes (2.5.29.9)		Yes	
2.12.1. Country of Citizenship	Country of nationality	Yes	
2.12.2. Country of Residence	Country of residence.	Yes	

4.2 Corporate certificate of registered body (individual) for identification, signature and encrypting

Field	Contents	Compulsory	Critical
1. Basic structure			
1.1. Version	"2"[9]	Yes	
1.2. Serial Number	Established automatically[10]	Yes	
1.3. Signature Algorithm	SHA-1 with RSA Signature	Yes	
1.4. Issuer Distinguished Name		Yes	
1.4.1. Country (C)	"ES"	Yes	
1.4.2. Organization (O)	"Organizacion Medica Colegial"[11]	Yes	
1.4.3. Organizational Unit (OU)	"Certification Entity" [12]	Yes	
1.4.4. Organizational Unit (OU)	"Class 2 Managed PKI Individual Subscriber CA"	Yes	
1.4.5. Organizational Unit (OU)	"VeriSign Trust Network"	Yes	
1.4.6. Common Name (CN)	"OMC"	Yes	
1.5. Validity	3 years.	Yes	
1.5.1. Not Before	Start date of validity	Yes	
1.5.2. Not After	Date of expiry	Yes	
1.6. Subject		Yes	
1.6.1. Country (C)	"ES"[13]	Yes	

[9] The literal "2" corresponds to version 3.

[10] It should not exceed 32 hexadecimal characters in hexadecimal notation.

[11] The text is included without accents.

[12] The text is included without accents.

Field	Contents	Compulsory	Critical
1.6.2. Organization (O)	Professional association	Yes	
1.6.3. Organizational Unit (OU)	"Conditions of use on https://www.cgcom.es/CertOrg (c)06"	Yes	
1.6.4. Organizational Unit (OU)	"Use is subject to terms at https://www.verisign.com/rpa (c)99"	Yes	
1.6.5. Surname	Surnames	Yes	
1.6.6. Given Name	Given name	Yes	
1.6.7. Title	Body / office	Yes	
1.6.8. Serial Number	National ID Document (DNI)/ Foreigner's ID Number (NIE)[14]	Yes	
1.6.9. Common Name (CN)	Name and surnames	Yes	
1.6.10. Email (E)	E-mail Address	Yes	
1.7. Subject Public Key Info	2048-Bit Public key encoded in accordance with RFC2459 & PKCS#1	Yes	
2. Extensions			
2.1. Authority Key Identifier	Present	Yes	
2.1.1. Authority Key Identifier			
2.1.2. AuthorityCertIssuer			
2.1.3. AuthorityCertSerialNumber			
2.2. Subject Key Identifier	Present	Yes	

[13] The field "country" will always be Spain, since the certificate shows the relation between a person that holds a body or office and a Spanish professional association, regardless of the nationality of that person.

[14] The field "serial number" should include the National ID Document (DNI) or the Foreigner's ID Number (NIE) of the body, in order to admit the certificate for performing formalities with the Spanish Administrations.

Field	Contents	Compulsory	Critical
2.3. Key Usage		Yes	Yes
2.3.1. Digital Signature	Selected. "1"	Yes	
2.3.2. Non Repudiation	Selected. "1"	Yes	
2.3.3. Key Encipherment	Selected. "1"	Yes	
2.3.4. Data Encipherment	Selected. "1"	Yes	
2.3.5. Key Agreement	Not selected. "0"		
2.3.6. Key Certificate Signature	Not selected. "0"		
2.3.7. CRL Signature	Not selected. "0"		
2.4. Qualified Certificate Statements		Yes	
2.4.1. qCCompliance (0.4.0.1862.1.1)		Yes	
2.4.2. QcEuRetentionPeriod (0.4.0.1862.1.3)	15	Yes	
2.4.3. QcSSCD (0.4.0.1862.1.4)		Yes	
2.5. Certificate Policies		Yes	
2.5.1. Policy Identifier	1.3.6.1.4.1.26852.1.1.4	Yes	
2.5.2. Policy Qualifier ID		Yes	
2.5.2.1. CPS Pointer	"https://www.cgcom.es/CerOrg"	Yes	
2.5.2.2. User Notice	"Corporate certificate of qualified electronic signature and registered body encipherment. Conditions of use at https://www.cgcom.es/CertOrg"	Yes	
2.5.3. Policy Identifier	OID of class 2 policy of VeriSign	Yes	
2.5.4. Policy Qualifier ID		Yes	
2.5.4.1. CPS Pointer	Reference to VeriSign RPA	Yes	
2.5.4.2. User Notice	Notice of VeriSign user	Yes	

Field	Contents	Compulsory	Critical
2.6. Subject Alternative Names		Yes	
2.6.1. rfc822Name	Corporate e-mail of registered body[15]	Yes	
2.6.2. directoryName[16]		Yes	
2.6.2.1. CGCOM.2.1	IdAssociation	Yes	
2.6.2.2. CGCOM.2.2	Professional association	Yes	
2.6.2.3. CGCOM.2.5	IdOBody	Yes	
2.6.2.4. CGCOM.2.6	Description of the registered body	Yes	
2.7. Issuer Alternative Name		Yes	
2.7.1. rfc822Name	"certificacion@cgcom.es"	Yes	
2.7.2. directoryName		Yes	
2.7.2.1. Organization (O)	"Consejo General de Colegios de Medicos"	Yes	
2.7.2.2. SerialNumber	"Q2866017C"	Yes	
2.7.2.3. Location (L)	"Plaza de las Cortes 11"	Yes	
2.7.2.4. Postal Code	"28014"	Yes	
2.7.2.5. State Or Province Name	"Madrid"	Yes	
2.7.2.6. Country (C)	ES	Yes	
2.8. Extended Key Usage		Yes	
2.8.1. emailProtection	Present	Yes	
2.8.2. clientAuth	Present	Yes	
2.9. cRLDistributionPoint		Yes	

[15] This field contains the corporate e-mail address of the body, for notification purposes.

[16] This field links with the CGCOM re-certification and validation system, permitting the efficient recovery of additional information. Certain information is included, although this may be redundant, in order to have complete information about the user in a single consultation against the certificate.

Field	Contents	Compulsory	Critical
2.9.1. distributionPoint	"http://crl1.cgcom.es/crl/ec-cgcom.crl"	Yes	
2.9.2. distributionPoint	"http://crl2.cgcom.es/crl/ec-cgcom.crl"	Yes	
2.10. Authority Info Access		Yes	
2.10.1. Access Method		Yes	
2.10.2. Access Location	http://pki-ocsp.verisign.com	Yes	
2.11. NetscapeCertType	"SSL client", "S/MIME"	Yes	
2.12. Subject Directory Attributes (2.5.29.9)		Yes	
2.12.1. Country of Citizenship	Country of nationality	Yes	
2.12.2. Country of Residence	Country of residence.	Yes	

4.3 Corporate certificate of administrative personnel for identification, signature and encrypting

Field	Contents	Compulsory	Critical
1. Basic structure			
1.1. Version	"2"[17]	Yes	
1.2. Serial Number	Established automatically[18]	Yes	
1.3. Signature Algorithm	SHA-1 with RSA Signature	Yes	
1.4. Issuer Distinguished Name		Yes	
1.4.1. Country (C)	"ES"	Yes	
1.4.2. Organization (O)	"Organizacion Medica Colegial" [19]	Yes	
1.4.3. Organizational Unit (OU)	"Certification Entity" [20]	Yes	
1.4.4. Organizational Unit (OU)	"Class 2 Managed PKI Individual Subscriber CA"	Yes	
1.4.5. Organizational Unit (OU)	"VeriSign Trust Network"	Yes	
1.4.6. Common Name (CN)	"OMC"	Yes	
1.5. Validity	3 years.	Yes	
1.5.1. Not Before	Start date of validity	Yes	
1.5.2. Not After	Date of expiry	Yes	
1.6. Subject		Yes	
1.6.1. Country (C)	"ES"[21]	Yes	

[17] The literal "2" corresponds to version 3.

[18] It should not exceed 32 hexadecimal characters in hexadecimal notation.

[19] The text is included without accents.

[20] The text is included without accents.

Field	Contents	Compulsory	Critical
1.6.2. Organization (O)	Professional association or legal entity in the health area	Yes	
1.6.3. Organizational Unit (OU)	"Conditions of use on https://www.cgcom.es/CertAdmin (c)06"	Yes	
1.6.4. Organizational Unit (OU)	"Use is subject to terms at https://www.verisign.com/rpa (c)99"	Yes	
1.6.5. Surname	Surnames	Yes	
1.6.6. Given Name	Given name	Yes	
1.6.7. Title	"Administrative and service personnel"	Yes	
1.6.8. Serial Number	National ID Document (DNI)/ Foreigner's ID Number (NIE)[22]	Yes	
1.6.9. Common Name (CN)	Name and surnames	Yes	
1.6.10. Email (E)	E-mail Address	Yes	
1.7. Subject Public Key Info	2048-Bit Public key encoded in accordance with RFC2459 & PKCS#1	Yes	
2. Extensions			
2.1. Authority Key Identifier	Present	Yes	
2.1.1. Authority Key Identifier			
2.1.2. AuthorityCertIssuer			
2.1.3. AuthorityCertSerialNumber			
2.2. Subject Key Identifier	Present	Yes	

[21] The field "country" will always be Spain, since the certificate shows the relation between a worker and a Spanish professional association, regardless of the nationality of the registered doctor.

[22] The field "serial number" should include the National ID Document (DNI) or the Foreigner's ID Number (NIE) of the worker, in order to admit the certificate for performing formalities with the Spanish Administrations.

Field	Contents	Compulsory	Critical
2.3. Key Usage		Yes	Yes
2.3.1. Digital Signature	Selected. "1"	Yes	
2.3.2. Non Repudiation	Selected. "1"	Yes	
2.3.3. Key Encipherment	Selected. "1"	Yes	
2.3.4. Data Encipherment	Selected. "1"	Yes	
2.3.5. Key Agreement	Not selected. "0"		
2.3.6. Key Certificate Signature	Not selected. "0"		
2.3.7. CRL Signature	Not selected. "0"		
2.4. Qualified Certificate Statements		Yes	
2.4.1. qCCompliance (0.4.0.1862.1.1)		Yes	
2.4.2. QcEuRetentionPeriod (0.4.0.1862.1.3)	15	Yes	
2.4.3. QcSSCD (0.4.0.1862.1.4)		Yes	
2.5. Certificate Policies		Yes	
2.5.1. Policy Identifier	1.3.6.1.4.1.26852.1.1.2	Yes	
2.5.2. Policy Qualifier ID		Yes	
2.5.2.1. CPS Pointer	"https://www.cgcom.es/CertAdmin"	Yes	
2.5.2.2. User Notice	"Corporate certificate of qualified electronic signature and administrative personnel and services encipherment. Conditions of use at https://www.cgcom.es/CertAdmin"	Yes	
2.5.3. Policy Identifier	OID of class 2 policy of VeriSign	Yes	
2.5.4. Policy Qualifier ID		Yes	

Field	Contents	Compulsory	Critical
2.5.4.1. CPS Pointer	Reference to VeriSign RPA	Yes	
2.5.4.2. User Notice	Notice of VeriSign user	Yes	
2.6. Subject Alternative Names		Yes	
2.6.1. rfc822Name	Corporate e-mail of administrative personnel[23]	Yes	
2.6.2. directoryName[24]		Yes	
2.6.2.1. CGCOM.2.1	IdAssociation / IdEntity	Yes	
2.6.2.2. CGCOM.2.2	Professional association / Legal entity in the health area	Yes	
2.6.2.3. CGCOM.2.7	IdAdminPersonnel	Yes	
2.6.2.4. CGCOM.2.8	Given name and surnames of administrative personnel	Yes	
2.7. Issuer Alternative Name		Yes	
2.7.1. rfc822Name	"certificacion@cgcom.es"	Yes	
2.7.2. directoryName		Yes	
2.7.2.1. Organization (O)	"Consejo General de Colegios de Medicos"	Yes	
2.7.2.2. SerialNumber	"Q2866017C"	Yes	
2.7.2.3. Location (L)	"Plaza de las Cortes 11"	Yes	
2.7.2.4. Postal Code	"28014"	Yes	
2.7.2.5. State Or Province Name	"Madrid"	Yes	
2.7.2.6. Country (C)	ES	Yes	

[23] This field contains the corporate e-mail address of the administrative personnel and services, for notification purposes.

[24] This field links with the CGCOM re-certification and validation system, permitting the efficient recovery of additional information. Certain information is included, although this may be redundant, in order to have complete information about the user in a single consultation against the certificate.

Field	Contents	Compulsory	Critical
2.8. Extended Key Usage		Yes	
2.8.1. emailProtection	Present	Yes	
2.8.2. clientAuth	Present	Yes	
2.9. cRLDistributionPoint		Yes	
2.9.1. distributionPoint	"http://crl1.cgcom.es/crl/ec-cgcom.crl"	Yes	
2.9.2. distributionPoint	"http://crl2.cgcom.es/crl/ec-cgcom.crl"	Yes	
2.10. Authority Info Access		Yes	
2.10.1. Access Method		Yes	
2.10.2. Access Location	http://pki-ocsp.verisign.com	Yes	
2.11. NetscapeCertType	"SSL client", "S/MIME"	Yes	
2.12. Subject Directory Attributes (2.5.29.9)		Yes	
2.12.1. Country of Citizenship	Country of nationality	Yes	
2.12.2. Country of Residence	Country of residence.	Yes	

4.4 Corporate certificate of legal entity for identification, signature and encipherment.

Field	Contents	Compulsory	Critical
1. Basic structure			
1.1. Version	"2"[25]	Yes	
1.2. Serial Number	Established automatically[26]	Yes	
1.3. Signature Algorithm	SHA-1 with RSA Signature	Yes	
1.4. Issuer Distinguished Name		Yes	
1.4.1. Country (C)	"ES"	Yes	
1.4.2. Organization (O)	"Organizacion Medica Colegial" [27]	Yes	
1.4.3. Organizational Unit (OU)	"Certification Entity" [28]	Yes	
1.4.4. Organizational Unit (OU)	"Class 2 Managed PKI Individual Subscriber CA"	Yes	
1.4.5. Organizational Unit (OU)	"VeriSign Trust Network"	Yes	
1.4.6. Common Name (CN)	"OMC"	Yes	
1.5. Validity	3 years.	Yes	
1.5.1. Not Before	Start date of validity	Yes	
1.5.2. Not After	Date of expiry	Yes	
1.6. Subject		Yes	
1.6.1. Country (C)	"ES"[29]	Yes	

[25] The literal "2" corresponds to version 3.

[26] It should not exceed 32 hexadecimal characters in hexadecimal notation.

[27] The text is included without accents.

[28] The text is included without accents.

Field	Contents	Compulsory	Critical
1.6.2. Organization (O)	Professional association or legal entity in the health area	Yes	
1.6.3. Organizational Unit (OU)	"Conditions of use on https://www.cgcom.es/CertJur (c)06"	Yes	
1.6.4. Organizational Unit (OU)	"Use is subject to terms at https://www.verisign.com/rpa (c)99"	Yes	
1.6.5. Surname	Custodian's surnames	Yes	
1.6.6. Given Name	Name of custodian	Yes	
1.6.7. 1.3.6.1.4.1.18838.1.1	National ID Document (DNI)/ Foreigner's ID Number (NIE)[30]	Yes	
1.6.8. Serial Number	Tax ID Number (NIF) of the entity[31]	Yes	
1.6.9. Common Name (CN)	Professional association or legal entity in the health area	Yes	
1.6.10. Email (E)	E-mail Address	Yes	
1.7. Subject Public Key Info	2048-Bit Public key encoded in accordance with RFC2459 & PKCS#1	Yes	
2. Extensions			
2.1. Authority Key Identifier	Present	Yes	
2.1.1. Authority Key Identifier			

[29] The field "country" will always be Spain, since the certificate shows the relation between a registered doctor and a Spanish professional association, regardless of the nationality of the registered doctor. This arises from the corporate nature of the certificate, whose subscriber is the association, and the registered doctor, the person authorised for its use.

[30] The field "serial number" should include the National ID Document (DNI) or the Foreigner's ID Number (NIE) of the worker, in order to admit the certificate for performing formalities with the Spanish Administrations.

[31] In accordance with the tax regulations, this field should show the Tax ID Number (NIF) of the legal entity.

Field	Contents	Compulsory	Critical
2.1.2. AuthorityCertIssuer			
2.1.3. AuthorityCertSerialNumber			
2.2. Subject Key Identifier	Present	Yes	
2.3. Key Usage		Yes	Yes
2.3.1. Digital Signature	Selected. “1”	Yes	
2.3.2. Non Repudiation	Selected. “1”	Yes	
2.3.3. Key Encipherment	Selected. “1”	Yes	
2.3.4. Data Encipherment	Selected. “1”	Yes	
2.3.5. Key Agreement	Not selected. “0”		
2.3.6. Key Certificate Signature	Not selected. “0”		
2.3.7. CRL Signature	Not selected. “0”		
2.4. Qualified Certificate Statements		Yes	
2.4.1. qCCompliance (0.4.0.1862.1.1)		Yes	
2.4.2. QcEuRetentionPeriod (0.4.0.1862.1.3)	15	Yes	
2.4.3. QcSSCD (0.4.0.1862.1.4)		Yes	
2.5. Certificate Policies		Yes	
2.5.1. Policy Identifier	1.3.6.1.4.1.26852.1.1.3	Yes	
2.5.2. Policy Qualifier ID		Yes	
2.5.2.1. CPS Pointer	“https://www.cgcom.es/CertJur”	Yes	
2.5.2.2. User Notice	“Corporate certificate of qualified electronic signature and legal entity encipherment. Conditions of use at https://www.cgcom.es/CertJur”	Yes	

Field	Contents	Compulsory	Critical
2.5.3. Policy Identifier	OID of class 2 policy of VeriSign	Yes	
2.5.4. Policy Qualifier ID		Yes	
2.5.4.1. CPS Pointer	Reference to VeriSign RPA	Yes	
2.5.4.2. User Notice	Notice of VeriSign user	Yes	
2.6. Subject Alternative Names		Yes	
2.6.1. rfc822Name	Corporate e-mail of custodian[32]	Yes	
2.6.2. directoryName[33]		Yes	
2.6.2.1. CGCOM.2.1	IdAssociation / IdEntity	Yes	
2.6.2.2. CGCOM.2.2	Professional association / Legal entity in the health area	Yes	
2.7. Issuer Alternative Name		Yes	
2.7.1. rfc822Name	"certificacion@cgcom.es"	Yes	
2.7.2. directoryName		Yes	
2.7.2.1. Organization (O)	"Consejo General de Colegios de Medicos"	Yes	
2.7.2.2. SerialNumber	"Q2866017C"	Yes	
2.7.2.3. Location (L)	"Plaza de las Cortes 11"	Yes	
2.7.2.4. Postal Code	"28014"	Yes	
2.7.2.5. State Or Province Name	"Madrid"	Yes	
2.7.2.6. Country (C)	ES	Yes	
2.8. Extended Key Usage		Yes	
2.8.1. emailProtection	Present	Yes	

[32] This field contains the corporate e-mail address of the registered doctor, for notification purposes.

[33] This field links with the CGCOM re-certification and validation system, permitting the efficient recovery of additional information. Certain information is included, although this may be redundant, in order to have complete information about the user in a single consultation against the certificate.

Field	Contents	Compulsory	Critical
2.8.2. clientAuth	Present	Yes	
2.9. cRLDistributionPoint		Yes	
2.9.1. distributionPoint	"http://crl1.cgcom.es/crl/ec-cgcom.crl"	Yes	
2.9.2. distributionPoint	"http://crl2.cgcom.es/crl/ec-cgcom.crl"	Yes	
2.10. Authority Info Access		Yes	
2.10.1. Access Method		Yes	
2.10.2. Access Location	http://pki-ocsp.verisign.com	Yes	
2.11. NetscapeCertType	"SSL client", "S/MIME"	Yes	
2.12. Subject Directory Attributes (2.5.29.9)		Yes	
2.12.1. Country of Citizenship	Country of nationality	Yes	
2.12.2. Country of Residence	Country of residence.	Yes	

4.5 Corporate certificate of legal entity on software for identification, signature and encipherment.

Field	Contents	Compulsory	Critical
1. Basic structure			
1.1. Version	"2"[34]	Yes	
1.2. Serial Number	Established automatically[35]	Yes	
1.3. Signature Algorithm	SHA-1 with RSA Signature	Yes	
1.4. Issuer Distinguished Name		Yes	
1.4.1. Country (C)	"ES"	Yes	
1.4.2. Organization (O)	"Organizacion Medica Colegial" [36]	Yes	
1.4.3. Organizational Unit (OU)	"Certification Entity" [37]	Yes	
1.4.4. Organizational Unit (OU)	"Class 2 Managed PKI Individual Subscriber CA"	Yes	
1.4.5. Organizational Unit (OU)	"VeriSign Trust Network"	Yes	
1.4.6. Common Name (CN)	"OMC"	Yes	
1.5. Validity	3 years.	Yes	
1.5.1. Not Before	Start date of validity	Yes	
1.5.2. Not After	Date of expiry	Yes	
1.6. Subject		Yes	
1.6.1. Country (C)	"ES"[38]	Yes	

[34] The literal "2" corresponds to version 3.

[35] It should not exceed 32 hexadecimal characters in hexadecimal notation.

[36] The text is included without accents.

[37] The text is included without accents.

[38] The field "country" will always be Spain.

Field	Contents	Compulsory	Critical
1.6.2. Organization (O)	Professional association or legal entity in the health area	Yes	
1.6.3. Organizational Unit (OU)	"Conditions of use at https://www.cgcom.es/CertJurSoft (c)11"	Yes	
1.6.4. Organizational Unit (OU)	"Use is subject to terms at https://www.verisign.com/rpa (c)99"	Yes	
1.6.5. Surname	Custodian's surnames	Yes	
1.6.6. Given Name	Name of custodian	Yes	
1.6.7. 1.3.6.1.4.1.18838.1.1	National ID Document (DNI)/ Foreigner's ID Number (NIE)[39]	Yes	
1.6.8. Serial Number	Tax ID Number (NIF) of the entity[40]	Yes	
1.6.9. Common Name (CN)	Professional association or legal entity in the health area	Yes	
1.6.10. Email (E)	E-mail Address	Yes	
1.7. Subject Public Key Info	2048-Bit Public key encoded in accordance with RFC2459 & PKCS#1	Yes	
2. Extensions			
2.1. Authority Key Identifier	Present	Yes	
2.1.1. Authority Key Identifier			
2.1.2. AuthorityCertIssuer			
2.1.3. AuthorityCertSerialNumber			

[39] The field "serial number" should include the National ID Document (DNI) or the Foreigner's ID Number (NIE) of the worker, in order to admit the certificate for performing formalities with the Spanish Administrations.

[40] In accordance with the tax regulations, this field should show the Tax ID Number (NIF) of the legal entity.

Field	Contents	Compulsory	Critical
2.2. Subject Key Identifier	Present	Yes	
2.3. Key Usage		Yes	Yes
2.3.1. Digital Signature	Selected. "1"	Yes	
2.3.2. Non Repudiation	Selected. "1"	Yes	
2.3.3. Key Encipherment	Selected. "1"	Yes	
2.3.4. Data Encipherment	Selected. "1"	Yes	
2.3.5. Key Agreement	Not selected. "0"		
2.3.6. Key Certificate Signature	Not selected. "0"		
2.3.7. CRL Signature	Not selected. "0"		
2.4. Qualified Certificate Statements		Yes	
2.4.1. qCCompliance (0.4.0.1862.1.1)		Yes	
2.4.2. QcEuRetentionPeriod (0.4.0.1862.1.3)	15	Yes	
2.5. Certificate Policies		Yes	
2.5.1. Policy Identifier	1.3.6.1.4.1.26852.1.1.5	Yes	
2.5.2. Policy Qualifier ID		Yes	
2.5.2.1. CPS Pointer	"https://www.cgcom.es/CertJurSoft"	Yes	
2.5.2.2. User Notice	"Corporate certificate of advanced electronic signature and legal entity encipherment on software. Conditions of use at https://www.cgcom.es/CertJurSoft"	Yes	
2.5.3. Policy Identifier	OID of class 2 policy of VeriSign	Yes	
2.5.4. Policy Qualifier ID		Yes	
2.5.4.1. CPS Pointer	Reference to VeriSign RPA	Yes	

Field	Contents	Compulsory	Critical
2.5.4.2. User Notice	Notice of VeriSign user	Yes	
2.6. Subject Alternative Names		Yes	
2.6.1. rfc822Name	Corporate e-mail of custodian[41]	Yes	
2.6.2. directoryName[42]		Yes	
2.6.2.1. CGCOM.2.1	IdAssociation / IdEntity	Yes	
2.6.2.2. CGCOM.2.2	Professional association / Legal entity in the health area	Yes	
2.7. Issuer Alternative Name		Yes	
2.7.1. rfc822Name	"certificacion@cgcom.es"	Yes	
2.7.2. directoryName		Yes	
2.7.2.1. Organization (O)	"Consejo General de Colegios de Medicos"	Yes	
2.7.2.2. SerialNumber	"Q2866017C"	Yes	
2.7.2.3. Location (L)	"Plaza de las Cortes 11"	Yes	
2.7.2.4. Postal Code	"28014"	Yes	
2.7.2.5. State Or Province Name	"Madrid"	Yes	
2.7.2.6. Country (C)	ES	Yes	
2.8. Extended Key Usage		Yes	
2.8.1. emailProtection	Present	Yes	
2.8.2. clientAuth	Present	Yes	
2.9. cRLDistributionPoint		Yes	
2.9.1. distributionPoint	"http://crl1.cgcom.es/crl/ec-cgcom.crl"	Yes	

[41] This field contains the corporate e-mail address of the registered doctor, for notification purposes.

[42] This field links with the CGCOM re-certification and validation system, permitting the efficient recovery of additional information. Certain information is included, although this may be redundant, in order to have complete information about the user in a single consultation against the certificate.

Field	Contents	Compulsory	Critical
2.9.2. distributionPoint	"http://crl2.cgcom.es/crl/ec-cgcom.crl"	Yes	
2.10. Authority Info Access		Yes	
2.10.1. Access Method		Yes	
2.10.2. Access Location	http://pki-ocsp.verisign.com	Yes	
2.11. NetscapeCertType	"SSL client", "S/MIME"	Yes	
2.12. Subject Directory Attributes (2.5.29.9)		Yes	
2.12.1. Country of Citizenship	Country of nationality	Yes	
2.12.2. Country of Residence	Country of residence.	Yes	

5. Corporate certificates (as from 2013)

5.1 Corporate certificate of registered doctor (individual) for identification.

Field	Contents	Compulsory	Critical
1. Basic structure			
1.1. Version	"2"[43]	Yes	
1.2. Serial Number	Established automatically[44]	Yes	
1.3. Signature Algorithm	SHA-1 with RSA Signature / SHA-256 with RSA Signature	Yes	
1.4. Issuer Distinguished Name		Yes	
1.4.1. Country (C)	"ES"	Yes	
1.4.2. Organization (O)	"Organizacion Medica Colegial"[45]	Yes	
1.4.3. Organizational Unit (OU)	"Certification Entity" [46]	Yes	
1.4.4. Organizational Unit (OU)	"Class 2 Managed PKI Individual Subscriber CA"	Yes	
1.4.5. Organizational Unit (OU)	"VeriSign Trust Network"	Yes	
1.4.6. Common Name (CN)	"OMC"	Yes	
1.5. Validity	3 years.	Yes	
1.5.1. Not Before	Start date of validity	Yes	

[43] The literal "2" corresponds to version 3.

[44] It should not exceed 32 hexadecimal characters in hexadecimal notation.

[45] The text is included without accents.

[46] The text is included without accents.

Field	Contents	Compulsory	Critical
1.5.2. Not After	Date of expiry	Yes	
1.6. Subject		Yes	
1.6.1. Country (C)	"ES"[47]	Yes	
1.6.2. Organization (O)	Professional association	Yes	
1.6.3. Organizational Unit (OU)	"Conditions of use on https://www.cgcom.es/CertCol (c)06"	Yes	
1.6.4. Organizational Unit (OU)	"Use is subject to terms at https://www.verisign.com/rpa (c)99"	Yes	
1.6.5. Surname	Surnames	Yes	
1.6.6. Given Name	Given name	Yes	
1.6.7. Title	"Registered doctor"	Yes	
1.6.8. Serial Number	National ID Document (DNI)/ Foreigner's ID Number (NIE)[48]	Yes	
1.6.9. Common Name (CN)	"(Registered Doctor)" + Given name and surnames + "-" + Registered Doctor's number + "(AUTHENTICATION)"	Yes	
1.6.10. Email (E)	E-mail Address	Yes	
1.7. Subject Public Key Info	2048-Bit Public key encoded in accordance with RFC2459 & PKCS#1	Yes	
2. Extensions			

[47] The field "country" will always be Spain, since the certificate shows the relation between a registered doctor and a Spanish professional association, regardless of the nationality of the registered doctor. This arises from the corporate nature of the certificate, whose subscriber is the association, and the registered doctor, the person authorised for its use.

[48] The field "serial number" should include the National ID Document (DNI) or the Foreigner's ID Number (NIE) of the registered doctor, in order to admit the certificate for performing formalities with the Spanish Administrations.

Field	Contents	Compulsory	Critical
2.1. Authority Key Identifier	Present	Yes	
2.1.1. Authority Key Identifier			
2.1.2. AuthorityCertIssuer			
2.1.3. AuthorityCertSerialNumber			
2.2. Subject Key Identifier	Present	Yes	
2.3. Key Usage		Yes	Yes
2.3.1. Digital Signature	Selected. “1”	Yes	
2.3.2. Content commitment	Not selected. “0”		
2.3.3. Key Encipherment	Not selected. “0”		
2.3.4. Data Encipherment	Not selected. “0”		
2.3.5. Key Agreement	Not selected. “0”		
2.3.6. Key Certificate Signature	Not selected. “0”		
2.3.7. CRL Signature	Not selected. “0”		
2.4. Qualified Certificate Statements		Yes	
2.4.1. qCCompliance (0.4.0.1862.1.1)		Yes	
2.4.2. QcEuRetentionPeriod (0.4.0.1862.1.3)	15	Yes	
2.4.3. QcSSCD (0.4.0.1862.1.4)		Yes	
2.5. Certificate Policies		Yes	
2.5.1. Policy Identifier	1.3.6.1.4.1.26852.1.1.1.1	Yes	
2.5.2. Policy Qualifier ID		Yes	
2.5.2.1. CPS Pointer	“https://www.cgcom.es/CertCol”	Yes	
2.5.2.2. User Notice	“Corporate identification certificate of registered doctor. “Conditions of use at	Yes	

Field	Contents	Compulsory	Critical
	https://www.cgcom.es/CertCol"		
2.5.3. Policy Identifier	OID of class 2 policy of VeriSign	Yes	
2.5.4. Policy Qualifier ID		Yes	
2.5.4.1. CPS Pointer	Reference to VeriSign RPA	Yes	
2.5.4.2. User Notice	Notice of VeriSign user	Yes	
2.6. Subject Alternative Names		Yes	
2.6.1. rfc822Name	Corporate e-mail of registered doctor[49]	Yes	
2.6.2. directoryName[50]		Yes	
2.6.2.1. CGCOM.2.1	IdAssociation	Yes	
2.6.2.2. CGCOM.2.2	Professional association	Yes	
2.6.2.3. CGCOM.2.3	IdAssociation	Yes	
2.6.2.4. CGCOM.2.4	Given name and surname of registered doctor	Yes	
2.7. Issuer Alternative Name		Yes	
2.7.1. rfc822Name	"certificacion@cgcom.es"	Yes	
2.7.2. directoryName		Yes	
2.7.2.1. Organization (O)	"Consejo General de Colegios de Medicos"	Yes	
2.7.2.2. SerialNumber	"Q2866017C"	Yes	
2.7.2.3. Location (L)	"Plaza de las Cortes 11"	Yes	
2.7.2.4. Postal Code	"28014"	Yes	
2.7.2.5. State Or Province Name	"Madrid"	Yes	

[49] This field contains the corporate e-mail address of the registered doctor, for notification purposes.

[50] This field links with the CGCOM re-certification and validation system, permitting the efficient recovery of additional information. Certain information is included, although this may be redundant, in order to have complete information about the user in a single consultation against the certificate.

Field	Contents	Compulsory	Critical
2.7.2.6. Country (C)	ES	Yes	
2.8. Extended Key Usage		Yes	
2.8.1. clientAuth	Present	Yes	
2.9. cRLDistributionPoint		Yes	
2.9.1. distributionPoint	"http://crl1.cgcom.es/crl/ec-cgcom.crl"	Yes	
2.9.2. distributionPoint	"http://crl2.cgcom.es/crl/ec-cgcom.crl"	Yes	
2.10. Authority Info Access		Yes	
2.10.1. Access Method		Yes	
2.10.2. Access Location	http://pki-ocsp.verisign.com	Yes	
2.11. NetscapeCertType	"SSL client", "S/MIME"	Yes	
2.12. Subject Directory Attributes (2.5.29.9)		Yes	
2.12.1. Country of Citizenship	Country of nationality	Yes	
2.12.2. Country of Residence	Country of residence.	Yes	

5.2 Corporate certificate of registered doctor (individual) for signature.

Field	Contents	Compulsory	Critical
1. Basic structure			
1.1. Version	"2"[51]	Yes	
1.2. Serial Number	Established automatically[52]	Yes	
1.3. Signature Algorithm	SHA-1 with RSA Signature / SHA-256 with RSA Signature	Yes	
1.4. Issuer Distinguished Name		Yes	
1.4.1. Country (C)	"ES"	Yes	
1.4.2. Organization (O)	"Organizacion Medica Colegial"[53]	Yes	
1.4.3. Organizational Unit (OU)	"Certification Entity" [54]	Yes	
1.4.4. Organizational Unit (OU)	"Class 2 Managed PKI Individual Subscriber CA"	Yes	
1.4.5. Organizational Unit (OU)	"VeriSign Trust Network"	Yes	
1.4.6. Common Name (CN)	"OMC"	Yes	
1.5. Validity	3 years.	Yes	
1.5.1. Not Before	Start date of validity	Yes	
1.5.2. Not After	Date of expiry	Yes	
1.6. Subject		Yes	
1.6.1. Country (C)	"ES"[55]	Yes	

[51] The literal "2" corresponds to version 3.

[52] It should not exceed 32 hexadecimal characters in hexadecimal notation.

[53] The text is included without accents.

[54] The text is included without accents.

Field	Contents	Compulsory	Critical
1.6.2. Organization (O)	Professional association	Yes	
1.6.3. Organizational Unit (OU)	"Conditions of use on https://www.cgcom.es/CertCol (c)06"	Yes	
1.6.4. Organizational Unit (OU)	"Use is subject to terms at https://www.verisign.com/rpa (c)99"	Yes	
1.6.5. Surname	Surnames	Yes	
1.6.6. Given Name	Given name	Yes	
1.6.7. Title	"Registered doctor"	Yes	
1.6.8. Serial Number	National ID Document (DNI)/ Foreigner's ID Number (NIE)[56]	Yes	
1.6.9. Common Name (CN)	"(Registered Doctor)" + Given name and surnames + "-" + Registered Doctor's number + "(SIGNATURE)"	Yes	
1.6.10. Email (E)	E-mail Address	Yes	
1.7. Subject Public Key Info	2048-Bit Public key encoded in accordance with RFC2459 & PKCS#1	Yes	
2. Extensions			
2.1. Authority Key Identifier	Present	Yes	
2.1.1. Authority Key Identifier			
2.1.2. AuthorityCertIssuer			

[55] The field "country" will always be Spain, since the certificate shows the relation between a registered doctor and a Spanish professional association, regardless of the nationality of the registered doctor. This arises from the corporate nature of the certificate, whose subscriber is the association, and the registered doctor, the person authorised for its use.

[56] The field "serial number" should include the National ID Document (DNI) or the Foreigner's ID Number (NIE) of the registered doctor, in order to admit the certificate for performing formalities with the Spanish Administrations.

Field	Contents	Compulsory	Critical
2.1.3. AuthorityCertSerialNumber			
2.2. Subject Key Identifier	Present	Yes	
2.3. Key Usage		Yes	Yes
2.3.1. Digital Signature	Not selected. “0”		
2.3.2. Content commitment	Selected. “1”	Yes	
2.3.3. Key Encipherment	Not selected. “0”		
2.3.4. Data Encipherment	Not selected. “0”		
2.3.5. Key Agreement	Not selected. “0”		
2.3.6. Key Certificate Signature	Not selected. “0”		
2.3.7. CRL Signature	Not selected. “0”		
2.4. Qualified Certificate Statements		Yes	
2.4.1. qCCompliance (0.4.0.1862.1.1)		Yes	
2.4.2. QcEuRetentionPeriod (0.4.0.1862.1.3)	15	Yes	
2.4.3. QcSSCD (0.4.0.1862.1.4)		Yes	
2.5. Certificate Policies		Yes	
2.5.1. Policy Identifier	1.3.6.1.4.1.26852.1.1.1.2	Yes	
2.5.2. Policy Qualifier ID		Yes	
2.5.2.1. CPS Pointer	“https://www.cgcom.es/CertCol”	Yes	
2.5.2.2. User Notice	“Corporate certificate of qualified electronic signature of registered doctor. Conditions of use at https://www.cgcom.es/CertCol”	Yes	
2.5.3. Policy Identifier	OID of class 2 policy of VeriSign	Yes	
2.5.4. Policy Qualifier ID		Yes	

Field	Contents	Compulsory	Critical
2.5.4.1. CPS Pointer	Reference to VeriSign RPA	Yes	
2.5.4.2. User Notice	Notice of VeriSign user	Yes	
2.6. Subject Alternative Names		Yes	
2.6.1. rfc822Name	Corporate e-mail of registered doctor[57]	Yes	
2.6.2. directoryName[58]		Yes	
2.6.2.1. CGCOM.2.1	IdAssociation	Yes	
2.6.2.2. CGCOM.2.2	Professional association	Yes	
2.6.2.3. CGCOM.2.3	IdAssociation	Yes	
2.6.2.4. CGCOM.2.4	Given name and surname of registered doctor	Yes	
2.7. Issuer Alternative Name		Yes	
2.7.1. rfc822Name	"certificacion@cgcom.es"	Yes	
2.7.2. directoryName		Yes	
2.7.2.1. Organization (O)	"Consejo General de Colegios de Medicos"	Yes	
2.7.2.2. SerialNumber	"Q2866017C"	Yes	
2.7.2.3. Location (L)	"Plaza de las Cortes 11"	Yes	
2.7.2.4. Postal Code	"28014"	Yes	
2.7.2.5. State Or Province Name	"Madrid"	Yes	
2.7.2.6. Country (C)	ES	Yes	
2.8. Extended Key Usage		Yes	
2.8.1. emailProtection	Present	Yes	

[57] This field contains the corporate e-mail address of the registered doctor, for notification purposes.

[58] This field links with the CGCOM re-certification and validation system, permitting the efficient recovery of additional information. Certain information is included, although this may be redundant, in order to have complete information about the user in a single consultation against the certificate.

Field	Contents	Compulsory	Critical
2.9. cRLDistributionPoint		Yes	
2.9.1. distributionPoint	"http://crl1.cgcom.es/crl/ec-cgcom.crl"	Yes	
2.9.2. distributionPoint	"http://crl2.cgcom.es/crl/ec-cgcom.crl"	Yes	
2.10. Authority Info Access		Yes	
2.10.1. Access Method		Yes	
2.10.2. Access Location	http://pki-ocsp.verisign.com	Yes	
2.11. NetscapeCertType	"SSL client", "S/MIME"	Yes	
2.12. Subject Directory Attributes (2.5.29.9)		Yes	
2.12.1. Country of Citizenship	Country of nationality	Yes	
2.12.2. Country of Residence	Country of residence.	Yes	

5.3 Certificate of encipherment on card for registered doctor

Field	Contents	Compulsory	Critical
1. Basic structure			
1.1. Version	"2"[59]	Yes	
1.2. Serial Number	Established automatically[60]	Yes	
1.3. Signature Algorithm	SHA-1 with RSA Signature / SHA-256 with RSA Signature	Yes	
1.4. Issuer Distinguished Name		Yes	
1.4.1. Country (C)	"ES"	Yes	
1.4.2. Organization (O)	"Organizacion Medica Colegial" [61]	Yes	
1.4.3. Organizational Unit (OU)	"Certification Entity" [62]	Yes	
1.4.4. Organizational Unit (OU)	"Class 2 Managed PKI Individual Subscriber CA"	Yes	
1.4.5. Organizational Unit (OU)	"VeriSign Trust Network"	Yes	
1.4.6. Common Name (CN)	"OMC"	Yes	
1.5. Validity	3 years.	Yes	
1.5.1. Not Before	Start date of validity	Yes	
1.5.2. Not After	Date of expiry	Yes	
1.6. Subject		Yes	

[59] The literal "2" corresponds to version 3.

[60] It should not exceed 32 hexadecimal characters in hexadecimal notation.

[61] The text is included without accents.

[62] The text is included without accents.

Field	Contents	Compulsory	Critical
1.6.1. Country (C)	"ES"[63]	Yes	
1.6.2. Organization (O)	Professional association	Yes	
1.6.3. Organizational Unit (OU)	"Conditions of use on https://www.cgcom.es/CertCol (c)06"	Yes	
1.6.4. Organizational Unit (OU)	"Use is subject to terms at https://www.verisign.com/rpa (c)99"	Yes	
1.6.5. Surname	Surnames	Yes	
1.6.6. Given Name	Given name	Yes	
1.6.7. Title	"Registered doctor"	Yes	
1.6.8. Serial Number	National ID Document (DNI)/ Foreigner's ID Number (NIE)[64]	Yes	
1.6.9. Common Name (CN)	"(Registered Doctor)" + Given name and surnames + "-" + Registered Doctor's number + "(CIPHERED)"	Yes	
1.6.10. Email (E)	E-mail Address	Yes	
1.7. Subject Public Key Info	2048-Bit Public key encoded in accordance with RFC2459 & PKCS#1	Yes	
2. Extensions			
2.1. Authority Key Identifier	Present	Yes	
2.1.1. Authority Key Identifier			
2.1.2. AuthorityCertIssuer			
2.1.3. AuthorityCertSerialNumber			

[63] The field "country" will always be Spain.

[64] The field "serial number" should include the National ID Document (DNI) or the Foreigner's ID Number (NIE) of the registered doctor, in order to admit the certificate for performing formalities with the Spanish Administrations.

Field	Contents	Compulsory	Critical
2.2. Subject Key Identifier	Present	Yes	
2.3. Key Usage		Yes	Yes
2.3.1. Digital Signature	Not selected. "0"		
2.3.2. Content commitment	Not selected. "0"		
2.3.3. Key Encipherment	Selected. "1"	Yes	
2.3.4. Data Encipherment	Selected. "1"	Yes	
2.3.5. Key Agreement	Not selected. "0"		
2.3.6. Key Certificate Signature	Not selected. "0"		
2.3.7. CRL Signature	Not selected. "0"		
2.4. Qualified Certificate Statements		Yes	
2.4.1. qCCompliance (0.4.0.1862.1.1)		Yes	
2.4.2. QcEuRetentionPeriod (0.4.0.1862.1.3)	15	Yes	
2.4.3. QcSSCD (0.4.0.1862.1.4)		Yes	
2.5. Certificate Policies		Yes	
2.5.1. Policy Identifier	1.3.6.1.4.1.26852.1.1.1.3	Yes	
2.5.2. Policy Qualifier ID		Yes	
2.5.2.1. CPS Pointer	"https://www.cgcom.es/CertCol"	Yes	
2.5.2.2. User Notice	"Corporate Certificate of encipherment of registered doctor. Conditions of use at https://www.cgcom.es/CertCol"	Yes	
2.5.3. Policy Identifier	OID of class 2 policy of VeriSign	Yes	
2.5.4. Policy Qualifier ID		Yes	
2.5.4.1. CPS Pointer	Reference to VeriSign RPA	Yes	

Field	Contents	Compulsory	Critical
2.5.4.2. User Notice	Notice of VeriSign user	Yes	
2.6. Subject Alternative Names		Yes	
2.6.1. rfc822Name	Corporate e-mail[65]	Yes	
2.6.2. directoryName[66]		Yes	
2.6.2.1. CGCOM.2.1	IdAssociation / IdEntity	Yes	
2.6.2.2. CGCOM.2.2	Professional association / Legal entity in the health area	Yes	
2.6.2.3. CGCOM.2.3	IdAssociation	Yes	
2.6.2.4. CGCOM.2.4	Given name and surname of registered doctor	Yes	
2.7. Issuer Alternative Name		Yes	
2.7.1. rfc822Name	"certificacion@cgcom.es"	Yes	
2.7.2. directoryName		Yes	
2.7.2.1. Organization (O)	"Consejo General de Colegios de Medicos"	Yes	
2.7.2.2. SerialNumber	"Q2866017C"	Yes	
2.7.2.3. Location (L)	"Plaza de las Cortes 11"	Yes	
2.7.2.4. Postal Code	"28014"	Yes	
2.7.2.5. State Or Province Name	"Madrid"	Yes	
2.7.2.6. Country (C)	ES	Yes	
2.8. Extended Key Usage		Yes	
2.8.1. emailProtection	Present	Yes	
2.9. cRLDistributionPoint		Yes	

[65] This field contains the corporate e-mail address of the registered doctor, for notification purposes.

[66] This field links with the CGCOM re-certification and validation system, permitting the efficient recovery of additional information. Certain information is included, although this may be redundant, in order to have complete information about the user in a single consultation against the certificate.

Field	Contents	Compulsory	Critical
2.9.1. distributionPoint	"http://crl1.cgcom.es/crl/ec-cgcom.crl"	Yes	
2.9.2. distributionPoint	"http://crl2.cgcom.es/crl/ec-cgcom.crl"	Yes	
2.10. Authority Info Access		Yes	
2.10.1. Access Method		Yes	
2.10.2. Access Location	http://pki-ocsp.verisign.com	Yes	
2.11. NetscapeCertType	"SSL client", "S/MIME"	Yes	
2.12. Subject Directory Attributes (2.5.29.9)		Yes	
2.12.1. Country of Citizenship	Country of nationality	Yes	
2.12.2. Country of Residence	Country of residence.	Yes	

5.4 Corporate certificate of registered body (individual) for identification.

Field	Contents	Compulsory	Critical
1. Basic structure			
1.1. Version	"2"[67]	Yes	
1.2. Serial Number	Established automatically[68]	Yes	
1.3. Signature Algorithm	SHA-1 with RSA Signature / SHA-256 with RSA Signature	Yes	
1.4. Issuer Distinguished Name		Yes	
1.4.1. Country (C)	"ES"	Yes	
1.4.2. Organization (O)	"Organizacion Medica Colegial"[69]	Yes	
1.4.3. Organizational Unit (OU)	"Certification Entity" [70]	Yes	
1.4.4. Organizational Unit (OU)	"Class 2 Managed PKI Individual Subscriber CA"	Yes	
1.4.5. Organizational Unit (OU)	"VeriSign Trust Network"	Yes	
1.4.6. Common Name (CN)	"OMC"	Yes	
1.5. Validity	3 years.	Yes	
1.5.1. Not Before	Start date of validity	Yes	
1.5.2. Not After	Date of expiry	Yes	
1.6. Subject		Yes	
1.6.1. Country (C)	"ES"[71]	Yes	

[67] The literal "2" corresponds to version 3.

[68] It should not exceed 32 hexadecimal characters in hexadecimal notation.

[69] The text is included without accents.

[70] The text is included without accents.

Field	Contents	Compulsory	Critical
1.6.2. Organization (O)	Professional association	Yes	
1.6.3. Organizational Unit (OU)	"Conditions of use on https://www.cgcom.es/CertOrg (c)06"	Yes	
1.6.4. Organizational Unit (OU)	"Use is subject to terms at https://www.verisign.com/rpa (c)99"	Yes	
1.6.5. Surname	Surnames	Yes	
1.6.6. Given Name	Given name	Yes	
1.6.7. Title	Body / office	Yes	
1.6.8. Serial Number	National ID Document (DNI)/ Foreigner's ID Number (NIE)[72]	Yes	
1.6.9. Common Name (CN)	Given name and surnames + "- "+ "(AUTENTICATION)"	Yes	
1.6.10. Email (E)	E-mail Address	Yes	
1.7. Subject Public Key Info	2048-Bit Public key encoded in accordance with RFC2459 & PKCS#1	Yes	
2. Extensions			
2.1. Authority Key Identifier	Present	Yes	
2.1.1. Authority Key Identifier			
2.1.2. AuthorityCertIssuer			
2.1.3. AuthorityCertSerialNumber			
2.2. Subject Key Identifier	Present	Yes	

[71] The field "country" will always be Spain, since the certificate shows the relation between a person that holds a body or office and a Spanish professional association, regardless of the nationality of that person.

[72] The field "serial number" should include the National ID Document (DNI) or the Foreigner's ID Number (NIE) of the body, in order to admit the certificate for performing formalities with the Spanish Administrations.

Field	Contents	Compulsory	Critical
2.3. Key Usage		Yes	Yes
2.3.1. Digital Signature	Selected. "1"	Yes	
2.3.2. Content commitment	Not selected. "0"		
2.3.3. Key Encipherment	Not selected. "0"		
2.3.4. Data Encipherment	Not selected. "0"		
2.3.5. Key Agreement	Not selected. "0"		
2.3.6. Key Certificate Signature	Not selected. "0"		
2.3.7. CRL Signature	Not selected. "0"		
2.4. Qualified Certificate Statements		Yes	
2.4.1. qCCompliance (0.4.0.1862.1.1)		Yes	
2.4.2. QcEuRetentionPeriod (0.4.0.1862.1.3)	15	Yes	
2.4.3. QcSSCD (0.4.0.1862.1.4)		Yes	
2.5. Certificate Policies		Yes	
2.5.1. Policy Identifier	1.3.6.1.4.1.26852.1.1.4.1	Yes	
2.5.2. Policy Qualifier ID		Yes	
2.5.2.1. CPS Pointer	"https://www.cgcom.es/CerOrg"	Yes	
2.5.2.2. User Notice	"Corporate identification certificate of registered body. Conditions of use at https://www.cgcom.es/CertOrg"	Yes	
2.5.3. Policy Identifier	OID of class 2 policy of VeriSign	Yes	
2.5.4. Policy Qualifier ID		Yes	
2.5.4.1. CPS Pointer	Reference to VeriSign RPA	Yes	
2.5.4.2. User Notice	Notice of VeriSign user	Yes	

Field	Contents	Compulsory	Critical
2.6. Subject Alternative Names		Yes	
2.6.1. rfc822Name	Corporate e-mail of registered body[73]	Yes	
2.6.2. directoryName[74]		Yes	
2.6.2.1. CGCOM.2.1	IdAssociation	Yes	
2.6.2.2. CGCOM.2.2	Professional association	Yes	
2.6.2.3. CGCOM.2.5	IdOBody	Yes	
2.6.2.4. CGCOM.2.6	Description of the registered body	Yes	
2.7. Issuer Alternative Name		Yes	
2.7.1. rfc822Name	"certificacion@cgcom.es"	Yes	
2.12.3. directoryName		Yes	
2.12.3.1. Organization (O)	"Consejo General de Colegios de Medicos"	Yes	
2.12.3.2. SerialNumber	"Q2866017C"	Yes	
2.12.3.3. Location (L)	"Plaza de las Cortes 11"	Yes	
2.12.3.4. Postal Code	"28014"	Yes	
2.12.3.5. State Or Province Name	"Madrid"	Yes	
2.12.3.6. Country (C)	ES	Yes	
2.8. Extended Key Usage		Yes	
2.8.1. clientAuth	Present	Yes	
2.9. cRLDistributionPoint		Yes	

[73] This field contains the corporate e-mail address of the body, for notification purposes.

[74] This field links with the CGCOM re-certification and validation system, permitting the efficient recovery of additional information. Certain information is included, although this may be redundant, in order to have complete information about the user in a single consultation against the certificate.

Field	Contents	Compulsory	Critical
2.9.1. distributionPoint	"http://crl1.cgcom.es/crl/ec-cgcom.crl"	Yes	
2.9.2. distributionPoint	"http://crl2.cgcom.es/crl/ec-cgcom.crl"	Yes	
2.10. Authority Info Access		Yes	
2.10.1. Access Method		Yes	
2.10.2. Access Location	http://pki-ocsp.verisign.com	Yes	
2.11. NetscapeCertType	"SSL client", "S/MIME"	Yes	
2.12. Subject Directory Attributes (2.5.29.9)		Yes	
2.12.1. Country of Citizenship	Country of nationality	Yes	
2.12.2. Country of Residence	Country of residence.	Yes	

5.5 Corporate certificate of registered body (individual) for signature.

Field	Contents	Compulsory	Critical
1. Basic structure			
1.1. Version	"2"[75]	Yes	
1.2. Serial Number	Established automatically[76]	Yes	
1.3. Signature Algorithm	SHA-1 with RSA Signature / SHA-256 with RSA Signature	Yes	
1.4. Issuer Distinguished Name		Yes	
1.4.1. Country (C)	"ES"	Yes	
1.4.2. Organization (O)	"Organizacion Medica Colegial"[77]	Yes	
1.4.3. Organizational Unit (OU)	"Certification Entity" [78]	Yes	
1.4.4. Organizational Unit (OU)	"Class 2 Managed PKI Individual Subscriber CA"	Yes	
1.4.5. Organizational Unit (OU)	"VeriSign Trust Network"	Yes	
1.4.6. Common Name (CN)	"OMC"	Yes	
1.5. Validity	3 years.	Yes	
1.5.1. Not Before	Start date of validity	Yes	
1.5.2. Not After	Date of expiry	Yes	
1.6. Subject		Yes	
1.6.1. Country (C)	"ES"[79]	Yes	

[75] The literal "2" corresponds to version 3.

[76] It should not exceed 32 hexadecimal characters in hexadecimal notation.

[77] The text is included without accents.

[78] The text is included without accents.

Field	Contents	Compulsory	Critical
1.6.2. Organization (O)	Professional association	Yes	
1.6.3. Organizational Unit (OU)	"Conditions of use on https://www.cgcom.es/CertOrg (c)06"	Yes	
1.6.4. Organizational Unit (OU)	"Use is subject to terms at https://www.verisign.com/rpa (c)99"	Yes	
1.6.5. Surname	Surnames	Yes	
1.6.6. Given Name	Given name	Yes	
1.6.7. Title	Body / office	Yes	
1.6.8. Serial Number	National ID Document (DNI)/ Foreigner's ID Number (NIE)[80]	Yes	
1.6.9. Common Name (CN)	Given name and surnames + "- "+ "(SIGNATURE)"	Yes	
1.6.10. Email (E)	E-mail Address	Yes	
1.7. Subject Public Key Info	2048-Bit Public key encoded in accordance with RFC2459 & PKCS#1	Yes	
2. Extensions			
2.1. Authority Key Identifier	Present	Yes	
2.1.1. Authority Key Identifier			
2.1.2. AuthorityCertIssuer			
2.1.3. AuthorityCertSerialNumber			
2.2. Subject Key Identifier	Present	Yes	

[79] The field "country" will always be Spain, since the certificate shows the relation between a person that holds a body or office and a Spanish professional association, regardless of the nationality of that person.

[80] The field "serial number" should include the National ID Document (DNI) or the Foreigner's ID Number (NIE) of the body, in order to admit the certificate for performing formalities with the Spanish Administrations.

Field	Contents	Compulsory	Critical
2.3. Key Usage		Yes	Yes
2.3.1. Digital Signature	Not selected. “0”		
2.3.2. Content commitment	Selected. “1”	Yes	
2.3.3. Key Encipherment	Not selected. “0”		
2.3.4. Data Encipherment	Not selected. “0”		
2.3.5. Key Agreement	Not selected. “0”		
2.3.6. Key Certificate Signature	Not selected. “0”		
2.3.7. CRL Signature	Not selected. “0”		
2.4. Qualified Certificate Statements		Yes	
2.4.1. qCCompliance (0.4.0.1862.1.1)		Yes	
2.4.2. QcEuRetentionPeriod (0.4.0.1862.1.3)	15	Yes	
2.4.3. QcSSCD (0.4.0.1862.1.4)		Yes	
2.5. Certificate Policies		Yes	
2.5.1. Policy Identifier	1.3.6.1.4.1.26852.1.1.4.2	Yes	
2.5.2. Policy Qualifier ID		Yes	
2.5.2.1. CPS Pointer	“https://www.cgcom.es/CerOrg”	Yes	
2.5.2.2. User Notice	“Corporate certificate of qualified electronic signature of registered body. Conditions of use at https://www.cgcom.es/CertOrg”	Yes	
2.5.3. Policy Identifier	OID of class 2 policy of VeriSign	Yes	
2.5.4. Policy Qualifier ID		Yes	
2.5.4.1. CPS Pointer	Reference to VeriSign RPA	Yes	
2.5.4.2. User Notice	Notice of VeriSign user	Yes	

Field	Contents	Compulsory	Critical
2.6. Subject Alternative Names		Yes	
2.6.1. rfc822Name	Corporate e-mail of registered body[81]	Yes	
2.6.2. directoryName[82]		Yes	
2.6.2.1. CGCOM.2.1	IdAssociation	Yes	
2.6.2.2. CGCOM.2.2	Professional association	Yes	
2.6.2.3. CGCOM.2.5	IdOBody	Yes	
2.6.2.4. CGCOM.2.6	Description of the registered body	Yes	
2.7. Issuer Alternative Name		Yes	
2.7.1. rfc822Name	"certificacion@cgcom.es"	Yes	
2.12.4. directoryName		Yes	
2.12.4.1. Organization (O)	"Consejo General de Colegios de Medicos"	Yes	
2.12.4.2. SerialNumber	"Q2866017C"	Yes	
2.12.4.3. Location (L)	"Plaza de las Cortes 11"	Yes	
2.12.4.4. Postal Code	"28014"	Yes	
2.12.4.5. State Or Province Name	"Madrid"	Yes	
2.12.4.6. Country (C)	ES	Yes	
2.8. Extended Key Usage		Yes	
2.8.1. emailProtection	Present	Yes	
2.9. cRLDistributionPoint		Yes	

[81] This field contains the corporate e-mail address of the body, for notification purposes.

[82] This field links with the CGCOM re-certification and validation system, permitting the efficient recovery of additional information. Certain information is included, although this may be redundant, in order to have complete information about the user in a single consultation against the certificate.

Field	Contents	Compulsory	Critical
2.9.1. distributionPoint	"http://crl1.cgcom.es/crl/ec-cgcom.crl"	Yes	
2.9.2. distributionPoint	"http://crl2.cgcom.es/crl/ec-cgcom.crl"	Yes	
2.10. Authority Info Access		Yes	
2.10.1. Access Method		Yes	
2.10.2. Access Location	http://pki-ocsp.verisign.com	Yes	
2.11. NetscapeCertType	"SSL client", "S/MIME"	Yes	
2.12. Subject Directory Attributes (2.5.29.9)		Yes	
2.12.1. Country of Citizenship	Country of nationality	Yes	
2.12.2. Country of Residence	Country of residence.	Yes	

5.6 Certificate of encipherment on card for registered body

Field	Contents	Compulsory	Critical
1. Basic structure			
1.1. Version	"2"[83]	Yes	
1.2. Serial Number	Established automatically[84]	Yes	
1.3. Signature Algorithm	SHA-1 with RSA Signature / SHA-256 with RSA Signature	Yes	
1.4. Issuer Distinguished Name		Yes	
1.4.1. Country (C)	"ES"	Yes	
1.4.2. Organization (O)	"Organizacion Medica Colegial" [85]	Yes	
1.4.3. Organizational Unit (OU)	"Certification Entity" [86]	Yes	
1.4.4. Organizational Unit (OU)	"Class 2 Managed PKI Individual Subscriber CA"	Yes	
1.4.5. Organizational Unit (OU)	"VeriSign Trust Network"	Yes	
1.4.6. Common Name (CN)	"OMC"	Yes	
1.5. Validity	3 years.	Yes	
1.5.1. Not Before	Start date of validity	Yes	
1.5.2. Not After	Date of expiry	Yes	
1.6. Subject		Yes	
1.6.1. Country (C)	"ES"[87]	Yes	

[83] The literal "2" corresponds to version 3.

[84] It should not exceed 32 hexadecimal characters in hexadecimal notation.

[85] The text is included without accents.

[86] The text is included without accents.

Field	Contents	Compulsory	Critical
1.6.2. Organization (O)	Professional association	Yes	
1.6.3. Organizational Unit (OU)	"Conditions of use on https://www.cgcom.es/CertOrg (c)06"	Yes	
1.6.4. Organizational Unit (OU)	"Use is subject to terms at https://www.verisign.com/rpa (c)99"	Yes	
1.6.5. Surname	Surnames	Yes	
1.6.6. Given Name	Given name	Yes	
1.6.7. Title	Body / office	Yes	
1.6.8. Serial Number	National ID Document (DNI)/ Foreigner's ID Number (NIE)[88]	Yes	
1.6.9. Common Name (CN)	Given name and surnames + "- "+ "(CIPHERED)"	Yes	
1.6.10. Email (E)	E-mail Address	Yes	
1.7. Subject Public Key Info	2048-Bit Public key encoded in accordance with RFC2459 & PKCS#1	Yes	
2. Extensions			
2.1. Authority Key Identifier	Present	Yes	
2.1.1. Authority Key Identifier			
2.1.2. AuthorityCertIssuer			
2.1.3. AuthorityCertSerialNumber			
2.2. Subject Key Identifier	Present	Yes	
2.3. Key Usage		Yes	Yes

[87] The field "country" will always be Spain.

[88] The field "serial number" should include the National ID Document (DNI) or the Foreigner's ID Number (NIE) of the body, in order to admit the certificate for performing formalities with the Spanish Administrations.

Field	Contents	Compulsory	Critical
2.3.1. Digital Signature	Not selected. "0"		
2.3.2. Content commitment	Not selected. "0"		
2.3.3. Key Encipherment	Selected. "1"	Yes	
2.3.4. Data Encipherment	Selected. "1"	Yes	
2.3.5. Key Agreement	Not selected. "0"		
2.3.6. Key Certificate Signature	Not selected. "0"		
2.3.7. CRL Signature	Not selected. "0"		
2.4. Qualified Certificate Statements		Yes	
2.4.1. qCCompliance (0.4.0.1862.1.1)		Yes	
2.4.2. QcEuRetentionPeriod (0.4.0.1862.1.3)	15	Yes	
2.4.3. QcSSCD		Yes	
2.5. Certificate Policies		Yes	
2.5.1. Policy Identifier	1.3.6.1.4.1.26852.1.1.4.3	Yes	
2.5.2. Policy Qualifier ID		Yes	
2.5.2.1. CPS Pointer	"https://www.cgcom.es/CerOrg"	Yes	
2.5.2.2. User Notice	"Corporate certificate of encipherment of registered body. Conditions of use at https://www.cgcom.es/CertOrg"	Yes	
2.5.3. Policy Identifier	OID of class 2 policy of VeriSign	Yes	
2.5.4. Policy Qualifier ID		Yes	
2.5.4.1. CPS Pointer	Reference to VeriSign RPA	Yes	
2.5.4.2. User Notice	Notice of VeriSign user	Yes	

Field	Contents	Compulsory	Critical
2.6. Subject Alternative Names		Yes	
2.6.1. rfc822Name	Corporate e-mail[89]	Yes	
2.6.2. directoryName[90]		Yes	
2.6.2.1. CGCOM.2.1	IdAssociation	Yes	
2.6.2.2. CGCOM.2.2	Professional association	Yes	
2.6.2.3. CGCOM.2.5	IdOBody	Yes	
2.6.2.4. CGCOM.2.6	Description of the registered body	Yes	
2.7. Issuer Alternative Name		Yes	
2.7.1. rfc822Name	"certificacion@cgcom.es"	Yes	
2.7.2. directoryName		Yes	
2.7.2.1. Organization (O)	"Consejo General de Colegios de Medicos"	Yes	
2.7.2.2. SerialNumber	"Q2866017C"	Yes	
2.7.2.3. Location (L)	"Plaza de las Cortes 11"	Yes	
2.7.2.4. Postal Code	"28014"	Yes	
2.7.2.5. State Or Province Name	"Madrid"	Yes	
2.7.2.6. Country (C)	ES	Yes	
2.8. Extended Key Usage		Yes	
2.8.1. emailProtection	Present	Yes	
2.9. cRLDistributionPoint		Yes	
2.9.1. distributionPoint	"http://crl1.cgcom.es/crl/ec-cgcom.crl"	Yes	

[89] This field contains the corporate e-mail address of the registered doctor, for notification purposes.

[90] This field links with the CGCOM re-certification and validation system, permitting the efficient recovery of additional information. Certain information is included, although this may be redundant, in order to have complete information about the user in a single consultation against the certificate.

Field	Contents	Compulsory	Critical
2.9.2. distributionPoint	"http://crl2.cgcom.es/crl/ec-cgcom.crl"	Yes	
2.10. Authority Info Access		Yes	
2.10.1. Access Method		Yes	
2.10.2. Access Location	http://pki-ocsp.verisign.com	Yes	
2.11. NetscapeCertType	"SSL client", "S/MIME"	Yes	
2.12. Subject Directory Attributes (2.5.29.9)		Yes	
2.12.1. Country of Citizenship	Country of nationality	Yes	
2.12.2. Country of Residence	Country of residence.	Yes	

5.7 Corporate certificate of administrative personnel (individual) for identification.

Field	Contents	Compulsory	Critical
1. Basic structure			
1.1. Version	"2"[91]	Yes	
1.2. Serial Number	Established automatically[92]	Yes	
1.3. Signature Algorithm	SHA-1 with RSA Signature / SHA-256 with RSA Signature	Yes	
1.4. Issuer Distinguished Name		Yes	
1.4.1. Country (C)	"ES"	Yes	
1.4.2. Organization (O)	"Organizacion Medica Colegial" [93]	Yes	
1.4.3. Organizational Unit (OU)	"Certification Entity" [94]	Yes	
1.4.4. Organizational Unit (OU)	"Class 2 Managed PKI Individual Subscriber CA"	Yes	
1.4.5. Organizational Unit (OU)	"VeriSign Trust Network"	Yes	
1.4.6. Common Name (CN)	"OMC"	Yes	
1.5. Validity	3 years.	Yes	
1.5.1. Not Before	Start date of validity	Yes	
1.5.2. Not After	Date of expiry	Yes	
1.6. Subject		Yes	
1.6.1. Country (C)	"ES"[95]	Yes	

[91] The literal "2" corresponds to version 3.

[92] It should not exceed 32 hexadecimal characters in hexadecimal notation.

[93] The text is included without accents.

[94] The text is included without accents.

Field	Contents	Compulsory	Critical
1.6.2. Organization (O)	Professional association or legal entity in the health area	Yes	
1.6.3. Organizational Unit (OU)	"Conditions of use on https://www.cgcom.es/CertAdmin (c)06"	Yes	
1.6.4. Organizational Unit (OU)	"Use is subject to terms at https://www.verisign.com/rpa (c)99"	Yes	
1.6.5. Surname	Surnames	Yes	
1.6.6. Given Name	Given name	Yes	
1.6.7. Title	"Administrative and service personnel"	Yes	
1.6.8. Serial Number	National ID Document (DNI)/ Foreigner's ID Number (NIE)[96]	Yes	
1.6.9. Common Name (CN)	Given name and surnames + "- "+ "(AUTENTICATION)"	Yes	
1.6.10. Email (E)	E-mail Address	Yes	
1.7. Subject Public Key Info	2048-Bit Public key encoded in accordance with RFC2459 & PKCS#1	Yes	
2. Extensions			
2.1. Authority Key Identifier	Present	Yes	
2.1.1. Authority Key Identifier			
2.1.2. AuthorityCertIssuer			
2.1.3. AuthorityCertSerialNumber			

[95] The field "country" will always be Spain, since the certificate shows the relation between a worker and a Spanish professional association, regardless of the nationality of the registered doctor.

[96] The field "serial number" should include the National ID Document (DNI) or the Foreigner's ID Number (NIE) of the worker, in order to admit the certificate for performing formalities with the Spanish Administrations.

Field	Contents	Compulsory	Critical
2.2. Subject Key Identifier	Present	Yes	
2.3. Key Usage		Yes	Yes
2.3.1. Digital Signature	Selected. "1"	Yes	
2.3.2. Content commitment	Not selected. "0"		
2.3.3. Key Encipherment	Not selected. "0"		
2.3.4. Data Encipherment	Not selected. "0"		
2.3.5. Key Agreement	Not selected. "0"		
2.3.6. Key Certificate Signature	Not selected. "0"		
2.3.7. CRL Signature	Not selected. "0"		
2.4. Qualified Certificate Statements		Yes	
2.4.1. qCCompliance (0.4.0.1862.1.1)		Yes	
2.4.2. QcEuRetentionPeriod (0.4.0.1862.1.3)	15	Yes	
2.4.3. QcSSCD (0.4.0.1862.1.4)		Yes	
2.5. Certificate Policies		Yes	
2.5.1. Policy Identifier	1.3.6.1.4.1.26852.1.1.2.1	Yes	
2.5.2. Policy Qualifier ID		Yes	
2.5.2.1. CPS Pointer	"https://www.cgcom.es/CertAdmin"	Yes	
2.5.2.2. User Notice	"Corporate certificate of identification of administrative personnel and services. Conditions of use at https://www.cgcom.es/CertAdmin"	Yes	
2.5.3. Policy Identifier	OID of class 2 policy of VeriSign	Yes	
2.5.4. Policy Qualifier ID		Yes	

Field	Contents	Compulsory	Critical
2.5.4.1. CPS Pointer	Reference to VeriSign RPA	Yes	
2.5.4.2. User Notice	Notice of VeriSign user	Yes	
2.6. Subject Alternative Names		Yes	
2.6.1. rfc822Name	Corporate e-mail of administrative personnel[97]	Yes	
2.6.2. directoryName[98]		Yes	
2.6.2.1. CGCOM.2.1	IdAssociation / IdEntity	Yes	
2.6.2.2. CGCOM.2.2	Professional association / Legal entity in the health area	Yes	
2.6.2.3. CGCOM.2.7	IdAdminPersonnel	Yes	
2.6.2.4. CGCOM.2.8	Given name and surnames of administrative personnel	Yes	
2.7. Issuer Alternative Name		Yes	
2.7.1. rfc822Name	"certificacion@cgcom.es"	Yes	
2.7.2. directoryName		Yes	
2.7.2.1. Organization (O)	"Consejo General de Colegios de Medicos"	Yes	
2.7.2.2. SerialNumber	"Q2866017C"	Yes	
2.7.2.3. Location (L)	"Plaza de las Cortes 11"	Yes	
2.7.2.4. Postal Code	"28014"	Yes	
2.7.2.5. State Or Province Name	"Madrid"	Yes	
2.7.2.6. Country (C)	ES	Yes	

[97] This field contains the corporate e-mail address of the administrative personnel and services, for notification purposes.

[98] This field links with the CGCOM re-certification and validation system, permitting the efficient recovery of additional information. Certain information is included, although this may be redundant, in order to have complete information about the user in a single consultation against the certificate.

Field	Contents	Compulsory	Critical
2.8. Extended Key Usage		Yes	
2.8.1. clientAuth	Present	Yes	
2.9. cRLDistributionPoint		Yes	
2.9.1. distributionPoint	"http://crl1.cgcom.es/crl/ec-cgcom.crl"	Yes	
2.9.2. distributionPoint	"http://crl2.cgcom.es/crl/ec-cgcom.crl"	Yes	
2.10. Authority Info Access		Yes	
2.10.1. Access Method		Yes	
2.10.2. Access Location	http://pki-ocsp.verisign.com	Yes	
2.11. NetscapeCertType	"SSL client", "S/MIME"	Yes	
2.12. Subject Directory Attributes (2.5.29.9)		Yes	
2.12.1. Country of Citizenship	Country of nationality	Yes	
2.12.2. Country of Residence	Country of residence.	Yes	

5.8 Corporate certificate of administrative personnel (individual) for signature.

Field	Contents	Compulsory	Critical
1. Basic structure			
1.1. Version	"2"[99]	Yes	
1.2. Serial Number	Established automatically[100]	Yes	
1.3. Signature Algorithm	SHA-1 with RSA Signature / SHA-256 with RSA Signature	Yes	
1.4. Issuer Distinguished Name		Yes	
1.4.1. Country (C)	"ES"	Yes	
1.4.2. Organization (O)	"Organizacion Medica Colegial" [101]	Yes	
1.4.3. Organizational Unit (OU)	"Certification Entity" [102]	Yes	
1.4.4. Organizational Unit (OU)	"Class 2 Managed PKI Individual Subscriber CA"	Yes	
1.4.5. Organizational Unit (OU)	"VeriSign Trust Network"	Yes	
1.4.6. Common Name (CN)	"OMC"	Yes	
1.5. Validity	3 years.	Yes	
1.5.1. Not Before	Start date of validity	Yes	
1.5.2. Not After	Date of expiry	Yes	
1.6. Subject		Yes	
1.6.1. Country (C)	"ES"[103]	Yes	

[99] The literal "2" corresponds to version 3.

[100] It should not exceed 32 hexadecimal characters in hexadecimal notation.

[101] The text is included without accents.

[102] The text is included without accents.

Field	Contents	Compulsory	Critical
1.6.2. Organization (O)	Professional association or legal entity in the health area	Yes	
1.6.3. Organizational Unit (OU)	"Conditions of use on https://www.cgcom.es/CertAdmin (c)06"	Yes	
1.6.4. Organizational Unit (OU)	"Use is subject to terms at https://www.verisign.com/rpa (c)99"	Yes	
1.6.5. Surname	Surnames	Yes	
1.6.6. Given Name	Given name	Yes	
1.6.7. Title	"Administrative and service personnel"	Yes	
1.6.8. Serial Number	National ID Document (DNI)/ Foreigner's ID Number (NIE)[104]	Yes	
1.6.9. Common Name (CN)	Given name and surnames + "- "+ "(SIGNATURE)"	Yes	
1.6.10. Email (E)	E-mail Address	Yes	
1.7. Subject Public Key Info	2048-Bit Public key encoded in accordance with RFC2459 & PKCS#1	Yes	
2. Extensions			
2.1. Authority Key Identifier	Present	Yes	
2.1.1. Authority Key Identifier			
2.1.2. AuthorityCertIssuer			
2.1.3. AuthorityCertSerialNumber			

[103] The field "country" will always be Spain, since the certificate shows the relation between a worker and a Spanish professional association, regardless of the nationality of the registered doctor.

[104] The field "serial number" should include the National ID Document (DNI) or the Foreigner's ID Number (NIE) of the worker, in order to admit the certificate for performing formalities with the Spanish Administrations.

Field	Contents	Compulsory	Critical
2.2. Subject Key Identifier	Present	Yes	
2.3. Key Usage		Yes	Yes
2.3.1. Digital Signature	Not selected. "0"		
2.3.2. Content commitment	Selected. "1"	Yes	
2.3.3. Key Encipherment	Not selected. "0"		
2.3.4. Data Encipherment	Not selected. "0"		
2.3.5. Key Agreement	Not selected. "0"		
2.3.6. Key Certificate Signature	Not selected. "0"		
2.3.7. CRL Signature	Not selected. "0"		
2.4. Qualified Certificate Statements		Yes	
2.4.1. qCCompliance (0.4.0.1862.1.1)		Yes	
2.4.2. QcEuRetentionPeriod (0.4.0.1862.1.3)	15	Yes	
2.4.3. QcSSCD (0.4.0.1862.1.4)		Yes	
2.5. Certificate Policies		Yes	
2.5.1. Policy Identifier	1.3.6.1.4.1.26852.1.1.2.2	Yes	
2.5.2. Policy Qualifier ID		Yes	
2.5.2.1. CPS Pointer	"https://www.cgcom.es/CertAdmin"	Yes	
2.5.2.2. User Notice	"Corporate certificate of qualified electronic signature of administrative personnel and services. Conditions of use at https://www.cgcom.es/CertAdmin"	Yes	
2.5.3. Policy Identifier	OID of class 2 policy of VeriSign	Yes	
2.5.4. Policy Qualifier ID		Yes	

Field	Contents	Compulsory	Critical
2.5.4.1. CPS Pointer	Reference to VeriSign RPA	Yes	
2.5.4.2. User Notice	Notice of VeriSign user	Yes	
2.6. Subject Alternative Names		Yes	
2.6.1. rfc822Name	Corporate e-mail of administrative personnel[105]	Yes	
2.6.2. directoryName[106]		Yes	
2.6.2.1. CGCOM.2.1	IdAssociation / IdEntity	Yes	
2.6.2.2. CGCOM.2.2	Professional association / Legal entity in the health area	Yes	
2.6.2.3. CGCOM.2.7	IdAdminPersonnel	Yes	
2.6.2.4. CGCOM.2.8	Given name and surnames of administrative personnel	Yes	
2.7. Issuer Alternative Name		Yes	
2.7.1. rfc822Name	"certificacion@cgcom.es"	Yes	
2.7.2. directoryName		Yes	
2.7.2.1. Organization (O)	"Consejo General de Colegios de Medicos"	Yes	
2.7.2.2. SerialNumber	"Q2866017C"	Yes	
2.7.2.3. Location (L)	"Plaza de las Cortes 11"	Yes	
2.7.2.4. Postal Code	"28014"	Yes	
2.7.2.5. State Or Province Name	"Madrid"	Yes	
2.7.2.6. Country (C)	ES	Yes	

[105] This field contains the corporate e-mail address of the administrative personnel and services, for notification purposes.

[106] This field links with the CGCOM re-certification and validation system, permitting the efficient recovery of additional information. Certain information is included, although this may be redundant, in order to have complete information about the user in a single consultation against the certificate.

Field	Contents	Compulsory	Critical
2.8. Extended Key Usage		Yes	
2.8.1. emailProtection	Present	Yes	
2.9. cRLDistributionPoint		Yes	
2.9.1. distributionPoint	"http://crl1.cgcom.es/crl/ec-cgcom.crl"	Yes	
2.9.2. distributionPoint	"http://crl2.cgcom.es/crl/ec-cgcom.crl"	Yes	
2.10. Authority Info Access		Yes	
2.10.1. Access Method		Yes	
2.10.2. Access Location	http://pki-ocsp.verisign.com	Yes	
2.11. NetscapeCertType	"SSL client", "S/MIME"	Yes	
2.12. Subject Directory Attributes (2.5.29.9)		Yes	
2.12.1. Country of Citizenship	Country of nationality	Yes	
2.12.2. Country of Residence	Country of residence.	Yes	

5.9 Certificate of encipherment on card for administrative personnel

Field	Contents	Compulsory	Critical
1. Basic structure			
1.1. Version	"2"[107]	Yes	
1.2. Serial Number	Established automatically[108]	Yes	
1.3. Signature Algorithm	SHA-1 with RSA Signature / SHA-256 with RSA Signature	Yes	
1.4. Issuer Distinguished Name		Yes	
1.4.1. Country (C)	"ES"	Yes	
1.4.2. Organization (O)	"Organizacion Medica Colegial" [109]	Yes	
1.4.3. Organizational Unit (OU)	"Certification Entity" [110]	Yes	
1.4.4. Organizational Unit (OU)	"Class 2 Managed PKI Individual Subscriber CA"	Yes	
1.4.5. Organizational Unit (OU)	"VeriSign Trust Network"	Yes	
1.4.6. Common Name (CN)	"OMC"	Yes	
1.5. Validity	3 years.	Yes	
1.5.1. Not Before	Start date of validity	Yes	
1.5.2. Not After	Date of expiry	Yes	
1.6. Subject		Yes	

[107] The literal "2" corresponds to version 3.

[108] It should not exceed 32 hexadecimal characters in hexadecimal notation.

[109] The text is included without accents.

[110] The text is included without accents.

Field	Contents	Compulsory	Critical
1.6.1. Country (C)	"ES"[111]	Yes	
1.6.2. Organization (O)	Professional association or legal entity in the health area	Yes	
1.6.3. Organizational Unit (OU)	"Conditions of use on https://www.cgcom.es/CertAdmin (c)06"	Yes	
1.6.4. Organizational Unit (OU)	"Use is subject to terms at https://www.verisign.com/rpa (c)99"	Yes	
1.6.5. Surname	Surnames	Yes	
1.6.6. Given Name	Given name	Yes	
1.6.7. Title	"Administrative and service personnel"	Yes	
1.6.8. Serial Number	National ID Document (DNI)/ Foreigner's ID Number (NIE)[112]	Yes	
1.6.9. Common Name (CN)	Given name and surnames + "- "+ "(CIPHERED)"	Yes	
1.6.10. Email (E)	E-mail Address	Yes	
1.7. Subject Public Key Info	2048-Bit Public key encoded in accordance with RFC2459 & PKCS#1	Yes	
2. Extensions			
2.1. Authority Key Identifier	Present	Yes	
2.1.1. Authority Key Identifier			
2.1.2. AuthorityCertIssuer			
2.1.3. AuthorityCertSerialNumber			

[111] The field "country" will always be Spain.

[112] The field "serial number" should include the National ID Document (DNI) or the Foreigner's ID Number (NIE) of the worker, in order to admit the certificate for performing formalities with the Spanish Administrations.

Field	Contents	Compulsory	Critical
2.2. Subject Key Identifier	Present	Yes	
2.3. Key Usage		Yes	Yes
2.3.1. Digital Signature	Not selected. "0"		
2.3.2. Content commitment	Not selected. "0"		
2.3.3. Key Encipherment	Selected. "1"	Yes	
2.3.4. Data Encipherment	Selected. "1"	Yes	
2.3.5. Key Agreement	Not selected. "0"		
2.3.6. Key Certificate Signature	Not selected. "0"		
2.3.7. CRL Signature	Not selected. "0"		
2.4. Qualified Certificate Statements		Yes	
2.4.1. qCCompliance (0.4.0.1862.1.1)		Yes	
2.4.2. QcEuRetentionPeriod (0.4.0.1862.1.3)	15	Yes	
2.4.3. QcSSCD		Yes	
2.5. Certificate Policies		Yes	
2.5.1. Policy Identifier	1.3.6.1.4.1.26852.1.1.2.3	Yes	
2.5.2. Policy Qualifier ID		Yes	
2.5.2.1. CPS Pointer	"https://www.cgcom.es/CertAdmin"	Yes	
2.5.2.2. User Notice	"Corporate certificate of encipherment of administrative personnel and services. Conditions of use at https://www.cgcom.es/CertAdmin"	Yes	
2.5.3. Policy Identifier	OID of class 2 policy of VeriSign	Yes	
2.5.4. Policy Qualifier ID		Yes	

Field	Contents	Compulsory	Critical
2.5.4.1. CPS Pointer	Reference to VeriSign RPA	Yes	
2.5.4.2. User Notice	Notice of VeriSign user	Yes	
2.6. Subject Alternative Names		Yes	
2.6.1. rfc822Name	Corporate e-mail[113]	Yes	
2.6.2. directoryName[114]		Yes	
2.6.2.1. CGCOM.2.1	IdAssociation / IdEntity	Yes	
2.6.2.2. CGCOM.2.2	Professional association / Legal entity in the health area	Yes	
2.6.2.3. CGCOM.2.7	IdAdminPersonnel	Yes	
2.6.2.4. CGCOM.2.8	Given name and surnames of administrative personnel	Yes	
2.7. Issuer Alternative Name		Yes	
2.7.1. rfc822Name	"certificacion@cgcom.es"	Yes	
2.7.2. directoryName		Yes	
2.7.2.1. Organization (O)	"Consejo General de Colegios de Medicos"	Yes	
2.7.2.2. SerialNumber	"Q2866017C"	Yes	
2.7.2.3. Location (L)	"Plaza de las Cortes 11"	Yes	
2.7.2.4. Postal Code	"28014"	Yes	
2.7.2.5. State Or Province Name	"Madrid"	Yes	
2.7.2.6. Country (C)	ES	Yes	
2.8. Extended Key Usage		Yes	
2.8.1. emailProtection	Present	Yes	

[113] This field contains the corporate e-mail address of the registered doctor, for notification purposes.

[114] This field links with the CGCOM re-certification and validation system, permitting the efficient recovery of additional information. Certain information is included, although this may be redundant, in order to have complete information about the user in a single consultation against the certificate.

Field	Contents	Compulsory	Critical
2.9. cRLDistributionPoint		Yes	
2.9.1. distributionPoint	"http://crl1.cgcom.es/crl/ec-cgcom.crl"	Yes	
2.9.2. distributionPoint	"http://crl2.cgcom.es/crl/ec-cgcom.crl"	Yes	
2.10. Authority Info Access		Yes	
2.10.1. Access Method		Yes	
2.10.2. Access Location	http://pki-ocsp.verisign.com	Yes	
2.11. NetscapeCertType	"SSL client", "S/MIME"	Yes	
2.12. Subject Directory Attributes (2.5.29.9)		Yes	
2.12.1. Country of Citizenship	Country of nationality	Yes	
2.12.2. Country of Residence	Country of residence.	Yes	

5.10 Corporate certificate of legal entity for identification.

Field	Contents	Compulsory	Critical
1. Basic structure			
1.1. Version	"2"[115]	Yes	
1.2. Serial Number	Established automatically[116]	Yes	
1.3. Signature Algorithm	SHA-1 with RSA Signature / SHA-256 with RSA Signature	Yes	
1.4. Issuer Distinguished Name		Yes	
1.4.1. Country (C)	"ES"	Yes	
1.4.2. Organization (O)	"Organizacion Medica Colegial" [117]	Yes	
1.4.3. Organizational Unit (OU)	"Certification Entity" [118]	Yes	
1.4.4. Organizational Unit (OU)	"Class 2 Managed PKI Individual Subscriber CA"	Yes	
1.4.5. Organizational Unit (OU)	"VeriSign Trust Network"	Yes	
1.4.6. Common Name (CN)	"OMC"	Yes	
1.5. Validity	3 years.	Yes	
1.5.1. Not Before	Start date of validity	Yes	
1.5.2. Not After	Date of expiry	Yes	
1.6. Subject		Yes	
1.6.1. Country (C)	"ES"[119]	Yes	

[115] The literal "2" corresponds to version 3.

[116] It should not exceed 32 hexadecimal characters in hexadecimal notation.

[117] The text is included without accents.

[118] The text is included without accents.

Field	Contents	Compulsory	Critical
1.6.2. Organization (O)	Professional association or legal entity in the health area	Yes	
1.6.3. Organizational Unit (OU)	"Conditions of use on https://www.cgcom.es/CertJur (c)06"	Yes	
1.6.4. Organizational Unit (OU)	"Use is subject to terms at https://www.verisign.com/rpa (c)99"	Yes	
1.6.5. Surname	Custodian's surnames	Yes	
1.6.6. Given Name	Name of custodian	Yes	
1.6.7. 1.3.6.1.4.1.18838.1.1	National ID Document (DNI)/ Foreigner's ID Number (NIE)[120]	Yes	
1.6.8. Serial Number	Tax ID Number (NIF) of the entity[121]	Yes	
1.6.9. Common Name (CN)	Professional association or other legal entity in the health area + "-"+ "(AUTHENTICATION)"	Yes	
1.6.10. Email (E)	E-mail Address	Yes	
1.7. Subject Public Key Info	2048-Bit Public key encoded in accordance with RFC2459 & PKCS#1	Yes	
2. Extensions			
2.1. Authority Key Identifier	Present	Yes	

[119] The field "country" will always be Spain, since the certificate shows the relation between a registered doctor and a Spanish professional association, regardless of the nationality of the registered doctor. This arises from the corporate nature of the certificate, whose subscriber is the association, and the registered doctor, the person authorised for its use.

[120] The field "serial number" should include the National ID Document (DNI) or the Foreigner's ID Number (NIE) of the worker, in order to admit the certificate for performing formalities with the Spanish Administrations.

[121] In accordance with the tax regulations, this field should show the Tax ID Number (NIF) of the legal entity.

Field	Contents	Compulsory	Critical
2.1.1. Authority Key Identifier			
2.1.2. AuthorityCertIssuer			
2.1.3. AuthorityCertSerialNumber			
2.2. Subject Key Identifier	Present	Yes	
2.3. Key Usage		Yes	Yes
2.3.1. Digital Signature	Selected. “1”	Yes	
2.3.2. Content commitment	Not selected. “0”		
2.3.3. Key Encipherment	Not selected. “0”		
2.3.4. Data Encipherment	Not selected. “0”		
2.3.5. Key Agreement	Not selected. “0”		
2.3.6. Key Certificate Signature	Not selected. “0”		
2.3.7. CRL Signature	Not selected. “0”		
2.4. Qualified Certificate Statements		Yes	
2.4.1. qCCompliance (0.4.0.1862.1.1)		Yes	
2.4.2. QcEuRetentionPeriod (0.4.0.1862.1.3)	15	Yes	
2.4.3. QcSSCD (0.4.0.1862.1.4)		Yes	
2.5. Certificate Policies		Yes	
2.5.1. Policy Identifier	1.3.6.1.4.1.26852.1.1.3.1	Yes	
2.5.2. Policy Qualifier ID		Yes	
2.5.2.1. CPS Pointer	“https://www.cgcom.es/CertJur”	Yes	
2.5.2.2. User Notice	“Corporate identification certificate of legal entity. Conditions of use at https://www.cgcom.es/CertJur”	Yes	

Field	Contents	Compulsory	Critical
2.5.3. Policy Identifier	OID of class 2 policy of VeriSign	Yes	
2.5.4. Policy Qualifier ID		Yes	
2.5.4.1. CPS Pointer	Reference to VeriSign RPA	Yes	
2.5.4.2. User Notice	Notice of VeriSign user	Yes	
2.6. Subject Alternative Names		Yes	
2.6.1. rfc822Name	Corporate e-mail of custodian[122]	Yes	
2.6.2. directoryName[123]		Yes	
2.6.2.1. CGCOM.2.1	IdAssociation / IdEntity	Yes	
2.6.2.2. CGCOM.2.2	Professional association / Legal entity in the health area	Yes	
2.7. Issuer Alternative Name		Yes	
2.7.1. rfc822Name	"certificacion@cgcom.es"	Yes	
2.7.2. directoryName		Yes	
2.7.2.1. Organization (O)	"Consejo General de Colegios de Medicos"	Yes	
2.7.2.2. SerialNumber	"Q2866017C"	Yes	
2.7.2.3. Location (L)	"Plaza de las Cortes 11"	Yes	
2.7.2.4. Postal Code	"28014"	Yes	
2.7.2.5. State Or Province Name	"Madrid"	Yes	
2.7.2.6. Country (C)	ES	Yes	
2.8. Extended Key Usage		Yes	
2.8.1. clientAuth	Present	Yes	

[122] This field contains the corporate e-mail address of the registered doctor, for notification purposes.

[123] This field links with the CGCOM re-certification and validation system, permitting the efficient recovery of additional information. Certain information is included, although this may be redundant, in order to have complete information about the user in a single consultation against the certificate.

Field	Contents	Compulsory	Critical
2.9. cRLDistributionPoint		Yes	
2.9.1. distributionPoint	"http://crl1.cgcom.es/crl/ec-cgcom.crl"	Yes	
2.9.2. distributionPoint	"http://crl2.cgcom.es/crl/ec-cgcom.crl"	Yes	
2.10. Authority Info Access		Yes	
2.10.1. Access Method		Yes	
2.10.2. Access Location	http://pki-ocsp.verisign.com	Yes	
2.11. NetscapeCertType	"SSL client", "S/MIME"	Yes	
2.12. Subject Directory Attributes (2.5.29.9)		Yes	
2.12.1. Country of Citizenship	Country of nationality	Yes	
2.12.2. Country of Residence	Country of residence.	Yes	

5.11 Corporate certificate of legal entity for signature.

Field	Contents	Compulsory	Critical
1. Basic structure			
1.1. Version	"2"[124]	Yes	
1.2. Serial Number	Established automatically[125]	Yes	
1.3. Signature Algorithm	SHA-1 with RSA Signature / SHA-256 with RSA Signature	Yes	
1.4. Issuer Distinguished Name		Yes	
1.4.1. Country (C)	"ES"	Yes	
1.4.2. Organization (O)	"Organizacion Medica Colegial" [126]	Yes	
1.4.3. Organizational Unit (OU)	"Certification Entity" [127]	Yes	
1.4.4. Organizational Unit (OU)	"Class 2 Managed PKI Individual Subscriber CA"	Yes	
1.4.5. Organizational Unit (OU)	"VeriSign Trust Network"	Yes	
1.4.6. Common Name (CN)	"OMC"	Yes	
1.5. Validity	3 years.	Yes	
1.5.1. Not Before	Start date of validity	Yes	
1.5.2. Not After	Date of expiry	Yes	
1.6. Subject		Yes	
1.6.1. Country (C)	"ES"[128]	Yes	

[124] The literal "2" corresponds to version 3.

[125] It should not exceed 32 hexadecimal characters in hexadecimal notation.

[126] The text is included without accents.

[127] The text is included without accents.

[128] The field "country" will always be Spain, since the certificate shows the relation between a registered doctor and a Spanish professional association, regardless of the nationality of the

Field	Contents	Compulsory	Critical
1.6.2. Organization (O)	Professional association or legal entity in the health area	Yes	
1.6.3. Organizational Unit (OU)	"Conditions of use on https://www.cgcom.es/CertJur (c)06"	Yes	
1.6.4. Organizational Unit (OU)	"Use is subject to terms at https://www.verisign.com/rpa (c)99"	Yes	
1.6.5. Surname	Custodian's surnames	Yes	
1.6.6. Given Name	Name of custodian	Yes	
1.6.7. 1.3.6.1.4.1.18838.1.1	National ID Document (DNI)/ Foreigner's ID Number (NIE)[129]	Yes	
1.6.8. Serial Number	Tax ID Number (NIF) of the entity[130]	Yes	
1.6.9. Common Name (CN)	Professional association or other legal entity in the health area + "-"+ "(SIGNATURE)"	Yes	
1.6.10. Email (E)	E-mail Address	Yes	
1.7. Subject Public Key Info	2048-Bit Public key encoded in accordance with RFC2459 & PKCS#1	Yes	
2. Extensions			
2.1. Authority Key Identifier	Present	Yes	
2.1.1. Authority Key Identifier			
2.1.2. AuthorityCertIssuer			

registered doctor. This arises from the corporate nature of the certificate, whose subscriber is the association, and the registered doctor, the person authorised for its use.

[129] The field "serial number" should include the National ID Document (DNI) or the Foreigner's ID Number (NIE) of the worker, in order to admit the certificate for performing formalities with the Spanish Administrations.

[130] In accordance with the tax regulations, this field should show the Tax ID Number (NIF) of the legal entity.

Field	Contents	Compulsory	Critical
2.1.3. AuthorityCertSerialNumber			
2.2. Subject Key Identifier	Present	Yes	
2.3. Key Usage		Yes	Yes
2.3.1. Digital Signature	Not selected. “0”		
2.3.2. Content commitment	Selected. “1”	Yes	
2.3.3. Key Encipherment	Not selected. “0”		
2.3.4. Data Encipherment	Not selected. “0”		
2.3.5. Key Agreement	Not selected. “0”		
2.3.6. Key Certificate Signature	Not selected. “0”		
2.3.7. CRL Signature	Not selected. “0”		
2.4. Qualified Certificate Statements		Yes	
2.4.1. qCCompliance (0.4.0.1862.1.1)		Yes	
2.4.2. QcEuRetentionPeriod (0.4.0.1862.1.3)	15	Yes	
2.4.3. QcSSCD (0.4.0.1862.1.4)		Yes	
2.5. Certificate Policies		Yes	
2.5.1. Policy Identifier	1.3.6.1.4.1.26852.1.1.3.2	Yes	
2.5.2. Policy Qualifier ID		Yes	
2.5.2.1. CPS Pointer	“https://www.cgcom.es/CertJur”	Yes	
2.5.2.2. User Notice	“Corporate certificate of qualified electronic signature of legal entity. Conditions of use at https://www.cgcom.es/CertJur”	Yes	
2.5.3. Policy Identifier	OID of class 2 policy of VeriSign	Yes	
2.5.4. Policy Qualifier ID		Yes	

Field	Contents	Compulsory	Critical
2.5.4.1. CPS Pointer	Reference to VeriSign RPA	Yes	
2.5.4.2. User Notice	Notice of VeriSign user	Yes	
2.6. Subject Alternative Names		Yes	
2.6.1. rfc822Name	Corporate e-mail of custodian[131]	Yes	
2.6.2. directoryName[132]		Yes	
2.6.2.1. CGCOM.2.1	IdAssociation / IdEntity	Yes	
2.6.2.2. CGCOM.2.2	Professional association / Legal entity in the health area	Yes	
2.7. Issuer Alternative Name		Yes	
2.7.1. rfc822Name	"certificacion@cgcom.es"	Yes	
2.7.2. directoryName		Yes	
2.7.2.1. Organization (O)	"Consejo General de Colegios de Medicos"	Yes	
2.7.2.2. SerialNumber	"Q2866017C"	Yes	
2.7.2.3. Location (L)	"Plaza de las Cortes 11"	Yes	
2.7.2.4. Postal Code	"28014"	Yes	
2.7.2.5. State Or Province Name	"Madrid"	Yes	
2.7.2.6. Country (C)	ES	Yes	
2.8. Extended Key Usage		Yes	
2.8.1. emailProtection	Present	Yes	
2.9. cRLDistributionPoint		Yes	
2.9.1. distributionPoint	"http://crl1.cgcom.es/crl/ec-cgcom.crl"	Yes	

[131] This field contains the corporate e-mail address of the registered doctor, for notification purposes.

[132] This field links with the CGCOM re-certification and validation system, permitting the efficient recovery of additional information. Certain information is included, although this may be redundant, in order to have complete information about the user in a single consultation against the certificate.

Field	Contents	Compulsory	Critical
2.9.2. distributionPoint	"http://crl2.cgcom.es/crl/ec-cgcom.crl"	Yes	
2.10. Authority Info Access		Yes	
2.10.1. Access Method		Yes	
2.10.2. Access Location	http://pki-ocsp.verisign.com	Yes	
2.11. NetscapeCertType	"SSL client", "S/MIME"	Yes	
2.12. Subject Directory Attributes (2.5.29.9)		Yes	
2.12.1. Country of Citizenship	Country of nationality	Yes	
2.12.2. Country of Residence	Country of residence.	Yes	

5.12 Certificate of encipherment on card for legal entity

Field	Contents	Compulsory	Critical
1. Basic structure			
1.1. Version	"2"[133]	Yes	
1.2. Serial Number	Established automatically[134]	Yes	
1.3. Signature Algorithm	SHA-1 with RSA Signature / SHA-256 with RSA Signature	Yes	
1.4. Issuer Distinguished Name		Yes	
1.4.1. Country (C)	"ES"	Yes	
1.4.2. Organization (O)	"Organizacion Medica Colegial" [135]	Yes	
1.4.3. Organizational Unit (OU)	"Certification Entity" [136]	Yes	
1.4.4. Organizational Unit (OU)	"Class 2 Managed PKI Individual Subscriber CA"	Yes	
1.4.5. Organizational Unit (OU)	"VeriSign Trust Network"	Yes	
1.4.6. Common Name (CN)	"OMC"	Yes	
1.5. Validity	3 years.	Yes	
1.5.1. Not Before	Start date of validity	Yes	
1.5.2. Not After	Date of expiry	Yes	
1.6. Subject		Yes	
1.6.1. Country (C)	"ES"[137]	Yes	

[133] The literal "2" corresponds to version 3.

[134] It should not exceed 32 hexadecimal characters in hexadecimal notation.

[135] The text is included without accents.

[136] The text is included without accents.

[137] The field "country" will always be Spain.

Field	Contents	Compulsory	Critical
1.6.2. Organization (O)	Professional association or legal entity in the health area	Yes	
1.6.3. Organizational Unit (OU)	"Conditions of use on https://www.cgcom.es/CertJur (c)06"	Yes	
1.6.4. Organizational Unit (OU)	"Use is subject to terms at https://www.verisign.com/rpa (c)99"	Yes	
1.6.5. Surname	Custodian's surnames	Yes	
1.6.6. Given Name	Name of custodian	Yes	
1.6.7. 1.3.6.1.4.1.18838.1.1	National ID Document (DNI)/ Foreigner's ID Number (NIE)[138]	Yes	
1.6.8. Serial Number	Tax ID Number (NIF) of the entity[139]	Yes	
1.6.9. Common Name (CN)	Professional association or other legal entity in the health area + "-"+ "(CIPHERING)"	Yes	
1.6.10. Email (E)	E-mail Address	Yes	
1.7. Subject Public Key Info	2048-Bit Public key encoded in accordance with RFC2459 & PKCS#1	Yes	
2. Extensions			
2.1. Authority Key Identifier	Present	Yes	
2.1.1. Authority Key Identifier			
2.1.2. AuthorityCertIssuer			
2.1.3. AuthorityCertSerialNum			

[138] The field "serial number" should include the National ID Document (DNI) or the Foreigner's ID Number (NIE) of the worker, in order to admit the certificate for performing formalities with the Spanish Administrations.

[139] In accordance with the tax regulations, this field should show the Tax ID Number (NIF) of the legal entity.

Field	Contents	Compulsory	Critical
ber			
2.2. Subject Key Identifier	Present	Yes	
2.3. Key Usage		Yes	Yes
2.3.1. Digital Signature	Not selected. “0”		
2.3.2. Content commitment	Not selected. “0”		
2.3.3. Key Encipherment	Selected. “1”	Yes	
2.3.4. Data Encipherment	Selected. “1”	Yes	
2.3.5. Key Agreement	Not selected. “0”		
2.3.6. Key Certificate Signature	Not selected. “0”		
2.3.7. CRL Signature	Not selected. “0”		
2.4. Qualified Certificate Statements		Yes	
2.4.1. qCCompliance (0.4.0.1862.1.1)		Yes	
2.4.2. QcEuRetentionPeriod (0.4.0.1862.1.3)	15	Yes	
2.4.3. QcSSCD		Yes	
2.5. Certificate Policies		Yes	
2.5.1. Policy Identifier	1.3.6.1.4.1.26852.1.1.3.3	Yes	
2.5.2. Policy Qualifier ID		Yes	
2.5.2.1. CPS Pointer	“https://www.cgcom.es/CertJur”	Yes	
2.5.2.2. User Notice	“Corporate identification of ciphering of of legal entity. Conditions of use at https://www.cgcom.es/CertJur”	Yes	
2.5.3. Policy Identifier	OID of class 2 policy of VeriSign	Yes	
2.5.4. Policy Qualifier ID		Yes	
2.5.4.1. CPS Pointer	Reference to VeriSign RPA	Yes	

Field	Contents	Compulsory	Critical
2.5.4.2. User Notice	Notice of VeriSign user	Yes	
2.6. Subject Alternative Names		Yes	
2.6.1. rfc822Name	Corporate e-mail[140]	Yes	
2.6.2. directoryName[141]		Yes	
2.6.2.1. CGCOM.2.1	IdAssociation / IdEntity	Yes	
2.6.2.2. CGCOM.2.2	Professional association / Legal entity in the health area	Yes	
2.7. Issuer Alternative Name		Yes	
2.7.1. rfc822Name	"certificacion@cgcom.es"	Yes	
2.7.2. directoryName		Yes	
2.7.2.1. Organization (O)	"Consejo General de Colegios de Medicos"	Yes	
2.7.2.2. SerialNumber	"Q2866017C"	Yes	
2.7.2.3. Location (L)	"Plaza de las Cortes 11"	Yes	
2.7.2.4. Postal Code	"28014"	Yes	
2.7.2.5. State Or Province Name	"Madrid"	Yes	
2.7.2.6. Country (C)	ES	Yes	
2.8. Extended Key Usage		Yes	
2.8.1. emailProtection	Present	Yes	
2.9. cRLDistributionPoint		Yes	
2.9.1. distributionPoint	"http://crl1.cgcom.es/crl/ec-cgcom.crl"	Yes	

[140] This field contains the corporate e-mail address of the registered doctor, for notification purposes.

[141] This field links with the CGCOM re-certification and validation system, permitting the efficient recovery of additional information. Certain information is included, although this may be redundant, in order to have complete information about the user in a single consultation against the certificate.

Field	Contents	Compulsory	Critical
2.9.2. distributionPoint	"http://crl2.cgcom.es/crl/ec-cgcom.crl"	Yes	
2.10. Authority Info Access		Yes	
2.10.1. Access Method		Yes	
2.10.2. Access Location	http://pki-ocsp.verisign.com	Yes	
2.11. NetscapeCertType	"SSL client", "S/MIME"	Yes	
2.12. Subject Directory Attributes (2.5.29.9)		Yes	
2.12.1. Country of Citizenship	Country of nationality	Yes	
2.12.2. Country of Residence	Country of residence.	Yes	

5.13 Corporate certificate of administrative personnel (individual) on software, for identification, signature and encipherment

Field	Contents	Compulsory	Critical
1. Basic structure			
1.1. Version	"2"[142]	Yes	
1.2. Serial Number	Established automatically[143]	Yes	
1.3. Signature Algorithm	SHA-1 with RSA Signature / SHA-256 with RSA Signature	Yes	
1.4. Issuer Distinguished Name		Yes	
1.4.1. Country (C)	"ES"	Yes	
1.4.2. Organization (O)	"Organizacion Medica Colegial" [144]	Yes	
1.4.3. Organizational Unit (OU)	"Certification Entity" [145]	Yes	
1.4.4. Organizational Unit (OU)	"Class 2 Managed PKI Individual Subscriber CA"	Yes	
1.4.5. Organizational Unit (OU)	"VeriSign Trust Network"	Yes	
1.4.6. Common Name (CN)	"OMC"	Yes	
1.5. Validity	3 years.	Yes	
1.5.1. Not Before	Start date of validity	Yes	
1.5.2. Not After	Date of expiry	Yes	
1.6. Subject		Yes	

[142] The literal "2" corresponds to version 3.

[143] It should not exceed 32 hexadecimal characters in hexadecimal notation.

[144] The text is included without accents.

[145] The text is included without accents.

Field	Contents	Compulsory	Critical
1.6.1. Country (C)	"ES"[146]	Yes	
1.6.2. Organization (O)	Professional association or legal entity in the health area	Yes	
1.6.3. Organizational Unit (OU)	"Conditions of use at https://www.cgcom.es/CertAdminSoft (c)13"	Yes	
1.6.4. Organizational Unit (OU)	"Use is subject to terms at https://www.verisign.com/rpa (c)99"	Yes	
1.6.5. Surname	Surnames	Yes	
1.6.6. Given Name	Given name	Yes	
1.6.7. Title	"Administrative and service personnel"	Yes	
1.6.8. Serial Number	National ID Document (DNI)/ Foreigner's ID Number (NIE)[147]	Yes	
1.6.9. Common Name (CN)	Name and surnames	Yes	
1.6.10. Email (E)	E-mail Address	Yes	
1.7. Subject Public Key Info	2048-Bit Public key encoded in accordance with RFC2459 & PKCS#1	Yes	
2. Extensions			
2.1. Authority Key Identifier	Present	Yes	
2.1.1. Authority Key Identifier			
2.1.2. AuthorityCertIssuer			
2.1.3. AuthorityCertSerialNumber			

[146] The field "country" will always be Spain, since the certificate shows the relation between a worker and a Spanish professional association, regardless of the nationality of the registered doctor.

[147] The field "serial number" should include the National ID Document (DNI) or the Foreigner's ID Number (NIE) of the worker, in order to admit the certificate for performing formalities with the Spanish Administrations.

Field	Contents	Compulsory	Critical
2.2. Subject Key Identifier	Present	Yes	
2.3. Key Usage		Yes	Yes
2.3.1. Digital Signature	Selected. "1"	Yes	
2.3.2. Content commitment	Selected. "1"	Yes	
2.3.3. Key Encipherment	Selected. "1"	Yes	
2.3.4. Data Encipherment	Selected. "1"	Yes	
2.3.5. Key Agreement	Not selected. "0"		
2.3.6. Key Certificate Signature	Not selected. "0"		
2.3.7. CRL Signature	Not selected. "0"		
2.4. Qualified Certificate Statements		Yes	
2.4.1. qCCompliance (0.4.0.1862.1.1)		Yes	
2.4.2. QcEuRetentionPeriod (0.4.0.1862.1.3)	15	Yes	
2.5. Certificate Policies		Yes	
2.5.1. Policy Identifier	1.3.6.1.4.1.26852.1.1.6	Yes	
2.5.2. Policy Qualifier ID		Yes	
2.5.2.1. CPS Pointer	"https://www.cgcom.es/CertAdminSoft"	Yes	
2.5.2.2. User Notice	"Corporate certificate of advanced electronic signature and encipherment of administrative personnel and services on software. Conditions of use at https://www.cgcom.es/CertAdminSoft"	Yes	
2.5.3. Policy Identifier	OID of class 2 policy of VeriSign	Yes	
2.5.4. Policy Qualifier ID		Yes	

Field	Contents	Compulsory	Critical
2.5.4.1. CPS Pointer	Reference to VeriSign RPA	Yes	
2.5.4.2. User Notice	Notice of VeriSign user	Yes	
2.6. Subject Alternative Names		Yes	
2.6.1. rfc822Name	Corporate e-mail of administrative personnel[148]	Yes	
2.6.2. directoryName[149]		Yes	
2.6.2.1. CGCOM.2.1	IdAssociation / IdEntity	Yes	
2.6.2.2. CGCOM.2.2	Professional association / Legal entity in the health area	Yes	
2.6.2.3. CGCOM.2.7	IdAdminPersonnel	Yes	
2.6.2.4. CGCOM.2.8	Given name and surnames of administrative personnel	Yes	
2.7. Issuer Alternative Name		Yes	
2.7.1. rfc822Name	"certificacion@cgcom.es"	Yes	
2.7.2. directoryName		Yes	
2.7.2.1. Organization (O)	"Consejo General de Colegios de Medicos"	Yes	
2.7.2.2. SerialNumber	"Q2866017C"	Yes	
2.7.2.3. Location (L)	"Plaza de las Cortes 11"	Yes	
2.7.2.4. Postal Code	"28014"	Yes	
2.7.2.5. State Or Province Name	"Madrid"	Yes	
2.7.2.6. Country (C)	ES	Yes	

[148] This field contains the corporate e-mail address of the administrative personnel and services, for notification purposes.

[149] This field links with the CGCOM re-certification and validation system, permitting the efficient recovery of additional information. Certain information is included, although this may be redundant, in order to have complete information about the user in a single consultation against the certificate.

Field	Contents	Compulsory	Critical
2.8. Extended Key Usage		Yes	
2.8.1. emailProtection	Present	Yes	
2.8.2. clientAuth	Present	Yes	
2.9. cRLDistributionPoint		Yes	
2.9.1. distributionPoint	"http://crl1.cgcom.es/crl/ec-cgcom.crl"	Yes	
2.9.2. distributionPoint	"http://crl2.cgcom.es/crl/ec-cgcom.crl"	Yes	
2.10. Authority Info Access		Yes	
2.10.1. Access Method		Yes	
2.10.2. Access Location	http://pki-ocsp.verisign.com	Yes	
2.11. NetscapeCertType	"SSL client", "S/MIME"	Yes	
2.12. Subject Directory Attributes (2.5.29.9)		Yes	
2.12.1. Country of Citizenship	Country of nationality	Yes	
2.12.2. Country of Residence	Country of residence.	Yes	

6. External certificates

6.1 External certificate of regional health service doctor group (individual) for identification, signature and enciphernment

Field	Contents	Compulsory	Critical
1. Basic structure			
1.1. Version	"2"[150]	Yes	
1.2. Serial Number	Established automatically[151]	Yes	
1.3. Signature Algorithm	SHA-1 with RSA Signature	Yes	
1.4. Issuer Distinguished Name		Yes	
1.4.1. Country (C)	"ES"	Yes	
1.4.2. Organization (O)	"Organizacion Medica Colegial" [152]	Yes	
1.4.3. Organizational Unit (OU)	"Certification Entity" [153]	Yes	
1.4.4. Organizational Unit (OU)	"Class 2 Managed PKI Individual Subscriber CA"	Yes	
1.4.5. Organizational Unit (OU)	"VeriSign Trust Network"	Yes	
1.4.6. Common Name (CN)	"OMC"	Yes	
1.5. Validity	3 years.	Yes	
1.5.1. Not Before	Start date of validity	Yes	
1.5.2. Not After	Date of expiry	Yes	

[150] The literal "2" corresponds to version 3.

[151] It should not exceed 32 hexadecimal characters in hexadecimal notation.

[152] The text is included without accents.

[153] The text is included without accents.

Field	Contents	Compulsory	Critical
1.6. Subject		Yes	
1.6.1. Country (C)	"ES"[154]	Yes	
1.6.2. Organization (O)	Name of the regional health service	Yes	
1.6.3. Organizational Unit (OU)	"Electronic certificate of public employed doctor"	Yes	
1.6.4. Organizational Unit (OU)	Administrative unit	No	
1.6.5. Organizational Unit (OU)	Employee number	No	
1.6.6. Surname	Surnames + " – " + Tax ID Number (NIF) of employee	Yes	
1.6.7. Given Name	Given name	Yes	
1.6.8. Title	Position or post held by the person responsible for certificate	Yes	
1.6.9. Serial Number	National ID Document (DNI)/Foreigner's ID Number (NIE) of the public employee	Yes	
1.6.10. Common Name (CN)	Name, surnames + " – " + Tax ID Number (NIF) of employee	Yes	
1.7. Subject Public Key Info	2048-Bit Public key encoded in accordance with RFC2459 & PKCS#1	Yes	
2. Extensions			
2.1. Authority Key Identifier	Present	Yes	
2.1.1. Authority Key Identifier			
2.1.2. AuthorityCertIssuer			

[154] The field "country" will always be Spain, since the certificate shows the relation between an employee and a Spanish regional health service, regardless of the nationality of the employee. This arises from the group nature of the external certificate, whose subscriber is the regional health service, and the employee, the person authorised for its use.

Field	Contents	Compulsory	Critical
2.1.3. AuthorityCertSerialNumber			
2.2. Subject Key Identifier	Present	Yes	
2.3. Key Usage		Yes	Yes
2.3.1. Digital Signature	Selected. “1”	Yes	
2.3.2. Non Repudiation	Selected. “1”	Yes	
2.3.3. Key Encipherment	Selected. “1”	Yes	
2.3.4. Data Encipherment	Selected. “1”	Yes	
2.3.5. Key Agreement	Not selected. “0”		
2.3.6. Key Certificate Signature	Not selected. “0”		
2.3.7. CRL Signature	Not selected. “0”		
2.4. Qualified Certificate Statements		Yes	
2.4.1. qCCompliance (0.4.0.1862.1.1)		Yes	
2.4.2. QcEuRetentionPeriod (0.4.0.1862.1.3)	15	Yes	
2.4.3. QcSSCD (0.4.0.1862.1.4)		Yes	
2.5. Certificate Policies		Yes	
2.5.1. Policy Identifier	1.3.6.1.4.1.26852.1.2.1	Yes	
2.5.2. Policy Qualifier ID		Yes	
2.5.2.1. CPS Pointer	“https://www.cgcom.es/CertECSAS”	Yes	
2.5.2.2. User Notice	“Certificate of qualified electronic signature and encipherment of regional health service doctor. Conditions of use at https://www.cgcom.es/CertECSAS”	Yes	

Field	Contents	Compulsory	Critical
2.5.3. Policy Identifier	OID of class 2 policy of VeriSign	Yes	
2.5.4. Policy Qualifier ID		Yes	
2.5.4.1. CPS Pointer	Reference to VeriSign RPA	Yes	
2.5.4.2. User Notice	Notice of VeriSign user	Yes	
2.6. Subject Alternative Names		Yes	
2.6.1. rfc822Name	Corporate e-mail of employee[155]	Yes	
2.6.2. Directory Name		Yes	
2.6.2.1. Type of certificate - OID 2.16.724.1.3.5.3.2.1	Electronic certificate of public employee	F[156]	
2.6.2.2. Name of subscriber entity - OID 2.16.724.1.3.5.3.2.2	Name of subscriber entity (health service)	F	
2.6.2.3. Tax ID Number (NIF) subscriber entity - OID 2.16.724.1.3.5.3.2.3	Tax ID Number (NIF) of subscriber entity	F	
2.6.2.4. National ID Document (DNI)/Foreigner's ID Number (NIE) of the responsible person - OID 2.16.724.1.3.5.3.2.4	National ID Document (DNI)/Foreigner's ID Number of the responsible person	F	
2.6.2.5. Personal identification number - OID 2.16.724.1.3.5.3.2.5	Identification number of doctor as public employee	O[157]	
2.6.2.6. Given name - OID 2.16.724.1.3.5.3.2.6	Given name of doctor - public employee	F	
2.6.2.7. First surname - OID 2.16.724.1.3.5.3.2.7	First surname of doctor - public employee	F	

[155] This field contains the corporate e-mail address of the employee, for notification purposes.

[156] Fixed field (F), in accordance with Certica profiles

[157] Optional field (O), in accordance with Certica profiles

Field	Contents	Compulsory	Critical
2.6.2.8. Second surname - OID 2.16.724.1.3.5.3.2.8	Second surname of doctor - public employee	F	
2.6.2.9. E-mail - OID 2.16.724.1.3.5.3.2.9	E-mail of doctor - public employee	O	
2.6.2.10. Organisational unit - OID 2.16.724.1.3.5.3.2.10	Unit, within the Administration, in which the doctor - public employee is included.	O	
2.6.2.11. Position or office - OID 2.16.724.1.3.5.3.2.11	Position held by doctor - public employee, within the Administration	O	
2.7. Issuer Alternative Name		Yes	
2.7.1. rfc822Name	"certificacion@cgcom.es"	Yes	
2.7.2. directoryName		Yes	
2.7.2.1. Organization (O)	"Consejo General de Colegios de Medicos"	Yes	
2.7.2.2. SerialNumber	"Q2866017C"	Yes	
2.7.2.3. Location (L)	"Plaza de las Cortes 11"	Yes	
2.7.2.4. Postal Code	"28014"	Yes	
2.7.2.5. State Or Province Name	"Madrid"	Yes	
2.7.2.6. Country (C)	ES	Yes	
2.8. Extended Key Usage		Yes	
2.8.1. emailProtection	Present	Yes	
2.8.2. clientAuth	Present	Yes	
2.9. cRLDistributionPoint		Yes	
2.9.1. distributionPoint	"http://crl1.cgcom.es/crl/ec-cgcom.crl"	Yes	
2.9.2. distributionPoint	"http://crl2.cgcom.es/crl/ec-cgcom.crl"	Yes	

Field	Contents	Compulsory	Critical
2.10. Authority Info Access		Yes	
2.10.1. Access Method		Yes	
2.10.2. Access Location	http://pki-ocsp.verisign.com	Yes	
2.11. NetscapeCertType	“SSL client”, “S/MIME”	Yes	
2.12. Subject Directory Attributes (2.5.29.9)		Yes	
2.12.1. Country of Citizenship	Country of nationality	Yes	
2.12.2. Country of Residence	Country of residence.	Yes	

7. External certificates (as from 2013)

7.1 External certificate of regional health service doctor group (individual) for identification

Field	Contents	Compulsory	Critical
1. Basic structure			
1.1. Version	"2"[158]	Yes	
1.2. Serial Number	Established automatically[159]	Yes	
1.3. Signature Algorithm	SHA-1 with RSA Signature / SHA-256 with RSA Signature	Yes	
1.4. Issuer Distinguished Name		Yes	
1.4.1. Country (C)	"ES"	Yes	
1.4.2. Organization (O)	"Organizacion Medica Colegial" [160]	Yes	
1.4.3. Organizational Unit (OU)	"Certification Entity" [161]	Yes	
1.4.4. Organizational Unit (OU)	"Class 2 Managed PKI Individual Subscriber CA"	Yes	
1.4.5. Organizational Unit (OU)	"VeriSign Trust Network"	Yes	
1.4.6. Common Name (CN)	"OMC"	Yes	
1.5. Validity	3 years.	Yes	
1.5.1. Not Before	Start date of validity	Yes	

[158] The literal "2" corresponds to version 3.

[159] It should not exceed 32 hexadecimal characters in hexadecimal notation.

[160] The text is included without accents.

[161] The text is included without accents.

Field	Contents	Compulsory	Critical
1.5.2. Not After	Date of expiry	Yes	
1.6. Subject		Yes	
1.6.1. Country (C)	"ES"[162]	Yes	
1.6.2. Organization (O)	Name of the regional health service	Yes	
1.6.3. Organizational Unit (OU)	"Electronic certificate of public employed doctor"	Yes	
1.6.4. Organizational Unit (OU)	Administrative unit	No	
1.6.5. Organizational Unit (OU)	Employee number	No	
1.6.6. Surname	Surnames + " – " + Tax ID Number (NIF) of employee	Yes	
1.6.7. Given Name	Given name	Yes	
1.6.8. Title	Position or post held by the person responsible for certificate	Yes	
1.6.9. Serial Number	National ID Document (DNI)/Foreigner's ID Number (NIE) of the public employee	Yes	
1.6.10. Common Name (CN)	Name, surnames + " – " + Tax ID Number (NIF) of employee + "(AUTHENTICATION)	Yes	
1.7. Subject Public Key Info	2048-Bit Public key encoded in accordance with RFC2459 & PKCS#1	Yes	
2. Extensions			
2.1. Authority Key Identifier	Present	Yes	

[162] The field "country" will always be Spain, since the certificate shows the relation between an employee and a Spanish regional health service, regardless of the nationality of the employee. This arises from the group nature of the external certificate, whose subscriber is the regional health service, and the employee, the person authorised for its use.

Field	Contents	Compulsory	Critical
2.1.1. Authority Key Identifier			
2.1.2. AuthorityCertIssuer			
2.1.3. AuthorityCertSerialNumber			
2.2. Subject Key Identifier	Present	Yes	
2.3. Key Usage		Yes	Yes
2.3.1. Digital Signature	Selected. “1”	Yes	
2.3.2. Content commitment	Not selected. “0”		
2.3.3. Key Encipherment	Not selected. “0”		
2.3.4. Data Encipherment	Not selected. “0”		
2.3.5. Key Agreement	Not selected. “0”		
2.3.6. Key Certificate Signature	Not selected. “0”		
2.3.7. CRL Signature	Not selected. “0”		
2.4. Qualified Certificate Statements		Yes	
2.4.1. qCCompliance (0.4.0.1862.1.1)		Yes	
2.4.2. QcEuRetentionPeriod (0.4.0.1862.1.3)	15	Yes	
2.4.3. QcSSCD (0.4.0.1862.1.4)		Yes	
2.5. Certificate Policies		Yes	
2.5.1. Policy Identifier	1.3.6.1.4.1.26852.1.2.1.1	Yes	
2.5.2. Policy Qualifier ID		Yes	
2.5.2.1. CPS Pointer	“https://www.cgcom.es/CertECSAS”	Yes	
2.5.2.2. User Notice	“Certificate of identification of regional health service doctor. Conditions of use at https://www.cgcom.es/CertECS	Yes	

Field	Contents	Compulsory	Critical
	AS"		
2.5.3. Policy Identifier	OID of class 2 policy of VeriSign	Yes	
2.5.4. Policy Qualifier ID		Yes	
2.5.4.1. CPS Pointer	Reference to VeriSign RPA	Yes	
2.5.4.2. User Notice	Notice of VeriSign user	Yes	
2.6. Subject Alternative Names		Yes	
2.6.1. rfc822Name	Corporate e-mail of worker[163]	Yes	
2.6.2. Directory Name		Yes	
2.6.2.1. Type of certificate - OID 2.16.724.1.3.5.3.2.1	Electronic certificate of public employee	F[164]	
2.6.2.2. Name of subscriber entity - OID 2.16.724.1.3.5.3.2.2	Name of subscriber entity (health service)	F	
2.6.2.3. Tax ID Number (NIF) subscriber entity - OID 2.16.724.1.3.5.3.2.3	Tax ID Number (NIF) of subscriber entity	F	
2.6.2.4. National ID Document (DNI)/Foreigner's ID Number (NIE) of the responsible person - OID 2.16.724.1.3.5.3.2.4	National ID Document (DNI)/Foreigner's ID Number of the responsible person	F	
2.6.2.5. Personal identification number - OID 2.16.724.1.3.5.3.2.5	Identification number of doctor as public employee	O[165]	
2.6.2.6. Given name - OID 2.16.724.1.3.5.3.2.6	Given name of doctor - public employee	F	

[163] This field contains the corporate e-mail address of the employee, for notification purposes.

[164] Fixed field (F), in accordance with Certica profiles

[165] Optional field (O), in accordance with Certica profiles

Field	Contents	Compulsory	Critical
2.6.2.7. First surname - OID 2.16.724.1.3.5.3.2.7	First surname of doctor - public employee	F	
2.6.2.8. Second surname - OID 2.16.724.1.3.5.3.2.8	Second surname of doctor - public employee	F	
2.6.2.9. E-mail - OID 2.16.724.1.3.5.3.2.9	E-mail of doctor - public employee	O	
2.6.2.10. Organisational unit - OID 2.16.724.1.3.5.3.2.10	Unit, within the Administration, in which the doctor - public employee is included.	O	
2.6.2.11. Position or office - OID 2.16.724.1.3.5.3.2.11	Position held by doctor - public employee, within the Administration	O	
2.7. Issuer Alternative Name		Yes	
2.7.1. rfc822Name	"certificacion@cgcom.es"	Yes	
2.7.2. directoryName		Yes	
2.7.2.1. Organization (O)	"Consejo General de Colegios de Medicos"	Yes	
2.7.2.2. SerialNumber	"Q2866017C"	Yes	
2.7.2.3. Location (L)	"Plaza de las Cortes 11"	Yes	
2.7.2.4. Postal Code	"28014"	Yes	
2.7.2.5. State Or Province Name	"Madrid"	Yes	
2.7.2.6. Country (C)	ES	Yes	
2.8. Extended Key Usage		Yes	
2.8.1. clientAuth	Present	Yes	
2.9. cRLDistributionPoint		Yes	
2.9.1. distributionPoint	"http://crl1.cgcom.es/crl/ec-cgcom.crl"	Yes	

Field	Contents	Compulsory	Critical
2.9.2. distributionPoint	"http://crl2.cgcom.es/crl/ec-cgcom.crl"	Yes	
2.10. Authority Info Access		Yes	
2.10.1. Access Method		Yes	
2.10.2. Access Location	http://pki-ocsp.verisign.com	Yes	
2.11. NetscapeCertType	"SSL client", "S/MIME"	Yes	
2.12. Subject Directory Attributes (2.5.29.9)		Yes	
2.12.1. Country of Citizenship	Country of nationality	Yes	
2.12.2. Country of Residence	Country of residence.	Yes	

7.2 External certificate of regional health service doctor group (individual) for signature

Field	Contents	Compulsory	Critical
1. Basic structure			
1.1. Version	"2"[166]	Yes	
1.2. Serial Number	Established automatically[167]	Yes	
1.3. Signature Algorithm	SHA-1 with RSA Signature / SHA-256 with RSA Signature	Yes	
1.4. Issuer Distinguished Name		Yes	
1.4.1. Country (C)	"ES"	Yes	
1.4.2. Organization (O)	"Organizacion Medica Colegial" [168]	Yes	
1.4.3. Organizational Unit (OU)	"Certification Entity" [169]	Yes	
1.4.4. Organizational Unit (OU)	"Class 2 Managed PKI Individual Subscriber CA"	Yes	
1.4.5. Organizational Unit (OU)	"VeriSign Trust Network"	Yes	
1.4.6. Common Name (CN)	"OMC"	Yes	
1.5. Validity	3 years.	Yes	
1.5.1. Not Before	Start date of validity	Yes	
1.5.2. Not After	Date of expiry	Yes	
1.6. Subject		Yes	
1.6.1. Country (C)	"ES"[170]	Yes	

[166] The literal "2" corresponds to version 3.

[167] It should not exceed 32 hexadecimal characters in hexadecimal notation.

[168] The text is included without accents.

[169] The text is included without accents.

Field	Contents	Compulsory	Critical
1.6.2. Organization (O)	Name of the regional health service	Yes	
1.6.3. Organizational Unit (OU)	"Electronic certificate of public employed doctor"	Yes	
1.6.4. Organizational Unit (OU)	Administrative unit	No	
1.6.5. Organizational Unit (OU)	Employee number	No	
1.6.6. Surname	Surnames + " – " + Tax ID Number (NIF) of employee	Yes	
1.6.7. Given Name	Given name	Yes	
1.6.8. Title	Position or post held by the person responsible for certificate	Yes	
1.6.9. Serial Number	National ID Document (DNI)/Foreigner's ID Number (NIE) of the public employee	Yes	
1.6.10. Common Name (CN)	Name, surnames + " – " + Tax ID Number (NIF) of employee + "(SIGNATURE)"	Yes	
1.7. Subject Public Key Info	2048-Bit Public key encoded in accordance with RFC2459 & PKCS#1	Yes	
2. Extensions			
2.1. Authority Key Identifier	Present	Yes	
2.1.1. Authority Key Identifier			
2.1.2. AuthorityCertIssuer			
2.1.3. AuthorityCertSerialNumber			

[170] The field "country" will always be Spain, since the certificate shows the relation between an employee and a Spanish regional health service, regardless of the nationality of the employee. This arises from the group nature of the external certificate, whose subscriber is the regional health service, and the employee, the person authorised for its use.

Field	Contents	Compulsory	Critical
2.2. Subject Key Identifier	Present	Yes	
2.3. Key Usage		Yes	Yes
2.3.1. Digital Signature	Not selected. “0”		
2.3.2. Content commitment	Selected. “1”	Yes	
2.3.3. Key Encipherment	Not selected. “0”		
2.3.4. Data Encipherment	Not selected. “0”		
2.3.5. Key Agreement	Not selected. “0”		
2.3.6. Key Certificate Signature	Not selected. “0”		
2.3.7. CRL Signature	Not selected. “0”		
2.4. Qualified Certificate Statements		Yes	
2.4.1. qCCompliance (0.4.0.1862.1.1)		Yes	
2.4.2. QcEuRetentionPeriod (0.4.0.1862.1.3)	15	Yes	
2.4.3. QcSSCD (0.4.0.1862.1.4)		Yes	
2.5. Certificate Policies		Yes	
2.5.1. Policy Identifier	1.3.6.1.4.1.26852.1.2.1.2	Yes	
2.5.2. Policy Qualifier ID		Yes	
2.5.2.1. CPS Pointer	“https://www.cgcom.es/CertECSAS”	Yes	
2.5.2.2. User Notice	“Certificate of qualified electronic signature of regional health service doctor. Conditions of use at https://www.cgcom.es/CertECSAS”	Yes	
2.5.3. Policy Identifier	OID of class 2 policy of VeriSign	Yes	
2.5.4. Policy Qualifier ID		Yes	

Field	Contents	Compulsory	Critical
2.5.4.1. CPS Pointer	Reference to VeriSign RPA	Yes	
2.5.4.2. User Notice	Notice of VeriSign user	Yes	
2.6. Subject Alternative Names		Yes	
2.6.1. rfc822Name	Corporate e-mail of employed doctor[171]	Yes	
2.6.2. Directory Name		Yes	
2.6.2.1. Type of certificate - OID 2.16.724.1.3.5.3.2.1	Electronic certificate of public employee	F[172]	
2.6.2.2. Name of subscriber entity - OID 2.16.724.1.3.5.3.2.2	Name of subscriber entity (health service)	F	
2.6.2.3. Tax ID Number (NIF) subscriber entity - OID 2.16.724.1.3.5.3.2.3	Tax ID Number (NIF) of subscriber entity	F	
2.6.2.4. National ID Document (DNI)/Foreigner's ID Number (NIE) of the responsible person - OID 2.16.724.1.3.5.3.2.4	National ID Document (DNI)/Foreigner's ID Number of the responsible person	F	
2.6.2.5. Personal identification number - OID 2.16.724.1.3.5.3.2.5	Identification number of doctor as public employee	O[173]	
2.6.2.6. Given name - OID 2.16.724.1.3.5.3.2.6	Given name of doctor - public employee	F	
2.6.2.7. First surname - OID 2.16.724.1.3.5.3.2.7	First surname of doctor - public employee	F	

[171] This field contains the corporate e-mail address of the employee, for notification purposes.

[172] Fixed field (F), in accordance with Certica profiles

[173] Optional field (O), in accordance with Certica profiles

Field	Contents	Compulsory	Critical
2.6.2.8. Second surname - OID 2.16.724.1.3.5.3.2.8	Second surname of doctor - public employee	F	
2.6.2.9. E-mail - OID 2.16.724.1.3.5.3.2.9	E-mail of doctor - public employee	O	
2.6.2.10. Organisational unit - OID 2.16.724.1.3.5.3.2.10	Unit, within the Administration, in which the doctor - public employee is included.	O	
2.6.2.11. Position or office - OID 2.16.724.1.3.5.3.2.11	Position held by doctor - public employee, within the Administration	O	
2.7. Issuer Alternative Name		Yes	
2.7.1. rfc822Name	"certificacion@cgcom.es"	Yes	
2.7.2. directoryName		Yes	
2.7.2.1. Organization (O)	"Consejo General de Colegios de Medicos"	Yes	
2.7.2.2. SerialNumber	"Q2866017C"	Yes	
2.7.2.3. Location (L)	"Plaza de las Cortes 11"	Yes	
2.7.2.4. Postal Code	"28014"	Yes	
2.7.2.5. State Or Province Name	"Madrid"	Yes	
2.7.2.6. Country (C)	ES	Yes	
2.8. Extended Key Usage		Yes	
2.8.1. emailProtection	Present	Yes	
2.9. cRLDistributionPoint		Yes	
2.9.1. distributionPoint	"http://crl1.cgcom.es/crl/ec-cgcom.crl"	Yes	
2.9.2. distributionPoint	"http://crl2.cgcom.es/crl/ec-cgcom.crl"	Yes	
2.10. Authority Info Access		Yes	

Field	Contents	Compulsory	Critical
2.10.1. Access Method		Yes	
2.10.2. Access Location	http://pki-ocsp.verisign.com	Yes	
2.11. NetscapeCertType	“SSL client”, “S/MIME”	Yes	
2.12. Subject Directory Attributes (2.5.29.9)		Yes	
2.12.1. Country of Citizenship	Country of nationality	Yes	
2.12.2. Country of Residence	Country of residence.	Yes	

7.3 Certificate of encipherment on card for external doctor

Field	Contents	Compulsory	Critical
1. Basic structure			
1.1. Version	"2"[174]	Yes	
1.2. Serial Number	Established automatically[175]	Yes	
1.3. Signature Algorithm	SHA-1 with RSA Signature / SHA-256 with RSA Signature	Yes	
1.4. Issuer Distinguished Name		Yes	
1.4.1. Country (C)	"ES"	Yes	
1.4.2. Organization (O)	"Organizacion Medica Colegial" [176]	Yes	
1.4.3. Organizational Unit (OU)	"Certification Entity" [177]	Yes	
1.4.4. Organizational Unit (OU)	"Class 2 Managed PKI Individual Subscriber CA"	Yes	
1.4.5. Organizational Unit (OU)	"VeriSign Trust Network"	Yes	
1.4.6. Common Name (CN)	"OMC"	Yes	
1.5. Validity	3 years.	Yes	
1.5.1. Not Before	Start date of validity	Yes	
1.5.2. Not After	Date of expiry	Yes	
1.6. Subject		Yes	

[174] The literal "2" corresponds to version 3.

[175] It should not exceed 32 hexadecimal characters in hexadecimal notation.

[176] The text is included without accents.

[177] The text is included without accents.

Field	Contents	Compulsory	Critical
1.6.1. Country (C)	"ES"[178]	Yes	
1.6.2. Organization (O)	Name of the regional health service	Yes	
1.6.3. Organizational Unit (OU)	"Electronic certificate of public employed doctor"	Yes	
1.6.4. Organizational Unit (OU)	Administrative unit	No	
1.6.5. Organizational Unit (OU)	Employee number	No	
1.6.6. Surname	Surnames + " – " + Tax ID Number (NIF) of employee	Yes	
1.6.7. Given Name	Given name	Yes	
1.6.8. Title	Position or post held by the person responsible for certificate	Yes	
1.6.9. Serial Number	National ID Document (DNI)/Foreigner's ID Number (NIE) of the public employee	Yes	
1.6.10. Common Name (CN)	Name, surnames + " – " + Tax ID Number (NIF) of employed doctor + "(CIPHERING)"	Yes	
1.7. Subject Public Key Info	2048-Bit Public key encoded in accordance with RFC2459 & PKCS#1	Yes	
2. Extensions			
2.1. Authority Key Identifier	Present	Yes	
2.1.1. Authority Key Identifier			
2.1.2. AuthorityCertIssuer			

[178] The field "country" will always be Spain, since the certificate shows the relation between an employee and a Spanish regional health service, regardless of the nationality of the employee. This arises from the group nature of the external certificate, whose subscriber is the regional health service, and the employee, the person authorised for its use.

Field	Contents	Compulsory	Critical
2.1.3. AuthorityCertSerialNumber			
2.2. Subject Key Identifier	Present	Yes	
2.3. Key Usage		Yes	Yes
2.3.1. Digital Signature	Not selected. “0”		
2.3.2. Content commitment	Not selected. “0”		
2.3.3. Key Encipherment	Selected. “1”	Yes	
2.3.4. Data Encipherment	Selected. “1”	Yes	
2.3.5. Key Agreement	Not selected. “0”		
2.3.6. Key Certificate Signature	Not selected. “0”		
2.3.7. CRL Signature	Not selected. “0”		
2.4. Qualified Certificate Statements		Yes	
2.4.1. qCCompliance (0.4.0.1862.1.1)		Yes	
2.4.2. QcEuRetentionPeriod (0.4.0.1862.1.3)	15	Yes	
2.4.3. QcSSCD (0.4.0.1862.1.4)		Yes	
2.5. Certificate Policies		Yes	
2.5.1. Policy Identifier	1.3.6.1.4.1.26852.1.2.1.3	Yes	
2.5.2. Policy Qualifier ID		Yes	
2.5.2.1. CPS Pointer	“https://www.cgcom.es/CertECSAS”	Yes	
2.5.2.2. User Notice	“Certificate of encipherment of regional health service doctor. Conditions of use at https://www.cgcom.es/CertECSAS”	Yes	
2.5.3. Policy Identifier	OID of class 2 policy of VeriSign	Yes	

Field	Contents	Compulsory	Critical
2.5.4. Policy Qualifier ID		Yes	
2.5.4.1. CPS Pointer	Reference to VeriSign RPA	Yes	
2.5.4.2. User Notice	Notice of VeriSign user	Yes	
2.6. Subject Alternative Names		Yes	
2.6.1. rfc822Name	Corporate e-mail of employed doctor[179]	Yes	
2.6.2. Directory Name		Yes	
2.6.2.1. Type of certificate - OID 2.16.724.1.3.5.3.2.1	Electronic certificate of public employee	F[180]	
2.6.2.2. Name of subscriber entity - OID 2.16.724.1.3.5.3.2.2	Name of subscriber entity (health service)	F	
2.6.2.3. Tax ID Number (NIF) subscriber entity - OID 2.16.724.1.3.5.3.2.3	Tax ID Number (NIF) of subscriber entity	F	
2.6.2.4. National ID Document (DNI)/Foreigner's ID Number (NIE) of the responsible person - OID 2.16.724.1.3.5.3.2.4	National ID Document (DNI)/Foreigner's ID Number of the responsible person	F	
2.6.2.5. Personal identification number - OID 2.16.724.1.3.5.3.2.5	Identification number of doctor as public employee	O[181]	
2.6.2.6. Given name - OID 2.16.724.1.3.5.3.2.6	Given name of doctor - public employee	F	
2.6.2.7. First surname - OID 2.16.724.1.3.5.3.2.7	First surname of doctor - public employee	F	

[179] This field contains the corporate e-mail address of the employee, for notification purposes.

[180] Fixed field (F), in accordance with Certica profiles

[181] Optional field (O), in accordance with Certica profiles

Field	Contents	Compulsory	Critical
2.6.2.8. Second surname - OID 2.16.724.1.3.5.3.2.8	Second surname of doctor - public employee	F	
2.6.2.9. E-mail - OID 2.16.724.1.3.5.3.2.9	E-mail of doctor - public employee	O	
2.6.2.10. Organisational unit - OID 2.16.724.1.3.5.3.2.10	Unit, within the Administration, in which the doctor - public employee is included.	O	
2.6.2.11. Position or office - OID 2.16.724.1.3.5.3.2.11	Position held by doctor - public employee, within the Administration	O	
2.7. Issuer Alternative Name		Yes	
2.7.1. rfc822Name	"certificacion@cgcom.es"	Yes	
2.7.2. directoryName		Yes	
2.7.2.1. Organization (O)	"Consejo General de Colegios de Medicos"	Yes	
2.7.2.2. SerialNumber	"Q2866017C"	Yes	
2.7.2.3. Location (L)	"Plaza de las Cortes 11"	Yes	
2.7.2.4. Postal Code	"28014"	Yes	
2.7.2.5. State Or Province Name	"Madrid"	Yes	
2.7.2.6. Country (C)	ES	Yes	
2.8. Extended Key Usage		Yes	
2.8.1. emailProtection	Present	Yes	
2.9. cRLDistributionPoint		Yes	
2.9.1. distributionPoint	"http://crl1.cgcom.es/crl/ec-cgcom.crl"	Yes	
2.9.2. distributionPoint	"http://crl2.cgcom.es/crl/ec-cgcom.crl"	Yes	
2.10. Authority Info Access		Yes	

Field	Contents	Compulsory	Critical
2.10.1. Access Method		Yes	
2.10.2. Access Location	http://pki-ocsp.verisign.com	Yes	
2.11. NetscapeCertType	“SSL client”, “S/MIME”	Yes	
2.12. Subject Directory Attributes (2.5.29.9)		Yes	
2.12.1. Country of Citizenship	Country of nationality	Yes	
2.12.2. Country of Residence	Country of residence.	Yes	