Perfiles de Certificados de la Entidad de Certificación

Organización Médica Colegial de España

1. Información general

1.1 Control documental

Proyecto:	**Documentación de prácticas de la Entidad de Certificación**
Entidad de destino:	**Organización Médica Colegial de España**
Versión:	**3.10**
Fecha de la edición:	**18/03/2015**
Archivo:	**Perfiles_CGCOM_v3r10.doc**
Formato:	**MS Word 2013**
Autores:	**Astrea**

1.2 Estado formal

Preparado por:	**Revisado por:**	**Aprobado por:**
Nombre: Astrea Fecha: **18/03/2015**	Nombre: OMC Fecha:	Nombre: OMC Fecha:

1.3 Control de versiones

Versión	Partes que cambian	Descripción cambio	Autor cambio	Fecha cambio
1.0	Todo	Original	Astrea	18/07/2006
2.0	Perfiles	Revisión OMC	Astrea	09/08/2006
2.1	Perfiles	Revisión VeriSign	Astrea	19/09/2006
2.2	Perfiles	Corrección OIDs política	Astrea	25/09/2006
3.0	Perfiles	Adición perfiles externos	Astrea	15/12/2009
3.1	Perfil externos	Adición Pol. Certica	Astrea	22/03/2011
3.2	Perfil software y otras	. Adición Perfil Persona Jurídica en software . Mejoras en el campo Qualified Certificate Statements de todos los perfiles	Astrea	13/07/2011
3.3	Perfiles	. Alineación con el contenido de los diversos certificados emitidos. . Se amplía el Issuer Alternative Name	Astrea	18/01/2012
3.4	Perfiles	Inclusión información OCSP	Astrea	13/07/2012
	Perfil externo	Modificación del Title del Subject.	Astrea	13/07/2012
3.5 3.6	Nuevos perfiles	. Cambio de nombre en el certificado de colegio por el de Persona jurídica. . Se añaden los certificados de cifrado. . Se añaden nuevos tipos de certificado para la identificación y la firma de forma separada. . Se añade perfil de certificado en software para personal administrativo	Astrea	07/06/2013
3.7	Perfiles	. Eliminación de perfiles antiguos . Revisión para la eliminación de anotaciones referentes a VeriSign . Inclusión perfil de certificado de colegiado en software y en HSM . Eliminación campo email en el *subject* . Eliminación del "*usernotice*" en el *Certificate Policy* . Se añade la dirección del certificado raíz en el *Authority Information Acces*	Astrea	05/11/2014

		. Corrección de errores en diversos perfiles incluyendo campo *OU* en el *subject* para el dispositivo		
3.8	Cambio URL	. Se cambia URL del certificado raíz de la EC OMC. . Se cambian las URL de las listas de revocación.	Astrea	15/01/2015
3.9	Perfil de personal administrativo	. Se añade la opción de smartCardLogon en EKU.	Astrea	23/02/2015
3.10	En todos los perfiles	. Se elimina el campo Locality en el Issuer DN	Astrea	18/03/2015

1.4 Referencias

- Política de certificación de la Organización Médica Colegial de España.
- Orden HAC/1181/2003, de 12 de mayo, por la que se establecen normas específicas sobre el uso de la firma electrónica en las relaciones tributarias por medios electrónicos, informáticos y telemáticos con la Agencia Estatal de Administración Tributaría. (B.O.E. 15-05-2003).
- Esquema de identificación y firma electrónica de las Administraciones públicas. Bloque I: Perfiles de certificados electrónicos (v1.7.3) CertiCA

2. Índice

1. Información general 2
1.1 Control documental 2
1.2 Estado formal 2
1.3 Control de versiones 3
1.4 Referencias 5
2. Índice 6
3. Introducción 7
3.1 Tipología de certificados a expedir 7
3.2 Perfiles efectivos a implantar 9
3.3 Cuadro resumen de los tipos de certificados 10
3.3.1 Certificados en vigor 10
3.3.2 Certificados obsoletos 11
4. CERTIFICADOS DE COLEGIADO 12
4.1 Certificado corporativo de colegiado (persona física) para identificación 12
4.2 Certificado corporativo de colegiado (persona física) para firma 16
4.3 Certificado de cifrado en tarjeta, para colegiado 20
4.4 Certificado corporativo de colegiado (persona física), en SOFTWARE, para identificación, firma y cifrado 24
4.5 Certificado corporativo de colegiado (persona física), en HSM, para identificación, firma y cifrado 28
4.6 Certificado de colectivo de médico empleado público (persona física) para identificación 32
4.7 Certificado de colectivo de médico empleado público (persona física) para firma 37
4.8 Certificado de cifrado en tarjeta, para médico empleado público 42
5. CERTIFICADOS DE PERSONAL ADMINISTRATIVO 47
5.1 Certificado corporativo de personal administrativo (persona física) para identificación 47
5.2 Certificado corporativo de personal administrativo (persona física) para firma 51
5.3 Certificado de cifrado en tarjeta, para personal administrativo 55
5.4 Certificado corporativo de personal administrativo (persona física), en software, para identificación, firma y cifrado 59
6. CERTIFICADOS DE PERSONA JURÍDICA 63
6.1 Certificado corporativo de persona jurídica para identificación 63
6.2 Certificado corporativo de persona jurídica para firma 67
6.3 Certificado de cifrado en tarjeta, para persona jurídica 71
6.4 Certificado corporativo de persona jurídica en software, para identificación, firma y cifrado 75

3. Introducción

3.1 Tipología de certificados a expedir

La política de certificación de la Organización Médica Colegial determina la posibilidad de expedir los siguientes tipos de certtificados:

a) Certificados de firma y certificados de cifrado

En cuanto al uso, existen dos tipos de certificados:

1) Certificados de firma electrónica, reconocidos, que se emplean como base de la firma electrónica avanzada, y en conjunción con un dispositivo seguro de creación de firma. También se pueden emplear para firmar mensajes de autenticación (confirmación de la identidad), así como para firmar otros tipos de mensajes.

2) Certificados de cifrado, ordinarios, que se emplean para producir o recibir documentos y mensajes cifrados.

b) Certificados corporativos y certificados de empleados

Los certificados de entidad final pueden ser certificados corporativos o certificados de empleados:

1) Los certificados corporativos se caracterizan por el hecho de que el suscriptor pertenece a una de las entidades que integran la Organización Médica Colegial. Los certificados corporativos siempre son de colectivo.

2) Los certificados de empleado son los restantes certificados. Es necesario realizar un registro completo de los datos a certificar.

Únicamente se expiden certificados de empleado, excepto cuando resulte necesario, como por ejemplo en el caso de médicos de un servicio autonómico de salud o de un centro privado de salud. Los certificados de empleado pueden ser individuales o de colectivo:

a) Certificados de empleado individuales, caracterizados por el hecho de que la persona identificada en el certificado actúa en su propio nombre y representación (siendo en este caso el suscriptor o titular del certificado)

b) Certificados de empleado de colectivo, en los que la persona identificada en el certificado actúa dentro del ámbito organizativo de una persona jurídica (que será el suscriptor o titular del certificado). Por ejemplo, los certificados emitidos a médicos,

adscritos a un servicio autonómico de salud o un centro privado de salud serán certificados de empleado de colectivo, donde el suscriptor será el citado servicio autonómico o centro privado de salud.

Los certificados de empleado de colectivo emitidos a un médico colegiado adscrito a un servicio autonómico o centro privado de salud pueden incluirse en la tarjeta profesional que el Colegio expide al médico colegiado, en cuyo caso la tarjeta incluirá dos certificados.

Asimismo, el certificado de empleado de colectivo podrá ser expedido de forma remota con la autenticación basada en la firma electrónica reconocida del médico colegiado.

c) Certificados de colegiado y certificados de personal administrativo

Los certificados corporativos pueden expedirse a colegiados o a personal administrativo:

1) Certificados de colegiado, emitidos con la intervención de su Colegio de Médicos, en calidad de registrador con la capacidad exclusiva de certificar la cualidad de “colegiado” de una persona identificada en el certificado.

2) Certificados de personal administrativo de las entidades que integran la Organización Médica Colegial.

d) Certificados de persona física y certificados de persona jurídica

Los certificados pueden expedirse a personas físicas o a personas jurídicas:

1) Certificados de persona física, que actúa como firmante, debiendo tomarse en cuenta sus apoderamientos y capacidades de actuación, indicadas o no en el certificado, antes de confiar en la firma.

2) Certificados de persona jurídica, a la cual se imputan los documentos firmados, como firmante, sin que sea necesario tener en cuenta los apoderamientos o capacidades de actuación de la persona que custodia el certificado de firma electrónica.

3.2 Perfiles efectivos a implantar

Este documento recoge los perfiles de certificados que expedirá la Entidad de Certificación de la Organización Médica Colegial del España.

Los certificados que se expiden en tarjeta criptográfica con la consideración de dispositivo seguro de creación de firma durarán un máximo de cinco años, con re-autenticación anual de los poseedores de claves, mediante procedimientos organizativos.
Los certificados que se expiden en soporte de software durarán un máximo de cinco años, con re-autenticación anual de los poseedores de claves, mediante procedimientos organizativos.

Los certificados de médico colegiado en tarjeta (carné colegial) son la pieza básica a partir de los cuales dependen el resto de certificados de médico (subordinados en software o HSM y de empleado público). Si un certificado de médico colegiado en tarjeta es revocado todos los demás también serán revocados.

El OID de OMC es 1.3.6.1.4.1.26852

La rama de OIDs de la EC-OMC para la certificación es el 1.3.6.1.4.1.26852.1

3.3 Cuadro resumen de los tipos de certificados

3.3.1 Certificados en vigor

Tipo de certificado	OID	Funciones
Certificados corporativos	**1.3.6.1.4.1.26852.1.**1	
Corporativos en tarjeta		
de colegiado en tarjeta (I)	1.3.6.1.4.1.26852.1.1.1.1	Identificación
de colegiado en tarjeta (F)	1.3.6.1.4.1.26852.1.1.1.2	Firma
de colegiado en tarjeta (C)	1.3.6.1.4.1.26852.1.1.1.3	Cifrado
de personal administrativo en tarjeta (I)	1.3.6.1.4.1.26852.1.1.2.1	Identificación
de personal administrativo en tarjeta (F)	1.3.6.1.4.1.26852.1.1.2.2	Firma
de personal administrativo en tarjeta (C)	1.3.6.1.4.1.26852.1.1.2.3	Cifrado
de persona jurídica en tarjeta (I)	1.3.6.1.4.1.26852.1.1.3.1	Identificación
de persona jurídica en tarjeta (F)	1.3.6.1.4.1.26852.1.1.3.2	Firma
de persona jurídica en tarjeta (C)	1.3.6.1.4.1.26852.1.1.3.3	Cifrado
Corporativos en software		
de persona jurídica en SOFTWARE	1.3.6.1.4.1.26852.1.1.5	Identificación, firma y cifrado
de personal administrativo en SOFTWARE	1.3.6.1.4.1.26852.1.1.6	Identificación, firma y cifrado
de colegiado en SOFTWARE	1.3.6.1.4.1.26852.1.1.7	Identificación, firma y cifrado
Corporativos en HSM		
de médico colegiado en HSM	1.3.6.1.4.1.26852.1.1.9	Identificación, firma y cifrado

Tipo de certificado	OID	Funciones
Certificados de empleados	**1.3.6.1.4.1.26852.1.**2	
De empleados públicos en tarjeta		
de médico empleado público en tarjeta (I)	1.3.6.1.4.1.26852.1.2.1.1	Identificación [1]
de médico empleado público en tarjeta (F)	1.3.6.1.4.1.26852.1.2.1.2	Firma [2]
de médico empleado público en tarjeta (C)	1.3.6.1.4.1.26852.1.2.1.3	Cifrado [3]

[1] Siguiendo perfil CERTICA para autenticación

[2] Siguiendo perfil CERTICA para firma

[3] Siguiendo perfil CERTICA para cifrado

3.3.2 Certificados obsoletos

Tipo de certificado	OID	Estado
Certificados corporativos	**1.3.6.1.4.1.26852.1.**1	
Corporativos en tarjeta		
*de **colegiado** (I,F,C)*	*1.3.6.1.4.1.26852.1.1.1*	*OBSOLETO*
*de **personal administrativo** (I,F,C)*	*1.3.6.1.4.1.26852.1.1.2*	*OBSOLETO*
*de **persona jurídica** (I,F,C)*	*1.3.6.1.4.1.26852.1.1.3*	*OBSOLETO*
*de **órgano colegial** (I,F,C)*	*1.3.6.1.4.1.26852.1.1.4*	*OBSOLETO*
de órgano colegial en tarjeta (I)	*1.3.6.1.4.1.26852.1.1.4.1*	*OBSOLETO*
de órgano colegial en tarjeta (F)	*1.3.6.1.4.1.26852.1.1.4.2*	*OBSOLETO*
de órgano colegial en tarjeta (C)	*1.3.6.1.4.1.26852.1.1.4.3*	*OBSOLETO*
Corporativos en software		
de órgano colegial en SOFTWARE	*1.3.6.1.4.1.26852.1.1.8*	*OBSOLETO*

Tipo de certificado	OID	Estado
Certificados de empleados	**1.3.6.1.4.1.26852.1.2**	
De empleados en tarjeta		
*de **médico empleado público***	*1.3.6.1.4.1.26852.1.2.1*	*OBSOLETO*

4. CERTIFICADOS DE COLEGIADO

4.1 Certificado corporativo de colegiado (persona física) para identificación

Campo	Contenido	Obligatorio	Crítico
1. Basic estructure			
1.1. Version	"2"[4]	Sí	
1.2. Serial Number	Establecido automáticamente[5]	Sí	
1.3. Signature Algorithm	SHA-256 with RSA Signature	Sí	
1.4. Issuer Distinguished Name		Sí	
1.4.1. Country (C)	"ES"	Sí	
1.4.2. Organization (O)	"Organizacion Medica Colegial"[6]	Sí	
1.4.3. Organizational Unit (OU)	"Entidad de Certificacion" [7]	Sí	
1.4.4. Common Name (CN)	"OMC"	Sí	
1.5. Validity	5 años	Sí	
1.5.1. Not Before	Fecha de inicio de validez	Sí	
1.5.2. Not After	Fecha de expiración	Sí	
1.6. Subject		Sí	
1.6.1. Country (C)	"ES"[8]	Sí	

[4] El literal "2" corresponde a la versión 3.

[5] No debe superar los 32 caracteres hexadecimales en notación hexadecimal.

[6] El texto se incluye sin acentos.

[7] El texto se incluye sin acentos.

[8] El campo "país" siempre será España, dado que el certificado muestra la relación entre un colegiado y un colegio profesional español, con independencia de la nacionalidad del colegiado. Ello deriva de

Campo	Contenido	Obligatorio	Crítico
1.6.2. Organization (O)	Colegio profesional	Sí	
1.6.3. Organizational Unit (OU)	"Condiciones de uso en https://www.cgcom.es/CertCol (c)06"	Sí	
1.6.4. Organizational Unit (OU)	"Carnet colegial"[9]	Sí	
1.6.5. Surname	Apellidos	Sí	
1.6.6. Given Name	Nombre	Sí	
1.6.7. Title	"Médico colegiado/a"	Sí	
1.6.8. Serial Number	DNI/NIE[10]	Sí	
1.6.9. Common Name (CN)	"(Col.)" + Nombre y apellidos + "-" + Número de colegiado + "(AUTENTICACION)"	Sí	
1.7. Subject Public Key Info	2048-Bit Public key encoded in accordance with RFC2459 & PKCS#1	Sí	
2. Extensions			
2.1. Authority Key Identifier	Presente	Sí	
2.1.1. Key Identifier			
2.1.2. AuthorityCertIssuer			
2.1.3. AuthorityCertSerialNumber			
2.2. Subject Key Identifier	Presente	Sí	
2.3. Key Usage		Sí	Sí
2.3.1. Digital Signature	Seleccionado. "1"	Sí	

la naturaleza corporativa del certificado, del cual es suscriptor el colegio, y el colegiado, la persona autorizada a su uso.

[9] Este campo se refiere al dispositivo usado, en este caso una tarjeta criptográfica que también sirve de carnet colegial.

[10] El campo "número de serie" debe incluir el DNI o el NIE del colegiado, al efecto de la admisión del certificado para la realización de trámites con las Administraciones españolas.

Campo	Contenido	Obligatorio	Crítico
2.3.2. Content commintment	No seleccionado. “0”		
2.3.3. Key Encipherment	No seleccionado. “0”		
2.3.4. Data Encipherment	No seleccionado. “0”		
2.3.5. Key Agreement	No seleccionado. “0”		
2.3.6. Key Certificate Signature	No seleccionado. “0”		
2.3.7. CRL Signature	No seleccionado. “0”		
2.4. Qualified Certificate Statements		Sí	
2.4.1. qCCompliance (0.4.0.1862.1.1)		Sí	
2.4.2. QcEuRetentionPeriod (0.4.0.1862.1.3)	15	Sí	
2.4.3. QcSSCD (0.4.0.1862.1.4)		Sí	
2.5. Certificate Policies		Sí	
2.5.1. Policy Identifier	1.3.6.1.4.1.26852.1.1.1.1	Sí	
2.5.2. Policy Qualifier ID		Sí	
2.5.2.1. CPS Pointer	“https://www.cgcom.es/CertCol”	Sí	
2.6. Subject Alternative Names		Sí	
2.6.1. rfc822Name	Correo electrónico corporativo del colegiado/a[11]	Sí	
2.6.2. directoryName[12]		Sí	
2.6.2.1. CGCOM.2.1	IdColegio	Sí	

[11] Este campo contiene la dirección de correo corporativo del colegiado, a efectos de notificaciones.

[12] Este campo enlaza con el sistema de validación y re-certificación del CGCOM, permitiendo recuperar informaciones adicionales de forma eficiente. Ciertas informacions se incluyen, aunque sean redundantes, para disponer de toda la información sobre el usuario en una sola consulta contra el certificado.

Campo	Contenido	Obligatorio	Crítico
2.6.2.2. CGCOM.2.2	Colegio profesional	Sí	
2.6.2.3. CGCOM.2.3	IdColegiado	Sí	
2.6.2.4. CGCOM.2.4	Nombre y apellidos del colegiado	Sí	
2.7. Issuer Alternative Name		Sí	
2.7.1. rfc822Name	"certificacion@cgcom.es"	Sí	
2.8. Extended Key Usage		Sí	
2.8.1. clientAuth	Presente	Sí	
2.9. cRLDistributionPoint		Sí	
2.9.1. distributionPoint	"http://crl3.cgcom.es/crl/eccgcom.crl"	Sí	
2.9.2. distributionPoint	"http://crl4.cgcom.es/crl/eccgcom.crl"	Sí	
2.10. Authority Info Acces		Sí	
2.10.1. OCSP Access Method		Sí	
2.10.1.1. Acces Location	"http://ocsp.cgcom.es"	Sí	
2.10.2. caIssuersAccessMethod		Sí	
2.10.2.1. Acces Location	"http://certificacion.cgcom.es/CA/OMC.crt"	Sí	
2.11. Subject Directory Attributes (2.5.29.9)		Sí	
2.11.1. Country of Citizenship	País de nacionalidad	Sí	
2.11.2. Country of Residence	País de residencia	Sí	

4.2 Certificado corporativo de colegiado (persona física) para firma

Campo	Contenido	Obligatorio	Crítico
1. Basic estructure			
1.1. Version	"2"[13]	Sí	
1.2. Serial Number	Establecido automáticamente[14]	Sí	
1.3. Signature Algorithm	SHA-256 with RSA Signature	Sí	
1.4. Issuer Distinguished Name		Sí	
1.4.1. Country (C)	"ES"	Sí	
1.4.2. Organization (O)	"Organizacion Medica Colegial"[15]	Sí	
1.4.3. Organizational Unit (OU)	"Entidad de Certificacion" [16]	Sí	
1.4.4. Common Name (CN)	"OMC"	Sí	
1.5. Validity	5 años	Sí	
1.5.1. Not Before	Fecha de inicio de validez	Sí	
1.5.2. Not After	Fecha de expiración	Sí	
1.6. Subject		Sí	
1.6.1. Country (C)	"ES"[17]	Sí	
1.6.2. Organization (O)	Colegio profesional	Sí	

[13] El literal "2" corresponde a la versión 3.

[14] No debe superar los 32 caracteres hexadecimales en notación hexadecimal.

[15] El texto se incluye sin acentos.

[16] El texto se incluye sin acentos.

[17] El campo "país" siempre será España, dado que el certificado muestra la relación entre un colegiado y un colegio profesional español, con independencia de la nacionalidad del colegiado. Ello deriva de la naturaleza corporativa del certificado, del cual es suscriptor el colegio, y el colegiado, la persona autorizada a su uso.

Campo	Contenido	Obligatorio	Crítico
1.6.3. Organizational Unit (OU)	"Condiciones de uso en https://www.cgcom.es/CertCol (c)06"	Sí	
1.6.4. Organizational Unit (OU)	"Carnet colegial"[18]	Sí	
1.6.5. Surname	Apellidos	Sí	
1.6.6. Given Name	Nombre	Sí	
1.6.7. Title	"Médico colegiado/a"	Sí	
1.6.8. Serial Number	DNI/NIE[19]	Sí	
1.6.9. Common Name (CN)	"(Col.)" + Nombre y apellidos + "-" + Número de colegiado + "-"+ "(FIRMA)"	Sí	
1.7. Subject Public Key Info	2048-Bit Public key encoded in accordance with RFC2459 & PKCS#1	Sí	
2. Extensions			
2.1. Authority Key Identifier	Presente	Sí	
2.1.1. Key Identifier			
2.1.2. AuthorityCertIssuer			
2.1.3. AuthorityCertSerialNumber			
2.2. Subject Key Identifier	Presente	Sí	
2.3. Key Usage		Sí	Sí
2.3.1. Digital Signature	No seleccionado. "0"		
2.3.2. Content commintment	Seleccionado. "1"	Sí	
2.3.3. Key Encipherment	No seleccionado. "0"		
2.3.4. Data Encipherment	No seleccionado. "0"		

[18] Este campo se refiere al dispositivo usado, en este caso una tarjeta criptográfica que también sirve de carnet colegial.

[19] El campo "número de serie" debe incluir el DNI o el NIE del colegiado, al efecto de la admisión del certificado para la realización de trámites con las Administraciones españolas.

Campo	Contenido	Obligatorio	Crítico
2.3.5. Key Agreement	No seleccionado. “0”		
2.3.6. Key Certificate Signature	No seleccionado. “0”		
2.3.7. CRL Signature	No seleccionado. “0”		
2.4. Qualified Certificate Statements		Sí	
2.4.1. qCCompliance (0.4.0.1862.1.1)		Sí	
2.4.2. QcEuRetentionPeriod (0.4.0.1862.1.3)	15	Sí	
2.4.3. QcSSCD (0.4.0.1862.1.4)		Sí	
2.5. Certificate Policies		Sí	
2.5.1. Policy Identifier	1.3.6.1.4.1.26852.1.1.1.2	Sí	
2.5.2. Policy Qualifier ID		Sí	
2.5.2.1. CPS Pointer	“https://www.cgcom.es/CertCol”	Sí	
2.6. Subject Alternative Names		Sí	
2.6.1. rfc822Name	Correo electrónico corporativo del colegiado/a[20]	Sí	
2.6.2. directoryName[21]		Sí	
2.6.2.1. CGCOM.2.1	IdColegio	Sí	
2.6.2.2. CGCOM.2.2	Colegio profesional	Sí	
2.6.2.3. CGCOM.2.3	IdColegiado	Sí	
2.6.2.4. CGCOM.2.4	Nombre y apellidos del colegiado	Sí	

[20] Este campo contiene la dirección de correo corporativo del colegiado, a efectos de notificaciones.

[21] Este campo enlaza con el sistema de validación y re-certificación del CGCOM, permitiendo recuperar informaciones adicionales de forma eficiente. Ciertas informacions se incluyen, aunque sean redundantes, para disponer de toda la información sobre el usuario en una sola consulta contra el certificado.

Campo	Contenido	Obligatorio	Crítico
2.7. Issuer Alternative Name		Sí	
2.7.1. rfc822Name	"certificacion@cgcom.es"	Sí	
2.8. Extended Key Usage		Sí	
2.8.1. emailProtection	Presente	Sí	
2.9. cRLDistributionPoint		Sí	
2.9.1. distributionPoint	"http://crl3.cgcom.es/crl/eccgcom.crl"	Sí	
2.9.2. distributionPoint	"http://crl4.cgcom.es/crl/eccgcom.crl"	Sí	
2.10. Authority Info Acces		Sí	
2.10.1. OCSP Access Method		Sí	
2.10.1.1. Acces Location	"http://ocsp.cgcom.es"	Sí	
2.10.2. caIssuersAccessMethod		Sí	
2.10.2.1. Acces Location	"http://certificacion.cgcom.es/CA/OMC.crt"	Sí	
2.11. Subject Directory Attributes (2.5.29.9)		Sí	
2.11.1. Country of Citizenship	País de nacionalidad	Sí	
2.11.2. Country of Residence	País de residencia	Sí	

4.3 Certificado de cifrado en tarjeta, para colegiado

Campo	Contenido	Obligatorio	Crítico
1. Basic estructure			
1.1. Version	"2"[22]	Sí	
1.2. Serial Number	Establecido automáticamente[23]	Sí	
1.3. Signature Algorithm	SHA-256 with RSA Signature	Sí	
1.4. Issuer Distinguished Name		Sí	
1.4.1. Country (C)	"ES"	Sí	
1.4.2. Organization (O)	"Organizacion Medica Colegial" [24]	Sí	
1.4.3. Organizational Unit (OU)	"Entidad de Certificacion" [25]	Sí	
1.4.4. Common Name (CN)	"OMC"	Sí	
1.5. Validity	5 años	Sí	
1.5.1. Not Before	Fecha de inicio de validez	Sí	
1.5.2. Not After	Fecha de expiración	Sí	
1.6. Subject		Sí	
1.6.1. Country (C)	"ES"[26]	Sí	
1.6.2. Organization (O)	Colegio profesional	Sí	
1.6.3. Organizational Unit (OU)	"Condiciones de uso en https://www.cgcom.es/CertCol (c)06"	Sí	
1.6.4. Organizational Unit	"Carnet colegial"[27]	Sí	

[22] El literal "2" corresponde a la versión 3.

[23] No debe superar los 32 caracteres hexadecimales en notación hexadecimal.

[24] El texto se incluye sin acentos.

[25] El texto se incluye sin acentos.

[26] El campo "país" siempre será España.

Campo	Contenido	Obligatorio	Crítico
(OU)			
1.6.5. Surname	Apellidos	Sí	
1.6.6. Given Name	Nombre	Sí	
1.6.7. Title	"Médico colegiado/a"	Sí	
1.6.8. Serial Number	DNI/NIE[28]	Sí	
1.6.9. Common Name (CN)	"(Col.)" + Nombre y apellidos + "-" + Número de colegiado + "(CIFRADO)"	Sí	
1.7. Subject Public Key Info	2048-Bit Public key encoded in accordance with RFC2459 & PKCS#1	Sí	
2. Extensions			
2.1. Authority Key Identifier	Presente	Sí	
2.1.1. Key Identifier			
2.1.2. AuthorityCertIssuer			
2.1.3. AuthorityCertSerialNumber			
2.2. Subject Key Identifier	Presente	Sí	
2.3. Key Usage		Sí	Sí
2.3.1. Digital Signature	No seleccionado. "0"		
2.3.2. Content commintment	No seleccionado. "0"		
2.3.3. Key Encipherment	Seleccionado. "1"	Sí	
2.3.4. Data Encipherment	Seleccionado. "1"	Sí	
2.3.5. Key Agreement	No seleccionado. "0"		
2.3.6. Key Certificate Signature	No seleccionado. "0"		

[27] Este campo se refiere al dispositivo usado, en este caso una tarjeta criptográfica que también sirve de carnet colegial.

[28] El campo "número de serie" debe incluir el DNI o el NIE del colegiado, al efecto de la admisión del certificado para la realización de trámites con las Administraciones españolas.

Campo	Contenido	Obligatorio	Crítico
2.3.7. CRL Signature	No seleccionado. "0"		
2.4. Qualified Certificate Statements		Sí	
2.4.1. qCCompliance (0.4.0.1862.1.1)		Sí	
2.4.2. QcEuRetentionPeriod (0.4.0.1862.1.3)	15	Sí	
2.4.3. QcSSCD (0.4.0.1862.1.4)		Sí	
2.5. Certificate Policies		Sí	
2.5.1. Policy Identifier	1.3.6.1.4.1.26852.1.1.1.3	Sí	
2.5.2. Policy Qualifier ID		Sí	
2.5.2.1. CPS Pointer	"https://www.cgcom.es/CertCol"	Sí	
2.6. Subject Alternative Names		Sí	
2.6.1. rfc822Name	Correo electrónico corporativo[29]	Sí	
2.6.2. directoryName[30]		Sí	
2.6.2.1. CGCOM.2.1	IdColegio / IdEntidad	Sí	
2.6.2.2. CGCOM.2.2	Colegio profesional / Entidad jurídica ámbito sanitario	Sí	
2.6.2.3. CGCOM.2.3	IdColegiado	Sí	
2.6.2.4. CGCOM.2.4	Nombre y apellidos del colegiado	Sí	
2.7. Issuer Alternative Name		Sí	
2.7.1. rfc822Name	"certificacion@cgcom.es"	Sí	
2.8. Extended Key Usage		Sí	

[29] Este campo contiene la dirección de correo corporativo del colegiado, a efectos de notificaciones.

[30] Este campo enlaza con el sistema de validación y re-certificación del CGCOM, permitiendo recuperar informaciones adicionales de forma eficiente. Ciertas informacions se incluyen, aunque sean redundantes, para disponer de toda la información sobre el usuario en una sola consulta contra el certificado.

Campo	Contenido	Obligatorio	Crítico
2.8.1. emailProtection	Presente	Sí	
2.9. cRLDistributionPoint		Sí	
2.9.1. distributionPoint	"http://crl3.cgcom.es/crl/eccgcom.crl"	Sí	
2.9.2. distributionPoint	"http://crl4.cgcom.es/crl/eccgcom.crl"	Sí	
2.10. Authority Info Acces		Sí	
2.10.1. OCSP Access Method		Sí	
2.10.1.1. Acces Location	"http://ocsp.cgcom.es"	Sí	
2.10.2. caIssuersAccessMethod		Sí	
2.10.2.1. Acces Location	"http://certificacion.cgcom.es/CA/OMC.crt"	Sí	
2.11. Subject Directory Attributes (2.5.29.9)		Sí	
2.11.1. Country of Citizenship	País de nacionalidad	Sí	
2.11.2. Country of Residence	País de residencia	Sí	

4.4 Certificado corporativo de colegiado (persona física), en SOFTWARE, para identificación, firma y cifrado

Campo	Contenido	Obligatorio	Crítico
1. Basic estructure			
1.1. Version	"2"[31]	Sí	
1.2. Serial Number	Establecido automáticamente[32]	Sí	
1.3. Signature Algorithm	SHA-256 with RSA Signature	Sí	
1.4. Issuer Distinguished Name		Sí	
1.4.1. Country (C)	"ES"	Sí	
1.4.2. Organization (O)	"Organizacion Medica Colegial" [33]	Sí	
1.4.3. Organizational Unit (OU)	"Entidad de Certificacion" [34]	Sí	
1.4.4. Common Name (CN)	"OMC"	Sí	
1.5. Validity	5 años	Sí	
1.5.1. Not Before	Fecha de inicio de validez	Sí	
1.5.2. Not After	Fecha de expiración	Sí	
1.6. Subject		Sí	
1.6.1. Country (C)	"ES"[35]	Sí	
1.6.2. Organization (O)	Colegio profesional u otra persona	Sí	

[31] El literal "2" corresponde a la versión 3.

[32] No debe superar los 32 caracteres hexadecimales en notación hexadecimal.

[33] El texto se incluye sin acentos.

[34] El texto se incluye sin acentos.

[35] El campo "país" siempre será España, dado que el certificado muestra la relación entre un colegiado y un colegio profesional español, con independencia de la nacionalidad del colegiado. Ello deriva de la naturaleza corporativa del certificado, del cual es suscriptor el colegio, y el colegiado, la persona autorizada a su uso..

Campo	Contenido	Obligatorio	Crítico
	jurídica del ámbito sanitario		
1.6.3. Organizational Unit (OU)	"Condiciones de uso en https://www.cgcom.es/CertColSoft (c)14"	Sí	
1.6.4. Organizational Unit (OU)	Dispositivo[36]	Sí	
1.6.5. Surname	Apellidos	Sí	
1.6.6. Given Name	Nombre	Sí	
1.6.7. Title	"Médico colegiado/a"	Sí	
1.6.8. Serial Number	DNI/NIE[37]	Sí	
1.6.9. Common Name (CN)	"(Col.)" + Nombre y apellidos + "-" + Número de colegiado + "(SOFTWARE)"	Sí	
1.7. Subject Public Key Info	2048-Bit Public key encoded in accordance with RFC2459 & PKCS#1	Sí	
2. Extensions			
2.1. Authority Key Identifier	Presente	Sí	
2.1.1. Key Identifier			
2.1.2. AuthorityCertIssuer			
2.1.3. AuthorityCertSerialNumber			
2.2. Subject Key Identifier	Presente	Sí	
2.3. Key Usage		Sí	Sí
2.3.1. Digital Signature	Seleccionado. "1"	Sí	
2.3.2. Content commintment	Seleccionado. "1"	Sí	

[36] Este campo se refiere al dispositivo usado por las claves y el certificado como puede ser: movil o tableta personal o del organismo público o del centro privado de salud.

[37] El campo "número de serie" debe incluir el DNI o el NIE del médico, al efecto de la admisión del certificado para la realización de trámites con las Administraciones españolas.

Campo	Contenido	Obligatorio	Crítico
2.3.3. Key Encipherment	Seleccionado. “1”	Sí	
2.3.4. Data Encipherment	Seleccionado. “1”	Sí	
2.3.5. Key Agreement	No seleccionado. “0”		
2.3.6. Key Certificate Signature	No seleccionado. “0”		
2.3.7. CRL Signature	No seleccionado. “0”		
2.4. Qualified Certificate Statements		Sí	
2.4.1. qCCompliance (0.4.0.1862.1.1)		Sí	
2.4.2. QcEuRetentionPeriod (0.4.0.1862.1.3)	15	Sí	
2.5. Certificate Policies		Sí	
2.5.1. Policy Identifier	1.3.6.1.4.1.26852.1.1.7	Sí	
2.5.2. Policy Qualifier ID		Sí	
2.5.2.1. CPS Pointer	“https://www.cgcom.es/CertColSoft”	Sí	
2.6. Subject Alternative Names		Sí	
2.6.1. rfc822Name	Correo electrónico corporativo del médico colegiado/a[38]	Sí	
2.6.2. directoryName[39]		Sí	
2.6.2.1. CGCOM.2.1	IdColegio / IdEntidad	Sí	
2.6.2.2. CGCOM.2.2	Colegio profesional / Entidad jurídica ámbito sanitario	Sí	
2.6.2.3. CGCOM.2.3	IdColegiado	Sí	

[38] Este campo contiene la dirección de correo corporativo del médico colegiado/a, a efectos de notificaciones.

[39] Este campo enlaza con el sistema de validación y re-certificación del CGCOM, permitiendo recuperar informaciones adicionales de forma eficiente. Ciertas informacions se incluyen, aunque sean redundantes, para disponer de toda la información sobre el usuario en una sola consulta contra el certificado.

Campo	Contenido	Obligatorio	Crítico
2.6.2.4. CGCOM.2.4	Nombre y apellidos del colegiado	Sí	
2.7. Issuer Alternative Name		Sí	
2.7.1. rfc822Name	"certificacion@cgcom.es"	Sí	
2.8. Extended Key Usage		Sí	
2.8.1. emailProtection	Presente	Sí	
2.8.2. clientAuth	Presente	Sí	
2.9. cRLDistributionPoint		Sí	
2.9.1. distributionPoint	"http://crl3.cgcom.es/crl/eccgcom.crl"	Sí	
2.9.2. distributionPoint	"http://crl4.cgcom.es/crl/eccgcom.crl"	Sí	
2.10. Authority Info Acces		Sí	
2.10.1. OCSP Access Method		Sí	
2.10.1.1. Acces Location	"http://ocsp.cgcom.es"	Sí	
2.10.2. caIssuersAccessMethod		Sí	
2.10.2.1. Acces Location	"http://certificacion.cgcom.es/CA/OMC.crt"	Si	
2.11. Subject Directory Attributes (2.5.29.9)		Sí	
2.11.1. Country of Citizenship	País de nacionalidad	Sí	
2.11.2. Country of Residence	País de residencia	Sí	

4.5 Certificado corporativo de colegiado (persona física), en HSM, para identificación, firma y cifrado

Campo	Contenido	Obligatorio	Crítico
1. Basic estructure			
1.1. Version	"2"[40]	Sí	
1.2. Serial Number	Establecido automáticamente[41]	Sí	
1.3. Signature Algorithm	SHA-256 with RSA Signature	Sí	
1.4. Issuer Distinguished Name		Sí	
1.4.1. Country (C)	"ES"	Sí	
1.4.2. Organization (O)	"Organizacion Medica Colegial" [42]	Sí	
1.4.3. Organizational Unit (OU)	"Entidad de Certificacion" [43]	Sí	
1.4.4. Common Name (CN)	"OMC"	Sí	
1.5. Validity	5 años	Sí	
1.5.1. Not Before	Fecha de inicio de validez	Sí	
1.5.2. Not After	Fecha de expiración	Sí	
1.6. Subject		Sí	
1.6.1. Country (C)	"ES"[44]	Sí	

[40] El literal "2" corresponde a la versión 3.

[41] No debe superar los 32 caracteres hexadecimales en notación hexadecimal.

[42] El texto se incluye sin acentos.

[43] El texto se incluye sin acentos.

[44] El campo "país" siempre será España, dado que el certificado muestra la relación entre un colegiado y un colegio profesional español, con independencia de la nacionalidad del colegiado. Ello deriva de la naturaleza corporativa del certificado, del cual es suscriptor el colegio, y el colegiado, la persona autorizada a su uso..

Campo	Contenido	Obligatorio	Crítico
1.6.2. Organization (O)	Colegio profesional u otra persona jurídica del ámbito sanitario	Sí	
1.6.3. Organizational Unit (OU)	"Condiciones de uso en https://www.cgcom.es/CertColHSM (c)14"	Sí	
1.6.4. Organizational Unit (OU)	Dispositivo[45]	Sí	
1.6.5. Surname	Apellidos	Sí	
1.6.6. Given Name	Nombre	Sí	
1.6.7. Title	"Médico colegiado/a"	Sí	
1.6.8. Serial Number	DNI/NIE[46]	Sí	
1.6.9. Common Name (CN)	"(Col.)" + Nombre y apellidos + "-" + Número de colegiado + "(HSM)"	Sí	
1.7. Subject Public Key Info	2048-Bit Public key encoded in accordance with RFC2459 & PKCS#1	Sí	
2. Extensions			
2.1. Authority Key Identifier	Presente	Sí	
2.1.1. Key Identifier			
2.1.2. AuthorityCertIssuer			
2.1.3. AuthorityCertSerialNumber			
2.2. Subject Key Identifier	Presente	Sí	
2.3. Key Usage		Sí	Sí
2.3.1. Digital Signature	Seleccionado. "1"	Sí	

[45] Este campo se refiere al dispositivo usado por las claves y el certificado que es un HSM (hardware criptográfico centralizado) en un Organismo público, un centro de salud privado o en el mismo CGCOM.

[46] El campo "número de serie" debe incluir el DNI o el NIE del médico, al efecto de la admisión del certificado para la realización de trámites con las Administraciones españolas.

Campo	Contenido	Obligatorio	Crítico
2.3.2. Content commintment	Seleccionado. “1”	Sí	
2.3.3. Key Encipherment	Seleccionado. “1”	Sí	
2.3.4. Data Encipherment	Seleccionado. “1”	Sí	
2.3.5. Key Agreement	No seleccionado. “0”		
2.3.6. Key Certificate Signature	No seleccionado. “0”		
2.3.7. CRL Signature	No seleccionado. “0”		
2.4. Qualified Certificate Statements		Sí	
2.4.1. qCCompliance (0.4.0.1862.1.1)		Sí	
2.4.2. QcEuRetentionPeriod (0.4.0.1862.1.3)	15	Sí	
2.4.3. QcSSCD (0.4.0.1862.1.4)		Sí	
2.5. Certificate Policies		Sí	
2.5.1. Policy Identifier	1.3.6.1.4.1.26852.1.1.9	Sí	
2.5.2. Policy Qualifier ID		Sí	
2.5.2.1. CPS Pointer	“https://www.cgcom.es/CertColHSM”	Sí	
2.6. Subject Alternative Names		Sí	
2.6.1. rfc822Name	Correo electrónico corporativo del médico colegiado/a[47]	Sí	
2.6.2. directoryName[48]		Sí	
2.6.2.1. CGCOM.2.1	IdColegio / IdEntidad	Sí	

[47] Este campo contiene la dirección de correo corporativo del médico colegiado/a, a efectos de notificaciones.

[48] Este campo enlaza con el sistema de validación y re-certificación del CGCOM, permitiendo recuperar informaciones adicionales de forma eficiente. Ciertas informacions se incluyen, aunque sean redundantes, para disponer de toda la información sobre el usuario en una sola consulta contra el certificado.

Campo	Contenido	Obligatorio	Crítico
2.6.2.2. CGCOM.2.2	Colegio profesional / Entidad jurídica ámbito sanitario	Sí	
2.6.2.3. CGCOM.2.3	IdColegiado	Sí	
2.6.2.4. CGCOM.2.4	Nombre y apellidos del colegiado	Sí	
2.7. Issuer Alternative Name		Sí	
2.7.1. rfc822Name	"certificacion@cgcom.es"	Sí	
2.8. Extended Key Usage		Sí	
2.8.1. emailProtection	Presente	Sí	
2.8.2. clientAuth	Presente	Sí	
2.9. cRLDistributionPoint		Sí	
2.9.1. distributionPoint	"http://crl3.cgcom.es/crl/eccgcom.crl"	Sí	
2.9.2. distributionPoint	"http://crl4.cgcom.es/crl/eccgcom.crl"	Sí	
2.10. Authority Info Acces		Sí	
2.10.1. OCSP Access Method		Sí	
2.10.1.1. Acces Location	"http://ocsp.cgcom.es"	Sí	
2.10.2. caIssuersAccessMethod		Sí	
2.10.2.1. Acces Location	"http://certificacion.cgcom.es/CA/OMC.crt"	Si	
2.11. Subject Directory Attributes (2.5.29.9)		Sí	
2.11.1. Country of Citizenship	País de nacionalidad	Sí	
2.11.2. Country of Residence	País de residencia	Sí	

4.6 Certificado de colectivo de médico empleado público (persona física) para identificación

Campo	Contenido	Obligatorio	Crítico
1. Basic estructure			
1.1. Version	"2"[49]	Sí	
1.2. Serial Number	Establecido automáticamente[50]	Sí	
1.3. Signature Algorithm	SHA-256 with RSA Signature	Sí	
1.4. Issuer Distinguished Name		Sí	
1.4.1. Country (C)	"ES"	Sí	
1.4.2. Organization (O)	"Organizacion Medica Colegial" [51]	Sí	
1.4.3. Organizational Unit (OU)	"Entidad de Certificacion" [52]	Sí	
1.4.4. Common Name (CN)	"OMC"	Sí	
1.5. Validity	5 años	Sí	
1.5.1. Not Before	Fecha de inicio de validez	Sí	
1.5.2. Not After	Fecha de expiración	Sí	
1.6. Subject		Sí	
1.6.1. Country (C)	"ES"[53]	Sí	
1.6.2. Organization (O)	Nombre del servicio autonómico de	Sí	

[49] El literal "2" corresponde a la versión 3.

[50] No debe superar los 32 caracteres hexadecimales en notación hexadecimal.

[51] El texto se incluye sin acentos.

[52] El texto se incluye sin acentos.

[53] El campo "país" siempre será España, dado que el certificado muestra la relación entre un empleado público y un servicio autonómico de salud español, con independencia de la nacionalidad del empleado. Ello deriva de la naturaleza colectiva del certificado de médico empleado, del cual es suscriptor el servicio autonómico de salud, y el empleado, la persona autorizada a su uso.

Campo	Contenido	Obligatorio	Crítico
	salud		
1.6.3. Organizational Unit (OU)	"Certificado electrónico de médico empleado público"	Sí	
1.6.4. Organizational Unit (OU)	"Carnet colegial"[54]	Sí	
1.6.5. Organizational Unit (OU)	Unidad administrativa	No	
1.6.6. Organizational Unit (OU)	Número de empleado	No	
1.6.7. Surname	Apellidos + " – " + NIF del empleado	Sí	
1.6.8. Given Name	Nombre	Sí	
1.6.9. Title	Puesto o cargo que ostenta el responsable del certificado	Sí	
1.6.10. Serial Number	DNI/NIE del empleado público	Sí	
1.6.11. Common Name (CN)	Nombre apellidos + " – " + NIF del empleado +"(AUTENTICACION)	Sí	
1.7. Subject Public Key Info	2048-Bit Public key encoded in accordance with RFC2459 & PKCS#1	Sí	
2. Extensions			
2.1. Authority Key Identifier	Presente	Sí	
2.1.1. Key Identifier			
2.1.2. AuthorityCertIssuer			
2.1.3. AuthorityCertSerialNumber			
2.2. Subject Key Identifier	Presente	Sí	
2.3. Key Usage		Sí	Sí
2.3.1. Digital Signature	Seleccionado. "1"	Sí	

[54] Este campo se refiere al dispositivo usado, en este caso una tarjeta criptográfica que también sirve de carnet colegial.

Campo	Contenido	Obligatorio	Crítico
2.3.2. Content commintment	No seleccionado. “0”		
2.3.3. Key Encipherment	No seleccionado. “0”		
2.3.4. Data Encipherment	No seleccionado. “0”		
2.3.5. Key Agreement	No seleccionado. “0”		
2.3.6. Key Certificate Signature	No seleccionado. “0”		
2.3.7. CRL Signature	No seleccionado. “0”		
2.4. Qualified Certificate Statements		Sí	
2.4.1. qCCompliance (0.4.0.1862.1.1)		Sí	
2.4.2. QcEuRetentionPeriod (0.4.0.1862.1.3)	15	Sí	
2.4.3. QcSSCD (0.4.0.1862.1.4)		Sí	
2.5. Certificate Policies		Sí	
2.5.1. Policy Identifier	1.3.6.1.4.1.26852.1.2.1.1	Sí	
2.5.2. Policy Qualifier ID		Sí	
2.5.2.1. CPS Pointer	“https://www.cgcom.es/CertMEP”	Sí	
2.6. Subject Alternative Names		Sí	
2.6.1. rfc822Name	Correo electrónico corporativo del empleado/a[55]	Sí	
2.6.2. Directory Name		Sí	
2.6.2.1. Tipo de certificado - OID 2.16.724.1.3.5.3.2.1	Certificado electrónico de empleado público	F[56]	

[55] Este campo contiene la dirección de correo corporativo del empleado, a efectos de notificaciones.

[56] Campo fijo (F), de acuerdo con perfiles Certica

Campo	Contenido	Obligatorio	Crítico
2.6.2.2. Nombre de la entidad suscriptora - OID 2.16.724.1.3.5.3.2.2	Nombre de la entidad suscriptora (servicio de salud)	F	
2.6.2.3. NIF entidad suscriptora - OID 2.16.724.1.3.5.3.2.3	NIF de la entidad suscriptora	F	
2.6.2.4. DNI/NIE del responsable - OID 2.16.724.1.3.5.3.2.4	DNI/NIE del responsable	F	
2.6.2.5. Número de identificación de personal - OID 2.16.724.1.3.5.3.2.5	Número de identificación del médico como empleado público	O[57]	
2.6.2.6. Nombre de pila - OID 2.16.724.1.3.5.3.2.6	Nombre de pila del médico – empleado público.	F	
2.6.2.7. Primer apellido - OID 2.16.724.1.3.5.3.2.7	Primer apellido del médico – empleado público	F	
2.6.2.8. Segundo apellido - OID 2.16.724.1.3.5.3.2.8	Segundo apellido del médico – empleado público	F	
2.6.2.9. Correo electrónico - OID 2.16.724.1.3.5.3.2.9	Correo electrónico del médico – empleado público	O	
2.6.2.10. Unidad organizativa - OID 2.16.724.1.3.5.3.2.10	Unidad, dentro de la Administración, en la que está incluida el médico – empleado público.	O	
2.6.2.11. Puesto o cargo - OID 2.16.724.1.3.5.3.2.11	Puesto desempañado por el médico – empleado público, dentro de la Administración	O	
2.7. Issuer Alternative Name		Sí	
2.7.1. rfc822Name	"certificacion@cgcom.es"	Sí	
2.8. Extended Key Usage		Sí	

[57] Campo opcional (O), de acuerdo con perfiles Certica

Campo	Contenido	Obligatorio	Crítico
2.8.1. clientAuth	Presente	Sí	
2.9. cRLDistributionPoint		Sí	
2.9.1. distributionPoint	"http://crl3.cgcom.es/crl/eccgcom.crl"	Sí	
2.9.2. distributionPoint	"http://crl4.cgcom.es/crl/eccgcom.crl"	Sí	
2.10. Authority Info Acces		Sí	
2.10.1. OCSP Access Method		Sí	
2.10.1.1. Acces Location	"http://ocsp.cgcom.es"	Sí	
2.10.2. caIssuersAccessMethod		Sí	
2.10.2.1. Acces Location	"http://certificacion.cgcom.es/CA/OMC.crt"	Si	
2.11. Subject Directory Attributes (2.5.29.9)		Sí	
2.11.1. Country of Citizenship	País de nacionalidad	Sí	
2.11.2. Country of Residence	País de residencia	Sí	

4.7 Certificado de colectivo de médico empleado público (persona física) para firma

Campo	Contenido	Obligatorio	Crítico
1. Basic estructure			
1.1. Version	"2"[58]	Sí	
1.2. Serial Number	Establecido automáticamente[59]	Sí	
1.3. Signature Algorithm	SHA-256 with RSA Signature	Sí	
1.4. Issuer Distinguished Name		Sí	
1.4.1. Country (C)	"ES"	Sí	
1.4.2. Organization (O)	"Organizacion Medica Colegial" [60]	Sí	
1.4.3. Organizational Unit (OU)	"Entidad de Certificacion" [61]	Sí	
1.4.4. Common Name (CN)	"OMC"	Sí	
1.5. Validity	5 años	Sí	
1.5.1. Not Before	Fecha de inicio de validez	Sí	
1.5.2. Not After	Fecha de expiración	Sí	
1.6. Subject		Sí	
1.6.1. Country (C)	"ES"[62]	Sí	
1.6.2. Organization (O)	Nombre del servicio autonómico de	Sí	

[58] El literal "2" corresponde a la versión 3.

[59] No debe superar los 32 caracteres hexadecimales en notación hexadecimal.

[60] El texto se incluye sin acentos.

[61] El texto se incluye sin acentos.

[62] El campo "país" siempre será España, dado que el certificado muestra la relación entre un empleado público y un servicio autonómico de salud español, con independencia de la nacionalidad del empleado. Ello deriva de la naturaleza colectiva del certificado de empleado público, del cual es suscriptor el servicio autonómico de salud, y el empleado, la persona autorizada a su uso.

Campo	Contenido	Obligatorio	Crítico
	salud		
1.6.3. Organizational Unit (OU)	"Certificado electrónico de médico empleado público"	Sí	
1.6.4. Organizational Unit (OU)	"Carnet colegial"[63]	Sí	
1.6.5. Organizational Unit (OU)	Unidad administrativa	No	
1.6.6. Organizational Unit (OU)	Número de empleado	No	
1.6.7. Surname	Apellidos + " – " + NIF del empleado	Sí	
1.6.8. Given Name	Nombre	Sí	
1.6.9. Title	Puesto o cargo que ostenta el responsable del certificado	Sí	
1.6.10. Serial Number	DNI/NIE del empleado público	Sí	
1.6.11. Common Name (CN)	Nombre, apellidos + " – " + NIF del empleado +"(FIRMA)"	Sí	
1.7. Subject Public Key Info	2048-Bit Public key encoded in accordance with RFC2459 & PKCS#1	Sí	
2. Extensions			
2.1. Authority Key Identifier	Presente	Sí	
2.1.1. Key Identifier			
2.1.2. AuthorityCertIssuer			
2.1.3. AuthorityCertSerialNumber			
2.2. Subject Key Identifier	Presente	Sí	
2.3. Key Usage		Sí	Sí
2.3.1. Digital Signature	No seleccionado. "0"		

[63] Este campo se refiere al dispositivo usado, en este caso una tarjeta criptográfica que también sirve de carnet colegial.

Campo	Contenido	Obligatorio	Crítico
2.3.2. Content commintment	Seleccionado. “1”	Sí	
2.3.3. Key Encipherment	No seleccionado. “0”		
2.3.4. Data Encipherment	No seleccionado. “0”		
2.3.5. Key Agreement	No seleccionado. “0”		
2.3.6. Key Certificate Signature	No seleccionado. “0”		
2.3.7. CRL Signature	No seleccionado. “0”		
2.4. Qualified Certificate Statements		Sí	
2.4.1. qCCompliance (0.4.0.1862.1.1)		Sí	
2.4.2. QcEuRetentionPeriod (0.4.0.1862.1.3)	15	Sí	
2.4.3. QcSSCD (0.4.0.1862.1.4)		Sí	
2.5. Certificate Policies		Sí	
2.5.1. Policy Identifier	1.3.6.1.4.1.26852.1.2.1.2	Sí	
2.5.2. Policy Qualifier ID		Sí	
2.5.2.1. CPS Pointer	“https://www.cgcom.es/CertMEP”	Sí	
2.6. Subject Alternative Names		Sí	
2.6.1. rfc822Name	Correo electrónico corporativo del empleado/a[64]	Sí	
2.6.2. Directory Name		Sí	
2.6.2.1. Tipo de certificado - OID 2.16.724.1.3.5.3.2.1	Certificado electrónico de empleado público	F[65]	

[64] Este campo contiene la dirección de correo corporativo del empleado, a efectos de notificaciones.

[65] Campo fijo (F), de acuerdo con perfiles Certica

Campo	Contenido	Obligatorio	Crítico
2.6.2.2. Nombre de la entidad suscriptora - OID 2.16.724.1.3.5.3.2.2	Nombre de la entidad suscriptora (servicio de salud)	F	
2.6.2.3. NIF entidad suscriptora - OID 2.16.724.1.3.5.3.2.3	NIF de la entidad suscriptora	F	
2.6.2.4. DNI/NIE del responsable - OID 2.16.724.1.3.5.3.2.4	DNI/NIE del responsable	F	
2.6.2.5. Número de identificación de personal - OID 2.16.724.1.3.5.3.2.5	Número de identificación del médico como empleado público	O[66]	
2.6.2.6. Nombre de pila - OID 2.16.724.1.3.5.3.2.6	Nombre de pila del médico – empleado público.	F	
2.6.2.7. Primer apellido - OID 2.16.724.1.3.5.3.2.7	Primer apellido del médico – empleado público	F	
2.6.2.8. Segundo apellido - OID 2.16.724.1.3.5.3.2.8	Segundo apellido del médico – empleado público	F	
2.6.2.9. Correo electrónico - OID 2.16.724.1.3.5.3.2.9	Correo electrónico del médico – empleado público	O	
2.6.2.10. Unidad organizativa - OID 2.16.724.1.3.5.3.2.10	Unidad, dentro de la Administración, en la que está incluida el médico – empleado público.	O	
2.6.2.11. Puesto o cargo - OID 2.16.724.1.3.5.3.2.11	Puesto desempañado por el médico – empleado público, dentro de la Administración	O	
2.7. Issuer Alternative Name		Sí	
2.7.1. rfc822Name	"certificacion@cgcom.es"	Sí	
2.8. Extended Key Usage		Sí	

[66] Campo opcional (O), de acuerdo con perfiles Certica

Campo	Contenido	Obligatorio	Crítico
2.8.1. emailProtection	Presente	Sí	
2.9. cRLDistributionPoint		Sí	
2.9.1. distributionPoint	"http://crl3.cgcom.es/crl/eccgcom.crl"	Sí	
2.9.2. distributionPoint	"http://crl4.cgcom.es/crl/eccgcom.crl"	Sí	
2.10. Authority Info Acces		Sí	
2.10.1. OCSP Access Method		Sí	
2.10.1.1. Acces Location	"http://ocsp.cgcom.es"	Sí	
2.10.2. caIssuersAccessMethod		Sí	
2.10.2.1. Acces Location	"http://certificacion.cgcom.es/CA/OMC.crt"	Si	
2.11. Subject Directory Attributes (2.5.29.9)		Sí	
2.11.1. Country of Citizenship	País de nacionalidad	Sí	
2.11.2. Country of Residence	País de residencia	Sí	

4.8 Certificado de cifrado en tarjeta, para médico empleado público

Campo	Contenido	Obligatorio	Crítico
1. Basic estructure			
1.1. Version	"2"[67]	Sí	
1.2. Serial Number	Establecido automáticamente[68]	Sí	
1.3. Signature Algorithm	SHA-256 with RSA Signature	Sí	
1.4. Issuer Distinguished Name		Sí	
1.4.1. Country (C)	"ES"	Sí	
1.4.2. Organization (O)	"Organizacion Medica Colegial" [69]	Sí	
1.4.3. Organizational Unit (OU)	"Entidad de Certificacion" [70]	Sí	
1.4.4. Common Name (CN)	"OMC"	Sí	
1.5. Validity	5 años	Sí	
1.5.1. Not Before	Fecha de inicio de validez	Sí	
1.5.2. Not After	Fecha de expiración	Sí	
1.6. Subject		Sí	
1.6.1. Country (C)	"ES"[71]	Sí	

[67] El literal "2" corresponde a la versión 3.

[68] No debe superar los 32 caracteres hexadecimales en notación hexadecimal.

[69] El texto se incluye sin acentos.

[70] El texto se incluye sin acentos.

[71] El campo "país" siempre será España, dado que el certificado muestra la relación entre un empleado público y un servicio autonómico de salud español, con independencia de la nacionalidad

Campo	Contenido	Obligatorio	Crítico
1.6.2. Organization (O)	Nombre del servicio autonómico de salud	Sí	
1.6.3. Organizational Unit (OU)	"Certificado electrónico de médico empleado público"	Sí	
1.6.4. Organizational Unit (OU)	"Carnet colegial"[72]	Sí	
1.6.5. Organizational Unit (OU)	Unidad administrativa	No	
1.6.6. Organizational Unit (OU)	Número de empleado	No	
1.6.7. Surname	Apellidos + " – " + NIF del empleado	Sí	
1.6.8. Given Name	Nombre	Sí	
1.6.9. Title	Puesto o cargo que ostenta el responsable del certificado	Sí	
1.6.10. Serial Number	DNI/NIE del empleado público	Sí	
1.6.11. Common Name (CN)	Nombre, apellidos + " – " + NIF del empleado +"(CIFRADO)"	Sí	
1.7. Subject Public Key Info	2048-Bit Public key encoded in accordance with RFC2459 & PKCS#1	Sí	
2. Extensions			
2.1. Authority Key Identifier	Presente	Sí	
2.1.1. Key Identifier			
2.1.2. AuthorityCertIssuer			
2.1.3. AuthorityCertSerialNumber			
2.2. Subject Key Identifier	Presente	Sí	

del empleado. Ello deriva de la naturaleza colectiva del certificado de empleado público, del cual es suscriptor el servicio autonómico de salud, y el empleado, la persona autorizada a su uso.

[72] Este campo se refiere al dispositivo usado, en este caso una tarjeta criptográfica que también sirve de carnet colegial.

Campo	Contenido	Obligatorio	Crítico
2.3. Key Usage		Sí	Sí
2.3.1. Digital Signature	No seleccionado. “0”		
2.3.2. Content commintment	No seleccionado. “0”		
2.3.3. Key Encipherment	Seleccionado. “1”	Sí	
2.3.4. Data Encipherment	Seleccionado. “1”	Sí	
2.3.5. Key Agreement	No seleccionado. “0”		
2.3.6. Key Certificate Signature	No seleccionado. “0”		
2.3.7. CRL Signature	No seleccionado. “0”		
2.4. Qualified Certificate Statements		Sí	
2.4.1. qCCompliance (0.4.0.1862.1.1)		Sí	
2.4.2. QcEuRetentionPeriod (0.4.0.1862.1.3)	15	Sí	
2.4.3. QcSSCD (0.4.0.1862.1.4)		Sí	
2.5. Certificate Policies		Sí	
2.5.1. Policy Identifier	1.3.6.1.4.1.26852.1.2.1.3	Sí	
2.5.2. Policy Qualifier ID		Sí	
2.5.2.1. CPS Pointer	“https://www.cgcom.es/CertMEP”	Sí	
2.6. Subject Alternative Names		Sí	
2.6.1. rfc822Name	Correo electrónico corporativo del empleado/a[73]	Sí	
2.6.2. Directory Name		Sí	
2.6.2.1. Tipo de certificado - OID 2.16.724.1.3.5.3.2.1	Certificado electrónico de empleado público	F[74]	

[73] Este campo contiene la dirección de correo corporativo del empleado, a efectos de notificaciones.

Campo	Contenido	Obligatorio	Crítico
2.6.2.2. Nombre de la entidad suscriptora - OID 2.16.724.1.3.5.3.2.2	Nombre de la entidad suscriptora (servicio de salud)	F	
2.6.2.3. NIF entidad suscriptora - OID 2.16.724.1.3.5.3.2.3	NIF de la entidad suscriptora	F	
2.6.2.4. DNI/NIE del responsable - OID 2.16.724.1.3.5.3.2.4	DNI/NIE del responsable	F	
2.6.2.5. Número de identificación de personal - OID 2.16.724.1.3.5.3.2.5	Número de identificación del médico como empleado público	O[75]	
2.6.2.6. Nombre de pila - OID 2.16.724.1.3.5.3.2.6	Nombre de pila del médico – empleado público.	F	
2.6.2.7. Primer apellido - OID 2.16.724.1.3.5.3.2.7	Primer apellido del médico – empleado público	F	
2.6.2.8. Segundo apellido - OID 2.16.724.1.3.5.3.2.8	Segundo apellido del médico – empleado público	F	
2.6.2.9. Correo electrónico - OID 2.16.724.1.3.5.3.2.9	Correo electrónico del médico – empleado público	O	
2.6.2.10. Unidad organizativa - OID 2.16.724.1.3.5.3.2.10	Unidad, dentro de la Administración, en la que está incluida el médico – empleado público.	O	
2.6.2.11. Puesto o cargo - OID 2.16.724.1.3.5.3.2.11	Puesto desempañado por el médico – empleado público, dentro de la Administración	O	
2.7. Issuer Alternative Name		Sí	
2.7.1. rfc822Name	"certificacion@cgcom.es"	Sí	
2.8. Extended Key Usage		Sí	

[74] Campo fijo (F), de acuerdo con perfiles Certica

[75] Campo opcional (O), de acuerdo con perfiles Certica

Campo	Contenido	Obligatorio	Crítico
2.8.1. emailProtection	Presente	Sí	
2.9. cRLDistributionPoint		Sí	
2.9.1. distributionPoint	"http://crl3.cgcom.es/crl/eccgcom.crl"	Sí	
2.9.2. distributionPoint	"http://crl4.cgcom.es/crl/eccgcom.crl"	Sí	
2.10. Authority Info Acces		Sí	
2.10.1. OCSP Access Method		Sí	
2.10.1.1. Acces Location	"http://ocsp.cgcom.es"	Sí	
2.10.2. caIssuersAccessMethod		Sí	
2.10.2.1. Acces Location	"http://certificacion.cgcom.es/CA/OMC.crt"	Si	
2.11. Subject Directory Attributes (2.5.29.9)		Sí	
2.11.1. Country of Citizenship	País de nacionalidad	Sí	
2.11.2. Country of Residence	País de residencia	Sí	

5. CERTIFICADOS DE PERSONAL ADMINISTRATIVO

5.1 Certificado corporativo de personal administrativo (persona física) para identificación

Campo	Contenido	Obligatorio	Crítico
1. Basic estructure			
1.1. Version	"2"[76]	Sí	
1.2. Serial Number	Establecido automáticamente[77]	Sí	
1.3. Signature Algorithm	SHA-256 with RSA Signature	Sí	
1.4. Issuer Distinguished Name		Sí	
1.4.1. Country (C)	"ES"	Sí	
1.4.2. Organization (O)	"Organizacion Medica Colegial" [78]	Sí	
1.4.3. Organizational Unit (OU)	"Entidad de Certificacion" [79]	Sí	
1.4.4. Common Name (CN)	"OMC"	Sí	
1.5. Validity	5 años	Sí	
1.5.1. Not Before	Fecha de inicio de validez	Sí	
1.5.2. Not After	Fecha de expiración	Sí	
1.6. Subject		Sí	
1.6.1. Country (C)	"ES"[80]	Sí	

[76] El literal "2" corresponde a la versión 3.

[77] No debe superar los 32 caracteres hexadecimales en notación hexadecimal.

[78] El texto se incluye sin acentos.

[79] El texto se incluye sin acentos.

[80] El campo "país" siempre será España, dado que el certificado muestra la relación entre un trabajador y un colegio profesional español, con independencia de la nacionalidad del trabajador.

Campo	Contenido	Obligatorio	Crítico
1.6.2. Organization (O)	Colegio profesional u otra persona jurídica del ámbito sanitario	Sí	
1.6.3. Organizational Unit (OU)	"Condiciones de uso en https://www.cgcom.es/CertAdmin (c)06"	Sí	
1.6.4. Organizational Unit (OU)	"Dispositivo"[81]	Sí	
1.6.5. Surname	Apellidos	Sí	
1.6.6. Given Name	Nombre	Sí	
1.6.7. Title	"Personal administrativo y de servicios"	Sí	
1.6.8. Serial Number	DNI/NIE[82]	Sí	
1.6.9. Common Name (CN)	Nombre y apellidos + "-"+ "(AUTENTICACION)"	Sí	
1.7. Subject Public Key Info	2048-Bit Public key encoded in accordance with RFC2459 & PKCS#1	Sí	
2. Extensions			
2.1. Authority Key Identifier	Presente	Sí	
2.1.1. Key Identifier			
2.1.2. AuthorityCertIssuer			
2.1.3. AuthorityCertSerialNumber			
2.2. Subject Key Identifier	Presente	Sí	
2.3. Key Usage		Sí	Sí
2.3.1. Digital Signature	Seleccionado. "1"	Sí	
2.3.2. Content commintment	No seleccionado. "0"		
2.3.3. Key Encipherment	No seleccionado. "0"		

[81] Este campo se refiere al dispositivo usado, en este caso una tarjeta criptográfica.

[82] El campo "número de serie" debe incluir el DNI o el NIE del trabajador, al efecto de la admisión del certificado para la realización de trámites con las Administraciones españolas.

Campo	Contenido	Obligatorio	Crítico
2.3.4. Data Encipherment	No seleccionado. “0”		
2.3.5. Key Agreement	No seleccionado. “0”		
2.3.6. Key Certificate Signature	No seleccionado. “0”		
2.3.7. CRL Signature	No seleccionado. “0”		
2.4. Qualified Certificate Statements		Sí	
2.4.1. qCCompliance (0.4.0.1862.1.1)		Sí	
2.4.2. QcEuRetentionPeriod (0.4.0.1862.1.3)	15	Sí	
2.4.3. QcSSCD (0.4.0.1862.1.4)		Sí	
2.5. Certificate Policies		Sí	
2.5.1. Policy Identifier	1.3.6.1.4.1.26852.1.1.2.1	Sí	
2.5.2. Policy Qualifier ID		Sí	
2.5.2.1. CPS Pointer	“https://www.cgcom.es/CertAdmin”	Sí	
2.6. Subject Alternative Names		Sí	
2.6.1. rfc822Name	Correo electrónico corporativo del personal administrativo[83]	Sí	
2.6.2. directoryName[84]		Sí	
2.6.2.1. CGCOM.2.1	IdColegio / IdEntidad	Sí	
2.6.2.2. CGCOM.2.2	Colegio profesional / Entidad jurídica ámbito sanitario	Sí	

[83] Este campo contiene la dirección de correo corporativo del personal administrativo y de servicios, a efectos de notificaciones.

[84] Este campo enlaza con el sistema de validación y re-certificación del CGCOM, permitiendo recuperar informaciones adicionales de forma eficiente. Ciertas informacions se incluyen, aunque sean redundantes, para disponer de toda la información sobre el usuario en una sola consulta contra el certificado.

Campo	Contenido	Obligatorio	Crítico
2.6.2.3. CGCOM.2.7	IdPersonalAdmin	Sí	
2.6.2.4. CGCOM.2.8	Nombre y apellidos del personal administrativo	Sí	
2.7. Issuer Alternative Name		Sí	
2.7.1. rfc822Name	"certificacion@cgcom.es"	Sí	
2.8. Extended Key Usage		Sí	
2.8.1. clientAuth	Presente	Sí	
2.8.2. SmartCardLogon	Presente		
2.9. cRLDistributionPoint		Sí	
2.9.1. distributionPoint	"http://crl3.cgcom.es/crl/eccgcom.crl"	Sí	
2.9.2. distributionPoint	"http://crl4.cgcom.es/crl/eccgcom.crl"	Sí	
2.10. Authority Info Acces		Sí	
2.10.1. OCSP Access Method		Sí	
2.10.1.1. Acces Location	"http://ocsp.cgcom.es"	Sí	
2.10.2. caIssuersAccessMethod		Sí	
2.10.2.1. Acces Location	"http://certificacion.cgcom.es/CA/OMC.crt"	Si	
2.11. Subject Directory Attributes (2.5.29.9)		Sí	
2.11.1. Country of Citizenship	País de nacionalidad	Sí	
2.11.2. Country of Residence	País de residencia	Sí	

5.2 Certificado corporativo de personal administrativo (persona física) para firma

Campo	Contenido	Obligatorio	Crítico
1. Basic estructure			
1.1. Version	"2"[85]	Sí	
1.2. Serial Number	Establecido automáticamente[86]	Sí	
1.3. Signature Algorithm	SHA-256 with RSA Signature	Sí	
1.4. Issuer Distinguished Name		Sí	
1.4.1. Country (C)	"ES"	Sí	
1.4.2. Organization (O)	"Organizacion Medica Colegial" [87]	Sí	
1.4.3. Organizational Unit (OU)	"Entidad de Certificacion" [88]	Sí	
1.4.4. Common Name (CN)	"OMC"	Sí	
1.5. Validity	5 años	Sí	
1.5.1. Not Before	Fecha de inicio de validez	Sí	
1.5.2. Not After	Fecha de expiración	Sí	
1.6. Subject		Sí	
1.6.1. Country (C)	"ES"[89]	Sí	
1.6.2. Organization (O)	Colegio profesional u otra persona jurídica del ámbito sanitario	Sí	
1.6.3. Organizational Unit	"Condiciones de uso en	Sí	

[85] El literal "2" corresponde a la versión 3.

[86] No debe superar los 32 caracteres hexadecimales en notación hexadecimal.

[87] El texto se incluye sin acentos.

[88] El texto se incluye sin acentos.

[89] El campo "país" siempre será España, dado que el certificado muestra la relación entre un trabajador y un colegio profesional español, con independencia de la nacionalidad del trabajador.

Campo	Contenido	Obligatorio	Crítico
(OU)	https://www.cgcom.es/CertAdmin (c)06"		
1.6.4. Organizational Unit (OU)	"Dispositivo"[90]	Sí	
1.6.5. Surname	Apellidos	Sí	
1.6.6. Given Name	Nombre	Sí	
1.6.7. Title	"Personal administrativo y de servicios"	Sí	
1.6.8. Serial Number	DNI/NIE[91]	Sí	
1.6.9. Common Name (CN)	Nombre y apellidos + "-"+ "(FIRMA)"	Sí	
1.7. Subject Public Key Info	2048-Bit Public key encoded in accordance with RFC2459 & PKCS#1	Sí	
2. Extensions			
2.1. Authority Key Identifier	Presente	Sí	
2.1.1. Key Identifier			
2.1.2. AuthorityCertIssuer			
2.1.3. AuthorityCertSerialNumber			
2.2. Subject Key Identifier	Presente	Sí	
2.3. Key Usage		Sí	Sí
2.3.1. Digital Signature	No seleccionado. "0"		
2.3.2. Content commintment	Seleccionado. "1"	Sí	
2.3.3. Key Encipherment	No seleccionado. "0"		
2.3.4. Data Encipherment	No seleccionado. "0"		
2.3.5. Key Agreement	No seleccionado. "0"		

[90] Este campo se refiere al dispositivo usado, en este caso una tarjeta.

[91] El campo "número de serie" debe incluir el DNI o el NIE del trabajador, al efecto de la admisión del certificado para la realización de trámites con las Administraciones españolas.

Campo	Contenido	Obligatorio	Crítico
2.3.6. Key Certificate Signature	No seleccionado. "0"		
2.3.7. CRL Signature	No seleccionado. "0"		
2.4. Qualified Certificate Statements		Sí	
2.4.1. qCCompliance (0.4.0.1862.1.1)		Sí	
2.4.2. QcEuRetentionPeriod (0.4.0.1862.1.3)	15	Sí	
2.4.3. QcSSCD (0.4.0.1862.1.4)		Sí	
2.5. Certificate Policies		Sí	
2.5.1. Policy Identifier	1.3.6.1.4.1.26852.1.1.2.2	Sí	
2.5.2. Policy Qualifier ID		Sí	
2.5.2.1. CPS Pointer	"https://www.cgcom.es/CertAdmin"	Sí	
2.6. Subject Alternative Names		Sí	
2.6.1. rfc822Name	Correo electrónico corporativo del personal administrativo[92]	Sí	
2.6.2. directoryName[93]		Sí	
2.6.2.1. CGCOM.2.1	IdColegio / IdEntidad	Sí	
2.6.2.2. CGCOM.2.2	Colegio profesional / Entidad jurídica ámbito sanitario	Sí	
2.6.2.3. CGCOM.2.7	IdPersonalAdmin	Sí	
2.6.2.4. CGCOM.2.8	Nombre y apellidos del personal administrativo	Sí	

[92] Este campo contiene la dirección de correo corporativo del personal administrativo y de servicios, a efectos de notificaciones.

[93] Este campo enlaza con el sistema de validación y re-certificación del CGCOM, permitiendo recuperar informaciones adicionales de forma eficiente. Ciertas informacions se incluyen, aunque sean redundantes, para disponer de toda la información sobre el usuario en una sola consulta contra el certificado.

Campo	Contenido	Obligatorio	Crítico
2.7. Issuer Alternative Name		Sí	
2.7.1. rfc822Name	"certificacion@cgcom.es"	Sí	
2.8. Extended Key Usage		Sí	
2.8.1. emailProtection	Presente	Sí	
2.9. cRLDistributionPoint		Sí	
2.9.1. distributionPoint	"http://crl3.cgcom.es/crl/eccgcom.crl"	Sí	
2.9.2. distributionPoint	"http://crl4.cgcom.es/crl/eccgcom.crl"	Sí	
2.10. Authority Info Acces		Sí	
2.10.1. OCSP Access Method		Sí	
2.10.1.1. Acces Location	"http://ocsp.cgcom.es"	Sí	
2.10.2. caIssuersAccessMethod		Sí	
2.10.2.1. Acces Location	"http://certificacion.cgcom.es/CA/OMC.crt"	Si	
2.11. Subject Directory Attributes (2.5.29.9)		Sí	
2.11.1. Country of Citizenship	País de nacionalidad	Sí	
2.11.2. Country of Residence	País de residencia	Sí	

5.3 Certificado de cifrado en tarjeta, para personal administrativo

Campo	Contenido	Obligatorio	Crítico
1. Basic estructure			
1.1. Version	"2"[94]	Sí	
1.2. Serial Number	Establecido automáticamente[95]	Sí	
1.3. Signature Algorithm	SHA-256 with RSA Signature	Sí	
1.4. Issuer Distinguished Name		Sí	
1.4.1. Country (C)	"ES"	Sí	
1.4.2. Organization (O)	"Organizacion Medica Colegial" [96]	Sí	
1.4.3. Organizational Unit (OU)	"Entidad de Certificacion" [97]	Sí	
1.4.4. Common Name (CN)	"OMC"	Sí	
1.5. Validity	5 años	Sí	
1.5.1. Not Before	Fecha de inicio de validez	Sí	
1.5.2. Not After	Fecha de expiración	Sí	
1.6. Subject		Sí	
1.6.1. Country (C)	"ES"[98]	Sí	
1.6.2. Organization (O)	Colegio profesional u otra persona jurídica del ámbito sanitario	Sí	
1.6.3. Organizational Unit	"Condiciones de uso en	Sí	

[94] El literal "2" corresponde a la versión 3.

[95] No debe superar los 32 caracteres hexadecimales en notación hexadecimal.

[96] El texto se incluye sin acentos.

[97] El texto se incluye sin acentos.

[98] El campo "país" siempre será España.

Campo	Contenido	Obligatorio	Crítico
(OU)	https://www.cgcom.es/CertAdmin (c)06"		
1.6.4. Organizational Unit (OU)	"Dispositivo"[99]	Sí	
1.6.5. Surname	Apellidos	Sí	
1.6.6. Given Name	Nombre	Sí	
1.6.7. Title	"Personal administrativo y de servicios"	Sí	
1.6.8. Serial Number	DNI/NIE[100]	Sí	
1.6.9. Common Name (CN)	Nombre y apellidos + "-"+ "(CIFRADO)"	Sí	
1.7. Subject Public Key Info	2048-Bit Public key encoded in accordance with RFC2459 & PKCS#1	Sí	
2. Extensions			
2.1. Authority Key Identifier	Presente	Sí	
2.1.1. Key Identifier			
2.1.2. AuthorityCertIssuer			
2.1.3. AuthorityCertSerialNumber			
2.2. Subject Key Identifier	Presente	Sí	
2.3. Key Usage		Sí	Sí
2.3.1. Digital Signature	No seleccionado. "0"		
2.3.2. Content commintment	No seleccionado. "0"		
2.3.3. Key Encipherment	Seleccionado. "1"	Sí	
2.3.4. Data Encipherment	Seleccionado. "1"	Sí	
2.3.5. Key Agreement	No seleccionado. "0"		

[99] Este campo se refiere al dispositivo usado, en este caso una tarjeta criptográfica.

[100] El campo "número de serie" debe incluir el DNI o el NIE del trabajador, al efecto de la admisión del certificado para la realización de trámites con las Administraciones españolas.

Campo	Contenido	Obligatorio	Crítico
2.3.6. Key Certificate Signature	No seleccionado. “0”		
2.3.7. CRL Signature	No seleccionado. “0”		
2.4. Qualified Certificate Statements		Sí	
2.4.1. qCCompliance (0.4.0.1862.1.1)		Sí	
2.4.2. QcEuRetentionPeriod (0.4.0.1862.1.3)	15	Sí	
2.4.3. QcSSCD		Sí	
2.5. Certificate Policies		Sí	
2.5.1. Policy Identifier	1.3.6.1.4.1.26852.1.1.2.3	Sí	
2.5.2. Policy Qualifier ID		Sí	
2.5.2.1. CPS Pointer	“https://www.cgcom.es/CertAdmin”	Sí	
2.6. Subject Alternative Names		Sí	
2.6.1. rfc822Name	Correo electrónico corporativo[101]	Sí	
2.6.2. directoryName[102]		Sí	
2.6.2.1. CGCOM.2.1	IdColegio / IdEntidad	Sí	
2.6.2.2. CGCOM.2.2	Colegio profesional / Entidad jurídica ámbito sanitario	Sí	
2.6.2.3. CGCOM.2.7	IdPersonalAdmin	Sí	
2.6.2.4. CGCOM.2.8	Nombre y apellidos del personal administrativo	Sí	
2.7. Issuer Alternative Name		Sí	

[101] Este campo contiene la dirección de correo corporativo del colegiado, a efectos de notificaciones.

[102] Este campo enlaza con el sistema de validación y re-certificación del CGCOM, permitiendo recuperar informaciones adicionales de forma eficiente. Ciertas informacions se incluyen, aunque sean redundantes, para disponer de toda la información sobre el usuario en una sola consulta contra el certificado.

Campo	Contenido	Obligatorio	Crítico
2.7.1. rfc822Name	"certificacion@cgcom.es"	Sí	
2.8. Extended Key Usage		Sí	
2.8.1. emailProtection	Presente	Sí	
2.9. cRLDistributionPoint		Sí	
2.9.1. distributionPoint	"http://crl3.cgcom.es/crl/eccgcom.crl"	Sí	
2.9.2. distributionPoint	"http://crl4.cgcom.es/crl/eccgcom.crl"	Sí	
2.10. Authority Info Acces		Sí	
2.10.1. OCSP Access Method		Sí	
2.10.1.1. Acces Location	"http://ocsp.cgcom.es"	Sí	
2.10.2. caIssuersAccessMethod		Sí	
2.10.2.1. Acces Location	"http://certificacion.cgcom.es/CA/OMC.crt"	Si	
2.11. Subject Directory Attributes (2.5.29.9)		Sí	
2.11.1. Country of Citizenship	País de nacionalidad	Sí	
2.11.2. Country of Residence	País de residencia	Sí	

5.4 Certificado corporativo de personal administrativo (persona física), en software, para identificación, firma y cifrado

Campo	Contenido	Obligatorio	Crítico
1. Basic estructure			
1.1. Version	"2"[103]	Sí	
1.2. Serial Number	Establecido automáticamente[104]	Sí	
1.3. Signature Algorithm	SHA-256 with RSA Signature	Sí	
1.4. Issuer Distinguished Name		Sí	
1.4.1. Country (C)	"ES"	Sí	
1.4.2. Organization (O)	"Organizacion Medica Colegial" [105]	Sí	
1.4.3. Organizational Unit (OU)	"Entidad de Certificacion" [106]	Sí	
1.4.4. Common Name (CN)	"OMC"	Sí	
1.5. Validity	5 años	Sí	
1.5.1. Not Before	Fecha de inicio de validez	Sí	
1.5.2. Not After	Fecha de expiración	Sí	
1.6. Subject		Sí	
1.6.1. Country (C)	"ES"[107]	Sí	
1.6.2. Organization (O)	Colegio profesional u otra persona jurídica del ámbito sanitario	Sí	

[103] El literal "2" corresponde a la versión 3.

[104] No debe superar los 32 caracteres hexadecimales en notación hexadecimal.

[105] El texto se incluye sin acentos.

[106] El texto se incluye sin acentos.

[107] El campo "país" siempre será España, dado que el certificado muestra la relación entre un trabajador y un colegio profesional español, con independencia de la nacionalidad del trabajador.

Campo	Contenido	Obligatorio	Crítico
1.6.3. Organizational Unit (OU)	"Condiciones de uso en https://www.cgcom.es/CertAdminSoft (c)13"	Sí	
1.6.4. Organizational Unit (OU)	Dispositivo[108]	Sí	
1.6.5. Surname	Apellidos	Sí	
1.6.6. Given Name	Nombre	Sí	
1.6.7. Title	"Personal administrativo y de servicios"	Sí	
1.6.8. Serial Number	DNI/NIE[109]	Sí	
1.6.9. Common Name (CN)	Nombre y apellidos	Sí	
1.7. Subject Public Key Info	2048-Bit Public key encoded in accordance with RFC2459 & PKCS#1	Sí	
2. Extensions			
2.1. Authority Key Identifier	Presente	Sí	
2.1.1. Key Identifier			
2.1.2. AuthorityCertIssuer			
2.1.3. AuthorityCertSerialNumber			
2.2. Subject Key Identifier	Presente	Sí	
2.3. Key Usage		Sí	Sí
2.3.1. Digital Signature	Seleccionado. "1"	Sí	
2.3.2. Content commintment	Seleccionado. "1"	Sí	
2.3.3. Key Encipherment	Seleccionado. "1"	Sí	
2.3.4. Data Encipherment	Seleccionado. "1"	Sí	

[108] Este campo se refiere al dispositivo usado por las claves y el certificado como puede ser: movil o tableta personal o de la entidad donde esté empleado.

[109] El campo "número de serie" debe incluir el DNI o el NIE del trabajador, al efecto de la admisión del certificado para la realización de trámites con las Administraciones españolas.

Campo	Contenido	Obligatorio	Crítico
2.3.5. Key Agreement	No seleccionado. “0”		
2.3.6. Key Certificate Signature	No seleccionado. “0”		
2.3.7. CRL Signature	No seleccionado. “0”		
2.4. Qualified Certificate Statements		Sí	
2.4.1. qCCompliance (0.4.0.1862.1.1)		Sí	
2.4.2. QcEuRetentionPeriod (0.4.0.1862.1.3)	15	Sí	
2.5. Certificate Policies		Sí	
2.5.1. Policy Identifier	1.3.6.1.4.1.26852.1.1.6	Sí	
2.5.2. Policy Qualifier ID		Sí	
2.5.2.1. CPS Pointer	“https://www.cgcom.es/CertAdminSoft”	Sí	
2.6. Subject Alternative Names		Sí	
2.6.1. rfc822Name	Correo electrónico corporativo del personal administrativo[110]	Sí	
2.6.2. directoryName[111]		Sí	
2.6.2.1. CGCOM.2.1	IdColegio / IdEntidad	Sí	
2.6.2.2. CGCOM.2.2	Colegio profesional / Entidad jurídica ámbito sanitario	Sí	
2.6.2.3. CGCOM.2.7	IdPersonalAdmin	Sí	
2.6.2.4. CGCOM.2.8	Nombre y apellidos del personal administrativo	Sí	

[110] Este campo contiene la dirección de correo corporativo del personal administrativo y de servicios, a efectos de notificaciones.

[111] Este campo enlaza con el sistema de validación y re-certificación del CGCOM, permitiendo recuperar informaciones adicionales de forma eficiente. Ciertas informacions se incluyen, aunque sean redundantes, para disponer de toda la información sobre el usuario en una sola consulta contra el certificado.

Campo	Contenido	Obligatorio	Crítico
2.7. Issuer Alternative Name		Sí	
2.7.1. rfc822Name	"certificacion@cgcom.es"	Sí	
2.8. Extended Key Usage		Sí	
2.8.1. emailProtection	Presente	Sí	
2.8.2. clientAuth	Presente	Sí	
2.9. cRLDistributionPoint		Sí	
2.9.1. distributionPoint	"http://crl3.cgcom.es/crl/eccgcom.crl"	Sí	
2.9.2. distributionPoint	"http://crl4.cgcom.es/crl/eccgcom.crl"	Sí	
2.10. Authority Info Acces		Sí	
2.10.1. OCSP Access Method		Sí	
2.10.1.1. Acces Location	"http://ocsp.cgcom.es"	Sí	
2.10.2. caIssuersAccessMethod		Sí	
2.10.2.1. Acces Location	"http://certificacion.cgcom.es/CA/OMC.crt"	Si	
2.11. Subject Directory Attributes (2.5.29.9)		Sí	
2.11.1. Country of Citizenship	País de nacionalidad	Sí	
2.11.2. Country of Residence	País de residencia	Sí	

6. CERTIFICADOS DE PERSONA JURÍDICA

6.1 Certificado corporativo de persona jurídica para identificación

Campo	Contenido	Obligatorio	Crítico
1. Basic estructure			
1.1. Version	"2"[112]	Sí	
1.2. Serial Number	Establecido automáticamente[113]	Sí	
1.3. Signature Algorithm	SHA-256 with RSA Signature	Sí	
1.4. Issuer Distinguished Name		Sí	
1.4.1. Country (C)	"ES"	Sí	
1.4.2. Organization (O)	"Organizacion Medica Colegial" [114]	Sí	
1.4.3. Organizational Unit (OU)	"Entidad de Certificacion" [115]	Sí	
1.4.4. Common Name (CN)	"OMC"	Sí	
1.5. Validity	5 años	Sí	
1.5.1. Not Before	Fecha de inicio de validez	Sí	
1.5.2. Not After	Fecha de expiración	Sí	
1.6. Subject		Sí	
1.6.1. Country (C)	"ES"[116]	Sí	

[112] El literal "2" corresponde a la versión 3.

[113] No debe superar los 32 caracteres hexadecimales en notación hexadecimal.

[114] El texto se incluye sin acentos.

[115] El texto se incluye sin acentos.

Campo	Contenido	Obligatorio	Crítico
1.6.2. Organization (O)	Colegio profesional u otra persona jurídica del ámbito sanitario	Sí	
1.6.3. Organizational Unit (OU)	"Condiciones de uso en https://www.cgcom.es/CertJur (c)06"	Sí	
1.6.4. Organizational Unit (OU)	"Dispositivo"[117]	Sí	
1.6.5. Surname	Apellidos del custodio	Sí	
1.6.6. Given Name	Nombre del custodio	Sí	
1.6.7. 1.3.6.1.4.1.18838.1.1	DNI/NIE[118]	Sí	
1.6.8. Serial Number	NIF de la entidad[119]	Sí	
1.6.9. Common Name (CN)	Colegio profesional u otra persona jurídica del ámbito sanitario + "-"+ "(AUTENTICACION)"	Sí	
1.7. Subject Public Key Info	2048-Bit Public key encoded in accordance with RFC2459 & PKCS#1	Sí	
2. Extensions			
2.1. Authority Key Identifier	Presente	Sí	
2.1.1. Key Identifier			
2.1.2. AuthorityCertIssuer			
2.1.3. AuthorityCertSerialNumber			
2.2. Subject Key Identifier	Presente	Sí	

[116] El campo "país" siempre será España, dado que el certificado muestra la relación entre un colegiado y un colegio profesional español, con independencia de la nacionalidad del colegiado. Ello deriva de la naturaleza corporativa del certificado, del cual es suscriptor el colegio, y el colegiado, la persona autorizada a su uso.

[117] Este campo se refiere al dispositivo usado, en este caso una tarjeta criptográfica.

[118] El campo "número de serie" debe incluir el DNI o el NIE del trabajador, al efecto de la admisión del certificado para la realización de trámites con las Administraciones españolas.

[119] De acuerdo con la normativa tributaria, en este campo debe figurar el NIF de la persona jurídica.

Campo	Contenido	Obligatorio	Crítico
2.3. Key Usage		Sí	Sí
2.3.1. Digital Signature	Seleccionado. “1”	Sí	
2.3.2. Content commintment	No seleccionado. “0”		
2.3.3. Key Encipherment	No seleccionado. “0”		
2.3.4. Data Encipherment	No seleccionado. “0”		
2.3.5. Key Agreement	No seleccionado. “0”		
2.3.6. Key Certificate Signature	No seleccionado. “0”		
2.3.7. CRL Signature	No seleccionado. “0”		
2.4. Qualified Certificate Statements		Sí	
2.4.1. qCCompliance (0.4.0.1862.1.1)		Sí	
2.4.2. QcEuRetentionPeriod (0.4.0.1862.1.3)	15	Sí	
2.4.3. QcSSCD (0.4.0.1862.1.4)		Sí	
2.5. Certificate Policies		Sí	
2.5.1. Policy Identifier	1.3.6.1.4.1.26852.1.1.3.1	Sí	
2.5.2. Policy Qualifier ID		Sí	
2.5.2.1. CPS Pointer	“https://www.cgcom.es/CertJur”	Sí	
2.6. Subject Alternative Names		Sí	
2.6.1. rfc822Name	Correo electrónico corporativo del custodio[120]	Sí	
2.6.2. directoryName[121]		Sí	

[120] Este campo contiene la dirección de correo corporativo del colegiado, a efectos de notificaciones.

[121] Este campo enlaza con el sistema de validación y re-certificación del CGCOM, permitiendo recuperar informaciones adicionales de forma eficiente. Ciertas informaciones se incluyen, aunque

Campo	Contenido	Obligatorio	Crítico
2.6.2.1. CGCOM.2.1	IdColegio / IdEntidad	Sí	
2.6.2.2. CGCOM.2.2	Colegio profesional / Entidad jurídica ámbito sanitario	Sí	
2.7. Issuer Alternative Name		Sí	
2.7.1. rfc822Name	"certificacion@cgcom.es"	Sí	
2.8. Extended Key Usage		Sí	
2.8.1. clientAuth	Presente	Sí	
2.9. cRLDistributionPoint		Sí	
2.9.1. distributionPoint	"http://crl3.cgcom.es/crl/eccgcom.crl"	Sí	
2.9.2. distributionPoint	"http://crl4.cgcom.es/crl/eccgcom.crl"	Sí	
2.10. Authority Info Acces		Sí	
2.10.1. OCSP Access Method		Sí	
2.10.1.1. Acces Location	"http://ocsp.cgcom.es"	Sí	
2.10.2. caIssuersAccessMethod		Sí	
2.10.2.1. Acces Location	"http://certificacion.cgcom.es/CA/OMC.crt"	Si	
2.11. Subject Directory Attributes (2.5.29.9)		Sí	
2.11.1. Country of Citizenship	País de nacionalidad	Sí	
2.11.2. Country of Residence	País de residencia	Sí	

sean redundantes, para disponer de toda la información sobre el usuario en una sola consulta contra el certificado.

6.2 Certificado corporativo de persona jurídica para firma

Campo	Contenido	Obligatorio	Crítico
1. Basic estructure			
1.1. Version	"2"[122]	Sí	
1.2. Serial Number	Establecido automáticamente[123]	Sí	
1.3. Signature Algorithm	SHA-256 with RSA Signature	Sí	
1.4. Issuer Distinguished Name		Sí	
1.4.1. Country (C)	"ES"	Sí	
1.4.2. Organization (O)	"Organizacion Medica Colegial" [124]	Sí	
1.4.3. Organizational Unit (OU)	"Entidad de Certificacion" [125]	Sí	
1.4.4. Common Name (CN)	"OMC"	Sí	
1.5. Validity	5 años	Sí	
1.5.1. Not Before	Fecha de inicio de validez	Sí	
1.5.2. Not After	Fecha de expiración	Sí	
1.6. Subject		Sí	
1.6.1. Country (C)	"ES"[126]	Sí	
1.6.2. Organization (O)	Colegio profesional u otra persona jurídica del ámbito sanitario	Sí	

[122] El literal "2" corresponde a la versión 3.

[123] No debe superar los 32 caracteres hexadecimales en notación hexadecimal.

[124] El texto se incluye sin acentos.

[125] El texto se incluye sin acentos.

[126] El campo "país" siempre será España, dado que el certificado muestra la relación entre un colegiado y un colegio profesional español, con independencia de la nacionalidad del colegiado. Ello deriva de la naturaleza corporativa del certificado, del cual es suscriptor el colegio, y el colegiado, la persona autorizada a su uso.

Campo	Contenido	Obligatorio	Crítico
1.6.3. Organizational Unit (OU)	"Condiciones de uso en https://www.cgcom.es/CertJur (c)06"	Sí	
1.6.4. Organizational Unit (OU)	"Dispositivo"[127]	Sí	
1.6.5. Surname	Apellidos del custodio	Sí	
1.6.6. Given Name	Nombre del custodio	Sí	
1.6.7. 1.3.6.1.4.1.18838.1.1	DNI/NIE[128]	Sí	
1.6.8. Serial Number	NIF de la entidad[129]	Sí	
1.6.9. Common Name (CN)	Colegio profesional u otra persona jurídica del ámbito sanitario + "-"+ "(FIRMA)"	Sí	
1.7. Subject Public Key Info	2048-Bit Public key encoded in accordance with RFC2459 & PKCS#1	Sí	
2. Extensions			
2.1. Authority Key Identifier	Presente	Sí	
2.1.1. Key Identifier			
2.1.2. AuthorityCertIssuer			
2.1.3. AuthorityCertSerialNumber			
2.2. Subject Key Identifier	Presente	Sí	
2.3. Key Usage		Sí	Sí
2.3.1. Digital Signature	No seleccionado. "0"		
2.3.2. Content commintment	Seleccionado. "1"	Sí	
2.3.3. Key Encipherment	No seleccionado. "0"		

[127] Este campo se refiere al dispositivo usado, en este caso una tarjeta criptográfica.

[128] El campo "número de serie" debe incluir el DNI o el NIE del trabajador, al efecto de la admisión del certificado para la realización de trámites con las Administraciones españolas.

[129] De acuerdo con la normativa tributaria, en este campo debe figurar el NIF de la persona jurídica.

Campo	Contenido	Obligatorio	Crítico
2.3.4. Data Encipherment	No seleccionado. “0”		
2.3.5. Key Agreement	No seleccionado. “0”		
2.3.6. Key Certificate Signature	No seleccionado. “0”		
2.3.7. CRL Signature	No seleccionado. “0”		
2.4. Qualified Certificate Statements		Sí	
2.4.1. qCCompliance (0.4.0.1862.1.1)		Sí	
2.4.2. QcEuRetentionPeriod (0.4.0.1862.1.3)	15	Sí	
2.4.3. QcSSCD (0.4.0.1862.1.4)		Sí	
2.5. Certificate Policies		Sí	
2.5.1. Policy Identifier	1.3.6.1.4.1.26852.1.1.3.2	Sí	
2.5.2. Policy Qualifier ID		Sí	
2.5.2.1. CPS Pointer	“https://www.cgcom.es/CertJur”	Sí	
2.6. Subject Alternative Names		Sí	
2.6.1. rfc822Name	Correo electrónico corporativo del custodio[130]	Sí	
2.6.2. directoryName[131]		Sí	
2.6.2.1. CGCOM.2.1	IdColegio / IdEntidad	Sí	
2.6.2.2. CGCOM.2.2	Colegio profesional / Entidad jurídica ámbito sanitario	Sí	
2.7. Issuer Alternative Name		Sí	

[130] Este campo contiene la dirección de correo corporativo del colegiado, a efectos de notificaciones.

[131] Este campo enlaza con el sistema de validación y re-certificación del CGCOM, permitiendo recuperar informaciones adicionales de forma eficiente. Ciertas informaciones se incluyen, aunque sean redundantes, para disponer de toda la información sobre el usuario en una sola consulta contra el certificado.

Campo	Contenido	Obligatorio	Crítico
2.7.1. rfc822Name	"certificacion@cgcom.es"	Sí	
2.8. Extended Key Usage		Sí	
2.8.1. emailProtection	Presente	Sí	
2.9. cRLDistributionPoint		Sí	
2.9.1. distributionPoint	"http://crl3.cgcom.es/crl/eccgcom.crl"	Sí	
2.9.2. distributionPoint	"http://crl4.cgcom.es/crl/eccgcom.crl"	Sí	
2.10. Authority Info Acces		Sí	
2.10.1. OCSP Access Method		Sí	
2.10.1.1. Acces Location	"http://ocsp.cgcom.es"	Sí	
2.10.2. caIssuersAccessMethod		Sí	
2.10.2.1. Acces Location	"http://certificacion.cgcom.es/CA/OMC.crt"	Si	
2.11. Subject Directory Attributes (2.5.29.9)		Sí	
2.11.1. Country of Citizenship	País de nacionalidad	Sí	
2.11.2. Country of Residence	País de residencia	Sí	

6.3 Certificado de cifrado en tarjeta, para persona jurídica

Campo	Contenido	Obligatorio	Crítico
1. Basic estructure			
1.1. Version	"2"[132]	Sí	
1.2. Serial Number	Establecido automáticamente[133]	Sí	
1.3. Signature Algorithm	SHA-256 with RSA Signature	Sí	
1.4. Issuer Distinguished Name		Sí	
1.4.1. Country (C)	"ES"	Sí	
1.4.2. Organization (O)	"Organizacion Medica Colegial" [134]	Sí	
1.4.3. Organizational Unit (OU)	"Entidad de Certificacion" [135]	Sí	
1.4.4. Common Name (CN)	"OMC"	Sí	
1.5. Validity	5 años	Sí	
1.5.1. Not Before	Fecha de inicio de validez	Sí	
1.5.2. Not After	Fecha de expiración	Sí	
1.6. Subject		Sí	
1.6.1. Country (C)	"ES"[136]	Sí	
1.6.2. Organization (O)	Colegio profesional u otra persona jurídica del ámbito sanitario	Sí	
1.6.3. Organizational Unit (OU)	"Condiciones de uso en https://www.cgcom.es/CertJur (c)06"	Sí	

[132] El literal "2" corresponde a la versión 3.

[133] No debe superar los 32 caracteres hexadecimales en notación hexadecimal.

[134] El texto se incluye sin acentos.

[135] El texto se incluye sin acentos.

[136] El campo "país" siempre será España.

Campo	Contenido	Obligatorio	Crítico
1.6.4. Organizational Unit (OU)	"Dispositivo"[137]	Sí	
1.6.5. Surname	Apellidos del custodio	Sí	
1.6.6. Given Name	Nombre del custodio	Sí	
1.6.7. 1.3.6.1.4.1.18838.1.1	DNI/NIE[138]	Sí	
1.6.8. Serial Number	NIF de la entidad[139]	Sí	
1.6.9. Common Name (CN)	Colegio profesional u otra persona jurídica del ámbito sanitario + "-"+ "(CIFRADO)"	Sí	
1.7. Subject Public Key Info	2048-Bit Public key encoded in accordance with RFC2459 & PKCS#1	Sí	
2. Extensions			
2.1. Authority Key Identifier	Presente	Sí	
2.1.1. Key Identifier			
2.1.2. AuthorityCertIssuer			
2.1.3. AuthorityCertSerialNumber			
2.2. Subject Key Identifier	Presente	Sí	
2.3. Key Usage		Sí	Sí
2.3.1. Digital Signature	No seleccionado. "0"		
2.3.2. Content commintment	No seleccionado. "0"		
2.3.3. Key Encipherment	Seleccionado. "1"	Sí	
2.3.4. Data Encipherment	Seleccionado. "1"	Sí	
2.3.5. Key Agreement	No seleccionado. "0"		

[137] Este campo se refiere al dispositivo usado, en este caso una tarjeta criptográfica.

[138] El campo "número de serie" debe incluir el DNI o el NIE del trabajador, al efecto de la admisión del certificado para la realización de trámites con las Administraciones españolas.

[139] De acuerdo con la normativa tributaria, en este campo debe figurar el NIF de la persona jurídica.

Campo	Contenido	Obligatorio	Crítico
2.3.6. Key Certificate Signature	No seleccionado. “0”		
2.3.7. CRL Signature	No seleccionado. “0”		
2.4. Qualified Certificate Statements		Sí	
2.4.1. qCCompliance (0.4.0.1862.1.1)		Sí	
2.4.2. QcEuRetentionPeriod (0.4.0.1862.1.3)	15	Sí	
2.4.3. QcSSCD		Sí	
2.5. Certificate Policies		Sí	
2.5.1. Policy Identifier	1.3.6.1.4.1.26852.1.1.3.3	Sí	
2.5.2. Policy Qualifier ID		Sí	
2.5.2.1. CPS Pointer	“https://www.cgcom.es/CertJur”	Sí	
2.6. Subject Alternative Names		Sí	
2.6.1. rfc822Name	Correo electrónico corporativo[140]	Sí	
2.6.2. directoryName[141]		Sí	
2.6.2.1. CGCOM.2.1	IdColegio / IdEntidad	Sí	
2.6.2.2. CGCOM.2.2	Colegio profesional / Entidad jurídica ámbito sanitario	Sí	
2.7. Issuer Alternative Name		Sí	
2.7.1. rfc822Name	“certificacion@cgcom.es”	Sí	
2.8. Extended Key Usage		Sí	
2.8.1. emailProtection	Presente	Sí	

[140] Este campo contiene la dirección de correo corporativo del colegiado, a efectos de notificaciones.

[141] Este campo enlaza con el sistema de validación y re-certificación del CGCOM, permitiendo recuperar informaciones adicionales de forma eficiente. Ciertas informacions se incluyen, aunque sean redundantes, para disponer de toda la información sobre el usuario en una sola consulta contra el certificado.

Campo	Contenido	Obligatorio	Crítico
2.9. cRLDistributionPoint		Sí	
2.9.1. distributionPoint	"http://crl3.cgcom.es/crl/eccgcom.crl"	Sí	
2.9.2. distributionPoint	"http://crl4.cgcom.es/crl/eccgcom.crl"	Sí	
2.10. Authority Info Acces		Sí	
2.10.1. OCSP Access Method		Sí	
2.10.1.1. Acces Location	"http://ocsp.cgcom.es"	Sí	
2.10.2. caIssuersAccessMethod		Sí	
2.10.2.1. Acces Location	"http://certificacion.cgcom.es/CA/OMC.crt"	Si	
2.11. Subject Directory Attributes (2.5.29.9)		Sí	
2.11.1. Country of Citizenship	País de nacionalidad	Sí	
2.11.2. Country of Residence	País de residencia	Sí	

6.4 Certificado corporativo de persona jurídica en software, para identificación, firma y cifrado

Campo	Contenido	Obligatorio	Crítico
1. Basic estructure			
1.1. Version	"2"[142]	Sí	
1.2. Serial Number	Establecido automáticamente[143]	Sí	
1.3. Signature Algorithm	SHA-256 with RSA Signature	Sí	
1.4. Issuer Distinguished Name		Sí	
1.4.1. Country (C)	"ES"	Sí	
1.4.2. Organization (O)	"Organizacion Medica Colegial" [144]	Sí	
1.4.3. Organizational Unit (OU)	"Entidad de Certificacion" [145]	Sí	
1.4.4. Common Name (CN)	"OMC"	Sí	
1.5. Validity	5 años	Sí	
1.5.1. Not Before	Fecha de inicio de validez	Sí	
1.5.2. Not After	Fecha de expiración	Sí	
1.6. Subject		Sí	
1.6.1. Country (C)	"ES"[146]	Sí	
1.6.2. Organization (O)	Colegio profesional u otra persona jurídica del ámbito sanitario	Sí	
1.6.3. Organizational Unit (OU)	"Condiciones de uso en https://www.cgcom.es/CertJurSoft (c)11"	Sí	

[142] El literal "2" corresponde a la versión 3.

[143] No debe superar los 32 caracteres hexadecimales en notación hexadecimal.

[144] El texto se incluye sin acentos.

[145] El texto se incluye sin acentos.

[146] El campo "país" siempre será España.

Campo	Contenido	Obligatorio	Crítico
1.6.4. Organizational Unit (OU)	Dispositivo[147]	Sí	
1.6.5. Surname	Apellidos del custodio	Sí	
1.6.6. Given Name	Nombre del custodio	Sí	
1.6.7. 1.3.6.1.4.1.18838.1.1	DNI/NIE[148]	Sí	
1.6.8. Serial Number	NIF de la entidad[149]	Sí	
1.6.9. Common Name (CN)	Colegio profesional u otra persona jurídica del ámbito sanitario	Sí	
1.7. Subject Public Key Info	2048-Bit Public key encoded in accordance with RFC2459 & PKCS#1	Sí	
2. Extensions			
2.1. Authority Key Identifier	Presente	Sí	
2.1.1. Key Identifier			
2.1.2. AuthorityCertIssuer			
2.1.3. AuthorityCertSerialNumber			
2.2. Subject Key Identifier	Presente	Sí	
2.3. Key Usage		Sí	Sí
2.3.1. Digital Signature	Seleccionado. “1”	Sí	
2.3.2. Non Repudiation	Seleccionado. “1”	Sí	
2.3.3. Key Encipherment	Seleccionado. “1”	Sí	
2.3.4. Data Encipherment	Seleccionado. “1”	Sí	
2.3.5. Key Agreement	No seleccionado. “0”		

[147] Este campo se refiere al dispositivo usado por las claves y el certificado como puede ser un movil o tableta.

[148] El campo “número de serie” debe incluir el DNI o el NIE del trabajador, al efecto de la admisión del certificado para la realización de trámites con las Administraciones españolas.

[149] De acuerdo con la normativa tributaria, en este campo debe figurar el NIF de la persona jurídica.

Campo	Contenido	Obligatorio	Crítico
2.3.6. Key Certificate Signature	No seleccionado. “0”		
2.3.7. CRL Signature	No seleccionado. “0”		
2.4. Qualified Certificate Statements		Sí	
2.4.1. qCCompliance (0.4.0.1862.1.1)		Sí	
2.4.2. QcEuRetentionPeriod (0.4.0.1862.1.3)	15	Sí	
2.5. Certificate Policies		Sí	
2.5.1. Policy Identifier	1.3.6.1.4.1.26852.1.1.5	Sí	
2.5.2. Policy Qualifier ID		Sí	
2.5.2.1. CPS Pointer	“https://www.cgcom.es/CertJurSoft”	Sí	
2.6. Subject Alternative Names		Sí	
2.6.1. rfc822Name	Correo electrónico corporativo del custodio[150]	Sí	
2.6.2. directoryName[151]		Sí	
2.6.2.1. CGCOM.2.1	IdColegio / IdEntidad	Sí	
2.6.2.2. CGCOM.2.2	Colegio profesional / Entidad jurídica ámbito sanitario	Sí	
2.7. Issuer Alternative Name		Sí	
2.7.1. rfc822Name	“certificacion@cgcom.es”	Sí	
2.8. Extended Key Usage		Sí	
2.8.1. emailProtection	Presente	Sí	

[150] Este campo contiene la dirección de correo corporativo del colegiado, a efectos de notificaciones.

[151] Este campo enlaza con el sistema de validación y re-certificación del CGCOM, permitiendo recuperar informaciones adicionales de forma eficiente. Ciertas informacions se incluyen, aunque sean redundantes, para disponer de toda la información sobre el usuario en una sola consulta contra el certificado.

Campo	Contenido	Obligatorio	Crítico
2.8.2. clientAuth	Presente	Sí	
2.9. cRLDistributionPoint		Sí	
2.9.1. distributionPoint	"http://crl3.cgcom.es/crl/eccgcom.crl"	Sí	
2.9.2. distributionPoint	"http://crl4.cgcom.es/crl/eccgcom.crl"	Sí	
2.10. Authority Info Acces		Sí	
2.10.1. OCSP Access Method		Sí	
2.10.1.1. Acces Location	"http://ocsp.cgcom.es"	Sí	
2.10.2. caIssuersAccessMethod		Sí	
2.10.2.1. Acces Location	"http://certificacion.cgcom.es/CA/OMC.crt"	Si	
2.11. Subject Directory Attributes (2.5.29.9)		Sí	
2.11.1. Country of Citizenship	País de nacionalidad	Sí	
2.11.2. Country of Residence	País de residencia	Sí	