Perfiles de Certificados de la Entidad de Certificación

Organización Médica Colegial de España

OMC ORGANIZACIÓN MÉDICA COLEGIAL DE ESPAÑA | CONSEJO GENERAL DE COLEGIOS OFICIALES DE MÉDICOS

1. Información general

1.1 Control documental

Proyecto:	**Autoridad de Certificación**
Entidad de destino:	**Organización Médica Colegial de España**
Versión:	**4.1**
Fecha de la edición:	**8/4/2022**
Archivo:	**Perfiles_CGCOM_v4r1.docx**
Autores:	**Astrea**

1.2 Estado formal

Preparado por:	**Revisado por:**	**Aprobado por:**
Nombre: Astrea Fecha: **8/4/2022**	Nombre: CGCOM Fecha: **8/4/2022**	Nombre: CGCOM 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
3.11	En los perfiles de empleados públicos	Se añade el campo “User Notice”	Astrea	14/12/2015
		Se elimina el perfil de certificados a emitir en HSM	Astrea	16/12/2015
3.12		Se reduce la caducidad de los certificados a 3 años	Astrea	15/07/2019
3.13		Se eliminan los certificados de médico empleado público	Astrea	01/09/2019
4		Actualización nueva jerarquía	Astrea	7/4/2021
4.1		Se añaden los perfiles en software	Astrea	8/4/2022

Índice

2. Introducción

Este documento recoge los perfiles de certificados que expedirá la Autoridad de Certificación del CGCOM.

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

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

El OID de OMC es 1.3.6.1.4.1.26852

La rama de OIDs de la AC-CGCOM para la certificación es el 1.3.6.1.4.1.26852.1

3. MATRIZ DE CERTIFICADOS

CERTIFICADO	EMITIDO EN	FUNCIONALIDAD	OID	POL ETSI
De Médico Colegiado	Tarjeta	Identificación	1.3.6.1.4.1.26852.1.1.1.1	NCP+
		Firma	1.3.6.1.4.1.26852.1.1.1.2	QCP-n-qscd
		Cifrado	1.3.6.1.4.1.26852.1.1.1.3	
	Nube	Identificación y firma	1.3.6.1.4.1.26852.1.1.1.4	QCP-n-qscd
	Software	Identificación y firma	1.3.6.1.4.1.26852.1.1.1.5	QCP-n

CERTIFICADO	EMITIDO EN	FUNCIONALIDAD	OID	POL ETSI
De Persona Física Vinculada	Tarjeta	Identificación	1.3.6.1.4.1.26852.1.1.2.1	NCP+
		Firma	1.3.6.1.4.1.26852.1.1.2.2	QCP-n-qscd
		Cifrado	1.3.6.1.4.1.26852.1.1.2.3	
	Nube	Identificación y firma	1.3.6.1.4.1.26852.1.1.6	QCP-n-qscd
	Software	Identificación y firma	1.3.6.1.4.1.26852.1.1.2.5	QCP-n

CERTIFICADO	EMITIDO EN	FUNCIONALIDAD	OID	POL ETSI
De Representante Legal	Tarjeta	Identificación	1.3.6.1.4.1.26852.1.1.11.1	NCP+
		Firma	1.3.6.1.4.1.26852.1.1.11.2	QCP-n-qscd
		Cifrado	1.3.6.1.4.1.26852.1.1.11.3	
	Nube	Identificación y firma	1.3.6.1.4.1.26852.1.1.12	QCP-n-qscd
	Software	Identificación y firma	1.3.6.1.4.1.26852.1.1.11.5	QCP-n

CERTIFICADO	EMITIDO EN	FUNCIONALIDAD	OID	POL ETSI
De Sello electrónico de Persona Jurídica	Nube	Identificación y firma	1.3.6.1.4.1.26852.1.1.10.2	QCP-l-qscd
	Software	Identificación y firma	1.3.6.1.4.1.26852.1.1.10.5	QCP-l

4. Certificados de médico colegiado en tarjeta

4.1 Para AUTENTICACIÓN

```
SEQUENCE (3 elem)
  SEQUENCE (8 elem)
    [0] (1 elem)
      INTEGER 2
    INTEGER (63 bit) 5142123253688973483
    SEQUENCE (2 elem)
      OBJECT IDENTIFIER 1.2.840.113549.1.1.13 sha512WithRSAEncryption (PKCS #1)
      NULL
    SEQUENCE (7 elem)
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.6 countryName (X.520 DN component)
          PrintableString ES
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.8 stateOrProvinceName (X.520 DN component)
          UTF8String MADRID
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.7 localityName (X.520 DN component)
          UTF8String MADRID
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.97
          UTF8String VATES-Q2866017C
```

```
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.11 organizationalUnitName (X.520 DN component)
          UTF8String ENTIDAD DE CERTIFICACION
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.10 organizationName (X.520 DN component)
          UTF8String CONSEJO GENERAL DE COLEGIOS OFICIALES DE MEDICOS
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.3 commonName (X.520 DN component)
          UTF8String CGCOM QUALIFIED 2020
    SEQUENCE (2 elem)
      UTCTime 2020-03-02 12:18:15 UTC
      UTCTime 2023-03-02 12:18:15 UTC
    SEQUENCE (10 elem)
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.3 commonName (X.520 DN component)
          UTF8String apellido1 apellido2 nombre - DNI 12345678Z (AUTENTICACIÓN)
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.5 serialNumber (X.520 DN component)
          PrintableString IDCES-12345678Z
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.42 givenName (X.520 DN component)
          UTF8String Nombre
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.4 surname (X.520 DN component)
          UTF8String apellido1 apellido2
```

```
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.12 title (X.520 DN component)
          UTF8String MEDICO COLEGIADO
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.11 organizationalUnitName (X.520 DN component)
          UTF8String UnidadOrganizativa
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.11 organizationalUnitName (X.520 DN component)
          UTF8String CARNET COLEGIAL
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.97
          UTF8String VATES-Q0000001
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.10 organizationName (X.520 DN component)
          UTF8String NombreColegio
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.6 countryName (X.520 DN component)
          PrintableString ES
    SEQUENCE (2 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 1.2.840.113549.1.1.1 rsaEncryption (PKCS #1)
        NULL
      BIT STRING (2160 bit) 001100001000001000000001000010100000001010000010000000010000000100000…
        SEQUENCE (2 elem)
          INTEGER (2048 bit) 216239978274880649812146602572249622354145968290758890281528893875878…
          INTEGER 65537
```

```
[3] (1 elem)
  SEQUENCE (9 elem)
    SEQUENCE (2 elem)
      OBJECT IDENTIFIER 1.3.6.1.5.5.7.1.1 authorityInfoAccess (PKIX private extension)
      OCTET STRING (99 byte) 3061303606082B06010505073002862A687474703A2F2F7073632E6367636F6D2E6573…
        SEQUENCE (2 elem)
          SEQUENCE (2 elem)
            OBJECT IDENTIFIER 1.3.6.1.5.5.7.48.2 caIssuers (PKIX subject/authority info access descriptor)
            [6] (42 byte) http://psc.cgcom.es/CA/root_cgcom_2020.crt
          SEQUENCE (2 elem)
            OBJECT IDENTIFIER 1.3.6.1.5.5.7.48.1 ocsp (PKIX)
            [6] (27 byte) http://ocspservice.cgcom.es
    SEQUENCE (2 elem)
      OBJECT IDENTIFIER 2.5.29.14 subjectKeyIdentifier (X.509 extension)
      OCTET STRING (20 byte) 5E867B9F5EFB981C6BDB5291488EA2C6A6A16B00
        OCTET STRING (20 byte) 5E867B9F5EFB981C6BDB5291488EA2C6A6A16B00
    SEQUENCE (3 elem)
      OBJECT IDENTIFIER 2.5.29.19 basicConstraints (X.509 extension)
      BOOLEAN true
      OCTET STRING (2 byte) 3000
        SEQUENCE (0 elem)
    SEQUENCE (2 elem)
      OBJECT IDENTIFIER 2.5.29.35 authorityKeyIdentifier (X.509 extension)
      OCTET STRING (24 byte) 3016801432416494D42D413ACDEB2B7209EBAB8D883AD1CF
        SEQUENCE (1 elem)
          [0] (20 byte) 32416494D42D413ACDEB2B7209EBAB8D883AD1CF
    SEQUENCE (2 elem)
      OBJECT IDENTIFIER 2.5.29.32 certificatePolicies (X.509 extension)
      OCTET STRING (156 byte) 30819930818C060C2B0601040181D16401010101307C302406082B060105050702011…
        SEQUENCE (2 elem)
          SEQUENCE (2 elem)
            OBJECT IDENTIFIER 1.3.6.1.4.1.26852.1.1.1.1
```

```
            SEQUENCE (2 elem)
              SEQUENCE (2 elem)
                OBJECT IDENTIFIER 1.3.6.1.5.5.7.2.1 cps (PKIX policy qualifier)
                IA5String https://psc.cgcom.es/dpc
              SEQUENCE (2 elem)
                OBJECT IDENTIFIER 1.3.6.1.5.5.7.2.2 unotice (PKIX policy qualifier)
                SEQUENCE (1 elem)
                  UTF8String "CERTIFICADO PARA LA IDENTIFICACION DE MEDICO COLEGIADO, EN TARJETA"
          SEQUENCE (1 elem)
            OBJECT IDENTIFIER 0.4.0.2042.1.2
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.29.31 cRLDistributionPoints (X.509 extension)
        OCTET STRING (90 byte) 3058302AA028A0268624687474703A2F2F63726C352E6367636F6D2E65732F63726C2F…
          SEQUENCE (2 elem)
            SEQUENCE (1 elem)
              [0] (1 elem)
                [0] (1 elem)
                  [6] (36 byte) http://crl5.cgcom.es/crl/eccgcom.crl
            SEQUENCE (1 elem)
              [0] (1 elem)
                [0] (1 elem)
                  [6] (36 byte) http://crl6.cgcom.es/crl/eccgcom.crl
      SEQUENCE (3 elem)
        OBJECT IDENTIFIER 2.5.29.15 keyUsage (X.509 extension)
        BOOLEAN true
        OCTET STRING (4 byte) 03020780
          BIT STRING (1 bit) 1
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.29.37 extKeyUsage (X.509 extension)
        OCTET STRING (12 byte) 300A06082B06010505070302
          SEQUENCE (1 elem)
            OBJECT IDENTIFIER 1.3.6.1.5.5.7.3.2 clientAuth (PKIX key purpose)
```

```
SEQUENCE (2 elem)
  OBJECT IDENTIFIER 2.5.29.17 subjectAltName (X.509 extension)
  OCTET STRING (204 byte) 3081C98110656D61696C407072756562612E636F6DA481B43081B131193017060A2B0…
    SEQUENCE (2 elem)
      [1] (16 byte) email@prueba.com
      [4] (1 elem)
        SEQUENCE (7 elem)
          SET (1 elem)
            SEQUENCE (2 elem)
              OBJECT IDENTIFIER 1.3.6.1.4.1.26852.2.12
              UTF8String 12345678Z
          SET (1 elem)
            SEQUENCE (2 elem)
              OBJECT IDENTIFIER 1.3.6.1.4.1.26852.2.11
              UTF8String Apellido2
          SET (1 elem)
            SEQUENCE (2 elem)
              OBJECT IDENTIFIER 1.3.6.1.4.1.26852.2.10
              UTF8String Apellido1
          SET (1 elem)
            SEQUENCE (2 elem)
              OBJECT IDENTIFIER 1.3.6.1.4.1.26852.2.9
              UTF8String Nombre
          SET (1 elem)
            SEQUENCE (2 elem)
              OBJECT IDENTIFIER 1.3.6.1.4.1.26852.2.3
              UTF8String 00003
          SET (1 elem)
            SEQUENCE (2 elem)
              OBJECT IDENTIFIER 1.3.6.1.4.1.26852.2.2
              UTF8String Colegio
          SET (1 elem)
```

```
                    SEQUENCE (2 elem)
                      OBJECT IDENTIFIER 1.3.6.1.4.1.26852.2.1
                      UTF8String 000035
  SEQUENCE (2 elem)
    OBJECT IDENTIFIER 1.2.840.113549.1.1.13 sha512WithRSAEncryption (PKCS #1)
    NULL
```

4.2 Para FIRMA

```
SEQUENCE (3 elem)
  SEQUENCE (8 elem)
    [0] (1 elem)
      INTEGER 2
    INTEGER (63 bit) 7418842431603200977
    SEQUENCE (2 elem)
      OBJECT IDENTIFIER 1.2.840.113549.1.1.13 sha512WithRSAEncryption (PKCS #1)
      NULL
    SEQUENCE (7 elem)
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.6 countryName (X.520 DN component)
          PrintableString ES
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.8 stateOrProvinceName (X.520 DN component)
          UTF8String MADRID
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.7 localityName (X.520 DN component)
          UTF8String MADRID
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.97
          UTF8String VATES-Q2866017C
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.11 organizationalUnitName (X.520 DN component)
```

```
        UTF8String ENTIDAD DE CERTIFICACION
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.10 organizationName (X.520 DN component)
        UTF8String CONSEJO GENERAL DE COLEGIOS OFICIALES DE MEDICOS
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.3 commonName (X.520 DN component)
        UTF8String CGCOM QUALIFIED 2020
  SEQUENCE (2 elem)
    UTCTime 2020-03-02 12:51:13 UTC
    UTCTime 2023-03-02 12:51:13 UTC
  SEQUENCE (10 elem)
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.3 commonName (X.520 DN component)
        UTF8String apellido1 apellido2 nombre - DNI 12345678Z (FIRMA)
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.5 serialNumber (X.520 DN component)
        PrintableString IDCES-12345678Z
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.42 givenName (X.520 DN component)
        UTF8String Nombre
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.4 surname (X.520 DN component)
        UTF8String apellido1 apellido2
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.12 title (X.520 DN component)
```

```
        UTF8String MEDICO COLEGIADO
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.11 organizationalUnitName (X.520 DN component)
        UTF8String UnidadOrganizativa
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.11 organizationalUnitName (X.520 DN component)
        UTF8String CARNET COLEGIAL
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.97
        UTF8String VATES-Q0000001
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.10 organizationName (X.520 DN component)
        UTF8String NombreColegio
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.6 countryName (X.520 DN component)
        PrintableString ES
  SEQUENCE (2 elem)
    SEQUENCE (2 elem)
      OBJECT IDENTIFIER 1.2.840.113549.1.1.1 rsaEncryption (PKCS #1)
      NULL
    BIT STRING (2160 bit) 001100001000001000000001000010100000001010000010000000010000000100000…
      SEQUENCE (2 elem)
        INTEGER (2048 bit) 22789374483297127607046923706701150301672922552843484587603333239931 1…
        INTEGER 65537
  [3] (1 elem)
    SEQUENCE (10 elem)
      SEQUENCE (2 elem)
```

```
    OBJECT IDENTIFIER 1.3.6.1.5.5.7.1.1 authorityInfoAccess (PKIX private extension)
    OCTET STRING (99 byte) 3061303606082B06010505073002862A687474703A2F2F7073632E6367636F6D2E6573…
      SEQUENCE (2 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 1.3.6.1.5.5.7.48.2 caIssuers (PKIX subject/authority info access descriptor)
          [6] (42 byte) http://psc.cgcom.es/CA/root_cgcom_2020.crt
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 1.3.6.1.5.5.7.48.1 ocsp (PKIX)
          [6] (27 byte) http://ocspservice.cgcom.es
  SEQUENCE (2 elem)
    OBJECT IDENTIFIER 2.5.29.14 subjectKeyIdentifier (X.509 extension)
    OCTET STRING (20 byte) A72B67E6A48648969F7A32F87566DDDF105111B1
      OCTET STRING (20 byte) A72B67E6A48648969F7A32F87566DDDF105111B1
  SEQUENCE (3 elem)
    OBJECT IDENTIFIER 2.5.29.19 basicConstraints (X.509 extension)
    BOOLEAN true
    OCTET STRING (2 byte) 3000
      SEQUENCE (0 elem)
  SEQUENCE (2 elem)
    OBJECT IDENTIFIER 2.5.29.35 authorityKeyIdentifier (X.509 extension)
    OCTET STRING (24 byte) 3016801432416494D42D413ACDEB2B7209EBAB8D883AD1CF
      SEQUENCE (1 elem)
        [0] (20 byte) 32416494D42D413ACDEB2B7209EBAB8D883AD1CF
  SEQUENCE (2 elem)
    OBJECT IDENTIFIER 1.3.6.1.5.5.7.1.3 qcStatements (PKIX private extension)
    OCTET STRING (159 byte) 30819C301506082B06010505070B023009060704008BEC4901013008060604008E460…
      SEQUENCE (6 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 1.3.6.1.5.5.7.11.2
          SEQUENCE (1 elem)
            OBJECT IDENTIFIER 0.4.0.194121.1.1
        SEQUENCE (1 elem)
```

```
            OBJECT IDENTIFIER 0.4.0.1862.1.1 etsiQcsCompliance (ETSI TS 101 862 qualified certificates)
          SEQUENCE (2 elem)
            OBJECT IDENTIFIER 0.4.0.1862.1.3 etsiQcsRetentionPeriod (ETSI TS 101 862 qualified certificates)
            INTEGER 15
          SEQUENCE (1 elem)
            OBJECT IDENTIFIER 0.4.0.1862.1.4 etsiQcsQcSSCD (ETSI TS 101 862 qualified certificates)
          SEQUENCE (2 elem)
            OBJECT IDENTIFIER 0.4.0.1862.1.6
            SEQUENCE (1 elem)
              OBJECT IDENTIFIER 0.4.0.1862.1.6.1
          SEQUENCE (2 elem)
            OBJECT IDENTIFIER 0.4.0.1862.1.5
            SEQUENCE (2 elem)
              SEQUENCE (2 elem)
                IA5String https://psc.cgcom.es/en/pds
                PrintableString en
              SEQUENCE (2 elem)
                IA5String https://psc.cgcom.es/pds
                PrintableString es
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.29.32 certificatePolicies (X.509 extension)
        OCTET STRING (157 byte) 30819A30818C060C2B0601040181D16401010102307C302406082B060105050702011…
          SEQUENCE (2 elem)
            SEQUENCE (2 elem)
              OBJECT IDENTIFIER 1.3.6.1.4.1.26852.1.1.1.2
              SEQUENCE (2 elem)
                SEQUENCE (2 elem)
                  OBJECT IDENTIFIER 1.3.6.1.5.5.7.2.1 cps (PKIX policy qualifier)
                  IA5String https://psc.cgcom.es/dpc
                SEQUENCE (2 elem)
                  OBJECT IDENTIFIER 1.3.6.1.5.5.7.2.2 unotice (PKIX policy qualifier)
                  SEQUENCE (1 elem)
```

```
                UTF8String "CERTIFICADO CUALIFICADO PARA FIRMA DE MEDICO COLEGIADO, EN TARJETA”
        SEQUENCE (1 elem)
          OBJECT IDENTIFIER 0.4.0.194112.1.2
SEQUENCE (2 elem)
  OBJECT IDENTIFIER 2.5.29.31 cRLDistributionPoints (X.509 extension)
  OCTET STRING (90 byte) 3058302AA028A0268624687474703A2F2F63726C352E6367636F6D2E65732F63726C2F…
    SEQUENCE (2 elem)
      SEQUENCE (1 elem)
        [0] (1 elem)
          [0] (1 elem)
            [6] (36 byte) http://crl5.cgcom.es/crl/eccgcom.crl
      SEQUENCE (1 elem)
        [0] (1 elem)
          [0] (1 elem)
            [6] (36 byte) http://crl6.cgcom.es/crl/eccgcom.crl
SEQUENCE (3 elem)
  OBJECT IDENTIFIER 2.5.29.15 keyUsage (X.509 extension)
  BOOLEAN true
  OCTET STRING (4 byte) 03020640
    BIT STRING (2 bit) 01
SEQUENCE (2 elem)
  OBJECT IDENTIFIER 2.5.29.37 extKeyUsage (X.509 extension)
  OCTET STRING (12 byte) 300A06082B06010505070304
    SEQUENCE (1 elem)
      OBJECT IDENTIFIER 1.3.6.1.5.5.7.3.4 emailProtection (PKIX key purpose)
SEQUENCE (2 elem)
  OBJECT IDENTIFIER 2.5.29.17 subjectAltName (X.509 extension)
  OCTET STRING (204 byte) 3081C98110656D61696C407072756562612E636F6DA481B43081B131193017060A2B0…
    SEQUENCE (2 elem)
      [1] (16 byte) email@prueba.com
      [4] (1 elem)
        SEQUENCE (7 elem)
```

```
                    SET (1 elem)
                      SEQUENCE (2 elem)
                        OBJECT IDENTIFIER 1.3.6.1.4.1.26852.2.12
                        UTF8String 12345678Z
                    SET (1 elem)
                      SEQUENCE (2 elem)
                        OBJECT IDENTIFIER 1.3.6.1.4.1.26852.2.11
                        UTF8String Apellido2
                    SET (1 elem)
                      SEQUENCE (2 elem)
                        OBJECT IDENTIFIER 1.3.6.1.4.1.26852.2.10
                        UTF8String Apellido1
                    SET (1 elem)
                      SEQUENCE (2 elem)
                        OBJECT IDENTIFIER 1.3.6.1.4.1.26852.2.9
                        UTF8String Nombre
                    SET (1 elem)
                      SEQUENCE (2 elem)
                        OBJECT IDENTIFIER 1.3.6.1.4.1.26852.2.3
                        UTF8String 00003
                    SET (1 elem)
                      SEQUENCE (2 elem)
                        OBJECT IDENTIFIER 1.3.6.1.4.1.26852.2.2
                        UTF8String Colegio
                    SET (1 elem)
                      SEQUENCE (2 elem)
                        OBJECT IDENTIFIER 1.3.6.1.4.1.26852.2.1
                        UTF8String 000035
  SEQUENCE (2 elem)
    OBJECT IDENTIFIER 1.2.840.113549.1.1.13 sha512WithRSAEncryption (PKCS #1)
    NULL
```

4.3 Para CIFRADO

```
SEQUENCE (3 elem)
  SEQUENCE (8 elem)
    [0] (1 elem)
      INTEGER 2
    INTEGER (63 bit) 8895758807097320788
    SEQUENCE (2 elem)
      OBJECT IDENTIFIER 1.2.840.113549.1.1.13 sha512WithRSAEncryption (PKCS #1)
      NULL
    SEQUENCE (7 elem)
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.6 countryName (X.520 DN component)
          PrintableString ES
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.8 stateOrProvinceName (X.520 DN component)
          UTF8String MADRID
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.7 localityName (X.520 DN component)
          UTF8String MADRID
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.97
          UTF8String VATES-Q2866017C
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.11 organizationalUnitName (X.520 DN component)
```

```
        UTF8String ENTIDAD DE CERTIFICACION
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.10 organizationName (X.520 DN component)
        UTF8String CONSEJO GENERAL DE COLEGIOS OFICIALES DE MEDICOS
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.3 commonName (X.520 DN component)
        UTF8String CGCOM QUALIFIED 2020
  SEQUENCE (2 elem)
    UTCTime 2020-03-02 12:21:10 UTC
    UTCTime 2023-03-02 12:21:10 UTC
  SEQUENCE (10 elem)
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.3 commonName (X.520 DN component)
        UTF8String apellido1 apellido2 nombre - DNI 12345678Z (CIFRADO)
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.5 serialNumber (X.520 DN component)
        PrintableString IDCES-12345678Z
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.42 givenName (X.520 DN component)
        UTF8String Nombre
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.4 surname (X.520 DN component)
        UTF8String apellido1 apellido2
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.12 title (X.520 DN component)
```

```
        UTF8String MEDICO COLEGIADO
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.11 organizationalUnitName (X.520 DN component)
        UTF8String UnidadOrganizativa
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.11 organizationalUnitName (X.520 DN component)
        UTF8String CARNET COLEGIAL
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.97
        UTF8String VATES-Q0000001
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.10 organizationName (X.520 DN component)
        UTF8String NombreColegio
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.6 countryName (X.520 DN component)
        PrintableString ES
  SEQUENCE (2 elem)
    SEQUENCE (2 elem)
      OBJECT IDENTIFIER 1.2.840.113549.1.1.1 rsaEncryption (PKCS #1)
      NULL
    BIT STRING (2160 bit) 001100001000001000000001000010100000001010000010000000010000000100000…
      SEQUENCE (2 elem)
        INTEGER (2048 bit) 288436562537003701336910653105228336529336082444105942572886805699351…
        INTEGER 65537
  [3] (1 elem)
    SEQUENCE (9 elem)
      SEQUENCE (2 elem)
```

```
    OBJECT IDENTIFIER 1.3.6.1.5.5.7.1.1 authorityInfoAccess (PKIX private extension)
    OCTET STRING (99 byte) 3061303606082B06010505073002862A687474703A2F2F7073632E6367636F6D2E6573…
      SEQUENCE (2 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 1.3.6.1.5.5.7.48.2 caIssuers (PKIX subject/authority info access descriptor)
          [6] (42 byte) http://psc.cgcom.es/CA/root_cgcom_2020.crt
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 1.3.6.1.5.5.7.48.1 ocsp (PKIX)
          [6] (27 byte) http://ocspservice.cgcom.es
  SEQUENCE (2 elem)
    OBJECT IDENTIFIER 2.5.29.14 subjectKeyIdentifier (X.509 extension)
    OCTET STRING (20 byte) CC4A57CDA7DA20C4CCDA4781F124946C0E45C73F
      OCTET STRING (20 byte) CC4A57CDA7DA20C4CCDA4781F124946C0E45C73F
  SEQUENCE (3 elem)
    OBJECT IDENTIFIER 2.5.29.19 basicConstraints (X.509 extension)
    BOOLEAN true
    OCTET STRING (2 byte) 3000
      SEQUENCE (0 elem)
  SEQUENCE (2 elem)
    OBJECT IDENTIFIER 2.5.29.35 authorityKeyIdentifier (X.509 extension)
    OCTET STRING (24 byte) 3016801432416494D42D413ACDEB2B7209EBAB8D883AD1CF
      SEQUENCE (1 elem)
        [0] (20 byte) 32416494D42D413ACDEB2B7209EBAB8D883AD1CF
  SEQUENCE (2 elem)
    OBJECT IDENTIFIER 2.5.29.32 certificatePolicies (X.509 extension)
    OCTET STRING (139 byte) 308188308185060C2B0601040181D16401010103307530240608 2B060105050702011…
      SEQUENCE (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 1.3.6.1.4.1.26852.1.1.1.3
          SEQUENCE (2 elem)
            SEQUENCE (2 elem)
              OBJECT IDENTIFIER 1.3.6.1.5.5.7.2.1 cps (PKIX policy qualifier)
```

```
                IA5String https://psc.cgcom.es/dpc
              SEQUENCE (2 elem)
                OBJECT IDENTIFIER 1.3.6.1.5.5.7.2.2 unotice (PKIX policy qualifier)
                SEQUENCE (1 elem)
                  UTF8String "CERTIFICADO PARA EL CIFRADO DE MEDICO COLEGIADO, EN TARJETA”
SEQUENCE (2 elem)
  OBJECT IDENTIFIER 2.5.29.31 cRLDistributionPoints (X.509 extension)
  OCTET STRING (90 byte) 3058302AA028A0268624687474703A2F2F63726C352E6367636F6D2E65732F63726C2F…
    SEQUENCE (2 elem)
      SEQUENCE (1 elem)
        [0] (1 elem)
          [0] (1 elem)
            [6] (36 byte) http://crl5.cgcom.es/crl/eccgcom.crl
      SEQUENCE (1 elem)
        [0] (1 elem)
          [0] (1 elem)
            [6] (36 byte) http://crl6.cgcom.es/crl/eccgcom.crl
SEQUENCE (3 elem)
  OBJECT IDENTIFIER 2.5.29.15 keyUsage (X.509 extension)
  BOOLEAN true
  OCTET STRING (4 byte) 03020520
    BIT STRING (3 bit) 001
SEQUENCE (2 elem)
  OBJECT IDENTIFIER 2.5.29.37 extKeyUsage (X.509 extension)
  OCTET STRING (12 byte) 300A06082B06010505070304
    SEQUENCE (1 elem)
      OBJECT IDENTIFIER 1.3.6.1.5.5.7.3.4 emailProtection (PKIX key purpose)
SEQUENCE (2 elem)
  OBJECT IDENTIFIER 2.5.29.17 subjectAltName (X.509 extension)
  OCTET STRING (204 byte) 3081C98110656D61696C407072756562612E636F6DA481B43081B131193017060A2B0…
    SEQUENCE (2 elem)
      [1] (16 byte) email@prueba.com
```

```
            [4] (1 elem)
              SEQUENCE (7 elem)
                SET (1 elem)
                  SEQUENCE (2 elem)
                    OBJECT IDENTIFIER 1.3.6.1.4.1.26852.2.12
                    UTF8String 12345678Z
                SET (1 elem)
                  SEQUENCE (2 elem)
                    OBJECT IDENTIFIER 1.3.6.1.4.1.26852.2.11
                    UTF8String Apellido2
                SET (1 elem)
                  SEQUENCE (2 elem)
                    OBJECT IDENTIFIER 1.3.6.1.4.1.26852.2.10
                    UTF8String Apellido1
                SET (1 elem)
                  SEQUENCE (2 elem)
                    OBJECT IDENTIFIER 1.3.6.1.4.1.26852.2.9
                    UTF8String Nombre
                SET (1 elem)
                  SEQUENCE (2 elem)
                    OBJECT IDENTIFIER 1.3.6.1.4.1.26852.2.3
                    UTF8String 00003
                SET (1 elem)
                  SEQUENCE (2 elem)
                    OBJECT IDENTIFIER 1.3.6.1.4.1.26852.2.2
                    UTF8String Colegio
                SET (1 elem)
                  SEQUENCE (2 elem)
                    OBJECT IDENTIFIER 1.3.6.1.4.1.26852.2.1
                    UTF8String 000035
SEQUENCE (2 elem)
  OBJECT IDENTIFIER 1.2.840.113549.1.1.13 sha512WithRSAEncryption (PKCS #1)
```

```
    NULL
```

5. Certificado de médico colegiado en nube

```
SEQUENCE (3 elem)
  SEQUENCE (8 elem)
    [0] (1 elem)
      INTEGER 2
    INTEGER (61 bit) 1411313107723834424
    SEQUENCE (2 elem)
      OBJECT IDENTIFIER 1.2.840.113549.1.1.13 sha512WithRSAEncryption (PKCS #1)
      NULL
    SEQUENCE (7 elem)
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.6 countryName (X.520 DN component)
          PrintableString ES
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.8 stateOrProvinceName (X.520 DN component)
          UTF8String MADRID
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.7 localityName (X.520 DN component)
          UTF8String MADRID
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.97
          UTF8String VATES-Q2866017C
      SET (1 elem)
        SEQUENCE (2 elem)
```

```
        OBJECT IDENTIFIER 2.5.4.11 organizationalUnitName (X.520 DN component)
        UTF8String ENTIDAD DE CERTIFICACION
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.10 organizationName (X.520 DN component)
        UTF8String CONSEJO GENERAL DE COLEGIOS OFICIALES DE MEDICOS
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.3 commonName (X.520 DN component)
        UTF8String CGCOM QUALIFIED 2020
  SEQUENCE (2 elem)
    UTCTime 2020-03-02 12:16:37 UTC
    UTCTime 2023-03-02 12:16:37 UTC
  SEQUENCE (10 elem)
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.3 commonName (X.520 DN component)
        UTF8String apellido1 apellido2 nombre - DNI 12345678Z
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.5 serialNumber (X.520 DN component)
        PrintableString IDCES-12345678Z
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.42 givenName (X.520 DN component)
        UTF8String Nombre
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.4 surname (X.520 DN component)
        UTF8String apellido1 apellido2
    SET (1 elem)
      SEQUENCE (2 elem)
```

```
        OBJECT IDENTIFIER 2.5.4.12 title (X.520 DN component)
        UTF8String MEDICO COLEGIADO
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.11 organizationalUnitName (X.520 DN component)
        UTF8String UnidadOrganizativa
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.11 organizationalUnitName (X.520 DN component)
        UTF8String CARNET COLEGIAL
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.97
        UTF8String VATES-Q0000001
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.10 organizationName (X.520 DN component)
        UTF8String NombreColegio
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.6 countryName (X.520 DN component)
        PrintableString ES
  SEQUENCE (2 elem)
    SEQUENCE (2 elem)
      OBJECT IDENTIFIER 1.2.840.113549.1.1.1 rsaEncryption (PKCS #1)
      NULL
    BIT STRING (2160 bit) 001100001000001000000001000010100000001010000010000000010000000100000…
      SEQUENCE (2 elem)
        INTEGER (2048 bit) 22826313063253572353223859965849368490221088448007288903783895236705 0…
        INTEGER 65537
  [3] (1 elem)
    SEQUENCE (10 elem)
```

```
SEQUENCE (2 elem)
  OBJECT IDENTIFIER 1.3.6.1.5.5.7.1.1 authorityInfoAccess (PKIX private extension)
  OCTET STRING (99 byte) 3061303606082B06010505073002862A687474703A2F2F7073632E6367636F6D2E6573…
    SEQUENCE (2 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 1.3.6.1.5.5.7.48.2 caIssuers (PKIX subject/authority info access descriptor)
        [6] (42 byte) http://psc.cgcom.es/CA/root_cgcom_2020.crt
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 1.3.6.1.5.5.7.48.1 ocsp (PKIX)
        [6] (27 byte) http://ocspservice.cgcom.es
SEQUENCE (2 elem)
  OBJECT IDENTIFIER 2.5.29.14 subjectKeyIdentifier (X.509 extension)
  OCTET STRING (20 byte) 233A6E64A1EC06A7AB9F889CAF6D23E5E1BB96EB
    OCTET STRING (20 byte) 233A6E64A1EC06A7AB9F889CAF6D23E5E1BB96EB
SEQUENCE (3 elem)
  OBJECT IDENTIFIER 2.5.29.19 basicConstraints (X.509 extension)
  BOOLEAN true
  OCTET STRING (2 byte) 3000
    SEQUENCE (0 elem)
SEQUENCE (2 elem)
  OBJECT IDENTIFIER 2.5.29.35 authorityKeyIdentifier (X.509 extension)
  OCTET STRING (24 byte) 3016801432416494D42D413ACDEB2B7209EBAB8D883AD1CF
    SEQUENCE (1 elem)
      [0] (20 byte) 32416494D42D413ACDEB2B7209EBAB8D883AD1CF
SEQUENCE (2 elem)
  OBJECT IDENTIFIER 1.3.6.1.5.5.7.1.3 qcStatements (PKIX private extension)
  OCTET STRING (159 byte) 30819C301506082B06010505070B023009060704008BEC4901013008060604008E460…
    SEQUENCE (6 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 1.3.6.1.5.5.7.11.2
        SEQUENCE (1 elem)
          OBJECT IDENTIFIER 0.4.0.194121.1.1
```

```
            SEQUENCE (1 elem)
              OBJECT IDENTIFIER 0.4.0.1862.1.1 etsiQcsCompliance (ETSI TS 101 862 qualified certificates)
            SEQUENCE (2 elem)
              OBJECT IDENTIFIER 0.4.0.1862.1.3 etsiQcsRetentionPeriod (ETSI TS 101 862 qualified certificates)
              INTEGER 15
            SEQUENCE (1 elem)
              OBJECT IDENTIFIER 0.4.0.1862.1.4 etsiQcsQcSSCD (ETSI TS 101 862 qualified certificates)
            SEQUENCE (2 elem)
              OBJECT IDENTIFIER 0.4.0.1862.1.6
              SEQUENCE (1 elem)
                OBJECT IDENTIFIER 0.4.0.1862.1.6.1
            SEQUENCE (2 elem)
              OBJECT IDENTIFIER 0.4.0.1862.1.5
              SEQUENCE (2 elem)
                SEQUENCE (2 elem)
                  IA5String https://psc.cgcom.es/en/pds
                  PrintableString en
                SEQUENCE (2 elem)
                  IA5String https://psc.cgcom.es/pds
                  PrintableString es
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.29.32 certificatePolicies (X.509 extension)
          OCTET STRING (142 byte) 30818B307E060C2B0601040181D16401010104306E302406082B06010505070201161…
            SEQUENCE (2 elem)
              SEQUENCE (2 elem)
                OBJECT IDENTIFIER 1.3.6.1.4.1.26852.1.1.1.4
                SEQUENCE (2 elem)
                  SEQUENCE (2 elem)
                    OBJECT IDENTIFIER 1.3.6.1.5.5.7.2.1 cps (PKIX policy qualifier)
                    IA5String https://psc.cgcom.es/dpc
                  SEQUENCE (2 elem)
                    OBJECT IDENTIFIER 1.3.6.1.5.5.7.2.2 unotice (PKIX policy qualifier)
```

```
                SEQUENCE (1 elem)
                  UTF8String "CERTIFICADO CUALIFICADO DE MEDICO COLEGIADO, EN NUBE”
          SEQUENCE (1 elem)
            OBJECT IDENTIFIER 0.4.0.194112.1.2
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.29.31 cRLDistributionPoints (X.509 extension)
        OCTET STRING (90 byte) 3058302AA028A0268624687474703A2F2F63726C352E6367636F6D2E65732F63726C2F…
          SEQUENCE (2 elem)
            SEQUENCE (1 elem)
              [0] (1 elem)
                [0] (1 elem)
                  [6] (36 byte) http://crl5.cgcom.es/crl/eccgcom.crl
            SEQUENCE (1 elem)
              [0] (1 elem)
                [0] (1 elem)
                  [6] (36 byte) http://crl6.cgcom.es/crl/eccgcom.crl
      SEQUENCE (3 elem)
        OBJECT IDENTIFIER 2.5.29.15 keyUsage (X.509 extension)
        BOOLEAN true
        OCTET STRING (4 byte) 030206C0
          BIT STRING (2 bit) 11
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.29.37 extKeyUsage (X.509 extension)
        OCTET STRING (22 byte) 301406082B06010505070302060 82B06010505070304
          SEQUENCE (2 elem)
            OBJECT IDENTIFIER 1.3.6.1.5.5.7.3.2 clientAuth (PKIX key purpose)
            OBJECT IDENTIFIER 1.3.6.1.5.5.7.3.4 emailProtection (PKIX key purpose)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.29.17 subjectAltName (X.509 extension)
        OCTET STRING (204 byte) 3081C98110656D61696C407072756562612E636F6DA481B43081B131193017060A2B0…
          SEQUENCE (2 elem)
            [1] (16 byte) email@prueba.com
```

```
            [4] (1 elem)
              SEQUENCE (7 elem)
                SET (1 elem)
                  SEQUENCE (2 elem)
                    OBJECT IDENTIFIER 1.3.6.1.4.1.26852.2.12
                    UTF8String 12345678Z
                SET (1 elem)
                  SEQUENCE (2 elem)
                    OBJECT IDENTIFIER 1.3.6.1.4.1.26852.2.11
                    UTF8String Apellido2
                SET (1 elem)
                  SEQUENCE (2 elem)
                    OBJECT IDENTIFIER 1.3.6.1.4.1.26852.2.10
                    UTF8String Apellido1
                SET (1 elem)
                  SEQUENCE (2 elem)
                    OBJECT IDENTIFIER 1.3.6.1.4.1.26852.2.9
                    UTF8String Nombre
                SET (1 elem)
                  SEQUENCE (2 elem)
                    OBJECT IDENTIFIER 1.3.6.1.4.1.26852.2.3
                    UTF8String 00003
                SET (1 elem)
                  SEQUENCE (2 elem)
                    OBJECT IDENTIFIER 1.3.6.1.4.1.26852.2.2
                    UTF8String Colegio
                SET (1 elem)
                  SEQUENCE (2 elem)
                    OBJECT IDENTIFIER 1.3.6.1.4.1.26852.2.1
                    UTF8String 000035
SEQUENCE (2 elem)
  OBJECT IDENTIFIER 1.2.840.113549.1.1.13 sha512WithRSAEncryption (PKCS #1)
```

```
NULL
```

6. Certificados de médico colegiado en software

```
SEQUENCE (3 elem)
  SEQUENCE (8 elem)
    [0] (1 elem)
      INTEGER 2
    INTEGER (154 bit) 159475157514205723859285497368694383082765828 49
    SEQUENCE (2 elem)
      OBJECT IDENTIFIER 1.2.840.113549.1.1.13 sha512WithRSAEncryption (PKCS #1)
      NULL
    SEQUENCE (7 elem)
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.6 countryName (X.520 DN component)
          PrintableString ES
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.8 stateOrProvinceName (X.520 DN component)
          UTF8String MADRID
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.7 localityName (X.520 DN component)
          UTF8String MADRID
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.97 organizationIdentifier (X.520 DN component)
          UTF8String VATES-Q2866017C
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.11 organizationalUnitName (X.520 DN component)
          UTF8String ENTIDAD DE CERTIFICACION
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.10 organizationName (X.520 DN component)
          UTF8String CONSEJO GENERAL DE COLEGIOS OFICIALES DE MEDICOS
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.3 commonName (X.520 DN component)
          UTF8String CGCOM QUALIFIED 2020
```

```
    SEQUENCE (2 elem)
      UTCTime 2022-03-24 11:00:00 UTC
      UTCTime 2023-03-24 11:00:00 UTC
    SEQUENCE (10 elem)
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.3 commonName (X.520 DN component)
          UTF8String APELLIDOUNO APELLIDODOS NOMBRE - 123456789Z
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.5 serialNumber (X.520 DN component)
          PrintableString IDCES-123456789Z
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.42 givenName (X.520 DN component)
          UTF8String NOMBRE
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.4 surname (X.520 DN component)
          UTF8String APELLIDOUNO APELLIDODOS
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.12 title (X.520 DN component)
          UTF8String MEDICO COLEGIADO/A
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.11 organizationalUnitName (X.520 DN component)
          UTF8String CARNET COLEGIAL
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.11 organizationalUnitName (X.520 DN component)
          UTF8String AREA DE TEST
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.97 organizationIdentifier (X.520 DN component)
          UTF8String VATES-Q0000000J
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.10 organizationName (X.520 DN component)
          UTF8String COLEGIO DE MEDICOS DE TEST
      SET (1 elem)
        SEQUENCE (2 elem)
```

```
        OBJECT IDENTIFIER 2.5.4.6 countryName (X.520 DN component)
        PrintableString ES
    SEQUENCE (2 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 1.2.840.113549.1.1.1 rsaEncryption (PKCS #1)
        NULL
      BIT STRING (2160 bit) 001100001000001000000001000010100000001010000010000000010000000100000…
        SEQUENCE (2 elem)
          INTEGER (2048 bit) 23800679027686441579100251841629806108295289574934568212183107345803 4…
          INTEGER 65537
    [3] (1 elem)
      SEQUENCE (11 elem)
        SEQUENCE (3 elem)
          OBJECT IDENTIFIER 2.5.29.19 basicConstraints (X.509 extension)
          BOOLEAN true
          OCTET STRING (2 byte) 3000
            SEQUENCE (0 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.29.35 authorityKeyIdentifier (X.509 extension)
          OCTET STRING (24 byte) 3016801432416494D42D413ACDEB2B7209EBAB8D883AD1CF
            SEQUENCE (1 elem)
              [0] (20 byte) 32416494D42D413ACDEB2B7209EBAB8D883AD1CF
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 1.3.6.1.5.5.7.1.1 authorityInfoAccess (PKIX private extension)
          OCTET STRING (99 byte) 3061303606082B06010505073002862A687474703A2F2F7073632E6367636F6D2E6573…
            SEQUENCE (2 elem)
              SEQUENCE (2 elem)
                OBJECT IDENTIFIER 1.3.6.1.5.5.7.48.2 caIssuers (PKIX subject/authority info access descriptor)
                [6] (42 byte) http://psc.cgcom.es/CA/root_cgcom_2020.crt
              SEQUENCE (2 elem)
                OBJECT IDENTIFIER 1.3.6.1.5.5.7.48.1 ocsp (PKIX)
                [6] (27 byte) http://ocspservice.cgcom.es
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.29.18 issuerAltName (X.509 extension)
          OCTET STRING (22 byte) 30148112696E666F4076696E63617369676E2E6E6574
            SEQUENCE (1 elem)
              [1] (18 byte) info@vincasign.net
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.29.17 subjectAltName (X.509 extension)
          OCTET STRING (257 byte) 3081FE811A6E6F6D6272652E6170756E6F6170646F73406367636F6D2E6573A481DF3…
            SEQUENCE (2 elem)
              [1] (26 byte) nombre.apunoapdos@cgcom.es
```

```
            [4] (1 elem)
              SEQUENCE (7 elem)
                SET (1 elem)
                  SEQUENCE (2 elem)
                    OBJECT IDENTIFIER 1.3.6.1.4.1.26852.2.1
                    UTF8String IDCOLEGIOTEST
                SET (1 elem)
                  SEQUENCE (2 elem)
                    OBJECT IDENTIFIER 1.3.6.1.4.1.26852.2.2
                    UTF8String COLEGIO DE MEDICOS DE TEST
                SET (1 elem)
                  SEQUENCE (2 elem)
                    OBJECT IDENTIFIER 1.3.6.1.4.1.26852.2.3
                    UTF8String IDCOLEGIADO
                SET (1 elem)
                  SEQUENCE (2 elem)
                    OBJECT IDENTIFIER 1.3.6.1.4.1.26852.2.9
                    UTF8String NOMBRE
                SET (1 elem)
                  SEQUENCE (2 elem)
                    OBJECT IDENTIFIER 1.3.6.1.4.1.26852.2.10
                    UTF8String APELLIDOUNO
                SET (1 elem)
                  SEQUENCE (2 elem)
                    OBJECT IDENTIFIER 1.3.6.1.4.1.26852.2.11
                    UTF8String APELLIDODOS
                SET (1 elem)
                  SEQUENCE (2 elem)
                    OBJECT IDENTIFIER 1.3.6.1.4.1.26852.2.12
                    UTF8String IDCES-123456789Z
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.29.32 certificatePolicies (X.509 extension)
          OCTET STRING (142 byte) 30818B307E060C2B0601040181D16401010105306E304606082B06010505070202303…
            SEQUENCE (2 elem)
              SEQUENCE (2 elem)
                OBJECT IDENTIFIER 1.3.6.1.4.1.26852.1.1.1.5
                SEQUENCE (2 elem)
                  SEQUENCE (2 elem)
                    OBJECT IDENTIFIER 1.3.6.1.5.5.7.2.2 unotice (PKIX policy qualifier)
                    SEQUENCE (1 elem)
                      UTF8String CERTIFICADO CUALIFICADO DE MEDICO COLEGIADO, EN SOFTWARE
                  SEQUENCE (2 elem)
```

```
                    OBJECT IDENTIFIER 1.3.6.1.5.5.7.2.1 cps (PKIX policy qualifier)
                    IA5String https://psc.cgcom.es/dpc
                SEQUENCE (1 elem)
                  OBJECT IDENTIFIER 0.4.0.194112.1.0
          SEQUENCE (2 elem)
            OBJECT IDENTIFIER 2.5.29.37 extKeyUsage (X.509 extension)
            OCTET STRING (22 byte) 301406082B06010505070302060 82B06010505070304
              SEQUENCE (2 elem)
                OBJECT IDENTIFIER 1.3.6.1.5.5.7.3.2 clientAuth (PKIX key purpose)
                OBJECT IDENTIFIER 1.3.6.1.5.5.7.3.4 emailProtection (PKIX key purpose)
          SEQUENCE (2 elem)
            OBJECT IDENTIFIER 1.3.6.1.5.5.7.1.3 qcStatements (PKIX private extension)
            OCTET STRING (35 byte) 3021301506082B06010505070B023009060704008BEC490101300806060 4008E460101
              SEQUENCE (2 elem)
                SEQUENCE (2 elem)
                  OBJECT IDENTIFIER 1.3.6.1.5.5.7.11.2 pkixQCSyntax-v2 (PKIX qualified certificates)
                  SEQUENCE (1 elem)
                    OBJECT IDENTIFIER 0.4.0.194121.1.1
                SEQUENCE (1 elem)
                  OBJECT IDENTIFIER 0.4.0.1862.1.1 etsiQcsCompliance (ETSI TS 101 862 qualified certificates)
          SEQUENCE (2 elem)
            OBJECT IDENTIFIER 2.5.29.31 cRLDistributionPoints (X.509 extension)
            OCTET STRING (90 byte) 3058302AA028A0268624687474703A2F2F63726C352E6367636F6D2E65732F63726C2F…
              SEQUENCE (2 elem)
                SEQUENCE (1 elem)
                  [0] (1 elem)
                    [0] (1 elem)
                      [6] (36 byte) http://crl5.cgcom.es/crl/eccgcom.crl
                SEQUENCE (1 elem)
                  [0] (1 elem)
                    [0] (1 elem)
                      [6] (36 byte) http://crl6.cgcom.es/crl/eccgcom.crl
          SEQUENCE (2 elem)
Offset: 1668
Length: 2+29
(constructed)
Value:
(2 elem)
            OBJECT IDENTIFIER 2.5.29.14 subjectKeyIdentifier (X.509 extension)
            OCTET STRING (22 byte) 04147C710DEBE62F8903DC0D82C4D9825AECB60AEF42
              OCTET STRING (20 byte) 7C710DEBE62F8903DC0D82C4D9825AECB60AEF42
          SEQUENCE (3 elem)
```

```
          OBJECT IDENTIFIER 2.5.29.15 keyUsage (X.509 extension)
          BOOLEAN true
          OCTET STRING (4 byte) 030206C0
            BIT STRING (2 bit) 11
  SEQUENCE (2 elem)
    OBJECT IDENTIFIER 1.2.840.113549.1.1.13 sha512WithRSAEncryption (PKCS #1)
    NULL
```

7. Certificados de Persona Física Vinculada, en tarjeta

7.1 Para Autenticación

```
SEQUENCE (3 elem)
  SEQUENCE (8 elem)
    [0] (1 elem)
      INTEGER 2
    INTEGER (60 bit) 955751553115066418
    SEQUENCE (2 elem)
      OBJECT IDENTIFIER 1.2.840.113549.1.1.13 sha512WithRSAEncryption (PKCS #1)
      NULL
    SEQUENCE (7 elem)
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.6 countryName (X.520 DN component)
          PrintableString ES
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.8 stateOrProvinceName (X.520 DN component)
          UTF8String MADRID
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.7 localityName (X.520 DN component)
          UTF8String MADRID
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.97
```

```
        UTF8String VATES-Q2866017C
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.11 organizationalUnitName (X.520 DN component)
        UTF8String ENTIDAD DE CERTIFICACION
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.10 organizationName (X.520 DN component)
        UTF8String CONSEJO GENERAL DE COLEGIOS OFICIALES DE MEDICOS
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.3 commonName (X.520 DN component)
        UTF8String CGCOM QUALIFIED 2020
  SEQUENCE (2 elem)
    UTCTime 2020-03-02 13:10:31 UTC
    UTCTime 2023-03-02 13:10:31 UTC
  SEQUENCE (10 elem)
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.3 commonName (X.520 DN component)
        UTF8String apellido1 apellido2 nombre - DNI 12345678Z (AUTENTICACIÓN)
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.5 serialNumber (X.520 DN component)
        PrintableString IDCES-12345678Z
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.42 givenName (X.520 DN component)
        UTF8String Nombre
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.4 surname (X.520 DN component)
```

```
        UTF8String apellido1 apellido2
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.12 title (X.520 DN component)
        UTF8String PERSONA FÍSICA VINCULADA
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.11 organizationalUnitName (X.520 DN component)
        UTF8String UnidadOrganizativa
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.11 organizationalUnitName (X.520 DN component)
        UTF8String UnidadOrganizativa2
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.97
        UTF8String VATES-Q0000001
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.10 organizationName (X.520 DN component)
        UTF8String NombreColegio
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.6 countryName (X.520 DN component)
        PrintableString ES
  SEQUENCE (2 elem)
    SEQUENCE (2 elem)
      OBJECT IDENTIFIER 1.2.840.113549.1.1.1 rsaEncryption (PKCS #1)
      NULL
    BIT STRING (2160 bit) 001100001000001000000001000010100000001010000010000000010000000100000…
      SEQUENCE (2 elem)
        INTEGER (2048 bit) 21567765760763313271045222223168088154688948259161037039949386093547 1…
```

```
        INTEGER 65537
    [3] (1 elem)
      SEQUENCE (9 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 1.3.6.1.5.5.7.1.1 authorityInfoAccess (PKIX private extension)
          OCTET STRING (99 byte) 3061303606082B06010505073002862A687474703A2F2F7073632E6367636F6D2E6573…
            SEQUENCE (2 elem)
              SEQUENCE (2 elem)
                OBJECT IDENTIFIER 1.3.6.1.5.5.7.48.2 caIssuers (PKIX subject/authority info access descriptor)
                [6] (42 byte) http://psc.cgcom.es/CA/root_cgcom_2020.crt
              SEQUENCE (2 elem)
                OBJECT IDENTIFIER 1.3.6.1.5.5.7.48.1 ocsp (PKIX)
                [6] (27 byte) http://ocspservice.cgcom.es
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.29.14 subjectKeyIdentifier (X.509 extension)
          OCTET STRING (20 byte) 563C8FFA71B36EACFB738651C3AF0431FB0A7825
            OCTET STRING (20 byte) 563C8FFA71B36EACFB738651C3AF0431FB0A7825
        SEQUENCE (3 elem)
          OBJECT IDENTIFIER 2.5.29.19 basicConstraints (X.509 extension)
          BOOLEAN true
          OCTET STRING (2 byte) 3000
            SEQUENCE (0 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.29.35 authorityKeyIdentifier (X.509 extension)
          OCTET STRING (24 byte) 3016801432416494D42D413ACDEB2B7209EBAB8D883AD1CF
            SEQUENCE (1 elem)
              [0] (20 byte) 32416494D42D413ACDEB2B7209EBAB8D883AD1CF
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.29.32 certificatePolicies (X.509 extension)
          OCTET STRING (168 byte) 3081A5308198060C2B0601040181D164010102013081873024060 82B0601050507020…
            SEQUENCE (2 elem)
              SEQUENCE (2 elem)
```

```
            OBJECT IDENTIFIER 1.3.6.1.4.1.26852.1.1.2.1
            SEQUENCE (2 elem)
              SEQUENCE (2 elem)
                OBJECT IDENTIFIER 1.3.6.1.5.5.7.2.1 cps (PKIX policy qualifier)
                IA5String https://psc.cgcom.es/dpc
              SEQUENCE (2 elem)
                OBJECT IDENTIFIER 1.3.6.1.5.5.7.2.2 unotice (PKIX policy qualifier)
                SEQUENCE (1 elem)
                  UTF8String "CERTIFICADO PARA LA IDENTIFICACION DE PERSONA FíSICA VINCULADA, EN TARJETA"
          SEQUENCE (1 elem)
            OBJECT IDENTIFIER 0.4.0.2042.1.2
    SEQUENCE (2 elem)
      OBJECT IDENTIFIER 2.5.29.31 cRLDistributionPoints (X.509 extension)
      OCTET STRING (90 byte) 3058302AA028A0268624687474703A2F2F63726C352E6367636F6D2E65732F63726C2F…
        SEQUENCE (2 elem)
          SEQUENCE (1 elem)
            [0] (1 elem)
              [0] (1 elem)
                [6] (36 byte) http://crl5.cgcom.es/crl/eccgcom.crl
          SEQUENCE (1 elem)
            [0] (1 elem)
              [0] (1 elem)
                [6] (36 byte) http://crl6.cgcom.es/crl/eccgcom.crl
    SEQUENCE (3 elem)
      OBJECT IDENTIFIER 2.5.29.15 keyUsage (X.509 extension)
      BOOLEAN true
      OCTET STRING (4 byte) 03020780
        BIT STRING (1 bit) 1
    SEQUENCE (2 elem)
      OBJECT IDENTIFIER 2.5.29.37 extKeyUsage (X.509 extension)
      OCTET STRING (12 byte) 300A06082B06010505070302
        SEQUENCE (1 elem)
```

```
          OBJECT IDENTIFIER 1.3.6.1.5.5.7.3.2 clientAuth (PKIX key purpose)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.29.17 subjectAltName (X.509 extension)
        OCTET STRING (210 byte) 3081CF8110656D61696C407072756562612E636F6DA481BA3081B7311F301D060A2B0…
          SEQUENCE (2 elem)
            [1] (16 byte) email@prueba.com
            [4] (1 elem)
              SEQUENCE (7 elem)
                SET (1 elem)
                  SEQUENCE (2 elem)
                    OBJECT IDENTIFIER 1.3.6.1.4.1.26852.2.12
                    UTF8String IDCES-12345678Z
                SET (1 elem)
                  SEQUENCE (2 elem)
                    OBJECT IDENTIFIER 1.3.6.1.4.1.26852.2.11
                    UTF8String Apellido2
                SET (1 elem)
                  SEQUENCE (2 elem)
                    OBJECT IDENTIFIER 1.3.6.1.4.1.26852.2.10
                    UTF8String Apellido1
                SET (1 elem)
                  SEQUENCE (2 elem)
                    OBJECT IDENTIFIER 1.3.6.1.4.1.26852.2.9
                    UTF8String Nombre
                SET (1 elem)
                  SEQUENCE (2 elem)
                    OBJECT IDENTIFIER 1.3.6.1.4.1.26852.2.3
                    UTF8String 00003
                SET (1 elem)
                  SEQUENCE (2 elem)
                    OBJECT IDENTIFIER 1.3.6.1.4.1.26852.2.2
                    UTF8String Colegio
```

```
                  SET (1 elem)
                    SEQUENCE (2 elem)
                      OBJECT IDENTIFIER 1.3.6.1.4.1.26852.2.1
                      UTF8String 000035
SEQUENCE (2 elem)
  OBJECT IDENTIFIER 1.2.840.113549.1.1.13 sha512WithRSAEncryption (PKCS #1)
  NULL
```

7.2 Para Firma

```
SEQUENCE (3 elem)
  SEQUENCE (8 elem)
    [0] (1 elem)
      INTEGER 2
    INTEGER (61 bit) 1542030852797787607
    SEQUENCE (2 elem)
      OBJECT IDENTIFIER 1.2.840.113549.1.1.13 sha512WithRSAEncryption (PKCS #1)
      NULL
    SEQUENCE (7 elem)
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.6 countryName (X.520 DN component)
          PrintableString ES
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.8 stateOrProvinceName (X.520 DN component)
          UTF8String MADRID
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.7 localityName (X.520 DN component)
          UTF8String MADRID
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.97
          UTF8String VATES-Q2866017C
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.11 organizationalUnitName (X.520 DN component)
```

```
        UTF8String ENTIDAD DE CERTIFICACION
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.10 organizationName (X.520 DN component)
        UTF8String CONSEJO GENERAL DE COLEGIOS OFICIALES DE MEDICOS
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.3 commonName (X.520 DN component)
        UTF8String CGCOM QUALIFIED 2020
  SEQUENCE (2 elem)
    UTCTime 2020-03-02 13:41:23 UTC
    UTCTime 2023-03-02 13:41:23 UTC
  SEQUENCE (10 elem)
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.3 commonName (X.520 DN component)
        UTF8String apellido1 apellido2 nombre - DNI 12345678Z (FIRMA)
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.5 serialNumber (X.520 DN component)
        PrintableString IDCES-12345678Z
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.42 givenName (X.520 DN component)
        UTF8String Nombre
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.4 surname (X.520 DN component)
        UTF8String apellido1 apellido2
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.12 title (X.520 DN component)
```

```
        UTF8String PERSONA FÍSICA VINCULADA
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.11 organizationalUnitName (X.520 DN component)
        UTF8String UnidadOrganizativa
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.11 organizationalUnitName (X.520 DN component)
        UTF8String UnidadOrganizativa2
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.97
        UTF8String VATES-Q0000001
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.10 organizationName (X.520 DN component)
        UTF8String NombreColegio
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.6 countryName (X.520 DN component)
        PrintableString ES
  SEQUENCE (2 elem)
    SEQUENCE (2 elem)
      OBJECT IDENTIFIER 1.2.840.113549.1.1.1 rsaEncryption (PKCS #1)
      NULL
    BIT STRING (2160 bit) 001100001000001000000001000010100000001010000010000000010000000100000…
      SEQUENCE (2 elem)
        INTEGER (2048 bit) 207844092127396932719101237457026762254601651379258219381540894745349…
        INTEGER 65537
  [3] (1 elem)
    SEQUENCE (10 elem)
      SEQUENCE (2 elem)
```

```
    OBJECT IDENTIFIER 1.3.6.1.5.5.7.1.1 authorityInfoAccess (PKIX private extension)
    OCTET STRING (99 byte) 3061303606082B06010505073002862A687474703A2F2F7073632E6367636F6D2E6573…
      SEQUENCE (2 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 1.3.6.1.5.5.7.48.2 caIssuers (PKIX subject/authority info access descriptor)
          [6] (42 byte) http://psc.cgcom.es/CA/root_cgcom_2020.crt
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 1.3.6.1.5.5.7.48.1 ocsp (PKIX)
          [6] (27 byte) http://ocspservice.cgcom.es
  SEQUENCE (2 elem)
    OBJECT IDENTIFIER 2.5.29.14 subjectKeyIdentifier (X.509 extension)
    OCTET STRING (20 byte) F4663AE2F6B65BA3F3356CD8907671694A2A172F
      OCTET STRING (20 byte) F4663AE2F6B65BA3F3356CD8907671694A2A172F
  SEQUENCE (3 elem)
    OBJECT IDENTIFIER 2.5.29.19 basicConstraints (X.509 extension)
    BOOLEAN true
    OCTET STRING (2 byte) 3000
      SEQUENCE (0 elem)
  SEQUENCE (2 elem)
    OBJECT IDENTIFIER 2.5.29.35 authorityKeyIdentifier (X.509 extension)
    OCTET STRING (24 byte) 3016801432416494D42D413ACDEB2B7209EBAB8D883AD1CF
      SEQUENCE (1 elem)
        [0] (20 byte) 32416494D42D413ACDEB2B7209EBAB8D883AD1CF
  SEQUENCE (2 elem)
    OBJECT IDENTIFIER 1.3.6.1.5.5.7.1.3 qcStatements (PKIX private extension)
    OCTET STRING (179 byte) 3081B0301506082B06010505070B023009060704008BEC490101300806060400 8E460…
      SEQUENCE (6 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 1.3.6.1.5.5.7.11.2
          SEQUENCE (1 elem)
            OBJECT IDENTIFIER 0.4.0.194121.1.1
        SEQUENCE (1 elem)
```

```
            OBJECT IDENTIFIER 0.4.0.1862.1.1 etsiQcsCompliance (ETSI TS 101 862 qualified certificates)
          SEQUENCE (2 elem)
            OBJECT IDENTIFIER 0.4.0.1862.1.3 etsiQcsRetentionPeriod (ETSI TS 101 862 qualified certificates)
            INTEGER 15
          SEQUENCE (1 elem)
            OBJECT IDENTIFIER 0.4.0.1862.1.4 etsiQcsQcSSCD (ETSI TS 101 862 qualified certificates)
          SEQUENCE (2 elem)
            OBJECT IDENTIFIER 0.4.0.1862.1.6
            SEQUENCE (1 elem)
              OBJECT IDENTIFIER 0.4.0.1862.1.6.1
          SEQUENCE (2 elem)
            OBJECT IDENTIFIER 0.4.0.1862.1.5
            SEQUENCE (2 elem)
              SEQUENCE (2 elem)
                IA5String https://certificacion.cgcom.es/en/pds
                PrintableString en
              SEQUENCE (2 elem)
                IA5String https://certificacion.cgcom.es/pds
                PrintableString es
  SEQUENCE (2 elem)
    OBJECT IDENTIFIER 2.5.29.32 certificatePolicies (X.509 extension)
    OCTET STRING (154 byte) 308197308189060C2B0601040181D164010102023079302406082B060105050702011…
      SEQUENCE (2 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 1.3.6.1.4.1.26852.1.1.2.2
          SEQUENCE (2 elem)
            SEQUENCE (2 elem)
              OBJECT IDENTIFIER 1.3.6.1.5.5.7.2.1 cps (PKIX policy qualifier)
              IA5String https://psc.cgcom.es/dpc
            SEQUENCE (2 elem)
              OBJECT IDENTIFIER 1.3.6.1.5.5.7.2.2 unotice (PKIX policy qualifier)
              SEQUENCE (1 elem)
```

```
                UTF8String "CERTIFICADO PARA FIRMA DE PERSONA FíSICA VINCULADA, EN TARJETA”
        SEQUENCE (1 elem)
          OBJECT IDENTIFIER 0.4.0.194112.1.2
  SEQUENCE (2 elem)
    OBJECT IDENTIFIER 2.5.29.31 cRLDistributionPoints (X.509 extension)
    OCTET STRING (90 byte) 3058302AA028A0268624687474703A2F2F63726C352E6367636F6D2E65732F63726C2F…
      SEQUENCE (2 elem)
        SEQUENCE (1 elem)
          [0] (1 elem)
            [0] (1 elem)
              [6] (36 byte) http://crl5.cgcom.es/crl/eccgcom.crl
        SEQUENCE (1 elem)
          [0] (1 elem)
            [0] (1 elem)
              [6] (36 byte) http://crl6.cgcom.es/crl/eccgcom.crl
  SEQUENCE (3 elem)
    OBJECT IDENTIFIER 2.5.29.15 keyUsage (X.509 extension)
    BOOLEAN true
    OCTET STRING (4 byte) 03020640
      BIT STRING (2 bit) 01
  SEQUENCE (2 elem)
    OBJECT IDENTIFIER 2.5.29.37 extKeyUsage (X.509 extension)
    OCTET STRING (12 byte) 300A06082B06010505070304
      SEQUENCE (1 elem)
        OBJECT IDENTIFIER 1.3.6.1.5.5.7.3.4 emailProtection (PKIX key purpose)
  SEQUENCE (2 elem)
    OBJECT IDENTIFIER 2.5.29.17 subjectAltName (X.509 extension)
    OCTET STRING (210 byte) 3081CF8110656D61696C407072756562612E636F6DA481BA3081B7311F301D060A2B0…
      SEQUENCE (2 elem)
        [1] (16 byte) email@prueba.com
        [4] (1 elem)
          SEQUENCE (7 elem)
```

```
                    SET (1 elem)
                      SEQUENCE (2 elem)
                        OBJECT IDENTIFIER 1.3.6.1.4.1.26852.2.12
                        UTF8String IDCES-12345678Z
                    SET (1 elem)
                      SEQUENCE (2 elem)
                        OBJECT IDENTIFIER 1.3.6.1.4.1.26852.2.11
                        UTF8String Apellido2
                    SET (1 elem)
                      SEQUENCE (2 elem)
                        OBJECT IDENTIFIER 1.3.6.1.4.1.26852.2.10
                        UTF8String Apellido1
                    SET (1 elem)
                      SEQUENCE (2 elem)
                        OBJECT IDENTIFIER 1.3.6.1.4.1.26852.2.9
                        UTF8String Nombre
                    SET (1 elem)
                      SEQUENCE (2 elem)
                        OBJECT IDENTIFIER 1.3.6.1.4.1.26852.2.3
                        UTF8String 00003
                    SET (1 elem)
                      SEQUENCE (2 elem)
                        OBJECT IDENTIFIER 1.3.6.1.4.1.26852.2.2
                        UTF8String Colegio
                    SET (1 elem)
                      SEQUENCE (2 elem)
                        OBJECT IDENTIFIER 1.3.6.1.4.1.26852.2.1
                        UTF8String 000035
  SEQUENCE (2 elem)
    OBJECT IDENTIFIER 1.2.840.113549.1.1.13 sha512WithRSAEncryption (PKCS #1)
    NULL
```

7.3 Para Cifrado

```
SEQUENCE (3 elem)
  SEQUENCE (8 elem)
    [0] (1 elem)
      INTEGER 2
    INTEGER (62 bit) 3598130400063286891
    SEQUENCE (2 elem)
      OBJECT IDENTIFIER 1.2.840.113549.1.1.13 sha512WithRSAEncryption (PKCS #1)
      NULL
    SEQUENCE (7 elem)
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.6 countryName (X.520 DN component)
          PrintableString ES
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.8 stateOrProvinceName (X.520 DN component)
          UTF8String MADRID
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.7 localityName (X.520 DN component)
          UTF8String MADRID
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.97
          UTF8String VATES-Q2866017C
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.11 organizationalUnitName (X.520 DN component)
```

```
        UTF8String ENTIDAD DE CERTIFICACION
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.10 organizationName (X.520 DN component)
        UTF8String CONSEJO GENERAL DE COLEGIOS OFICIALES DE MEDICOS
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.3 commonName (X.520 DN component)
        UTF8String CGCOM QUALIFIED 2020
  SEQUENCE (2 elem)
    UTCTime 2020-03-02 13:33:20 UTC
    UTCTime 2023-03-02 13:33:20 UTC
  SEQUENCE (10 elem)
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.3 commonName (X.520 DN component)
        UTF8String apellido1 apellido2 nombre - DNI 12345678Z (CIFRADO)
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.5 serialNumber (X.520 DN component)
        PrintableString IDCES-12345678Z
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.42 givenName (X.520 DN component)
        UTF8String Nombre
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.4 surname (X.520 DN component)
        UTF8String apellido1 apellido2
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.12 title (X.520 DN component)
```

```
        UTF8String PERSONA FÍSICA VINCULADA
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.11 organizationalUnitName (X.520 DN component)
        UTF8String UnidadOrganizativa
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.11 organizationalUnitName (X.520 DN component)
        UTF8String UnidadOrganizativa2
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.97
        UTF8String VATES-Q0000001
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.10 organizationName (X.520 DN component)
        UTF8String NombreColegio
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.6 countryName (X.520 DN component)
        PrintableString ES
  SEQUENCE (2 elem)
    SEQUENCE (2 elem)
      OBJECT IDENTIFIER 1.2.840.113549.1.1.1 rsaEncryption (PKCS #1)
      NULL
    BIT STRING (2160 bit) 001100001000001000000001000010100000001010000010000000010000000100000…
      SEQUENCE (2 elem)
        INTEGER (2048 bit) 28190483423658552341968670476829566990441255504126484800161299995217 8…
        INTEGER 65537
  [3] (1 elem)
    SEQUENCE (10 elem)
      SEQUENCE (2 elem)
```

```
    OBJECT IDENTIFIER 1.3.6.1.5.5.7.1.1 authorityInfoAccess (PKIX private extension)
    OCTET STRING (99 byte) 3061303606082B06010505073002862A687474703A2F2F7073632E6367636F6D2E6573…
      SEQUENCE (2 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 1.3.6.1.5.5.7.48.2 caIssuers (PKIX subject/authority info access descriptor)
          [6] (42 byte) http://psc.cgcom.es/CA/root_cgcom_2020.crt
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 1.3.6.1.5.5.7.48.1 ocsp (PKIX)
          [6] (27 byte) http://ocspservice.cgcom.es
  SEQUENCE (2 elem)
    OBJECT IDENTIFIER 2.5.29.14 subjectKeyIdentifier (X.509 extension)
    OCTET STRING (20 byte) DB0D6FE3DFF6785C9BB1C91D9C4669A107FE669B
      OCTET STRING (20 byte) DB0D6FE3DFF6785C9BB1C91D9C4669A107FE669B
  SEQUENCE (3 elem)
    OBJECT IDENTIFIER 2.5.29.19 basicConstraints (X.509 extension)
    BOOLEAN true
    OCTET STRING (2 byte) 3000
      SEQUENCE (0 elem)
  SEQUENCE (2 elem)
    OBJECT IDENTIFIER 2.5.29.35 authorityKeyIdentifier (X.509 extension)
    OCTET STRING (24 byte) 3016801432416494D42D413ACDEB2B7209EBAB8D883AD1CF
      SEQUENCE (1 elem)
        [0] (20 byte) 32416494D42D413ACDEB2B7209EBAB8D883AD1CF
  SEQUENCE (2 elem)
    OBJECT IDENTIFIER 2.5.29.18 issuerAltName (X.509 extension)
    OCTET STRING (22 byte) 30148112696E666F4076696E63617369676E2E6E6574
      SEQUENCE (1 elem)
        [1] (18 byte) info@vincasign.net
  SEQUENCE (2 elem)
    OBJECT IDENTIFIER 2.5.29.32 certificatePolicies (X.509 extension)
    OCTET STRING (155 byte) 308198308195060C2B0601040181D164010102033081843030060 82B0601050507020…
      SEQUENCE (1 elem)
```

```
          SEQUENCE (2 elem)
            OBJECT IDENTIFIER 1.3.6.1.4.1.26852.1.1.2.3
            SEQUENCE (2 elem)
              SEQUENCE (2 elem)
                OBJECT IDENTIFIER 1.3.6.1.5.5.7.2.1 cps (PKIX policy qualifier)
                IA5String https://psc.cgcom.es/declaracion_dpc
              SEQUENCE (2 elem)
                OBJECT IDENTIFIER 1.3.6.1.5.5.7.2.2 unotice (PKIX policy qualifier)
                SEQUENCE (1 elem)
                  UTF8String CERTIFICADO PARA EL CIFRADO DE PERSONA FISICA VINCULADA EN TARJETA
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.29.31 cRLDistributionPoints (X.509 extension)
        OCTET STRING (90 byte) 3058302AA028A0268624687474703A2F2F63726C352E6367636F6D2E65732F63726C2F…
          SEQUENCE (2 elem)
            SEQUENCE (1 elem)
              [0] (1 elem)
                [0] (1 elem)
                  [6] (36 byte) http://crl5.cgcom.es/crl/eccgcom.crl
            SEQUENCE (1 elem)
              [0] (1 elem)
                [0] (1 elem)
                  [6] (36 byte) http://crl6.cgcom.es/crl/eccgcom.crl
      SEQUENCE (3 elem)
        OBJECT IDENTIFIER 2.5.29.15 keyUsage (X.509 extension)
        BOOLEAN true
        OCTET STRING (4 byte) 03020520
          BIT STRING (3 bit) 001
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.29.37 extKeyUsage (X.509 extension)
        OCTET STRING (12 byte) 300A06082B06010505070304
          SEQUENCE (1 elem)
            OBJECT IDENTIFIER 1.3.6.1.5.5.7.3.4 emailProtection (PKIX key purpose)
```

```
SEQUENCE (2 elem)
  OBJECT IDENTIFIER 2.5.29.17 subjectAltName (X.509 extension)
  OCTET STRING (210 byte) 3081CF8110656D61696C407072756562612E636F6DA481BA3081B7311F301D060A2B0…
    SEQUENCE (2 elem)
      [1] (16 byte) email@prueba.com
      [4] (1 elem)
        SEQUENCE (7 elem)
          SET (1 elem)
            SEQUENCE (2 elem)
              OBJECT IDENTIFIER 1.3.6.1.4.1.26852.2.12
              UTF8String IDCES-12345678Z
          SET (1 elem)
            SEQUENCE (2 elem)
              OBJECT IDENTIFIER 1.3.6.1.4.1.26852.2.11
              UTF8String Apellido2
          SET (1 elem)
            SEQUENCE (2 elem)
              OBJECT IDENTIFIER 1.3.6.1.4.1.26852.2.10
              UTF8String Apellido1
          SET (1 elem)
            SEQUENCE (2 elem)
              OBJECT IDENTIFIER 1.3.6.1.4.1.26852.2.9
              UTF8String Nombre
          SET (1 elem)
            SEQUENCE (2 elem)
              OBJECT IDENTIFIER 1.3.6.1.4.1.26852.2.3
              UTF8String 00003
          SET (1 elem)
            SEQUENCE (2 elem)
              OBJECT IDENTIFIER 1.3.6.1.4.1.26852.2.2
              UTF8String Colegio
          SET (1 elem)
```

```
                    SEQUENCE (2 elem)
                      OBJECT IDENTIFIER 1.3.6.1.4.1.26852.2.1
                      UTF8String 000035
  SEQUENCE (2 elem)
    OBJECT IDENTIFIER 1.2.840.113549.1.1.13 sha512WithRSAEncryption (PKCS #1)
    NULL
```

8. Certificados de Persona Física Vinculada, en nube

```
SEQUENCE (3 elem)
  SEQUENCE (8 elem)
    [0] (1 elem)
      INTEGER 2
    INTEGER (63 bit) 7275461763768266514
    SEQUENCE (2 elem)
      OBJECT IDENTIFIER 1.2.840.113549.1.1.13 sha512WithRSAEncryption (PKCS #1)
      NULL
    SEQUENCE (7 elem)
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.6 countryName (X.520 DN component)
          PrintableString ES
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.8 stateOrProvinceName (X.520 DN component)
          UTF8String MADRID
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.7 localityName (X.520 DN component)
          UTF8String MADRID
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.97
          UTF8String VATES-Q2866017C
      SET (1 elem)
        SEQUENCE (2 elem)
```

```
        OBJECT IDENTIFIER 2.5.4.11 organizationalUnitName (X.520 DN component)
        UTF8String ENTIDAD DE CERTIFICACION
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.10 organizationName (X.520 DN component)
        UTF8String CONSEJO GENERAL DE COLEGIOS OFICIALES DE MEDICOS
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.3 commonName (X.520 DN component)
        UTF8String CGCOM QUALIFIED 2020
  SEQUENCE (2 elem)
    UTCTime 2020-03-02 13:49:28 UTC
    UTCTime 2023-03-02 13:49:28 UTC
  SEQUENCE (10 elem)
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.3 commonName (X.520 DN component)
        UTF8String apellido1 apellido2 nombre - DNI 12345678Z
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.5 serialNumber (X.520 DN component)
        PrintableString IDCES-12345678Z
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.42 givenName (X.520 DN component)
        UTF8String Nombre
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.4 surname (X.520 DN component)
        UTF8String apellido1 apellido2
    SET (1 elem)
      SEQUENCE (2 elem)
```

```
        OBJECT IDENTIFIER 2.5.4.12 title (X.520 DN component)
        UTF8String PERSONA FÍSICA VINCULADA
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.11 organizationalUnitName (X.520 DN component)
        UTF8String UnidadOrganizativa
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.11 organizationalUnitName (X.520 DN component)
        UTF8String UnidadOrganizativa2
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.97
        UTF8String VATES-Q0000001
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.10 organizationName (X.520 DN component)
        UTF8String NombreColegio
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.6 countryName (X.520 DN component)
        PrintableString ES
  SEQUENCE (2 elem)
    SEQUENCE (2 elem)
      OBJECT IDENTIFIER 1.2.840.113549.1.1.1 rsaEncryption (PKCS #1)
      NULL
    BIT STRING (2160 bit) 001100001000001000000001000010100000001010000010000000010000000100000…
      SEQUENCE (2 elem)
        INTEGER (2048 bit) 237719905331402001762633476944572475967838715166994949677911756524207…
        INTEGER 65537
  [3] (1 elem)
    SEQUENCE (10 elem)
```

```
SEQUENCE (2 elem)
  OBJECT IDENTIFIER 1.3.6.1.5.5.7.1.1 authorityInfoAccess (PKIX private extension)
  OCTET STRING (99 byte) 3061303606082B06010505073002862A687474703A2F2F7073632E6367636F6D2E6573…
    SEQUENCE (2 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 1.3.6.1.5.5.7.48.2 caIssuers (PKIX subject/authority info access descriptor)
        [6] (42 byte) http://psc.cgcom.es/CA/root_cgcom_2020.crt
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 1.3.6.1.5.5.7.48.1 ocsp (PKIX)
        [6] (27 byte) http://ocspservice.cgcom.es
SEQUENCE (2 elem)
  OBJECT IDENTIFIER 2.5.29.14 subjectKeyIdentifier (X.509 extension)
  OCTET STRING (20 byte) B1623DD29398229F38461E0D51F58599F2AAEEDF
    OCTET STRING (20 byte) B1623DD29398229F38461E0D51F58599F2AAEEDF
SEQUENCE (3 elem)
  OBJECT IDENTIFIER 2.5.29.19 basicConstraints (X.509 extension)
  BOOLEAN true
  OCTET STRING (2 byte) 3000
    SEQUENCE (0 elem)
SEQUENCE (2 elem)
  OBJECT IDENTIFIER 2.5.29.35 authorityKeyIdentifier (X.509 extension)
  OCTET STRING (24 byte) 3016801432416494D42D413ACDEB2B7209EBAB8D883AD1CF
    SEQUENCE (1 elem)
      [0] (20 byte) 32416494D42D413ACDEB2B7209EBAB8D883AD1CF
SEQUENCE (2 elem)
  OBJECT IDENTIFIER 1.3.6.1.5.5.7.1.3 qcStatements (PKIX private extension)
  OCTET STRING (159 byte) 30819C301506082B06010505070B023009060704008BEC4901013008060604008E460…
    SEQUENCE (6 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 1.3.6.1.5.5.7.11.2
        SEQUENCE (1 elem)
          OBJECT IDENTIFIER 0.4.0.194121.1.1
```

```
            SEQUENCE (1 elem)
              OBJECT IDENTIFIER 0.4.0.1862.1.1 etsiQcsCompliance (ETSI TS 101 862 qualified certificates)
            SEQUENCE (2 elem)
              OBJECT IDENTIFIER 0.4.0.1862.1.3 etsiQcsRetentionPeriod (ETSI TS 101 862 qualified certificates)
              INTEGER 15
            SEQUENCE (1 elem)
              OBJECT IDENTIFIER 0.4.0.1862.1.4 etsiQcsQcSSCD (ETSI TS 101 862 qualified certificates)
            SEQUENCE (2 elem)
              OBJECT IDENTIFIER 0.4.0.1862.1.6
              SEQUENCE (1 elem)
                OBJECT IDENTIFIER 0.4.0.1862.1.6.1
            SEQUENCE (2 elem)
              OBJECT IDENTIFIER 0.4.0.1862.1.5
              SEQUENCE (2 elem)
                SEQUENCE (2 elem)
                  IA5String https://psc.cgcom.es/en/pds
                  PrintableString en
                SEQUENCE (2 elem)
                  IA5String https://psc.cgcom.es/pds
                  PrintableString es
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.29.32 certificatePolicies (X.509 extension)
          OCTET STRING (152 byte) 308195308187060B2B0601040181D164010106307830240608 2B06010505070201161…
            SEQUENCE (2 elem)
              SEQUENCE (2 elem)
                OBJECT IDENTIFIER 1.3.6.1.4.1.26852.1.1.6
                SEQUENCE (2 elem)
                  SEQUENCE (2 elem)
                    OBJECT IDENTIFIER 1.3.6.1.5.5.7.2.1 cps (PKIX policy qualifier)
                    IA5String https://psc.cgcom.es/dpc
                  SEQUENCE (2 elem)
                    OBJECT IDENTIFIER 1.3.6.1.5.5.7.2.2 unotice (PKIX policy qualifier)
```

```
                SEQUENCE (1 elem)
                  UTF8String "CERTIFICADO CUALIFICADO DE PERSONA FÍSICA VINCULADA EN DCCF"
          SEQUENCE (1 elem)
            OBJECT IDENTIFIER 0.4.0.194112.1.2
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.29.31 cRLDistributionPoints (X.509 extension)
        OCTET STRING (90 byte) 3058302AA028A0268624687474703A2F2F63726C352E6367636F6D2E65732F63726C2F…
          SEQUENCE (2 elem)
            SEQUENCE (1 elem)
              [0] (1 elem)
                [0] (1 elem)
                  [6] (36 byte) http://crl5.cgcom.es/crl/eccgcom.crl
            SEQUENCE (1 elem)
              [0] (1 elem)
                [0] (1 elem)
                  [6] (36 byte) http://crl6.cgcom.es/crl/eccgcom.crl
      SEQUENCE (3 elem)
        OBJECT IDENTIFIER 2.5.29.15 keyUsage (X.509 extension)
        BOOLEAN true
        OCTET STRING (4 byte) 030206C0
          BIT STRING (2 bit) 11
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.29.37 extKeyUsage (X.509 extension)
        OCTET STRING (22 byte) 301406082B06010505070302060 82B06010505070304
          SEQUENCE (2 elem)
            OBJECT IDENTIFIER 1.3.6.1.5.5.7.3.2 clientAuth (PKIX key purpose)
            OBJECT IDENTIFIER 1.3.6.1.5.5.7.3.4 emailProtection (PKIX key purpose)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.29.17 subjectAltName (X.509 extension)
        OCTET STRING (210 byte) 3081CF8110656D61696C407072756562612E636F6DA481BA3081B7311F301D060A2B0…
          SEQUENCE (2 elem)
            [1] (16 byte) email@prueba.com
```

```
            [4] (1 elem)
              SEQUENCE (7 elem)
                SET (1 elem)
                  SEQUENCE (2 elem)
                    OBJECT IDENTIFIER 1.3.6.1.4.1.26852.2.12
                    UTF8String IDCES-12345678Z
                SET (1 elem)
                  SEQUENCE (2 elem)
                    OBJECT IDENTIFIER 1.3.6.1.4.1.26852.2.11
                    UTF8String Apellido2
                SET (1 elem)
                  SEQUENCE (2 elem)
                    OBJECT IDENTIFIER 1.3.6.1.4.1.26852.2.10
                    UTF8String Apellido1
                SET (1 elem)
                  SEQUENCE (2 elem)
                    OBJECT IDENTIFIER 1.3.6.1.4.1.26852.2.9
                    UTF8String Nombre
                SET (1 elem)
                  SEQUENCE (2 elem)
                    OBJECT IDENTIFIER 1.3.6.1.4.1.26852.2.3
                    UTF8String 00003
                SET (1 elem)
                  SEQUENCE (2 elem)
                    OBJECT IDENTIFIER 1.3.6.1.4.1.26852.2.2
                    UTF8String Colegio
                SET (1 elem)
                  SEQUENCE (2 elem)
                    OBJECT IDENTIFIER 1.3.6.1.4.1.26852.2.1
                    UTF8String 000035
SEQUENCE (2 elem)
  OBJECT IDENTIFIER 1.2.840.113549.1.1.13 sha512WithRSAEncryption (PKCS #1)
```

```
NULL
```

9. Certificados de persona física vinculada en software

```
SEQUENCE (3 elem)
  SEQUENCE (8 elem)
    [0] (1 elem)
      INTEGER 2
    INTEGER (159 bit) 447754420391871716931813083136490715486776441593
    SEQUENCE (2 elem)
      OBJECT IDENTIFIER 1.2.840.113549.1.1.13 sha512WithRSAEncryption (PKCS #1)
      NULL
    SEQUENCE (7 elem)
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.6 countryName (X.520 DN component)
          PrintableString ES
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.8 stateOrProvinceName (X.520 DN component)
          UTF8String MADRID
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.7 localityName (X.520 DN component)
          UTF8String MADRID
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.97 organizationIdentifier (X.520 DN component)
          UTF8String VATES-Q2866017C
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.11 organizationalUnitName (X.520 DN component)
          UTF8String ENTIDAD DE CERTIFICACION
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.10 organizationName (X.520 DN component)
          UTF8String CONSEJO GENERAL DE COLEGIOS OFICIALES DE MEDICOS
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.3 commonName (X.520 DN component)
          UTF8String CGCOM QUALIFIED 2020
```

```
    SEQUENCE (2 elem)
      UTCTime 2022-03-24 11:00:28 UTC
      UTCTime 2023-03-24 11:00:28 UTC
    SEQUENCE (8 elem)
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.3 commonName (X.520 DN component)
          UTF8String APELLIDOUNO APELLIDODOS NOMBRE - 1234567892
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.5 serialNumber (X.520 DN component)
          PrintableString IDCES-1234567892
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.42 givenName (X.520 DN component)
          UTF8String NOMBRE
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.4 surname (X.520 DN component)
          UTF8String APELLIDOUNO APELLIDODOS
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.12 title (X.520 DN component)
          UTF8String PERSONA FÍSICA VINCULADA
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.97 organizationIdentifier (X.520 DN component)
          UTF8String VATES-Q0000000J
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.10 organizationName (X.520 DN component)
          UTF8String ENTIDAD VINCULADA
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.6 countryName (X.520 DN component)
          PrintableString ES
    SEQUENCE (2 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 1.2.840.113549.1.1.1 rsaEncryption (PKCS #1)
        NULL
      BIT STRING (2160 bit) 001100001000001000000001000010100000001010000010000000010000000100000…
        SEQUENCE (2 elem)
```

```
        INTEGER (2048 bit) 232767285925823255068776391820133023635441328229933160208273141064101…
        INTEGER 65537
    [3] (1 elem)
      SEQUENCE (11 elem)
        SEQUENCE (3 elem)
          OBJECT IDENTIFIER 2.5.29.19 basicConstraints (X.509 extension)
          BOOLEAN true
          OCTET STRING (2 byte) 3000
            SEQUENCE (0 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.29.35 authorityKeyIdentifier (X.509 extension)
          OCTET STRING (24 byte) 3016801432416494D42D413ACDEB2B7209EBAB8D883AD1CF
            SEQUENCE (1 elem)
              [0] (20 byte) 32416494D42D413ACDEB2B7209EBAB8D883AD1CF
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 1.3.6.1.5.5.7.1.1 authorityInfoAccess (PKIX private extension)
          OCTET STRING (99 byte) 3061303606082B06010505073002862A687474703A2F2F7073632E6367636F6D2E6573…
            SEQUENCE (2 elem)
              SEQUENCE (2 elem)
                OBJECT IDENTIFIER 1.3.6.1.5.5.7.48.2 caIssuers (PKIX subject/authority info access descriptor)
                [6] (42 byte) http://psc.cgcom.es/CA/root_cgcom_2020.crt
              SEQUENCE (2 elem)
                OBJECT IDENTIFIER 1.3.6.1.5.5.7.48.1 ocsp (PKIX)
                [6] (27 byte) http://ocspservice.cgcom.es
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.29.18 issuerAltName (X.509 extension)
          OCTET STRING (22 byte) 30148112696E666F4076696E63617369676E2E6E6574
            SEQUENCE (1 elem)
              [1] (18 byte) info@vincasign.net
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.29.17 subjectAltName (X.509 extension)
          OCTET STRING (228 byte) 3081E1811A6E6F6D6272652E6170756E6F6170646F73406367636F6D2E6573A481C23…
            SEQUENCE (2 elem)
              [1] (26 byte) nombre.apunoapdos@cgcom.es
              [4] (1 elem)
                SEQUENCE (6 elem)
                  SET (1 elem)
                    SEQUENCE (2 elem)
                      OBJECT IDENTIFIER 1.3.6.1.4.1.26852.2.1
                      UTF8String IDCOLEGIOTEST
                  SET (1 elem)
                    SEQUENCE (2 elem)
```

```
                    OBJECT IDENTIFIER 1.3.6.1.4.1.26852.2.2
                    UTF8String COLEGIO DE MEDICOS DE TEST
                SET (1 elem)
                  SEQUENCE (2 elem)
                    OBJECT IDENTIFIER 1.3.6.1.4.1.26852.2.9
                    UTF8String NOMBRE
                SET (1 elem)
                  SEQUENCE (2 elem)
                    OBJECT IDENTIFIER 1.3.6.1.4.1.26852.2.10
                    UTF8String APELLIDOUNO
                SET (1 elem)
                  SEQUENCE (2 elem)
                    OBJECT IDENTIFIER 1.3.6.1.4.1.26852.2.11
                    UTF8String APELLIDODOS
                SET (1 elem)
                  SEQUENCE (2 elem)
                    OBJECT IDENTIFIER 1.3.6.1.4.1.26852.2.12
                    UTF8String IDCES-123456789Z
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.29.32 certificatePolicies (X.509 extension)
          OCTET STRING (164 byte) 3081A1308193060C2B0601040181D164010102053081823 04E06082B0601050507020…
            SEQUENCE (2 elem)
              SEQUENCE (2 elem)
                OBJECT IDENTIFIER 1.3.6.1.4.1.26852.1.1.2.5
                SEQUENCE (2 elem)
                  SEQUENCE (2 elem)
                    OBJECT IDENTIFIER 1.3.6.1.5.5.7.2.2 unotice (PKIX policy qualifier)
                    SEQUENCE (1 elem)
                      UTF8String CERTIFICADO CUALIFICADO DE PERSONA FÍSICA VINCULADA EN SOFTWARE
                  SEQUENCE (2 elem)
                    OBJECT IDENTIFIER 1.3.6.1.5.5.7.2.1 cps (PKIX policy qualifier)
                    IA5String https://psc.cgcom.es/declaracion_dpc
              SEQUENCE (1 elem)
                OBJECT IDENTIFIER 0.4.0.194112.1.0
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.29.37 extKeyUsage (X.509 extension)
          OCTET STRING (22 byte) 301406082B06010505070302 06082B06010505070304
            SEQUENCE (2 elem)
              OBJECT IDENTIFIER 1.3.6.1.5.5.7.3.2 clientAuth (PKIX key purpose)
              OBJECT IDENTIFIER 1.3.6.1.5.5.7.3.4 emailProtection (PKIX key purpose)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 1.3.6.1.5.5.7.1.3 qcStatements (PKIX private extension)
```

```
          OCTET STRING (35 byte) 3021301506082B06010505070B023009060704008BEC490101300806060400 8E460101
            SEQUENCE (2 elem)
              SEQUENCE (2 elem)
                OBJECT IDENTIFIER 1.3.6.1.5.5.7.11.2 pkixQCSyntax-v2 (PKIX qualified certificates)
                SEQUENCE (1 elem)
                  OBJECT IDENTIFIER 0.4.0.194121.1.1
              SEQUENCE (1 elem)
                OBJECT IDENTIFIER 0.4.0.1862.1.1 etsiQcsCompliance (ETSI TS 101 862 qualified certificates)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.29.31 cRLDistributionPoints (X.509 extension)
          OCTET STRING (90 byte) 3058302AA028A0268624687474703A2F2F63726C352E6367636F6D2E65732F63726C2F…
            SEQUENCE (2 elem)
              SEQUENCE (1 elem)
                [0] (1 elem)
                  [0] (1 elem)
                    [6] (36 byte) http://crl5.cgcom.es/crl/eccgcom.crl
              SEQUENCE (1 elem)
                [0] (1 elem)
                  [0] (1 elem)
                    [6] (36 byte) http://crl6.cgcom.es/crl/eccgcom.crl
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.29.14 subjectKeyIdentifier (X.509 extension)
          OCTET STRING (22 byte) 041427753E8F54573F3157D6A39239BD10F1CAA72518
            OCTET STRING (20 byte) 27753E8F54573F3157D6A39239BD10F1CAA72518
Offset: 1616
Length: 2+20
Value:
(20 byte)
27753E8F54573F3157D6A39239BD10F1CAA72518
        SEQUENCE (3 elem)
          OBJECT IDENTIFIER 2.5.29.15 keyUsage (X.509 extension)
          BOOLEAN true
          OCTET STRING (4 byte) 030206C0
            BIT STRING (2 bit) 11
  SEQUENCE (2 elem)
    OBJECT IDENTIFIER 1.2.840.113549.1.1.13 sha512WithRSAEncryption (PKCS #1)
    NULL
```

10. Certificado de Persona Física Representante, en tarjeta

10.1 Para autenticación

```
SEQUENCE (3 elem)
  SEQUENCE (8 elem)
    [0] (1 elem)
      INTEGER 2
    INTEGER (62 bit) 2453915011011873084
    SEQUENCE (2 elem)
      OBJECT IDENTIFIER 1.2.840.113549.1.1.13 sha512WithRSAEncryption (PKCS #1)
      NULL
    SEQUENCE (7 elem)
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.6 countryName (X.520 DN component)
          PrintableString ES
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.8 stateOrProvinceName (X.520 DN component)
          UTF8String MADRID
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.7 localityName (X.520 DN component)
          UTF8String MADRID
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.97
```

```
        UTF8String VATES-Q2866017C
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.11 organizationalUnitName (X.520 DN component)
        UTF8String ENTIDAD DE CERTIFICACION
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.10 organizationName (X.520 DN component)
        UTF8String CONSEJO GENERAL DE COLEGIOS OFICIALES DE MEDICOS
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.3 commonName (X.520 DN component)
        UTF8String CGCOM QUALIFIED 2020
  SEQUENCE (2 elem)
    UTCTime 2020-03-02 12:55:42 UTC
    UTCTime 2023-03-02 12:55:42 UTC
  SEQUENCE (11 elem)
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.13 description (X.520 DN component)
        UTF8String Reg: XXX /Hoja: XXX /Tomo:XXX /Fecha: dd mm aaaa /Inscripción: XXX
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.3 commonName (X.520 DN component)
        UTF8String 12345678Z Nombre Apellidos (R: Q00000001) (AUTENTICACIÓN)
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.5 serialNumber (X.520 DN component)
        PrintableString IDCES-12345678Z
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.42 givenName (X.520 DN component)
```

```
        UTF8String Nombre
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.4 surname (X.520 DN component)
        UTF8String apellido1 apellido2
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.12 title (X.520 DN component)
        UTF8String PERSONA FÍSICA REPRESENTANTE
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.11 organizationalUnitName (X.520 DN component)
        UTF8String UnidadOrganizativa2
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.11 organizationalUnitName (X.520 DN component)
        UTF8String UnidadOrganizativa
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.97
        UTF8String VATES-Q0000001
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.10 organizationName (X.520 DN component)
        UTF8String NombreColegio
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.6 countryName (X.520 DN component)
        PrintableString ES
  SEQUENCE (2 elem)
    SEQUENCE (2 elem)
      OBJECT IDENTIFIER 1.2.840.113549.1.1.1 rsaEncryption (PKCS #1)
```

```
      NULL
    BIT STRING (2160 bit) 001100001000001000000001000010100000001010000010000000010000000100000…
      SEQUENCE (2 elem)
        INTEGER (2048 bit) 209085259414219622363928817223737810348721062600624325334725571079784…
        INTEGER 65537
  [3] (1 elem)
    SEQUENCE (9 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 1.3.6.1.5.5.7.1.1 authorityInfoAccess (PKIX private extension)
        OCTET STRING (99 byte) 3061303606082B06010505073002862A687474703A2F2F7073632E6367636F6D2E6573…
          SEQUENCE (2 elem)
            SEQUENCE (2 elem)
              OBJECT IDENTIFIER 1.3.6.1.5.5.7.48.2 caIssuers (PKIX subject/authority info access descriptor)
              [6] (42 byte) http://psc.cgcom.es/CA/root_cgcom_2020.crt
            SEQUENCE (2 elem)
              OBJECT IDENTIFIER 1.3.6.1.5.5.7.48.1 ocsp (PKIX)
              [6] (27 byte) http://ocspservice.cgcom.es
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.29.14 subjectKeyIdentifier (X.509 extension)
        OCTET STRING (20 byte) 732D32AB981D4901B407A08444A5AD3BD7AF9D97
          OCTET STRING (20 byte) 732D32AB981D4901B407A08444A5AD3BD7AF9D97
      SEQUENCE (3 elem)
        OBJECT IDENTIFIER 2.5.29.19 basicConstraints (X.509 extension)
        BOOLEAN true
        OCTET STRING (2 byte) 3000
          SEQUENCE (0 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.29.35 authorityKeyIdentifier (X.509 extension)
        OCTET STRING (24 byte) 3016801432416494D42D413ACDEB2B7209EBAB8D883AD1CF
          SEQUENCE (1 elem)
            [0] (20 byte) 32416494D42D413ACDEB2B7209EBAB8D883AD1CF
      SEQUENCE (2 elem)
```

```
    OBJECT IDENTIFIER 2.5.29.32 certificatePolicies (X.509 extension)
    OCTET STRING (181 byte) 3081B230819A060C2B0601040181D16401010B0130818930300608 2B0601050507020…
      SEQUENCE (3 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 1.3.6.1.4.1.26852.1.1.11.1
          SEQUENCE (2 elem)
            SEQUENCE (2 elem)
              OBJECT IDENTIFIER 1.3.6.1.5.5.7.2.1 cps (PKIX policy qualifier)
              IA5String https://psc.cgcom.es/declaracion_dpc
            SEQUENCE (2 elem)
              OBJECT IDENTIFIER 1.3.6.1.5.5.7.2.2 unotice (PKIX policy qualifier)
              SEQUENCE (1 elem)
                UTF8String "CERTIFICADO PARA LA IDENTIFICACION DEL REPRESENTANTE DE PJ EN TARJETA"
        SEQUENCE (1 elem)
          OBJECT IDENTIFIER 0.4.0.2042.1.2
        SEQUENCE (1 elem)
          OBJECT IDENTIFIER 2.16.724.1.3.5.8
  SEQUENCE (2 elem)
    OBJECT IDENTIFIER 2.5.29.31 cRLDistributionPoints (X.509 extension)
    OCTET STRING (90 byte) 3058302AA028A0268624687474703A2F2F63726C352E6367636F6D2E65732F63726C2F…
      SEQUENCE (2 elem)
        SEQUENCE (1 elem)
          [0] (1 elem)
            [0] (1 elem)
              [6] (36 byte) http://crl5.cgcom.es/crl/eccgcom.crl
        SEQUENCE (1 elem)
          [0] (1 elem)
            [0] (1 elem)
              [6] (36 byte) http://crl6.cgcom.es/crl/eccgcom.crl
  SEQUENCE (3 elem)
    OBJECT IDENTIFIER 2.5.29.15 keyUsage (X.509 extension)
    BOOLEAN true
```

```
    OCTET STRING (4 byte) 03020780
      BIT STRING (1 bit) 1
  SEQUENCE (2 elem)
    OBJECT IDENTIFIER 2.5.29.37 extKeyUsage (X.509 extension)
    OCTET STRING (12 byte) 300A06082B06010505070302
      SEQUENCE (1 elem)
        OBJECT IDENTIFIER 1.3.6.1.5.5.7.3.2 clientAuth (PKIX key purpose)
  SEQUENCE (2 elem)
    OBJECT IDENTIFIER 2.5.29.17 subjectAltName (X.509 extension)
    OCTET STRING (210 byte) 3081CF8110656D61696C407072756562612E636F6DA481BA3081B7311F301D060A2B0…
      SEQUENCE (2 elem)
        [1] (16 byte) email@prueba.com
        [4] (1 elem)
          SEQUENCE (7 elem)
            SET (1 elem)
              SEQUENCE (2 elem)
                OBJECT IDENTIFIER 1.3.6.1.4.1.26852.2.12
                UTF8String IDCES-12345678Z
            SET (1 elem)
              SEQUENCE (2 elem)
                OBJECT IDENTIFIER 1.3.6.1.4.1.26852.2.11
                UTF8String Apellido2
            SET (1 elem)
              SEQUENCE (2 elem)
                OBJECT IDENTIFIER 1.3.6.1.4.1.26852.2.10
                UTF8String Apellido1
            SET (1 elem)
              SEQUENCE (2 elem)
                OBJECT IDENTIFIER 1.3.6.1.4.1.26852.2.9
                UTF8String Nombre
            SET (1 elem)
              SEQUENCE (2 elem)
```

```
                    OBJECT IDENTIFIER 1.3.6.1.4.1.26852.2.3
                    UTF8String 00003
                SET (1 elem)
                  SEQUENCE (2 elem)
                    OBJECT IDENTIFIER 1.3.6.1.4.1.26852.2.2
                    UTF8String Colegio
                SET (1 elem)
                  SEQUENCE (2 elem)
                    OBJECT IDENTIFIER 1.3.6.1.4.1.26852.2.1
                    UTF8String 000035
SEQUENCE (2 elem)
  OBJECT IDENTIFIER 1.2.840.113549.1.1.13 sha512WithRSAEncryption (PKCS #1)
  NULL
```

10.2 Para firma

```
EQUENCE (3 elem)
  SEQUENCE (8 elem)
    [0] (1 elem)
      INTEGER 2
    INTEGER (63 bit) 6678473187083793914
    SEQUENCE (2 elem)
      OBJECT IDENTIFIER 1.2.840.113549.1.1.13 sha512WithRSAEncryption (PKCS #1)
      NULL
    SEQUENCE (7 elem)
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.6 countryName (X.520 DN component)
          PrintableString ES
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.8 stateOrProvinceName (X.520 DN component)
          UTF8String MADRID
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.7 localityName (X.520 DN component)
          UTF8String MADRID
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.97
          UTF8String VATES-Q2866017C
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.11 organizationalUnitName (X.520 DN component)
```

```
        UTF8String ENTIDAD DE CERTIFICACION
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.10 organizationName (X.520 DN component)
        UTF8String CONSEJO GENERAL DE COLEGIOS OFICIALES DE MEDICOS
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.3 commonName (X.520 DN component)
        UTF8String CGCOM QUALIFIED 2020
  SEQUENCE (2 elem)
    UTCTime 2020-03-17 16:20:08 UTC
    UTCTime 2023-03-17 16:20:08 UTC
  SEQUENCE (11 elem)
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.13 description (X.520 DN component)
        UTF8String Reg: XXX /Hoja: XXX /Tomo:XXX /Fecha: dd mm aaaa /Inscripción: XXX
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.3 commonName (X.520 DN component)
        UTF8String 12345678Z Nombre Apellidos (R: Q00000001) (FIRMA)
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.5 serialNumber (X.520 DN component)
        PrintableString IDCES-12345678Z
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.42 givenName (X.520 DN component)
        UTF8String Nombre
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.4 surname (X.520 DN component)
```

```
        UTF8String apellido1 apellido2
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.12 title (X.520 DN component)
        UTF8String PERSONA FÍSICA REPRESENTANTE
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.11 organizationalUnitName (X.520 DN component)
        UTF8String UnidadOrganizativa2
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.11 organizationalUnitName (X.520 DN component)
        UTF8String UnidadOrganizativa
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.97
        UTF8String VATES-Q0000001
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.10 organizationName (X.520 DN component)
        UTF8String NombreColegio
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.6 countryName (X.520 DN component)
        PrintableString ES
  SEQUENCE (2 elem)
    SEQUENCE (2 elem)
      OBJECT IDENTIFIER 1.2.840.113549.1.1.1 rsaEncryption (PKCS #1)
      NULL
    BIT STRING (2160 bit) 001100001000001000000001000010100000001010000010000000010000000100000…
      SEQUENCE (2 elem)
        INTEGER (2048 bit) 193432951903032486724049016538914447081888119840515466722282832290354…
```

```
        INTEGER 65537
    [3] (1 elem)
      SEQUENCE (10 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 1.3.6.1.5.5.7.1.1 authorityInfoAccess (PKIX private extension)
          OCTET STRING (99 byte) 3061303606082B06010505073002862A687474703A2F2F7073632E6367636F6D2E6573…
            SEQUENCE (2 elem)
              SEQUENCE (2 elem)
                OBJECT IDENTIFIER 1.3.6.1.5.5.7.48.2 caIssuers (PKIX subject/authority info access descriptor)
                [6] (42 byte) http://psc.cgcom.es/CA/root_cgcom_2020.crt
              SEQUENCE (2 elem)
                OBJECT IDENTIFIER 1.3.6.1.5.5.7.48.1 ocsp (PKIX)
                [6] (27 byte) http://ocspservice.cgcom.es
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.29.14 subjectKeyIdentifier (X.509 extension)
          OCTET STRING (20 byte) 4EF92B476FB5C6E96CDCF9072A47289281D0BAEF
            OCTET STRING (20 byte) 4EF92B476FB5C6E96CDCF9072A47289281D0BAEF
        SEQUENCE (3 elem)
          OBJECT IDENTIFIER 2.5.29.19 basicConstraints (X.509 extension)
          BOOLEAN true
          OCTET STRING (2 byte) 3000
            SEQUENCE (0 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.29.35 authorityKeyIdentifier (X.509 extension)
          OCTET STRING (24 byte) 3016801432416494D42D413ACDEB2B7209EBAB8D883AD1CF
            SEQUENCE (1 elem)
              [0] (20 byte) 32416494D42D413ACDEB2B7209EBAB8D883AD1CF
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 1.3.6.1.5.5.7.1.3 qcStatements (PKIX private extension)
          OCTET STRING (159 byte) 30819C301506082B06010505070B023009060704008BEC4901013008060604008E460…
            SEQUENCE (6 elem)
              SEQUENCE (2 elem)
```

```
            OBJECT IDENTIFIER 1.3.6.1.5.5.7.11.2
            SEQUENCE (1 elem)
              OBJECT IDENTIFIER 0.4.0.194121.1.1
          SEQUENCE (1 elem)
            OBJECT IDENTIFIER 0.4.0.1862.1.1 etsiQcsCompliance (ETSI TS 101 862 qualified certificates)
          SEQUENCE (2 elem)
            OBJECT IDENTIFIER 0.4.0.1862.1.3 etsiQcsRetentionPeriod (ETSI TS 101 862 qualified certificates)
            INTEGER 15
          SEQUENCE (1 elem)
            OBJECT IDENTIFIER 0.4.0.1862.1.4 etsiQcsQcSSCD (ETSI TS 101 862 qualified certificates)
          SEQUENCE (2 elem)
            OBJECT IDENTIFIER 0.4.0.1862.1.6
            SEQUENCE (1 elem)
              OBJECT IDENTIFIER 0.4.0.1862.1.6.1
          SEQUENCE (2 elem)
            OBJECT IDENTIFIER 0.4.0.1862.1.5
            SEQUENCE (2 elem)
              SEQUENCE (2 elem)
                IA5String https://psc.cgcom.es/en/pds
                PrintableString en
              SEQUENCE (2 elem)
                IA5String https://psc.cgcom.es/pds
                PrintableString es
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.29.32 certificatePolicies (X.509 extension)
        OCTET STRING (182 byte) 3081B330819A060C2B0601040181D16401010B02308189303006082B0601050507020…
          SEQUENCE (3 elem)
            SEQUENCE (2 elem)
              OBJECT IDENTIFIER 1.3.6.1.4.1.26852.1.1.11.2
              SEQUENCE (2 elem)
                SEQUENCE (2 elem)
                  OBJECT IDENTIFIER 1.3.6.1.5.5.7.2.1 cps (PKIX policy qualifier)
```

```
                IA5String https://psc.cgcom.es/declaracion_dpc
              SEQUENCE (2 elem)
                OBJECT IDENTIFIER 1.3.6.1.5.5.7.2.2 unotice (PKIX policy qualifier)
                SEQUENCE (1 elem)
                  UTF8String "CERTIFIACDO CUALIFICADO PARA FIRMA DEL REPRESENTANTE DE PJ EN TARJETA"
        SEQUENCE (1 elem)
          OBJECT IDENTIFIER 0.4.0.194112.1.2
        SEQUENCE (1 elem)
          OBJECT IDENTIFIER 2.16.724.1.3.5.8
SEQUENCE (2 elem)
  OBJECT IDENTIFIER 2.5.29.31 cRLDistributionPoints (X.509 extension)
  OCTET STRING (90 byte) 3058302AA028A0268624687474703A2F2F63726C352E6367636F6D2E65732F63726C2F…
    SEQUENCE (2 elem)
      SEQUENCE (1 elem)
        [0] (1 elem)
          [0] (1 elem)
            [6] (36 byte) http://crl5.cgcom.es/crl/eccgcom.crl
      SEQUENCE (1 elem)
        [0] (1 elem)
          [0] (1 elem)
            [6] (36 byte) http://crl6.cgcom.es/crl/eccgcom.crl
SEQUENCE (3 elem)
  OBJECT IDENTIFIER 2.5.29.15 keyUsage (X.509 extension)
  BOOLEAN true
  OCTET STRING (4 byte) 03020640
    BIT STRING (2 bit) 01
SEQUENCE (2 elem)
  OBJECT IDENTIFIER 2.5.29.37 extKeyUsage (X.509 extension)
  OCTET STRING (12 byte) 300A06082B06010505070304
    SEQUENCE (1 elem)
      OBJECT IDENTIFIER 1.3.6.1.5.5.7.3.4 emailProtection (PKIX key purpose)
SEQUENCE (2 elem)
```

```
OBJECT IDENTIFIER 2.5.29.17 subjectAltName (X.509 extension)
OCTET STRING (210 byte) 3081CF8110656D61696C407072756562612E636F6DA481BA3081B7311F301D060A2B0…
  SEQUENCE (2 elem)
    [1] (16 byte) email@prueba.com
    [4] (1 elem)
      SEQUENCE (7 elem)
        SET (1 elem)
          SEQUENCE (2 elem)
            OBJECT IDENTIFIER 1.3.6.1.4.1.26852.2.12
            UTF8String IDCES-12345678Z
        SET (1 elem)
          SEQUENCE (2 elem)
            OBJECT IDENTIFIER 1.3.6.1.4.1.26852.2.11
            UTF8String Apellido2
        SET (1 elem)
          SEQUENCE (2 elem)
            OBJECT IDENTIFIER 1.3.6.1.4.1.26852.2.10
            UTF8String Apellido1
        SET (1 elem)
          SEQUENCE (2 elem)
            OBJECT IDENTIFIER 1.3.6.1.4.1.26852.2.9
            UTF8String Nombre
        SET (1 elem)
          SEQUENCE (2 elem)
            OBJECT IDENTIFIER 1.3.6.1.4.1.26852.2.3
            UTF8String 00003
        SET (1 elem)
          SEQUENCE (2 elem)
            OBJECT IDENTIFIER 1.3.6.1.4.1.26852.2.2
            UTF8String Colegio
        SET (1 elem)
          SEQUENCE (2 elem)
```

```
                    OBJECT IDENTIFIER 1.3.6.1.4.1.26852.2.1
                    UTF8String 000035
SEQUENCE (2 elem)
  OBJECT IDENTIFIER 1.2.840.113549.1.1.13 sha512WithRSAEncryption (PKCS #1)
  NULL
```

10.3 Para cifrado

```
SEQUENCE (3 elem)
  SEQUENCE (8 elem)
    [0] (1 elem)
      INTEGER 2
    INTEGER (63 bit) 4824211083861723780
    SEQUENCE (2 elem)
      OBJECT IDENTIFIER 1.2.840.113549.1.1.13 sha512WithRSAEncryption (PKCS #1)
      NULL
    SEQUENCE (7 elem)
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.6 countryName (X.520 DN component)
          PrintableString ES
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.8 stateOrProvinceName (X.520 DN component)
          UTF8String MADRID
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.7 localityName (X.520 DN component)
          UTF8String MADRID
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.97
          UTF8String VATES-Q2866017C
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.11 organizationalUnitName (X.520 DN component)
```

```
        UTF8String ENTIDAD DE CERTIFICACION
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.10 organizationName (X.520 DN component)
        UTF8String CONSEJO GENERAL DE COLEGIOS OFICIALES DE MEDICOS
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.3 commonName (X.520 DN component)
        UTF8String CGCOM QUALIFIED 2020
  SEQUENCE (2 elem)
    UTCTime 2020-03-02 12:57:45 UTC
    UTCTime 2023-03-02 12:57:45 UTC
  SEQUENCE (11 elem)
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.13 description (X.520 DN component)
        UTF8String Reg: XXX /Hoja: XXX /Tomo:XXX /Fecha: dd mm aaaa /Inscripción: XXX
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.3 commonName (X.520 DN component)
        UTF8String 12345678Z Nombre Apellidos (R: Q00000001) (CIFRADO)
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.5 serialNumber (X.520 DN component)
        PrintableString IDCES-12345678Z
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.42 givenName (X.520 DN component)
        UTF8String Nombre
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.4 surname (X.520 DN component)
```

```
        UTF8String apellido1 apellido2
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.12 title (X.520 DN component)
        UTF8String PERSONA FÍSICA REPRESENTANTE
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.11 organizationalUnitName (X.520 DN component)
        UTF8String UnidadOrganizativa2
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.11 organizationalUnitName (X.520 DN component)
        UTF8String UnidadOrganizativa
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.97
        UTF8String VATES-Q0000001
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.10 organizationName (X.520 DN component)
        UTF8String NombreColegio
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.6 countryName (X.520 DN component)
        PrintableString ES
  SEQUENCE (2 elem)
    SEQUENCE (2 elem)
      OBJECT IDENTIFIER 1.2.840.113549.1.1.1 rsaEncryption (PKCS #1)
      NULL
    BIT STRING (2160 bit) 001100001000001000000001000010100000001010000010000000010000000100000…
      SEQUENCE (2 elem)
        INTEGER (2048 bit) 261389622656441211290622956155083819401016706181855506699745213881228…
```

```
        INTEGER 65537
    [3] (1 elem)
      SEQUENCE (9 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 1.3.6.1.5.5.7.1.1 authorityInfoAccess (PKIX private extension)
          OCTET STRING (99 byte) 3061303606082B06010505073002862A687474703A2F2F7073632E6367636F6D2E6573…
            SEQUENCE (2 elem)
              SEQUENCE (2 elem)
                OBJECT IDENTIFIER 1.3.6.1.5.5.7.48.2 caIssuers (PKIX subject/authority info access descriptor)
                [6] (42 byte) http://psc.cgcom.es/CA/root_cgcom_2020.crt
              SEQUENCE (2 elem)
                OBJECT IDENTIFIER 1.3.6.1.5.5.7.48.1 ocsp (PKIX)
                [6] (27 byte) http://ocspservice.cgcom.es
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.29.14 subjectKeyIdentifier (X.509 extension)
          OCTET STRING (20 byte) DA3D1CC29597BD23186C8A96EAF1B3A1ACC59D62
            OCTET STRING (20 byte) DA3D1CC29597BD23186C8A96EAF1B3A1ACC59D62
        SEQUENCE (3 elem)
          OBJECT IDENTIFIER 2.5.29.19 basicConstraints (X.509 extension)
          BOOLEAN true
          OCTET STRING (2 byte) 3000
            SEQUENCE (0 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.29.35 authorityKeyIdentifier (X.509 extension)
          OCTET STRING (24 byte) 3016801432416494D42D413ACDEB2B7209EBAB8D883AD1CF
            SEQUENCE (1 elem)
              [0] (20 byte) 32416494D42D413ACDEB2B7209EBAB8D883AD1CF
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.29.32 certificatePolicies (X.509 extension)
          OCTET STRING (156 byte) 30819930818B060C2B0601040181D16401010B03307B302406082B060105050702011…
            SEQUENCE (2 elem)
              SEQUENCE (2 elem)
```

```
            OBJECT IDENTIFIER 1.3.6.1.4.1.26852.1.1.11.3
            SEQUENCE (2 elem)
              SEQUENCE (2 elem)
                OBJECT IDENTIFIER 1.3.6.1.5.5.7.2.1 cps (PKIX policy qualifier)
                IA5String https://psc.cgcom.es/dpc
              SEQUENCE (2 elem)
                OBJECT IDENTIFIER 1.3.6.1.5.5.7.2.2 unotice (PKIX policy qualifier)
                SEQUENCE (1 elem)
                  UTF8String "CERTIFICADO PARA EL CIFRADO DEL REPRESENTANTE DE PJ, EN TARJETA"
          SEQUENCE (1 elem)
            OBJECT IDENTIFIER 2.16.724.1.3.5.8
    SEQUENCE (2 elem)
      OBJECT IDENTIFIER 2.5.29.31 cRLDistributionPoints (X.509 extension)
      OCTET STRING (90 byte) 3058302AA028A0268624687474703A2F2F63726C352E6367636F6D2E65732F63726C2F…
        SEQUENCE (2 elem)
          SEQUENCE (1 elem)
            [0] (1 elem)
              [0] (1 elem)
                [6] (36 byte) http://crl5.cgcom.es/crl/eccgcom.crl
          SEQUENCE (1 elem)
            [0] (1 elem)
              [0] (1 elem)
                [6] (36 byte) http://crl6.cgcom.es/crl/eccgcom.crl
    SEQUENCE (3 elem)
      OBJECT IDENTIFIER 2.5.29.15 keyUsage (X.509 extension)
      BOOLEAN true
      OCTET STRING (4 byte) 03020520
        BIT STRING (3 bit) 001
    SEQUENCE (2 elem)
      OBJECT IDENTIFIER 2.5.29.37 extKeyUsage (X.509 extension)
      OCTET STRING (12 byte) 300A06082B06010505070304
        SEQUENCE (1 elem)
```

```
        OBJECT IDENTIFIER 1.3.6.1.5.5.7.3.4 emailProtection (PKIX key purpose)
    SEQUENCE (2 elem)
      OBJECT IDENTIFIER 2.5.29.17 subjectAltName (X.509 extension)
      OCTET STRING (210 byte) 3081CF8110656D61696C407072756562612E636F6DA481BA3081B7311F301D060A2B0…
        SEQUENCE (2 elem)
          [1] (16 byte) email@prueba.com
          [4] (1 elem)
            SEQUENCE (7 elem)
              SET (1 elem)
                SEQUENCE (2 elem)
                  OBJECT IDENTIFIER 1.3.6.1.4.1.26852.2.12
                  UTF8String IDCES-12345678Z
              SET (1 elem)
                SEQUENCE (2 elem)
                  OBJECT IDENTIFIER 1.3.6.1.4.1.26852.2.11
                  UTF8String Apellido2
              SET (1 elem)
                SEQUENCE (2 elem)
                  OBJECT IDENTIFIER 1.3.6.1.4.1.26852.2.10
                  UTF8String Apellido1
              SET (1 elem)
                SEQUENCE (2 elem)
                  OBJECT IDENTIFIER 1.3.6.1.4.1.26852.2.9
                  UTF8String Nombre
              SET (1 elem)
                SEQUENCE (2 elem)
                  OBJECT IDENTIFIER 1.3.6.1.4.1.26852.2.3
                  UTF8String 00003
              SET (1 elem)
                SEQUENCE (2 elem)
                  OBJECT IDENTIFIER 1.3.6.1.4.1.26852.2.2
                  UTF8String Colegio
```

```
                  SET (1 elem)
                    SEQUENCE (2 elem)
                      OBJECT IDENTIFIER 1.3.6.1.4.1.26852.2.1
                      UTF8String 000035
  SEQUENCE (2 elem)
    OBJECT IDENTIFIER 1.2.840.113549.1.1.13 sha512WithRSAEncryption (PKCS #1)
    NULL
```

11. Certificado de Persona Física Representante, en nube

```
SEQUENCE (3 elem)
  SEQUENCE (8 elem)
    [0] (1 elem)
      INTEGER 2
    INTEGER (62 bit) 3384215515672259242
    SEQUENCE (2 elem)
      OBJECT IDENTIFIER 1.2.840.113549.1.1.13 sha512WithRSAEncryption (PKCS #1)
      NULL
    SEQUENCE (7 elem)
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.6 countryName (X.520 DN component)
          PrintableString ES
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.8 stateOrProvinceName (X.520 DN component)
          UTF8String MADRID
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.7 localityName (X.520 DN component)
          UTF8String MADRID
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.97
          UTF8String VATES-Q2866017C
      SET (1 elem)
        SEQUENCE (2 elem)
```

```
        OBJECT IDENTIFIER 2.5.4.11 organizationalUnitName (X.520 DN component)
        UTF8String ENTIDAD DE CERTIFICACION
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.10 organizationName (X.520 DN component)
        UTF8String CONSEJO GENERAL DE COLEGIOS OFICIALES DE MEDICOS
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.3 commonName (X.520 DN component)
        UTF8String CGCOM QUALIFIED 2020
  SEQUENCE (2 elem)
    UTCTime 2020-03-02 12:53:03 UTC
    UTCTime 2023-03-02 12:53:03 UTC
  SEQUENCE (11 elem)
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.13 description (X.520 DN component)
        UTF8String Reg: XXX /Hoja: XXX /Tomo:XXX /Fecha: dd mm aaaa /Inscripción: XXX
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.3 commonName (X.520 DN component)
        UTF8String 12345678Z Nombre Apellidos (R: Q00000001)
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.5 serialNumber (X.520 DN component)
        PrintableString IDCES-12345678Z
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.42 givenName (X.520 DN component)
        UTF8String Nombre
    SET (1 elem)
      SEQUENCE (2 elem)
```

```
        OBJECT IDENTIFIER 2.5.4.4 surname (X.520 DN component)
        UTF8String apellido1 apellido2
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.12 title (X.520 DN component)
        UTF8String PERSONA FÍSICA REPRESENTANTE
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.11 organizationalUnitName (X.520 DN component)
        UTF8String UnidadOrganizativa2
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.11 organizationalUnitName (X.520 DN component)
        UTF8String UnidadOrganizativa
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.97
        UTF8String VATES-Q0000001
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.10 organizationName (X.520 DN component)
        UTF8String NombreColegio
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.6 countryName (X.520 DN component)
        PrintableString ES
  SEQUENCE (2 elem)
    SEQUENCE (2 elem)
      OBJECT IDENTIFIER 1.2.840.113549.1.1.1 rsaEncryption (PKCS #1)
      NULL
    BIT STRING (2160 bit) 001100001000001000000001000010100000001010000010000000010000000100000…
      SEQUENCE (2 elem)
```

```
        INTEGER (2048 bit) 28120724813154891846124868614368515413270629037027842436998874362879 6…
        INTEGER 65537
    [3] (1 elem)
      SEQUENCE (10 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 1.3.6.1.5.5.7.1.1 authorityInfoAccess (PKIX private extension)
          OCTET STRING (99 byte) 3061303606082B06010505073002862A687474703A2F2F7073632E6367636F6D2E6573…
            SEQUENCE (2 elem)
              SEQUENCE (2 elem)
                OBJECT IDENTIFIER 1.3.6.1.5.5.7.48.2 caIssuers (PKIX subject/authority info access descriptor)
                [6] (42 byte) http://psc.cgcom.es/CA/root_cgcom_2020.crt
              SEQUENCE (2 elem)
                OBJECT IDENTIFIER 1.3.6.1.5.5.7.48.1 ocsp (PKIX)
                [6] (27 byte) http://ocspservice.cgcom.es
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.29.14 subjectKeyIdentifier (X.509 extension)
          OCTET STRING (20 byte) A931F351F6FF85E1EFFA49DF57B219A9BA1C3FBE
            OCTET STRING (20 byte) A931F351F6FF85E1EFFA49DF57B219A9BA1C3FBE
        SEQUENCE (3 elem)
          OBJECT IDENTIFIER 2.5.29.19 basicConstraints (X.509 extension)
          BOOLEAN true
          OCTET STRING (2 byte) 3000
            SEQUENCE (0 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.29.35 authorityKeyIdentifier (X.509 extension)
          OCTET STRING (24 byte) 3016801432416494D42D413ACDEB2B7209EBAB8D883AD1CF
            SEQUENCE (1 elem)
              [0] (20 byte) 32416494D42D413ACDEB2B7209EBAB8D883AD1CF
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 1.3.6.1.5.5.7.1.3 qcStatements (PKIX private extension)
          OCTET STRING (159 byte) 30819C301506082B06010505070B023009060704008BEC4901013008060604008E460…
            SEQUENCE (6 elem)
```

```
            SEQUENCE (2 elem)
              OBJECT IDENTIFIER 1.3.6.1.5.5.7.11.2
              SEQUENCE (1 elem)
                OBJECT IDENTIFIER 0.4.0.194121.1.1
            SEQUENCE (1 elem)
              OBJECT IDENTIFIER 0.4.0.1862.1.1 etsiQcsCompliance (ETSI TS 101 862 qualified certificates)
            SEQUENCE (2 elem)
              OBJECT IDENTIFIER 0.4.0.1862.1.3 etsiQcsRetentionPeriod (ETSI TS 101 862 qualified certificates)
              INTEGER 15
            SEQUENCE (1 elem)
              OBJECT IDENTIFIER 0.4.0.1862.1.4 etsiQcsQcSSCD (ETSI TS 101 862 qualified certificates)
            SEQUENCE (2 elem)
              OBJECT IDENTIFIER 0.4.0.1862.1.6
              SEQUENCE (1 elem)
                OBJECT IDENTIFIER 0.4.0.1862.1.6.1
            SEQUENCE (2 elem)
              OBJECT IDENTIFIER 0.4.0.1862.1.5
              SEQUENCE (2 elem)
                SEQUENCE (2 elem)
                  IA5String https://psc.cgcom.es/en/pds
                  PrintableString en
                SEQUENCE (2 elem)
                  IA5String https://psc.cgcom.es/pds
                  PrintableString es
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.29.32 certificatePolicies (X.509 extension)
          OCTET STRING (154 byte) 308197307F060B2B0601040181D16401010C3070302406082B060105050702011618…
            SEQUENCE (3 elem)
              SEQUENCE (2 elem)
                OBJECT IDENTIFIER 1.3.6.1.4.1.26852.1.1.12
                SEQUENCE (2 elem)
                  SEQUENCE (2 elem)
```

```
                OBJECT IDENTIFIER 1.3.6.1.5.5.7.2.1 cps (PKIX policy qualifier)
                IA5String https://psc.cgcom.es/dpc
              SEQUENCE (2 elem)
                OBJECT IDENTIFIER 1.3.6.1.5.5.7.2.2 unotice (PKIX policy qualifier)
                SEQUENCE (1 elem)
                  UTF8String "CERTIFICADO CUALIFICADO DE REPRESENTANTE PJ, EN DCCF"
        SEQUENCE (1 elem)
          OBJECT IDENTIFIER 0.4.0.194112.1.2
        SEQUENCE (1 elem)
          OBJECT IDENTIFIER 2.16.724.1.3.5.8
SEQUENCE (2 elem)
  OBJECT IDENTIFIER 2.5.29.31 cRLDistributionPoints (X.509 extension)
  OCTET STRING (90 byte) 3058302AA028A0268624687474703A2F2F63726C352E6367636F6D2E65732F63726C2F…
    SEQUENCE (2 elem)
      SEQUENCE (1 elem)
        [0] (1 elem)
          [0] (1 elem)
            [6] (36 byte) http://crl5.cgcom.es/crl/eccgcom.crl
      SEQUENCE (1 elem)
        [0] (1 elem)
          [0] (1 elem)
            [6] (36 byte) http://crl6.cgcom.es/crl/eccgcom.crl
SEQUENCE (3 elem)
  OBJECT IDENTIFIER 2.5.29.15 keyUsage (X.509 extension)
  BOOLEAN true
  OCTET STRING (4 byte) 030206C0
    BIT STRING (2 bit) 11
SEQUENCE (2 elem)
  OBJECT IDENTIFIER 2.5.29.37 extKeyUsage (X.509 extension)
  OCTET STRING (22 byte) 301406082B06010505070302060 82B06010505070304
    SEQUENCE (2 elem)
      OBJECT IDENTIFIER 1.3.6.1.5.5.7.3.2 clientAuth (PKIX key purpose)
```

```
        OBJECT IDENTIFIER 1.3.6.1.5.5.7.3.4 emailProtection (PKIX key purpose)
    SEQUENCE (2 elem)
      OBJECT IDENTIFIER 2.5.29.17 subjectAltName (X.509 extension)
      OCTET STRING (210 byte) 3081CF8110656D61696C407072756562612E636F6DA481BA3081B7311F301D060A2B0…
        SEQUENCE (2 elem)
          [1] (16 byte) email@prueba.com
          [4] (1 elem)
            SEQUENCE (7 elem)
              SET (1 elem)
                SEQUENCE (2 elem)
                  OBJECT IDENTIFIER 1.3.6.1.4.1.26852.2.12
                  UTF8String IDCES-12345678Z
              SET (1 elem)
                SEQUENCE (2 elem)
                  OBJECT IDENTIFIER 1.3.6.1.4.1.26852.2.11
                  UTF8String Apellido2
              SET (1 elem)
                SEQUENCE (2 elem)
                  OBJECT IDENTIFIER 1.3.6.1.4.1.26852.2.10
                  UTF8String Apellido1
              SET (1 elem)
                SEQUENCE (2 elem)
                  OBJECT IDENTIFIER 1.3.6.1.4.1.26852.2.9
                  UTF8String Nombre
              SET (1 elem)
                SEQUENCE (2 elem)
                  OBJECT IDENTIFIER 1.3.6.1.4.1.26852.2.3
                  UTF8String 00003
              SET (1 elem)
                SEQUENCE (2 elem)
                  OBJECT IDENTIFIER 1.3.6.1.4.1.26852.2.2
                  UTF8String Colegio
```

```
                  SET (1 elem)
                    SEQUENCE (2 elem)
                      OBJECT IDENTIFIER 1.3.6.1.4.1.26852.2.1
                      UTF8String 000035
SEQUENCE (2 elem)
  OBJECT IDENTIFIER 1.2.840.113549.1.1.13 sha512WithRSAEncryption (PKCS #1)
  NULL
```

12. Certificado de persona física representante en software

```
SEQUENCE (3 elem)
  SEQUENCE (8 elem)
    [0] (1 elem)
      INTEGER 2
    INTEGER (159 bit) 394058079430449106403318884058571534318369730762
    SEQUENCE (2 elem)
      OBJECT IDENTIFIER 1.2.840.113549.1.1.13 sha512WithRSAEncryption (PKCS #1)
      NULL
    SEQUENCE (7 elem)
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.6 countryName (X.520 DN component)
          PrintableString ES
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.8 stateOrProvinceName (X.520 DN component)
          UTF8String MADRID
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.7 localityName (X.520 DN component)
          UTF8String MADRID
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.97 organizationIdentifier (X.520 DN component)
          UTF8String VATES-Q2866017C
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.11 organizationalUnitName (X.520 DN component)
          UTF8String ENTIDAD DE CERTIFICACION
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.10 organizationName (X.520 DN component)
          UTF8String CONSEJO GENERAL DE COLEGIOS OFICIALES DE MEDICOS
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.3 commonName (X.520 DN component)
```

```
        UTF8String CGCOM QUALIFIED 2020
    SEQUENCE (2 elem)
      UTCTime 2022-03-24 11:11:11 UTC
      UTCTime 2023-03-24 11:11:11 UTC
    SEQUENCE (8 elem)
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.13 description (X.520 DN component)
          UTF8String Reg: XXX /Hoja: XXX /Tomo:XXX /Sección:XXX /Libro:XXX /Folio:XXX /Fecha: dd mm a…
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.3 commonName (X.520 DN component)
          UTF8String 123456789Z NOMBRE APELLIDOUNO APELLIDODOS (R: Q0000000J)
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.5 serialNumber (X.520 DN component)
          PrintableString IDCES-123456789Z
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.42 givenName (X.520 DN component)
          UTF8String NOMBRE
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.4 surname (X.520 DN component)
          UTF8String APELLIDOUNO APELLIDODOS
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.97 organizationIdentifier (X.520 DN component)
          UTF8String VATES-Q0000000J
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.10 organizationName (X.520 DN component)
          UTF8String COLEGIO DE MEDICOS DE TEST
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.6 countryName (X.520 DN component)
          PrintableString ES
    SEQUENCE (2 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 1.2.840.113549.1.1.1 rsaEncryption (PKCS #1)
        NULL
      BIT STRING (2160 bit) 001100001000001000000001000010100000001010000010000000010000000100000…
```

```
      SEQUENCE (2 elem)
        INTEGER (2048 bit) 279953973516322533167593311147781931606016977721072330116613588954266…
        INTEGER 65537
    [3] (1 elem)
      SEQUENCE (11 elem)
        SEQUENCE (3 elem)
          OBJECT IDENTIFIER 2.5.29.19 basicConstraints (X.509 extension)
          BOOLEAN true
          OCTET STRING (2 byte) 3000
            SEQUENCE (0 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.29.35 authorityKeyIdentifier (X.509 extension)
          OCTET STRING (24 byte) 3016801432416494D42D413ACDEB2B7209EBAB8D883AD1CF
            SEQUENCE (1 elem)
              [0] (20 byte) 32416494D42D413ACDEB2B7209EBAB8D883AD1CF
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 1.3.6.1.5.5.7.1.1 authorityInfoAccess (PKIX private extension)
          OCTET STRING (99 byte) 3061303606082B06010505073002862A687474703A2F2F7073632E6367636F6D2E6573…
            SEQUENCE (2 elem)
              SEQUENCE (2 elem)
                OBJECT IDENTIFIER 1.3.6.1.5.5.7.48.2 caIssuers (PKIX subject/authority info access descriptor)
                [6] (42 byte) http://psc.cgcom.es/CA/root_cgcom_2020.crt
              SEQUENCE (2 elem)
                OBJECT IDENTIFIER 1.3.6.1.5.5.7.48.1 ocsp (PKIX)
                [6] (27 byte) http://ocspservice.cgcom.es
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.29.18 issuerAltName (X.509 extension)
          OCTET STRING (22 byte) 30148112696E666F4076696E63617369676E2E6E6574
            SEQUENCE (1 elem)
              [1] (18 byte) info@vincasign.net
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.29.17 subjectAltName (X.509 extension)
          OCTET STRING (228 byte) 3081E1811A6E6F6D6272652E6170756E6F6170646F73406367636F6D2E6573A481C23…
            SEQUENCE (2 elem)
              [1] (26 byte) nombre.apunoapdos@cgcom.es
              [4] (1 elem)
                SEQUENCE (6 elem)
                  SET (1 elem)
                    SEQUENCE (2 elem)
                      OBJECT IDENTIFIER 1.3.6.1.4.1.26852.2.1
                      UTF8String IDCOLEGIOTEST
                  SET (1 elem)
```

```
                SEQUENCE (2 elem)
                  OBJECT IDENTIFIER 1.3.6.1.4.1.26852.2.2
                  UTF8String COLEGIO DE MEDICOS DE TEST
              SET (1 elem)
                SEQUENCE (2 elem)
                  OBJECT IDENTIFIER 1.3.6.1.4.1.26852.2.9
                  UTF8String NOMBRE
              SET (1 elem)
                SEQUENCE (2 elem)
                  OBJECT IDENTIFIER 1.3.6.1.4.1.26852.2.10
                  UTF8String APELLIDOUNO
              SET (1 elem)
                SEQUENCE (2 elem)
                  OBJECT IDENTIFIER 1.3.6.1.4.1.26852.2.11
                  UTF8String APELLIDODOS
              SET (1 elem)
                SEQUENCE (2 elem)
                  OBJECT IDENTIFIER 1.3.6.1.4.1.26852.2.12
                  UTF8String IDCES-123456789Z
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.29.32 certificatePolicies (X.509 extension)
        OCTET STRING (166 byte) 3081A330818A060C2B0601040181D16401010B05307A304606082B060105050702023…
          SEQUENCE (3 elem)
            SEQUENCE (2 elem)
              OBJECT IDENTIFIER 1.3.6.1.4.1.26852.1.1.11.5
              SEQUENCE (2 elem)
                SEQUENCE (2 elem)
                  OBJECT IDENTIFIER 1.3.6.1.5.5.7.2.2 unotice (PKIX policy qualifier)
                  SEQUENCE (1 elem)
                    UTF8String CERTIFICADO CUALIFICADO DE REPRESENTANTE PJ, EN SOFTWARE
                SEQUENCE (2 elem)
                  OBJECT IDENTIFIER 1.3.6.1.5.5.7.2.1 cps (PKIX policy qualifier)
                  IA5String https://psc.cgcom.es/declaracion_dpc
            SEQUENCE (1 elem)
              OBJECT IDENTIFIER 0.4.0.194112.1.0
            SEQUENCE (1 elem)
              OBJECT IDENTIFIER 2.16.724.1.3.5.8
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.29.37 extKeyUsage (X.509 extension)
        OCTET STRING (22 byte) 301406082B060105050703020 6082B06010505070304
          SEQUENCE (2 elem)
            OBJECT IDENTIFIER 1.3.6.1.5.5.7.3.2 clientAuth (PKIX key purpose)
```

```
            OBJECT IDENTIFIER 1.3.6.1.5.5.7.3.4 emailProtection (PKIX key purpose)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 1.3.6.1.5.5.7.1.3 qcStatements (PKIX private extension)
          OCTET STRING (35 byte) 3021301506082B06010505070B023009060704008BEC4901013008060604008E460101
            SEQUENCE (2 elem)
              SEQUENCE (2 elem)
                OBJECT IDENTIFIER 1.3.6.1.5.5.7.11.2 pkixQCSyntax-v2 (PKIX qualified certificates)
                SEQUENCE (1 elem)
                  OBJECT IDENTIFIER 0.4.0.194121.1.1
              SEQUENCE (1 elem)
                OBJECT IDENTIFIER 0.4.0.1862.1.1 etsiQcsCompliance (ETSI TS 101 862 qualified certificates)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.29.31 cRLDistributionPoints (X.509 extension)
          OCTET STRING (90 byte) 3058302AA028A0268624687474703A2F2F63726C352E6367636F6D2E65732F63726C2F…
            SEQUENCE (2 elem)
              SEQUENCE (1 elem)
                [0] (1 elem)
                  [0] (1 elem)
                    [6] (36 byte) http://crl5.cgcom.es/crl/eccgcom.crl
              SEQUENCE (1 elem)
                [0] (1 elem)
                  [0] (1 elem)
                    [6] (36 byte) http://crl6.cgcom.es/crl/eccgcom.crl
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.29.14 subjectKeyIdentifier (X.509 extension)
          OCTET STRING (22 byte) 0414DC3FBD532F6EDE8A2A7E2BB729A30C2337C413A3
            OCTET STRING (20 byte) DC3FBD532F6EDE8A2A7E2BB729A30C2337C413A3
        SEQUENCE (3 elem)
          OBJECT IDENTIFIER 2.5.29.15 keyUsage (X.509 extension)
          BOOLEAN true
          OCTET STRING (4 byte) 030206C0
Offset: 1751
Length: 2+4
(encapsulates)
Value:
(4 byte)
030206C0
            BIT STRING (2 bit) 11
  SEQUENCE (2 elem)
    OBJECT IDENTIFIER 1.2.840.113549.1.1.13 sha512WithRSAEncryption (PKCS #1)
    NULL
```

13. Certificado de Sello electrónico de Persona Jurídica, en Nube

```
SEQUENCE (3 elem)
  SEQUENCE (8 elem)
    [0] (1 elem)
      INTEGER 2
    INTEGER (63 bit) 4632926126371875612
    SEQUENCE (2 elem)
      OBJECT IDENTIFIER 1.2.840.113549.1.1.13 sha512WithRSAEncryption (PKCS #1)
      NULL
    SEQUENCE (7 elem)
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.6 countryName (X.520 DN component)
          PrintableString ES
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.8 stateOrProvinceName (X.520 DN component)
          UTF8String MADRID
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.7 localityName (X.520 DN component)
          UTF8String MADRID
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.97
          UTF8String VATES-Q2866017C
      SET (1 elem)
        SEQUENCE (2 elem)
```

```
        OBJECT IDENTIFIER 2.5.4.11 organizationalUnitName (X.520 DN component)
        UTF8String ENTIDAD DE CERTIFICACION
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.10 organizationName (X.520 DN component)
        UTF8String CONSEJO GENERAL DE COLEGIOS OFICIALES DE MEDICOS
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.3 commonName (X.520 DN component)
        UTF8String CGCOM QUALIFIED 2020
  SEQUENCE (2 elem)
    UTCTime 2020-03-02 13:42:54 UTC
    UTCTime 2022-03-02 13:42:54 UTC
  SEQUENCE (6 elem)
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.3 commonName (X.520 DN component)
        UTF8String Organizacion (Q0000001)
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.11 organizationalUnitName (X.520 DN component)
        UTF8String UnidadOrganizativa
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.11 organizationalUnitName (X.520 DN component)
        UTF8String SELLO ELECTRONICO
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.97
        UTF8String VATES-Q0000001
    SET (1 elem)
      SEQUENCE (2 elem)
```

```
        OBJECT IDENTIFIER 2.5.4.10 organizationName (X.520 DN component)
        UTF8String ColegioProfesional
    SET (1 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.4.6 countryName (X.520 DN component)
        PrintableString ES
  SEQUENCE (2 elem)
    SEQUENCE (2 elem)
      OBJECT IDENTIFIER 1.2.840.113549.1.1.1 rsaEncryption (PKCS #1)
      NULL
    BIT STRING (2160 bit) 001100001000001000000001000010100000001010000010000000010000000100000…
      SEQUENCE (2 elem)
        INTEGER (2048 bit) 22907018030934378213256523518543497579725700149477212272287520239431 5…
        INTEGER 65537
  [3] (1 elem)
    SEQUENCE (10 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 1.3.6.1.5.5.7.1.1 authorityInfoAccess (PKIX private extension)
        OCTET STRING (99 byte) 3061303606082B06010505073002862A687474703A2F2F7073632E6367636F6D2E6573…
          SEQUENCE (2 elem)
            SEQUENCE (2 elem)
              OBJECT IDENTIFIER 1.3.6.1.5.5.7.48.2 caIssuers (PKIX subject/authority info access descriptor)
              [6] (42 byte) http://psc.cgcom.es/CA/root_cgcom_2020.crt
            SEQUENCE (2 elem)
              OBJECT IDENTIFIER 1.3.6.1.5.5.7.48.1 ocsp (PKIX)
              [6] (27 byte) http://ocspservice.cgcom.es
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 2.5.29.14 subjectKeyIdentifier (X.509 extension)
        OCTET STRING (20 byte) B4844A34A3249BA2F3BAE4FD856D3D64EECD5180
          OCTET STRING (20 byte) B4844A34A3249BA2F3BAE4FD856D3D64EECD5180
      SEQUENCE (3 elem)
        OBJECT IDENTIFIER 2.5.29.19 basicConstraints (X.509 extension)
```

```
    BOOLEAN true
    OCTET STRING (2 byte) 3000
      SEQUENCE (0 elem)
  SEQUENCE (2 elem)
    OBJECT IDENTIFIER 2.5.29.35 authorityKeyIdentifier (X.509 extension)
    OCTET STRING (24 byte) 3016801432416494D42D413ACDEB2B7209EBAB8D883AD1CF
      SEQUENCE (1 elem)
        [0] (20 byte) 32416494D42D413ACDEB2B7209EBAB8D883AD1CF
  SEQUENCE (2 elem)
    OBJECT IDENTIFIER 1.3.6.1.5.5.7.1.3 qcStatements (PKIX private extension)
    OCTET STRING (159 byte) 30819C301506082B06010505070B023009060704008BEC490101300806060400 8E460…
      SEQUENCE (6 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 1.3.6.1.5.5.7.11.2
          SEQUENCE (1 elem)
            OBJECT IDENTIFIER 0.4.0.194121.1.1
        SEQUENCE (1 elem)
          OBJECT IDENTIFIER 0.4.0.1862.1.1 etsiQcsCompliance (ETSI TS 101 862 qualified certificates)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 0.4.0.1862.1.3 etsiQcsRetentionPeriod (ETSI TS 101 862 qualified certificates)
          INTEGER 15
        SEQUENCE (1 elem)
          OBJECT IDENTIFIER 0.4.0.1862.1.4 etsiQcsQcSSCD (ETSI TS 101 862 qualified certificates)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 0.4.0.1862.1.6
          SEQUENCE (1 elem)
            OBJECT IDENTIFIER 0.4.0.1862.1.6.2
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 0.4.0.1862.1.5
          SEQUENCE (2 elem)
            SEQUENCE (2 elem)
              IA5String https://psc.cgcom.es/en/pds
```

```
                    PrintableString en
                  SEQUENCE (2 elem)
                    IA5String https://psc.cgcom.es/pds
                    PrintableString es
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.29.32 certificatePolicies (X.509 extension)
          OCTET STRING (221 byte) 3081DA3081CC060C2B0601040181D16401010A023081BB302406082B0601050507020…
            SEQUENCE (2 elem)
              SEQUENCE (2 elem)
                OBJECT IDENTIFIER 1.3.6.1.4.1.26852.1.1.10.2
                SEQUENCE (2 elem)
                  SEQUENCE (2 elem)
                    OBJECT IDENTIFIER 1.3.6.1.5.5.7.2.1 cps (PKIX policy qualifier)
                    IA5String https://psc.cgcom.es/dpc
                  SEQUENCE (2 elem)
                    OBJECT IDENTIFIER 1.3.6.1.5.5.7.2.2 unotice (PKIX policy qualifier)
                    SEQUENCE (1 elem)
                      UTF8String CERTIFICADO CUALIFICADO DE SELLO ELECTRONICO PARA LA ACTUACION AUTOMATIZADA CON
…
              SEQUENCE (1 elem)
                OBJECT IDENTIFIER 0.4.0.194112.1.3
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.29.31 cRLDistributionPoints (X.509 extension)
          OCTET STRING (90 byte) 3058302AA028A0268624687474703A2F2F63726C352E6367636F6D2E65732F63726C2F…
            SEQUENCE (2 elem)
              SEQUENCE (1 elem)
                [0] (1 elem)
                  [0] (1 elem)
                    [6] (36 byte) http://crl5.cgcom.es/crl/eccgcom.crl
              SEQUENCE (1 elem)
                [0] (1 elem)
                  [0] (1 elem)
```

```
                    [6] (36 byte) http://crl6.cgcom.es/crl/eccgcom.crl
        SEQUENCE (3 elem)
          OBJECT IDENTIFIER 2.5.29.15 keyUsage (X.509 extension)
          BOOLEAN true
          OCTET STRING (4 byte) 030206C0
            BIT STRING (2 bit) 11
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.29.37 extKeyUsage (X.509 extension)
          OCTET STRING (22 byte) 301406082B06010505070302060 82B06010505070304
            SEQUENCE (2 elem)
              OBJECT IDENTIFIER 1.3.6.1.5.5.7.3.2 clientAuth (PKIX key purpose)
              OBJECT IDENTIFIER 1.3.6.1.5.5.7.3.4 emailProtection (PKIX key purpose)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.29.17 subjectAltName (X.509 extension)
          OCTET STRING (73 byte) 30478110656D61696C407072756562612E636F6DA433303131173015060A2B06010401…
            SEQUENCE (2 elem)
              [1] (16 byte) email@prueba.com
              [4] (1 elem)
                SEQUENCE (2 elem)
                  SET (1 elem)
                    SEQUENCE (2 elem)
                      OBJECT IDENTIFIER 1.3.6.1.4.1.26852.2.2
                      UTF8String Colegio
                  SET (1 elem)
                    SEQUENCE (2 elem)
                      OBJECT IDENTIFIER 1.3.6.1.4.1.26852.2.1
                      UTF8String 000035
SEQUENCE (2 elem)
  OBJECT IDENTIFIER 1.2.840.113549.1.1.13 sha512WithRSAEncryption (PKCS #1)
  NULL
```

14. Certificado de sello electrónico de persona jurídica en software

```
SEQUENCE (3 elem)
  SEQUENCE (8 elem)
    [0] (1 elem)
      INTEGER 2
    INTEGER (159 bit) 374361513477440033720051203112172174676936987779
    SEQUENCE (2 elem)
      OBJECT IDENTIFIER 1.2.840.113549.1.1.13 sha512WithRSAEncryption (PKCS #1)
      NULL
    SEQUENCE (7 elem)
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.6 countryName (X.520 DN component)
          PrintableString ES
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.8 stateOrProvinceName (X.520 DN component)
          UTF8String MADRID
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.7 localityName (X.520 DN component)
          UTF8String MADRID
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.97 organizationIdentifier (X.520 DN component)
          UTF8String VATES-Q2866017C
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.11 organizationalUnitName (X.520 DN component)
          UTF8String ENTIDAD DE CERTIFICACION
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.10 organizationName (X.520 DN component)
          UTF8String CONSEJO GENERAL DE COLEGIOS OFICIALES DE MEDICOS
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.3 commonName (X.520 DN component)
```

```
        UTF8String CGCOM QUALIFIED 2020
    SEQUENCE (2 elem)
      UTCTime 2022-03-24 11:11:35 UTC
      UTCTime 2023-03-24 11:11:35 UTC
    SEQUENCE (5 elem)
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.3 commonName (X.520 DN component)
          UTF8String SELLO ELECTRONICO DE TEST
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.11 organizationalUnitName (X.520 DN component)
          UTF8String SELLO ELECTRONICO
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.97 organizationIdentifier (X.520 DN component)
          UTF8String VATES-Q0000000J
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.10 organizationName (X.520 DN component)
          UTF8String ENTIDAD DE TEST
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.6 countryName (X.520 DN component)
          PrintableString ES
    SEQUENCE (2 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 1.2.840.113549.1.1.1 rsaEncryption (PKCS #1)
        NULL
      BIT STRING (2160 bit) 001100001000001000000001000010100000001010000010000000010000000100000…
        SEQUENCE (2 elem)
          INTEGER (2048 bit) 263719896659486113738912049898643775030978562191660038974404609802335…
          INTEGER 65537
    [3] (1 elem)
      SEQUENCE (11 elem)
        SEQUENCE (3 elem)
          OBJECT IDENTIFIER 2.5.29.19 basicConstraints (X.509 extension)
          BOOLEAN true
          OCTET STRING (2 byte) 3000
            SEQUENCE (0 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.29.35 authorityKeyIdentifier (X.509 extension)
```

```
      OCTET STRING (24 byte) 3016801432416494D42D413ACDEB2B7209EBAB8D883AD1CF
        SEQUENCE (1 elem)
          [0] (20 byte) 32416494D42D413ACDEB2B7209EBAB8D883AD1CF
    SEQUENCE (2 elem)
      OBJECT IDENTIFIER 1.3.6.1.5.5.7.1.1 authorityInfoAccess (PKIX private extension)
      OCTET STRING (99 byte) 3061303606082B06010505073002862A687474703A2F2F7073632E6367636F6D2E6573…
        SEQUENCE (2 elem)
          SEQUENCE (2 elem)
            OBJECT IDENTIFIER 1.3.6.1.5.5.7.48.2 caIssuers (PKIX subject/authority info access descriptor)
            [6] (42 byte) http://psc.cgcom.es/CA/root_cgcom_2020.crt
          SEQUENCE (2 elem)
            OBJECT IDENTIFIER 1.3.6.1.5.5.7.48.1 ocsp (PKIX)
            [6] (27 byte) http://ocspservice.cgcom.es
    SEQUENCE (2 elem)
      OBJECT IDENTIFIER 2.5.29.18 issuerAltName (X.509 extension)
      OCTET STRING (22 byte) 30148112696E666F4076696E63617369676E2E6E6574
        SEQUENCE (1 elem)
          [1] (18 byte) info@vincasign.net
    SEQUENCE (2 elem)
      OBJECT IDENTIFIER 2.5.29.17 subjectAltName (X.509 extension)
      OCTET STRING (101 byte) 3063811273656C6C6F7465737440636763636F6D2E6573A44D304B311D301B060A2B060…
        SEQUENCE (2 elem)
          [1] (18 byte) sellotest@cgcom.es
          [4] (1 elem)
            SEQUENCE (2 elem)
              SET (1 elem)
                SEQUENCE (2 elem)
                  OBJECT IDENTIFIER 1.3.6.1.4.1.26852.2.1
                  UTF8String IDCOLEGIOTEST
              SET (1 elem)
                SEQUENCE (2 elem)
                  OBJECT IDENTIFIER 1.3.6.1.4.1.26852.2.2
                  UTF8String COLEGIO DE MEDICOS DE TEST
    SEQUENCE (2 elem)
      OBJECT IDENTIFIER 2.5.29.32 certificatePolicies (X.509 extension)
      OCTET STRING (193 byte) 3081BE3081B0060C2B0601040181D16401010A0530819F306606082B0601050507020…
        SEQUENCE (2 elem)
          SEQUENCE (2 elem)
            OBJECT IDENTIFIER 1.3.6.1.4.1.26852.1.1.10.5
            SEQUENCE (2 elem)
              SEQUENCE (2 elem)
                OBJECT IDENTIFIER 1.3.6.1.5.5.7.2.2 unotice (PKIX policy qualifier)
```

```
                    SEQUENCE (1 elem)
                      UTF8String CERTIFICADO CUALIFICADO DE SELLO ELECTRONICO PARA LA ACTUACION AUTOMATIZADA, EN
…
                  SEQUENCE (2 elem)
                    OBJECT IDENTIFIER 1.3.6.1.5.5.7.2.1 cps (PKIX policy qualifier)
                    IA5String https://psc-test.cgcom.es/declaracion_dpc
              SEQUENCE (1 elem)
                OBJECT IDENTIFIER 0.4.0.194112.1.1
          SEQUENCE (2 elem)
            OBJECT IDENTIFIER 2.5.29.37 extKeyUsage (X.509 extension)
            OCTET STRING (22 byte) 301406082B06010505070302060 82B06010505070304
              SEQUENCE (2 elem)
                OBJECT IDENTIFIER 1.3.6.1.5.5.7.3.2 clientAuth (PKIX key purpose)
                OBJECT IDENTIFIER 1.3.6.1.5.5.7.3.4 emailProtection (PKIX key purpose)
          SEQUENCE (2 elem)
            OBJECT IDENTIFIER 1.3.6.1.5.5.7.1.3 qcStatements (PKIX private extension)
            OCTET STRING (35 byte) 3021301506082B06010505070B023009060704008BEC4901023008060604008E460101
              SEQUENCE (2 elem)
                SEQUENCE (2 elem)
                  OBJECT IDENTIFIER 1.3.6.1.5.5.7.11.2 pkixQCSyntax-v2 (PKIX qualified certificates)
                  SEQUENCE (1 elem)
                    OBJECT IDENTIFIER 0.4.0.194121.1.2
                SEQUENCE (1 elem)
                  OBJECT IDENTIFIER 0.4.0.1862.1.1 etsiQcsCompliance (ETSI TS 101 862 qualified certificates)
          SEQUENCE (2 elem)
            OBJECT IDENTIFIER 2.5.29.31 cRLDistributionPoints (X.509 extension)
            OCTET STRING (90 byte) 3058302AA028A0268624687474703A2F2F63726C352E6367636F6D2E65732F63726C2F…
              SEQUENCE (2 elem)
                SEQUENCE (1 elem)
                  [0] (1 elem)
                    [0] (1 elem)
                      [6] (36 byte) http://crl5.cgcom.es/crl/eccgcom.crl
                SEQUENCE (1 elem)
                  [0] (1 elem)
                    [0] (1 elem)
                      [6] (36 byte) http://crl6.cgcom.es/crl/eccgcom.crl
          SEQUENCE (2 elem)
            OBJECT IDENTIFIER 2.5.29.14 subjectKeyIdentifier (X.509 extension)
            OCTET STRING (22 byte) 04147897BF86FC52870E13D2FA248AFCB18E5E7BAA94
              OCTET STRING (20 byte) 7897BF86FC52870E13D2FA248AFCB18E5E7BAA94
          SEQUENCE (3 elem)
            OBJECT IDENTIFIER 2.5.29.15 keyUsage (X.509 extension)
```

```
          BOOLEAN true
          OCTET STRING (4 byte) 030206C0
            BIT STRING (2 bit) 11
  SEQUENCE (2 elem)
    OBJECT IDENTIFIER 1.2.840.113549.1.1.13 sha512WithRSAEncryption (PKCS #1)
    NULL
```