

Perfiles de Certificados

ENTIDAD FINAL

Versión 1.2



Control de versiones

Versión	Partes que cambian	Descripción del cambio	Autor del cambio	Fecha del cambio
1.0		Creación documento	vinCAsign	08/03/2016
1.1		Revisión perfiles de REPRESENTANTE para @firma	vinCAsign	27/07/2016
1.2		Cambio de formato. Se incluyen OIDs de políticas europeas y españolas. Se añade perfil de sello electrónico de empresa. Se añade perfil de sello electrónico de IoT.	VinCAsign	20/04/2017

1. Índice

Control de versiones.....	2
1. Índice.....	3
2. Certificado de PERSONA FÍSICA VINCULADA a una Organización	4
3. Certificado de PERSONA FÍSICA REPRESENTANTE de una Organización	13
4. Certificado de PERSONA FÍSICA EMPLEADO PÚBLICO de una AAPP	24
5. Certificado de SELLO DE ÓRGANO para una Administración Pública	36
6. Certificado de SELLO ELECTRÓNICO de persona jurídica	48
7. Certificado de SELLO IoT.....	58

2. Certificado de PERSONA FÍSICA VINCULADA a una Organización

Existe un perfil emitido en HSM centralizado y otro perfil emitido en software.

Ambos perfiles se gestionan desde la aplicación NebulaCert.

Campo	Emitido en <u>HSM</u>	Emitido en <u>Software</u>	Oblig	Crít	Observaciones
<i>PERSONA FÍSICA vinculada</i>	Identificación y Firma	Identificación y Firma			
1. Basic structure					
1.1. Version	"2"		Sí		Integer=2 [RFC5280] El literal "2" corresponde a la versión 3.
1.2. Serial Number	Establecido automáticamente por la CA. Número identificativo único del certificado.		Sí		Integer. SerialNumber = ej: 111222. // [RFC5280] No superior a 20 octetos y no puede ser un número negativo ni 0.
1.3. Signature Algorithm	SHA-256 with RSA Signature		Sí		1.2.840.113549.1.1.11
1.4. Issuer Distinguished Name			Sí		Todos los campos tienen que estar codificados en UTF8

Campo	Emitido en <u>HSM</u>	Emitido en <u>Software</u>	Oblig	Crít	Observaciones
PERSONA FÍSICA vinculada	Identificación y Firma	Identificación y Firma			
1.4.1. Country (C)	"ES"		Sí		OID 2.5.4.6 Size [RFC 5280] 2 (PrintableString)
1.4.2. Organization (O)	"VINTEGRIS SL"		Sí		OID 2.5.4.10 Size [RFC 5280] 128 (String UTF8)
1.4.3. Locality (L)	"Barcelona"				OID 2.5.4.7 Size [RFC 5280] 128 (String UTF8)
1.4.4. Organizational Unit (OU)	"EC-VINTEGRIS"				OID 2.5.4.11 Size [RFC 5280] 64 (String UTF8)
1.4.5. Organizational Unit (OU)	"see current address at https://www.vincasign.net/contact "				OID 2.5.4.11 Size [RFC 5280] 64 (String UTF8)
1.4.6. Serial Number	"B62913926"		Sí		OID 2.5.4.5 (Printable String) Size = 9
1.4.7. Organizational Identifier	"VATES-B62913926"				OID 2.5.4.97 (String UTF8)
1.4.8. Common Name (CN)	"vinCAsign NEBULASUITE Authority"		Sí		Size [RFC 5280] 80 (String UTF8)
1.5. Validity			Sí		

Campo	Emitido en <u>HSM</u>	Emitido en <u>Software</u>	Oblig	Crít	Observaciones
<i>PERSONA FÍSICA vinculada</i>	Identificación y Firma	Identificación y Firma			
1.5.1. Not Before	Fecha de inicio de validez		Sí		UTCTime YMMDDHHMMSSZ
1.5.2. Not After	Fecha de expiración		Sí		UTCTime YMMDDHHMMSSZ
1.6. Subject			Sí		Todos los campos tienen que estar codificados en UTF8
1.6.1. Country (C)	"ES"		Sí		OID 2.5.4.6 <i>(PrintableString)</i>
1.6.2. Organization (O)	Organización a la que pertenece el firmante.		Sí		OID 2.5.4.10
1.6.3. Organizational Unit (OU)	Primera Indicación del Departamento en la Organización a la que pertenece el firmante u otra información sobre la Organización.		Sí		OID 2.5.4.11 Size [RFC 5280] 64 <i>(String UTF8)</i>
1.6.4. OrganizationIdentifier	NIF de la persona jurídica a la que está vinculado el titular del certificado, en formato ETSI EN 319412-1 (Ejemplo: "VATES-Q0000000J)		Sí		OID 2.5.4.97
1.6.5. Title	Cargo del firmante en la organización				OID 2.5.4.12
1.6.6. Surname	Apellidos de la persona física (como consta en el DNI/NIE)		Sí		OID 2.5.4.4
1.6.7. Given Name	Nombre de la persona física (como consta en el DNI/NIE)		Sí		OID 2.5.4.42

Campo	Emitido en <u>HSM</u>	Emitido en <u>Software</u>	Oblig	Crít	Observaciones
PERSONA FÍSICA vinculada	Identificación y Firma	Identificación y Firma			
1.6.8. Serial Number ¹	NIF del titular acorde a ETSI EN 319 412-1 "IDCES-123456789Z")		Sí		OID 2.5.4.5 (PrintableString)
1.6.9. Common Name (CN) ²	GARCIA LOPEZ ANTONIO – DNI 123456789Z		Sí		OID 2.5.4.3
1.6.10. emailAddress (EA)	Correo electrónico del firmante		Sí		(IA5String)
1.7. Subject Public Key Info	Clave pública del firmante, codificada en RSA encryption (2048 bits)		Sí		OID 1.2.840.113549.1.1.1
2. Extensions					
2.1. Authority Key Identifier	Presente		Sí	No	OID 2.5.29.35 (Marcado como NO crítico según EN 319412-2)
2.2. Subject Key Identifier	Presente		Sí	No	OID 2.5.29.14 Identificador de la clave pública del suscriptor

¹ Se recomienda codificación acorde a ETSI EN 319 412-1

² De acuerdo con los perfiles de certificados electrónicos (Anexo 1) del MHAP en su edición de abril de 2016 <http://administracionelectronica.gob.es/> para una correcta interoperabilidad de los ciudadanos con la Administración Pública.

Campo	Emitido en <u>HSM</u>	Emitido en <u>Software</u>	Oblig	Crít	Observaciones
PERSONA FÍSICA vinculada	Identificación y Firma	Identificación y Firma			(derivada hash clave pub subj). (Marcado como NO crítico según EN 319412-2)
2.3. Key Usage			Sí	Sí	OID 2.5.29.15
2.3.1. Digital Signature	Seleccionado "1"	Seleccionado "1"	Sí		
2.3.2. Content commintment	Seleccionado "1"	Seleccionado "1"	Sí		
2.3.3. Key Encipherment	No seleccionado. "0"	No seleccionado. "0"			
2.3.4. Data Encipherment	No seleccionado. "0"	No seleccionado. "0"			
2.3.5. Key Agreement	No seleccionado. "0"	No seleccionado. "0"			
2.3.6. Key Certificate Signature	No seleccionado. "0"	No seleccionado. "0"			
2.3.7. CRL Signature	No seleccionado. "0"	No seleccionado. "0"			
2.4. Certificate Policies			Si	No	OID 2.5.29.32 (Marcado como NO crítico según EN 319412-2)

Campo	Emitido en <u>HSM</u>	Emitido en <u>Software</u>	Oblig	Crít	Observaciones
PERSONA FÍSICA vinculada	Identificación y Firma	Identificación y Firma			
2.4.1. Policy Identifier ³	1.3.6.1.4.1.47155.1.1.1	1.3.6.1.4.1.47155.1.1.2			
2.4.2. Policy Identifier ⁴	0.4.0.194112.1.2		Sí		
2.4.3. Policy Identifier ⁵		0.4.0.194112.1.0	Sí		
2.4.4. Policy Qualifier ID			Sí		
2.4.4.1. CPS Pointer	https://policy.vincasign.net		Sí		
2.4.4.2. User Notice	“Certificado cualificado de persona física vinculada emitido en un DCCF. Ver https://policy.vincasign.net “	“Certificado cualificado de persona física vinculada emitido en software. Ver https://policy.vincasign.net “	Sí		
2.5. Subject Alternative Names			Sí	No	Este apartado puede disponer de más campos

³ Política perteneciente a vinCAsign

⁴ QCP-n-qscd, política para los certificados EU cualificados emitidos a personas físicas en un QSCD o dispositivo cualificado de creación de firma (DCCF).

⁵ QCP-n, política para los certificados EU cualificados emitidos a personas físicas en software, **SIN** EL USO de un QSCD o dispositivo cualificado de creación de firma (DCCF).

Campo	Emitido en <u>HSM</u>	Emitido en <u>Software</u>	Oblig	Crít	Observaciones
PERSONA FÍSICA vinculada	Identificación y Firma	Identificación y Firma			(Marcado como NO crítico según EN 319412-2).
2.5.1. rfc822Name	Correo electrónico de la persona física		Sí		
2.6. Extended Key Usage			Sí	No	OID 2.5.29.37 (Marcado como NO crítico según EN 319412-2)
2.6.1. clientAuth	Presente (1.3.6.1.5.5.7.3.2)		Sí		
2.6.2. Email protection	Presente (1.3.6.1.5.5.7.3.4)		Sí		
2.7. cRLDistributionPoint			Sí	No	OID 2.5.29.31 Este apartado no es obligatorio siempre que exista la funcionalidad de OCSP. (Marcado como NO crítico según EN 319412-2)
2.7.1. distributionPoint	http://crl3.vincasign.net/casub.crl		Sí		
2.7.2. distributionPoint	http://crl4.vincasign.net/casub.crl		Sí		
2.8. Authority Info Acces			Sí	No	OID 1.3.6.1.5.5.7.1.1 (Marcado como NO crítico)

Campo	Emitido en <u>HSM</u>	Emitido en <u>Software</u>	Oblig	Crít	Observaciones
PERSONA FÍSICA vinculada	Identificación y Firma	Identificación y Firma			según EN 319412-2)
2.8.1. OCSP Access Method	Id-ad-ocsp		Sí		
2.8.1.1. Acces Location	http://ocsp3.vincasign.net		Sí		
2.8.1.2. Acces Location	http://ocsp4.vincasign.net				
2.8.2. calssuersAccessMethod	id-ad-calssuers		Sí		
2.8.2.1. Acces Location	http://www.vincasign.net/publickeys/casub.crt		Si		
2.9. Qualified Certificate Statements			Sí	No	
2.9.1. qCCompliance	id-etsi-qcs-QcCompliance		Sí		OID 0.4.0.1862.1.1 id-etsi-qcs-QcCompliance
2.9.2. QcEuRetentionPeriod	"15"		Sí		OID 0.4.0.1862.1.3 id-etsi-qcs- QcRetentionPeriod INTEGER
2.9.3. QcSSCD	id-etsi-qcs-QcSSCD		Sí/No		OID 0.4.0.1862.1.4 id-etsi-qcs-QcSSCD

Campo	Emitido en <u>HSM</u>	Emitido en <u>Software</u>	Oblig	Crít	Observaciones
PERSONA FÍSICA vinculada	Identificación y Firma	Identificación y Firma			
2.9.4. QcPDS	{https://www.vincasign.net/policy/es/PDS-PF-hard/pds-pf-hard-es.pdf,es},{https://www.vincasign.net/policy/en/PDS-PF-hard/pds-pf-hard-en.pdf,en}	{https://www.vincasign.net/policy/es/PDS-PF-soft/pds-pf-soft-es.pdf,es},{https://www.vincasign.net/policy/en/PDS-PF-soft/pds-pf-soft-en.pdf,en}	Sí		OID 0.4.0.1862.1.5 id-etsi-qcs-QcPDS PdsLocation ::= SEQUENCE { url IA5String, language PrintableString (SIZE(2))} -- ISO 639-1 language code
2.9.5. QcType	id-etsi-qct-esign (0.4.0.1862.1.6.1)		Sí		OID 0.4.0.1862.1.6.1 id-etsi-qct-esign OBJECT IDENTIFIER ::= { id-etsi-qcs- QcType 1 } -- Certificate for electronic signatures as defined in Regulation (EU) No 910/2014
2.9.6. semnaticIdNatural	0.4.0.194121.1.1				Para indicar semántica de persona fisica definida por la EN 319 412-1
2.10. Basic Constraints			Sí	Sí	
2.10.1. cA	FALSE		Sí		

3. Certificado de PERSONA FÍSICA REPRESENTANTE de una Organización

Existe un perfil emitido en HSM centralizado y otro perfil emitido en software.

Ambos perfiles se gestionan desde la aplicación NebulaCert.

Campo	Emitido en <u>HSM</u>	Emitido en <u>Software</u>	Oblig	Crít	Observaciones
<i>P. Física REPRESENTANTE</i>	Identificación y Firma	Identificación y Firma			
1. Basic structure					
1.1. Version	"2"		Sí		Integer=2 [RFC5280] El literal "2" corresponde a la versión 3.
1.2. Serial Number	Establecido automáticamente por la CA. Número identificativo único del certificado.		Sí		Integer. SerialNumber = ej: 111222. // [RFC5280] No superior a 20 octetos y no puede ser un número negativo ni 0.
1.3. Signature Algorithm	SHA-256 with RSA Signature		Sí		1.2.840.113549.1.1.11
1.4. Issuer			Sí		Todos los campos tienen que

Campo	Emitido en <u>HSM</u>	Emitido en <u>Software</u>	Oblig	Crít	Observaciones
P. Física REPRESENTANTE	Identificación y Firma	Identificación y Firma			
Distinguished Name					estar codificados en UTF8
1.4.1. Country (C)	"ES"		Sí		OID 2.5.4.6 Size [RFC 5280] 2 (PrintableString)
1.4.2. Organization (O)	"VINTEGRIS SL"		Sí		OID 2.5.4.10 Size [RFC 5280] 128 (String UTF8)
1.4.3. Locality (L)	"Barcelona"				OID 2.5.4.7 Size [RFC 5280] 128 (String UTF8)
1.4.4. Organizational Unit (OU)	"EC-VINTEGRIS"				OID 2.5.4.11 Size [RFC 5280] 64 (String UTF8)
1.4.5. Organizational Unit (OU)	"see current address at https://www.vincasign.net/contact "				OID 2.5.4.11 Size [RFC 5280] 64 (String UTF8)
1.4.6. Serial Number	"B62913926"		Sí		OID 2.5.4.5 (Printable String) Size = 9

Campo	Emitido en <u>HSM</u>	Emitido en <u>Software</u>	Oblig	Crít	Observaciones
P. Física REPRESENTANTE	Identificación y Firma	Identificación y Firma			
1.4.7. OrganizationalIdentifier	"VATES-B62913926"				OID 2.5.4.97 (String UTF8)
1.4.8. Common Name (CN)	"vinCAsign NEBULASUITE Authority"		Sí		Size [RFC 5280] 80 (String UTF8)
1.5. Validity			Sí		
1.5.1. Not Before	Fecha de inicio de validez		Sí		UTCTime YYMMDDHHMMSSZ
1.5.2. Not After	Fecha de expiración		Sí		UTCTime YYMMDDHHMMSSZ
1.6. Subject			Sí		Todos los campos tienen que estar codificados en UTF8
1.6.1. Country (C)	"ES"		Sí		OID 2.5.4.6 (PrintableString)
1.6.2. Organization (O)	Organización a la que pertenece el representante.		Sí		OID 2.5.4.10
1.6.3. Organizational Unit (OU)	Primera Indicación del Departamento en la Organización a la que pertenece el representante u otra información sobre la Organización.		Sí		OID 2.5.4.11 Size [RFC 5280] 64 (String UTF8)
1.6.4. OrganizationIdentifier	NIF de la persona jurídica de la que es representante el titular del certificado, en formato ETSI EN 319412-1 (Ejemplo: "VATES-Q0000000J)		Sí		OID 2.5.4.97

Campo	Emitido en <u>HSM</u>	Emitido en <u>Software</u>	Oblig	Crít	Observaciones
P. Física REPRESENTANTE	Identificación y Firma	Identificación y Firma			
1.6.5. Title	Representante legal ...				OID 2.5.4.12
1.6.6. Surname	Apellidos de la persona física (como consta en el DNI/NIE)		Sí		OID 2.5.4.4
1.6.7. Given Name	Nombre de la persona física (como consta en el DNI/NIE)		Sí		OID 2.5.4.42
1.6.8. Serial Number ⁶	NIF del titular acorde a ETSI EN 319 412-1 "IDCES-123456789Z")		Sí		OID 2.5.4.5 (PrintableString)
1.6.9. Common Name (CN) ⁷	123456789Z Antonio Casas (R: Q0000000J)		Sí		OID 2.5.4.3
1.6.10. Description ⁸	<ul style="list-style-type: none"> Reg: XXX /Hoja: XXX /Tomo:XXX /Sección:XXX /Libro:XXX /Folio:XXX /Fecha: dd-mm-aaaa /Inscripción: XXX 		Sí		OID 2.5.4.13

⁶ De acuerdo con la propuesta del apartado 14.1.3.3 (codificación del campo Subject) del documento de "Perfiles de certificados Electrónicos (abril del 2016)" del Ministerio de Hacienda y Administraciones Públicas.

⁷ De acuerdo con la propuesta del apartado 14.1.3.3 (codificación del atributo Common Name) del documento de "Perfiles de certificados Electrónicos (abril del 2016)" del Ministerio de Hacienda y Administraciones Públicas: DNI/NIE, Nombre y Apellido, "(R:", Nif de la empresa representada, ")". Máximo 64 caracteres según la RFC 5280

⁸ De acuerdo con la propuesta del apartado 14.1.3.3 (Codificación del documento público que acredita las facultades del firmante o los datos registrales) del documento de "Perfiles de certificados Electrónicos (abril del 2016)" del Ministerio de Hacienda y Administraciones Públicas. Se escoge una de las tres opciones. Puede ampliarse en un futuro.

Campo	Emitido en <u>HSM</u>	Emitido en <u>Software</u>	Oblig	Crít	Observaciones
P. Física REPRESENTANTE	Identificación y Firma	Identificación y Firma			
	<ul style="list-style-type: none"> Notario: Nombre Apellido1 Apellido2 /Núm Protocolo: XXX /Fecha Otorgamiento: dd-mm-aaaa En Boletines Oficiales: Boletín: XXX/ /Fecha: dd-mm-aaaa /Numero resolución: XXX 				
1.6.11. emailAddress (EA)	Correo electrónico del firmante		Sí		(IA5String)
1.7. Subject Public Key Info	Clave pública del firmante, codificada en RSA encryption (2048 bits)		Sí		OID 1.2.840.113549.1.1.1
2. Extensions					
2.1. Authority Key Identifier	Presente		Sí	No	OID 2.5.29.35 (Marcado como NO crítico según EN 319412-2)
2.2. Subject Key Identifier	Presente		Sí	No	OID 2.5.29.14 Identificador de la clave pública del suscriptor (derivada hash clave pub subj). (Marcado como NO crítico según EN 319412-2)

Campo	Emitido en <u>HSM</u>	Emitido en <u>Software</u>	Oblig	Crít	Observaciones
P. Física REPRESENTANTE	Identificación y Firma	Identificación y Firma			
2.3. Key Usage			Sí	Sí	OID 2.5.29.15
2.3.1. Digital Signature	Seleccionado "1"	Seleccionado "1"	Sí		
2.3.2. Content commintment	Seleccionado "1"	Seleccionado "1"	Sí		
2.3.3. Key Encipherment	No seleccionado. "0"	No seleccionado. "0"			
2.3.4. Data Encipherment	No seleccionado. "0"	No seleccionado. "0"			
2.3.5. Key Agreement	No seleccionado. "0"	No seleccionado. "0"			
2.3.6. Key Certificate Signature	No seleccionado. "0"	No seleccionado. "0"			
2.3.7. CRL Signature	No seleccionado. "0"	No seleccionado. "0"			
2.4. Certificate Policies			Si	No	OID 2.5.29.32 (Marcado como NO crítico según EN 319412-2)

Campo	Emitido en <u>HSM</u>	Emitido en <u>Software</u>	Oblig	Crít	Observaciones
P. Física REPRESENTANTE	Identificación y Firma	Identificación y Firma			
2.4.1. Policy Identifier ⁹	1.3.6.1.4.1.47155.1.2.1	1.3.6.1.4.1.47155.1.2.2			
2.4.2. Policy Identifier ¹⁰	0.4.0.194112.1.2		Sí		
2.4.3. Policy Identifier ¹¹		0.4.0.194112.1.0	Sí		
2.4.4. Policy Identifier ¹²	2.16.724.1.3.5.8				
2.4.5. Policy Qualifier ID			Sí		
2.4.5.1. CPS Pointer	https://policy.vincasign.net		Sí		

⁹ Política perteneciente a vinCAsign

¹⁰ QCP-n-qscd, política para los certificados EU cualificados emitidos a personas físicas en un QSCD o dispositivo cualificado de creación de firma (DCCF).

¹¹ QCP-n, política para los certificados EU cualificados emitidos a personas físicas en software, **SIN** EL USO de un QSCD o dispositivo cualificado de creación de firma (DCCF).

¹² De acuerdo con la propuesta del apartado 14.1.3.3 (codificación de la extensión Certificate Policies) del documento de “Perfiles de certificados Electrónicos (abril del 2016)” del Ministerio de Hacienda y Administraciones Públicas, en el que se describe que: “OID = 2.16.724.1.3.5.8. Indica que el certificado es un certificado de representante de persona jurídica, con poderes totales, administrador único o solidario de la organización, o al menos con poderes específicos generales para actuar ante las AAPP”.

Campo	Emitido en <u>HSM</u>	Emitido en <u>Software</u>	Oblig	Crít	Observaciones
P. Física REPRESENTANTE	Identificación y Firma	Identificación y Firma			
2.4.5.2. User Notice	“Certificado cualificado de persona física representante emitido en un DCCF. Ver https://policy.vincasign.net “	“Certificado cualificado de persona física vinculada emitido en software. Ver https://policy.vincasign.net “	Sí		
2.5. Subject Alternative Names			Sí	No	Este apartado puede disponer de más campos (Marcado como NO crítico según EN 319412-2).
2.5.1. rfc822Name	Correo electrónico de la persona física representante		Sí		
2.6. Extended Key Usage			Sí	No	OID 2.5.29.37 (Marcado como NO crítico según EN 319412-2)
2.6.1. clientAuth	Presente (1.3.6.1.5.5.7.3.2)		Sí		
2.6.2. Email protection	Presente (1.3.6.1.5.5.7.3.4)		Sí		
2.7. cRLDistributionPoint			Sí	No	OID 2.5.29.31 Este apartado no es obligatorio siempre que exista la funcionalidad de

Campo	Emitido en <u>HSM</u>	Emitido en <u>Software</u>	Oblig	Crít	Observaciones
P. Física REPRESENTANTE	Identificación y Firma	Identificación y Firma			
					OCSF. (Marcado como NO crítico según EN 319412-2)
2.7.1. distributionPoint	http://crl3.vincasign.net/casub.crl		Sí		
2.7.2. distributionPoint	http://crl4.vincasign.net/casub.crl		Sí		
2.8. Authority Info Acces			Sí	No	OID 1.3.6.1.5.5.7.1.1 (Marcado como NO crítico según EN 319412-2)
2.8.1. OCSF Access Method	id-ad-ocsp		Sí		
2.8.1.1. Acces Location	http://ocsp3.vincasign.net		Sí		
2.8.1.2. Acces Location	http://ocsp4.vincasign.net				
2.8.2. calssuersAccessMethod	id-ad-calssuers		Sí		
2.8.2.1. Acces Location	http://www.vincasign.net/publickeys/casub.crt		Si		
2.9. Qualified Certificate Statements			Sí	No	

Campo	Emitido en <u>HSM</u>	Emitido en <u>Software</u>	Oblig	Crít	Observaciones
P. Física REPRESENTANTE	Identificación y Firma	Identificación y Firma			
2.9.1. qCCompliance	id-etsi-qcs-QcCompliance		Sí		OID 0.4.0.1862.1.1 id-etsi-qcs-QcCompliance
2.9.2. QcEuRetentionPeriod	"15"		Sí		OID 0.4.0.1862.1.3 id-etsi-qcs- QcRetentionPeriod INTEGER
2.9.3. QcSSCD	id-etsi-qcs-QcSSCD		Sí/No		OID 0.4.0.1862.1.4 id-etsi-qcs-QcSSCD
2.9.4. QcPDS	{https://www.vincasign.net/policy/es/PDS-REP-hard/pds-rep-hard-es.pdf,es},{https://www.vincasign.net/policy/en/PDS-REP-hard/pds-rep-hard-en.pdf,en}	{https://www.vincasign.net/policy/es/PDS-REP-soft/pds-rep-soft-es.pdf,es},{https://www.vincasign.net/policy/en/PDS-REP-soft/pds-rep-soft-en.pdf,en}	Sí		OID 0.4.0.1862.1.5 id-etsi-qcs-QcPDS PdsLocation ::= SEQUENCE { url IA5String, language PrintableString (SIZE(2))} -- ISO 639-1 language code
2.9.5. QcType	id-etsi-qct-esign (0.4.0.1862.1.6.1)		Sí		OID 0.4.0.1862.1.6.1 id-etsi-qct-esign OBJECT IDENTIFIER ::= { id-etsi-qcs- QcType 1 } -- Certificate for electronic signatures as defined in Regulation (EU) No 910/2014
2.9.6. semnaticIdNatur	0.4.0.194121.1.1				Para indicar semántica de persona física definida por

Campo	Emitido en <u>HSM</u>	Emitido en <u>Software</u>	Oblig	Crít	Observaciones
<i>P. Física REPRESENTANTE</i>	Identificación y Firma	Identificación y Firma			
al					la EN 319 412-1
2.10. Basic Constraints			Sí	Sí	
2.10.1.cA		FALSE	Sí		

4. Certificado de PERSONA FÍSICA EMPLEADO PÚBLICO de una AAPP

Existe un perfil emitido en HSM centralizado (nivel Alto) y otro perfil emitido en software (Nivel Medio).

Ambos perfiles se gestionan desde la aplicación NebulaCert.

Campo	Nivel ALTO	Nivel MEDIO	Oblig	Crít	Observaciones
<i>P.F. EMPLEADO PÚBLICO</i>	Identificación y Firma	Identificación y Firma			
1. Basic structure					
1.1. Version	"2"		Sí		Integer=2 [RFC5280] El literal "2" corresponde a la versión 3.
1.2. Serial Number	Establecido automáticamente por la CA. Número identificativo único del certificado.		Sí		Integer. SerialNumber = ej: 111222. // [RFC5280] No superior a 20 octetos y no puede ser un número negativo ni 0.
1.3. Signature Algorithm	SHA-256 with RSA Signature		Sí		1.2.840.113549.1.1.11
1.4. Issuer Distinguished Name			Sí		Todos los campos tienen que estar codificados en UTF8

Campo	Nivel ALTO	Nivel MEDIO	Oblig	Crít	Observaciones
P.F. EMPLEADO PÚBLICO	Identificación y Firma	Identificación y Firma			
1.4.1. Country (C)	"ES"		Sí		OID 2.5.4.6 Size [RFC 5280] 2 (PrintableString)
1.4.2. Organization (O)	"VINTEGRIS SL"		Sí		OID 2.5.4.10 Size [RFC 5280] 128 (String UTF8)
1.4.3. Locality (L)	"Barcelona"				OID 2.5.4.7 Size [RFC 5280] 128 (String UTF8)
1.4.4. Organizational Unit (OU)	"EC-VINTEGRIS"				OID 2.5.4.11 Size [RFC 5280] 64 (String UTF8)
1.4.5. Organizational Unit (OU)	"see current address at https://www.vincasign.net/contact "				OID 2.5.4.11 Size [RFC 5280] 64 (String UTF8)
1.4.6. Serial Number	"B62913926"		Sí		OID 2.5.4.5 (Printable String) Size = 9
1.4.7. Organizational Unit (OU)	"VATES-B62913926"				OID 2.5.4.97 (String UTF8)

Campo	Nivel ALTO	Nivel MEDIO	Oblig	Crít	Observaciones
P.F. EMPLEADO PÚBLICO	Identificación y Firma	Identificación y Firma			
Identifier					
1.4.8. Common Name (CN)	"vinCAsign NEBULASUITE Authority"		Sí		Size [RFC 5280] 80 (String UTF8)
1.5. Validity			Sí		
1.5.1. Not Before	Fecha de inicio de validez		Sí		UTCTime YYMMDDHHMMSSZ
1.5.2. Not After	Fecha de expiración		Sí		UTCTime YYMMDDHHMMSSZ
1.6. Subject			Sí		Todos los campos tienen que estar codificados en UTF8
1.6.1. Country (C)	"ES"		Sí		OID 2.5.4.6 (PrintableString)
1.6.2. Organization (O)	Denominación (nombre "oficial") de la Administración, organismo o entidad de derecho público suscriptora del certificado, a la que se encuentra vinculada el empleado.		Sí		OID 2.5.4.10
1.6.3. Organizational Unit (OU)	"Certificado electrónico de empleado público nivel Alto"		Sí		OID 2.5.4.11 Size [RFC 5280] 64 (String UTF8)
1.6.4. OrganizationIdentifier	NIF de la AAPP a la que está vinculado el empleado público titular del certificado, en formato ETSI EN 319412-1 (Ejemplo: "VATES-Q0000000J)				OID 2.5.4.97

Campo	Nivel ALTO	Nivel MEDIO	Oblig	Crít	Observaciones
P.F. EMPLEADO PÚBLICO	Identificación y Firma	Identificación y Firma			
1.6.5. Title	Debe incluir el puesto o cargo de la persona física, que le vincula con la Administración, organismo o entidad de derecho público suscriptora del certificado				OID 2.5.4.12
1.6.6. Surname	Apellidos de la persona física (como consta en el DNI/NIE)		Sí		OID 2.5.4.4
1.6.7. Given Name	Nombre de la persona física (como consta en el DNI/NIE)		Sí		OID 2.5.4.42
1.6.8. Serial Number ¹³	NIF del titular acorde a ETSI EN 319 412-1 “IDCES-123456789Z”)		Sí		OID 2.5.4.5 (PrintableString)
1.6.9. Common Name (CN) ¹⁴	Nombre Apellido1 Apellido2 – DNI 00000000G		Sí		OID 2.5.4.3
1.7. Subject Public Key Info	Clave pública del firmante, codificada en RSA encryption (2048 bits)		Sí		OID 1.2.840.113549.1.1.1
2. Extensions					
2.1. Authority Key Identifier	Presente		Sí	No	OID 2.5.29.35

¹³ Se recomienda codificación acorde a ETSI EN 319 412-1

¹⁴ Se deben introducir el nombre y dos apellidos de acuerdo con documento de identidad (DNI/Pasaporte), así como DNI (Ver Criterios de Composición del campo CN para un empleado público)

Campo	Nivel ALTO	Nivel MEDIO	Oblig	Crít	Observaciones
P.F. EMPLEADO PÚBLICO	Identificación y Firma	Identificación y Firma			(Marcado como NO crítico según EN 319412-2)
2.2. Subject Key Identifier	Presente		Sí	No	OID 2.5.29.14 Identificador de la clave pública del suscriptor (derivada hash clave pub subj). (Marcado como NO crítico según EN 319412-2)
2.3. Key Usage			Sí	Sí	OID 2.5.29.15
2.3.1. Digital Signature	No seleccionado. "0"	Seleccionado "1"	No/Sí		
2.3.2. Content commintment	Seleccionado "1"	Seleccionado "1"	Sí		
2.3.3. Key Encipherment	No seleccionado. "0"	Seleccionado "1"	No/si		
2.3.4. Data Encipherment	No seleccionado. "0"	No seleccionado. "0"			
2.3.5. Key Agreement	No seleccionado. "0"	No seleccionado. "0"			
2.3.6. Key Certificate	No seleccionado. "0"	No seleccionado. "0"			

Campo	Nivel ALTO	Nivel MEDIO	Oblig	Crít	Observaciones
P.F. EMPLEADO PÚBLICO	Identificación y Firma	Identificación y Firma			
Signature					
2.3.7. CRL Signature	No seleccionado. "0"	No seleccionado. "0"			
2.4. Certificate Policies			Si	No	OID 2.5.29.32 (Marcado como NO crítico según EN 319412-2)
2.4.1. Policy Identifier ¹⁵	1.3.6.1.4.1.47155.1.4.1	1.3.6.1.4.1.47155.1.4.2			
2.4.2. Policy Identifier ¹⁶	0.4.0.194112.1.2		Sí		
2.4.3. Policy Identifier ¹⁷		0.4.0.194112.1.0	Sí		
2.4.4. Policy Identifier	2.16.724.1.3.5.7.1	2.16.724.1.3.5.7.2	Sí		OID asociado a certificado de empleado público
2.4.5. Policy Qualifier ID			Sí		

¹⁵ Política perteneciente a vinCAsign

¹⁶ QCP-n-qscd, política para los certificados EU cualificados emitidos a personas físicas en un QSCD o dispositivo cualificado de creación de firma (DCCF).

¹⁷ QCP-n, política para los certificados EU cualificados emitidos a personas físicas en software, **SIN** EL USO de un QSCD o dispositivo cualificado de creación de firma (DCCF).

Campo	Nivel ALTO	Nivel MEDIO	Oblig	Crít	Observaciones
P.F. EMPLEADO PÚBLICO	Identificación y Firma	Identificación y Firma			
2.4.5.1. CPS Pointer	https://policy.vincasign.net		Sí		
2.4.5.2. User Notice	“Certificado cualificado de persona física empleado público de nivel alto. Ver https://policy.vincasign.net “	“Certificado cualificado de persona física empleado público de nivel medio. Ver https://policy.vincasign.net “	Sí		
2.5. Subject Alternative Names			Sí	No	Este apartado puede disponer de más campos (Marcado como NO crítico según EN 319412-2).
2.5.1. rfc822Name	Correo electrónico del firmante		Sí		
2.5.2. Directory Name	Identidad administrativa		Sí		
2.5.2.1. Tipo de certificado	“certificado electrónico de empleado público”		Sí		OID ALTO: 2.16.724.1.3.5.7.1.1 OID MEDIO: 2.16.724.1.3.5.7.2.1
2.5.2.2. Nombre de la entidad subscriptora	Entidad propietaria del certificado		Sí		OID ALTO: 2.16.724.1.3.5.7.1.2 OID MEDIO: 2.16.724.1.3.5.7.2.2
2.5.2.3. NIF de la entidad	Número de identificación fiscal de la entidad propietaria del certificado		Sí		OID ALTO: 2.16.724.1.3.5.7.1.3 OID MEDIO: 2.16.724.1.3.5.7.2.3

Campo	Nivel ALTO	Nivel MEDIO	Oblig	Crít	Observaciones
P.F. EMPLEADO PÚBLICO	Identificación y Firma	Identificación y Firma			
subscriptora					
2.5.2.4. DNI/NIE del Responsable	DNI o NIE del responsable		Sí		OID ALTO: 2.16.724.1.3.5.7.1.4 OID MEDIO: 2.16.724.1.3.5.7.2.4
2.5.2.5. Número de identificación personal	NRP o NIP del responsable del suscriptor del certificado				OID ALTO: 2.16.724.1.3.5.7.1.5 OID MEDIO: 2.16.724.1.3.5.7.2.5
2.5.2.6. Nombre de pila	Nombre de pila del responsable del certificado		Sí		OID ALTO: 2.16.724.1.3.5.7.1.6 OID MEDIO: 2.16.724.1.3.5.7.2.6
2.5.2.7. Primer apellido	Primer apellido del responsable del certificado		Sí		OID ALTO: 2.16.724.1.3.5.7.1.7 OID MEDIO: 2.16.724.1.3.5.7.2.7
2.5.2.8. Segundo apellido	Segundo apellido del responsable del certificado		Sí		OID ALTO: 2.16.724.1.3.5.7.1.8 OID MEDIO: 2.16.724.1.3.5.7.2.8
2.5.2.9. Correo electrónico	Correo electrónico del responsable del certificado				OID ALTO: 2.16.724.1.3.5.7.1.9 OID MEDIO: 2.16.724.1.3.5.7.2.9
2.5.2.10. Unidad organizativa	Unidad, dentro de la Administración, en la que está incluido el suscriptor del certificado				OID ALTO: 2.16.724.1.3.5.7.1.10 OID MEDIO: 2.16.724.1.3.5.7.2.10

Campo	Nivel ALTO	Nivel MEDIO	Oblig	Crít	Observaciones
P.F. EMPLEADO PÚBLICO	Identificación y Firma	Identificación y Firma			
2.5.2.11. Puesto o cargo	Puesto desempeñado por el suscriptor del certificado dentro de la Administración				OID ALTO: 2.16.724.1.3.5.7.1.11 OID MEDIO: 2.16.724.1.3.5.7.2.11
2.6. Extended Key Usage			Sí	No	OID 2.5.29.37 (Marcado como NO crítico según EN 319412-2)
2.6.1. clientAuth	Presente (1.3.6.1.5.5.7.3.2)		Sí		
2.6.2. Email protection	Presente (1.3.6.1.5.5.7.3.4)		Sí		
2.7. cRLDistributionPoint			Sí	No	OID 2.5.29.31 Este apartado no es obligatorio siempre que exista la funcionalidad de OCSP. (Marcado como NO crítico según EN 319412-2)
2.7.1. distributionPoint	http://crl3.vincasign.net/casub.crl		Sí		
2.7.2. distributionPoint	http://crl4.vincasign.net/casub.crl		Sí		
2.8. Authority Info Acces			Sí	No	OID 1.3.6.1.5.5.7.1.1 (Marcado como NO crítico)

Campo	Nivel ALTO	Nivel MEDIO	Oblig	Crít	Observaciones
P.F. EMPLEADO PÚBLICO	Identificación y Firma	Identificación y Firma			según EN 319412-2)
2.8.1. OCSP Access Method	Id-ad-ocsp		Sí		
2.8.1.1. Acces Location	http://ocsp3.vincasign.net		Sí		
2.8.1.2. Acces Location	http://ocsp4.vincasign.net				
2.8.2. calssuersAccessMethod	id-ad-calssuers		Sí		
2.8.2.1. Acces Location	http://www.vincasign.net/publickeys/casub.crt		Si		
2.9. Qualified Certificate Statements			Sí	No	
2.9.1. qCCompliance	id-etsi-qcs-QcCompliance		Sí		OID 0.4.0.1862.1.1 id-etsi-qcs-QcCompliance
2.9.2. QcEuRetentionPeriod	"15"		Sí		OID 0.4.0.1862.1.3 id-etsi-qcs- QcRetentionPeriod INTEGER
2.9.3. QcSSCD	id-etsi-qcs-QcSSCD		Sí/No		OID 0.4.0.1862.1.4 id-etsi-qcs-QcSSCD

Campo	Nivel ALTO	Nivel MEDIO	Oblig	Crít	Observaciones
P.F. EMPLEADO PÚBLICO	Identificación y Firma	Identificación y Firma			
2.9.4. QcPDS	{https://www.vincasign.net/policy/es/PDS-EP-ALTO/pds-ep-alto-es.pdf,es},{https://www.vincasign.net/policy/en/PDS-EP-ALTO/pds-ep-alto-en.pdf,en}	{https://www.vincasign.net/policy/es/PDS-EP-MEDIO/pds-ep-medio-es.pdf,es},{https://www.vincasign.net/policy/en/PDS-EP-MEDIO/pds-ep-medio-en.pdf,en}	Sí		OID 0.4.0.1862.1.5 id-etsi-qcs-QcPDS PdsLocation ::= SEQUENCE { url IA5String, language PrintableString (SIZE(2))} -- ISO 639-1 language code
2.9.5. QcType	Qct-esign (0.4.0.1862.1.6.1)		Sí		OID 0.4.0.1862.1.6.1 id-etsi-qct-esign OBJECT IDENTIFIER ::= { id-etsi-qcs-QcType 1 } -- Certificate for electronic signatures as defined in Regulation (EU) No 910/2014
2.9.6. semnaticIdNatural	0.4.0.194121.1.1				Para indicar semántica de persona fisica definida por la EN 319 412-1
2.10. Basic Constraints			Sí	Sí	
2.10.1. cA	FALSE		Sí		

5. Certificado de SELLO DE ÓRGANO para una Administración Pública

Existe un perfil emitido en HSM centralizado (nivel Alto) y otro perfil emitido en software (Nivel Medio).

Ambos perfiles se gestionan desde la aplicación NebulaCert.

Campo	Nivel ALTO	Nivel MEDIO	Oblig	Crít	Observaciones
SELLO-E ÓRGANO AAPP	Identificación y Firma	Identificación y Firma			
1. Basic structure					
1.1. Version	"2"		Sí		Integer=2 [RFC5280] El literal "2" corresponde a la versión 3.
1.2. Serial Number	Establecido automáticamente por la CA. Número identificativo único del certificado.		Sí		Integer. SerialNumber = ej: 111222. // [RFC5280] No superior a 20 octetos y no puede ser un número negativo ni 0.
1.3. Signature Algorithm	SHA-256 with RSA Signature		Sí		1.2.840.113549.1.1.11
1.4. Issuer Distinguished Name			Sí		Todos los campos tienen que estar codificados en UTF8

Campo	Nivel ALTO	Nivel MEDIO	Oblig	Crít	Observaciones
SELLO-E ÓRGANO AAPP	Identificación y Firma	Identificación y Firma			
1.4.1. Country (C)	"ES"		Sí		OID 2.5.4.6 Size [RFC 5280] 2 (PrintableString)
1.4.2. Organization (O)	"VINTEGRIS SL"		Sí		OID 2.5.4.10 Size [RFC 5280] 128 (String UTF8)
1.4.3. Locality (L)	"Barcelona"				OID 2.5.4.7 Size [RFC 5280] 128 (String UTF8)
1.4.4. Organizational Unit (OU)	"EC-VINTEGRIS"				OID 2.5.4.11 Size [RFC 5280] 64 (String UTF8)
1.4.5. Organizational Unit (OU)	"see current address at https://www.vincasign.net/contact "				OID 2.5.4.11 Size [RFC 5280] 64 (String UTF8)
1.4.6. Serial Number	"B62913926"		Sí		OID 2.5.4.5 (Printable String) Size = 9
1.4.7. OrganizationalIdentifier	"VATES-B62913926"				OID 2.5.4.97 (String UTF8)

Campo	Nivel ALTO	Nivel MEDIO	Oblig	Crít	Observaciones
SELLO-E ÓRGANO AAPP	Identificación y Firma	Identificación y Firma			
1.4.8. Common Name (CN)	"vinCAsign NEBULASUITE Authority"		Sí		Size [RFC 5280] 80 (String UTF8)
1.5. Validity			Sí		
1.5.1. Not Before	Fecha de inicio de validez		Sí		UTCTime YYMMDDHHMMSSZ
1.5.2. Not After	Fecha de expiración		Sí		UTCTime YYMMDDHHMMSSZ
1.6. Subject			Sí		Todos los campos tienen que estar codificados en UTF8
1.6.1. Country (C)	"ES"		Sí		OID 2.5.4.6 (PrintableString)
1.6.2. Organization (O)	Denominación (nombre "oficial" de la organización) del creador del sello (p.ej: Ministerio de Hacienda)		Sí		OID 2.5.4.10
1.6.3. Organizational Unit (OU)	"SELLO ELECTRONICO"		Sí		OID 2.5.4.11 Size [RFC 5280] 64 (String UTF8)
1.6.4. Organizational Unit (OU)	Código DIR3 de la unidad de la AAPP (p. ej: E04976701)				OID 2.5.4.11 Size [RFC 5280] 64 (String UTF8)
1.6.5. OrganizationIdentifier	NIF de la AAPP a la que está vinculado este sello, en formato ETSI EN 319412-1 (Ejemplo: "VATES-Q0000000J)		Sí		OID 2.5.4.97

Campo	Nivel ALTO	Nivel MEDIO	Oblig	Crít	Observaciones
SELLO-E ÓRGANO AAPP	Identificación y Firma	Identificación y Firma			
1.6.6. Surname	Apellidos de la persona física (como consta en el DNI/NIE)				OID 2.5.4.4
1.6.7. Given Name	Nombre de la persona física (como consta en el DNI/NIE)				OID 2.5.4.42
1.6.8. Serial Number	NIF de la entidad		Sí		OID 2.5.4.5 (PrintableString)
1.6.9. Common Name (CN)	Nombre descriptivo del sistema automático. Asegurando que dicho nombre tenga sentido y no dé lugar a ambigüedades.		Sí		OID 2.5.4.3
1.7. Subject Public Key Info	Clave pública del firmante, codificada en RSA encryption (2048 bits)		Sí		OID 1.2.840.113549.1.1.1
2. Extensions					
2.1. Authority Key Identifier	Presente		Sí	No	OID 2.5.29.35 (Marcado como NO crítico según EN 319412-2)
2.2. Subject Key Identifier	Presente		Sí	No	OID 2.5.29.14 Identificador de la clave pública del suscriptor (derivada hash clave pub subj). (Marcado como NO crítico según EN 319412-2)

Campo	Nivel ALTO	Nivel MEDIO	Oblig	Crít	Observaciones
SELLO-E ÓRGANO AAPP	Identificación y Firma	Identificación y Firma			
2.3. Key Usage			Sí	Sí	OID 2.5.29.15
2.3.1. Digital Signature	Seleccionado "1"	Seleccionado "1"	Sí		Se utiliza cuando se realiza la función de autenticación de activo digital de la persona jurídica
2.3.2. Content commintment	Seleccionado "1"	Seleccionado "1"	Sí		Se utiliza cuando se realiza la función de sello electrónico de documento expedido por persona jurídica
2.3.3. Key Encipherment	Seleccionado "1"	Seleccionado "1"	Sí		Se utiliza para gestión y transporte de claves
2.3.4. Data Encipherment	No seleccionado. "0"	No seleccionado. "0"			
2.3.5. Key Agreement	No seleccionado. "0"	No seleccionado. "0"			
2.3.6. Key Certificate Signature	No seleccionado. "0"	No seleccionado. "0"			
2.3.7. CRL Signature	No seleccionado. "0"	No seleccionado. "0"			
2.4. Certificate Policies			Si	No	OID 2.5.29.32 (Marcado como NO crítico)

Campo	Nivel ALTO	Nivel MEDIO	Oblig	Crít	Observaciones
SELLO-E ÓRGANO AAPP	Identificación y Firma	Identificación y Firma			según EN 319412-2)
2.4.1. Policy Identifier ¹⁸	1.3.6.1.4.1.47155.1.5.1	1.3.6.1.4.1.47155.1.5.2			
2.4.2. Policy Identifier ¹⁹	0.4.0.194112.1.3		Sí		
2.4.3. Policy Identifier ²⁰		0.4.0.194112.1.1	Sí		
2.4.4. Policy Identifier	2.16.724.1.3.5.6.1	2.16.724.1.3.5.6.2	Sí		OID asociado a certificado de sello electrónico de órgano para AAPP.
2.4.5. Policy Qualifier ID			Sí		
2.4.5.1. CPS Pointer	https://policy.vincasign.net		Sí		
2.4.5.2. User Notice	“Certificado cualificado de sello electrónico para la Administración Pública, Órgano o Entidad de	“Certificado cualificado de sello electrónico para la Administración Pública,	Sí		

¹⁸ Política perteneciente a vinCAsign

¹⁹ QCP-I-qscd, política para los certificados EU cualificados emitidos a personas jurídicas en un QSCD o dispositivo cualificado de creación de firma (DCCF).

²⁰ QCP-I, política para los certificados EU cualificados emitidos a personas jurídicas en software, **SIN** EL USO de un QSCD o dispositivo cualificado de creación de firma (DCCF).

Campo	Nivel ALTO	Nivel MEDIO	Oblig	Crít	Observaciones
SELLO-E ÓRGANO AAPP	Identificación y Firma	Identificación y Firma			
	Derecho Público, nivel alto. Ver https://policy.vincasign.net “	Órgano o Entidad de Derecho Público, nivel medio. Ver https://policy.vincasign.net “			
2.5. Subject Alternative Names			Sí	No	Este apartado puede disponer de más campos (Marcado como NO crítico según EN 319412-2).
2.5.1. rfc822Name	Correo electrónico de la entidad suscriptora del sello electrónico				
2.5.2. Directory Name	Identidad administrativa		Sí		
2.5.2.1. Tipo de certificado	“SELLO ELECTRONICO DE NIVEL ALTO”	“SELLO ELECTRONICO DE NIVEL MEDIO”	Sí		OID ALTO: 2.16.724.1.3.5.6.1.1 OID MEDIO: 2.16.724.1.3.5.6.2.1
2.5.2.2. Nombre de la entidad suscriptora	Entidad propietaria del certificado		Sí		OID ALTO: 2.16.724.1.3.5.6.1.2 OID MEDIO: 2.16.724.1.3.5.6.2.2
2.5.2.3. NIF de la entidad suscriptora	Número de identificación fiscal de la entidad propietaria del certificado		Sí		OID ALTO: 2.16.724.1.3.5.6.1.3 OID MEDIO: 2.16.724.1.3.5.6.2.3
2.5.2.4. DNI/NIE del	DNI o NIE del responsable del sello				OID ALTO: 2.16.724.1.3.5.6.1.4

Campo	Nivel ALTO	Nivel MEDIO	Oblig	Crít	Observaciones
SELLO-E ÓRGANO AAPP	Identificación y Firma	Identificación y Firma			
Responsable					OID MEDIO: 2.16.724.1.3.5.6.2.4
2.5.2.5. Denominación de sistema o componente	Breve descripción del componente que posee el certificado de sello				OID ALTO: 2.16.724.1.3.5.6.1.5 OID MEDIO: 2.16.724.1.3.5.6.2.5
2.5.2.6. Nombre de pila (titular del órgano)	Nombre de pila del responsable del certificado de sello				OID ALTO: 2.16.724.1.3.5.6.1.6 OID MEDIO: 2.16.724.1.3.5.6.2.6
2.5.2.7. Primer apellido (titular del órgano)	Primer apellido del responsable del certificado de sello				OID ALTO: 2.16.724.1.3.5.6.1.7 OID MEDIO: 2.16.724.1.3.5.6.2.7
2.5.2.8. Segundo apellido (titular del órgano)	Segundo apellido del responsable del certificado de sello				OID ALTO: 2.16.724.1.3.5.6.1.8 OID MEDIO: 2.16.724.1.3.5.6.2.8
2.5.2.9. Correo electrónico	Correo electrónico de la persona responsable del certificado de sello				OID ALTO: 2.16.724.1.3.5.6.1.9 OID MEDIO: 2.16.724.1.3.5.6.2.9
2.6. Extended Key Usage			Sí	No	OID 2.5.29.37 (Marcado como NO crítico según EN 319412-2)

Campo	Nivel ALTO	Nivel MEDIO	Oblig	Crít	Observaciones
SELLO-E ÓRGANO AAPP	Identificación y Firma	Identificación y Firma			
2.6.1. clientAuth	Presente (1.3.6.1.5.5.7.3.2)				Protección de mail
2.6.2. Email protection	Presente (1.3.6.1.5.5.7.3.4)				Autenticación cliente
2.6.3.					
2.6.4.					
2.7. cRLDistributionPoint			Sí	No	OID 2.5.29.31 Este apartado no es obligatorio siempre que exista la funcionalidad de OCSP. (Marcado como NO crítico según EN 319412-2)
2.7.1. distributionPoint	http://crl3.vincasign.net/casub.crl		Sí		
2.7.2. distributionPoint	http://crl4.vincasign.net/casub.crl				
2.8. Authority Info Acces			Sí	No	OID 1.3.6.1.5.5.7.1.1 (Marcado como NO crítico según EN 319412-2)
2.8.1. OCSP Access Method	Id-ad-ocsp		Sí		

Campo	Nivel ALTO	Nivel MEDIO	Oblig	Crít	Observaciones
SELLO-E ÓRGANO AAPP	Identificación y Firma	Identificación y Firma			
2.8.1.1. Acc es Location	http://ocsp3.vincasign.net		Sí		
2.8.1.2. Acc es Location	http://ocsp4.vincasign.net				
2.8.2. calssuersAccessM ethod	id-ad-calssuers		Sí		
2.8.2.1. Acc es Location	http://www.vincasign.net/publickeys/casub.crt		Si		
2.9. Qualified Certificate Statements			Sí	No	
2.9.1. qCCompliance	id-etsi-qcs-QcCompliance		Sí		OID 0.4.0.1862.1.1 id-etsi-qcs-QcCompliance
2.9.2. QcEuRetentionPer iod	"15"		Sí		OID 0.4.0.1862.1.3 id-etsi-qcs- QcRetentionPeriod INTEGER
2.9.3. QcSSCD	id-etsi-qcs-QcSSCD		Sí/No		OID 0.4.0.1862.1.4 id-etsi-qcs-QcSSCD
2.9.4. QcPDS	{ https://www.vincasign.net/policy/ es/PDS-SELLO-ALTO/pds-sello-alto-	{ https://www.vincasign.net/p olicy/es/PDS-SELLO-	Sí		OID 0.4.0.1862.1.5 id-etsi-qcs-QcPDS

Campo	Nivel ALTO	Nivel MEDIO	Oblig	Crít	Observaciones
SELLO-E ÓRGANO AAPP	Identificación y Firma	Identificación y Firma			
	es.pdf,es},{https://www.vincasign.net/policy/en/PDS-SELLO-ALTO/pds-sello-alto-en.pdf,en}	MEDIO/pds-sello-medio-es.pdf,es},{https://www.vincasign.net/policy/en/PDS-SELLO-MEDIO/pds-sello-medio-en.pdf,en}			PdsLocation ::= SEQUENCE { url IA5String, language PrintableString (SIZE(2))} -- ISO 639-1 language code
2.9.5. QcType	id-etsi-qct-eseal (0.4.0.1862.1.6.2)		Sí		OID 0.4.0.1862.1.6.2 id-etsi-qct-eseal OBJECT IDENTIFIER ::= { id-etsi-qcs-QcType 2 } -- Certificate for electronic signatures as defined in Regulation (EU) No 910/2014
2.9.6. semnaticsdlegal	0.4.0.194121.1.2				Para indicar semántica de persona jurídica definida por la EN 319 412-1
2.10. Basic Constraints			Sí	Sí	
2.10.1. cA	FALSE		Sí		

6. Certificado de SELLO ELECTRÓNICO de persona jurídica

Existe un perfil emitido en HSM centralizado (nivel Alto) y otro perfil emitido en software (Nivel Medio).

Ambos perfiles se gestionan desde la aplicación NebulaCert.

Campo	Emitido en HSM	Emitido en Software	Oblig	Crít	Observaciones
<i>SELLO-E de PJ</i>	Identificación y Firma	Identificación y Firma			
1. Basic structure					
1.1. Version	"2"		Sí		Integer=2 [RFC5280] El literal "2" corresponde a la versión 3.
1.2. Serial Number	Establecido automáticamente por la CA. Número identificativo único del certificado.		Sí		Integer. SerialNumber = ej: 111222. // [RFC5280] No superior a 20 octetos y no puede ser un número negativo ni 0.
1.3. Signature Algorithm	SHA-256 with RSA Signature		Sí		1.2.840.113549.1.1.11
1.4. Issuer Distinguished Name			Sí		Todos los campos tienen que estar codificados en UTF8

Campo	Emitido en HSM	Emitido en Software	Oblig	Crít	Observaciones
<i>SELLO-E de PJ</i>	Identificación y Firma	Identificación y Firma			
1.4.1. Country (C)	"ES"		Sí		OID 2.5.4.6 Size [RFC 5280] 2 (PrintableString)
1.4.2. Organization (O)	"VINTEGRIS SL"		Sí		OID 2.5.4.10 Size [RFC 5280] 128 (String UTF8)
1.4.3. Locality (L)	"Barcelona"				OID 2.5.4.7 Size [RFC 5280] 128 (String UTF8)
1.4.4. Organizational Unit (OU)	"EC-VINTEGRIS"				OID 2.5.4.11 Size [RFC 5280] 64 (String UTF8)
1.4.5. Organizational Unit (OU)	"see current address at https://www.vincasign.net/contact "				OID 2.5.4.11 Size [RFC 5280] 64 (String UTF8)
1.4.6. Serial Number	"B62913926"		Sí		OID 2.5.4.5 (Printable String) Size = 9
1.4.7. OrganizationalIdentifier	"VATES-B62913926"				OID 2.5.4.97 (String UTF8)

Campo	Emitido en HSM	Emitido en Software	Oblig	Crít	Observaciones
<i>SELLO-E de PJ</i>	Identificación y Firma	Identificación y Firma			
1.4.8. Common Name (CN)	"vinCAsign NEBULASUITE Authority"		Sí		Size [RFC 5280] 80 (String UTF8)
1.4.9.					
1.5. Validity			Sí		
1.5.1. Not Before	Fecha de inicio de validez		Sí		UTCTime YYMMDDHHMMSSZ
1.5.2. Not After	Fecha de expiración		Sí		UTCTime YYMMDDHHMMSSZ
1.6. Subject			Sí		Todos los campos tienen que estar codificados en UTF8
1.6.1. Country (C)	"ES"		Sí		OID 2.5.4.6 (PrintableString)
1.6.2. Organization (O)	Denominación (nombre "oficial" de la persona jurídica) del creador del sello (Empresa, Organización, Entidad)		Sí		OID 2.5.4.10
1.6.3. Organizational Unit (OU)	"SELLO ELECTRONICO"		Sí		OID 2.5.4.11 Size [RFC 5280] 64 (String UTF8)
1.6.4. OrganizationIdentifier	NIF de la persona jurídica a la que está vinculado este sello, en formato ETSI EN 319412-1 (Ejemplo: "VATES-Q0000000J)		Sí		OID 2.5.4.97

Campo	Emitido en HSM	Emitido en Software	Oblig	Crít	Observaciones
<i>SELLO-E de PJ</i>	Identificación y Firma	Identificación y Firma			
1.6.5. Surname	Apellidos de la persona física (como consta en el DNI/NIE)				OID 2.5.4.4
1.6.6. Given Name	Nombre de la persona física (como consta en el DNI/NIE)				OID 2.5.4.42
1.6.7. Serial Number	NIF de la persona jurídica		Sí		OID 2.5.4.5 (PrintableString)
1.6.8. Common Name (CN)	Nombre descriptivo del sistema automático. Asegurando que dicho nombre tenga sentido y no dé lugar a ambigüedades.		Sí		OID 2.5.4.3
1.7. Subject Public Key Info	Clave pública del firmante, codificada en RSA encryption (2048 bits)		Sí		OID 1.2.840.113549.1.1.1
2. Extensions					
2.1. Authority Key Identifier	Presente		Sí	No	OID 2.5.29.35 (Marcado como NO crítico según EN 319412-2)
2.2. Subject Key Identifier	Presente		Sí	No	OID 2.5.29.14 Identificador de la clave pública del suscriptor (derivada hash clave pub subj). (Marcado como NO crítico según EN 319412-2)

Campo	Emitido en HSM	Emitido en Software	Oblig	Crít	Observaciones
<i>SELLO-E de PJ</i>	Identificación y Firma	Identificación y Firma			
2.3. Key Usage			Sí	Sí	OID 2.5.29.15
2.3.1. Digital Signature	Seleccionado "1"	Seleccionado "1"	Sí		Se utiliza cuando se realiza la función de autenticación de activo digital de la persona jurídica
2.3.2. Content commintment	Seleccionado "1"	Seleccionado "1"	Sí		Se utiliza cuando se realiza la función de sello electrónico de documento expedido por persona jurídica
2.3.3. Key Encipherment	Seleccionado "1"	Seleccionado "1"	Sí		Se utiliza para gestión y transporte de claves
2.3.4. Data Encipherment	No seleccionado. "0"	No seleccionado. "0"			
2.3.5. Key Agreement	No seleccionado. "0"	No seleccionado. "0"			
2.3.6. Key Certificate Signature	No seleccionado. "0"	No seleccionado. "0"			
2.3.7. CRL Signature	No seleccionado. "0"	No seleccionado. "0"			
2.4. Certificate Policies			Si	No	OID 2.5.29.32 (Marcado como NO crítico)

Campo	Emitido en HSM	Emitido en Software	Oblig	Crít	Observaciones
<i>SELLO-E de PJ</i>	Identificación y Firma	Identificación y Firma			según EN 319412-2)
2.4.1. Policy Identifier ²¹	1.3.6.1.4.1.47155.1.6.1	1.3.6.1.4.1.47155.1.6.2			
2.4.2. Policy Identifier ²²	0.4.0.194112.1.3		Sí		
2.4.3. Policy Identifier ²³		0.4.0.194112.1.1	Sí		
2.4.4. Policy Qualifier ID			Sí		
2.4.4.1. CPS Pointer	https://policy.vincasign.net		Sí		
2.4.4.2. User Notice	“Certificado cualificado de sello electrónico de persona jurídica emitido en HSM-QSCD. Ver https://policy.vincasign.net “	“Certificado cualificado de sello electrónico emitido en software. Ver https://policy.vincasign.net “	Sí		
2.5. Subject			Sí	No	Este apartado puede

²¹ Política perteneciente a vinCAsign

²² QCP-I-qscd, política para los certificados EU cualificados emitidos a personas jurídicas en un QSCD o dispositivo cualificado de creación de firma (DCCF).

²³ QCP-I, política para los certificados EU cualificados emitidos a personas jurídicas en software, **SIN** EL USO de un QSCD o dispositivo cualificado de creación de firma (DCCF).

Campo	Emitido en HSM	Emitido en Software	Oblig	Crít	Observaciones
<i>SELLO-E de PJ</i>	Identificación y Firma	Identificación y Firma			
Alternative Names					disponer de más campos (Marcado como NO crítico según EN 319412-2).
2.5.1. rfc822Name	Correo electrónico de la entidad suscriptora del sello electrónico				
2.6. Extended Key Usage			Sí	No	OID 2.5.29.37 (Marcado como NO crítico según EN 319412-2)
2.6.1. clientAuth	Presente (1.3.6.1.5.5.7.3.2)				Protección de mail
2.6.2. Email protection	Presente (1.3.6.1.5.5.7.3.4)				Autenticación cliente
2.6.3.					
2.6.4.					
2.7. cRLDistributionPoint			Sí	No	OID 2.5.29.31 Este apartado no es obligatorio siempre que exista la funcionalidad de OCSP. (Marcado como NO crítico según EN 319412-2)

Campo	Emitido en HSM	Emitido en Software	Oblig	Crít	Observaciones
SELLO-E de PJ	Identificación y Firma	Identificación y Firma			
2.7.1. distributionPoint	http://crl3.vincasign.net/casub.crl		Sí		
2.7.2. distributionPoint	http://crl4.vincasign.net/casub.crl				
2.8. Authority Info Acces			Sí	No	OID 1.3.6.1.5.5.7.1.1 (Marcado como NO crítico según EN 319412-2)
2.8.1. OCSP Access Method	Id-ad-ocsp		Sí		
2.8.1.1. Acces Location	http://ocsp3.vincasign.net		Sí		
2.8.1.2. Acces Location	http://ocsp4.vincasign.net				
2.8.2. calssuersAccessMethod	id-ad-calssuers		Sí		
2.8.2.1. Acces Location	http://www.vincasign.net/publickeys/casub.crt		Si		
2.9. Qualified Certificate Statements			Sí	No	

Campo	Emitido en HSM	Emitido en Software	Oblig	Crít	Observaciones
SELLO-E de PJ	Identificación y Firma	Identificación y Firma			
2.9.1. qCCompliance	id-etsi-qcs-QcCompliance		Sí		OID 0.4.0.1862.1.1 id-etsi-qcs-QcCompliance
2.9.2. QcEuRetentionPeriod	"15"		Sí		OID 0.4.0.1862.1.3 id-etsi-qcs- QcRetentionPeriod INTEGER
2.9.3. QcSSCD	id-etsi-qcs-QcSSCD		Sí/No		OID 0.4.0.1862.1.4 id-etsi-qcs-QcSSCD
2.9.4. QcPDS	{https://www.vincasign.net/policy/es/PDS-SELLOPJ-HSM/pds-sellopj-hsm-es.pdf,es},{https://www.vincasign.net/policy/en/PDS-SELLOPJ-HSM/pds-sellopj-hsm-en.pdf,en}	{https://www.vincasign.net/policy/es/PDS-SELLOPJ-soft/pds-sellopj-soft-es.pdf,es},{https://www.vincasign.net/policy/en/PDS-SELLOPJ-soft/pds-sellopj-soft-en.pdf,en}	Sí		OID 0.4.0.1862.1.5 id-etsi-qcs-QcPDS PdsLocation ::= SEQUENCE { url IA5String, language PrintableString (SIZE(2))} -- ISO 639-1 language code
2.9.5. QcType	id-etsi-qct-eseal (0.4.0.1862.1.6.2)		Sí		OID 0.4.0.1862.1.6.2 id-etsi-qct-eseal OBJECT IDENTIFIER ::= { id-etsi-qcs- QcType 2 } -- Certificate for electronic signatures as defined in Regulation (EU) No 910/2014

Campo	Emitido en HSM	Emitido en Software	Oblig	Crít	Observaciones
<i>SELLO-E de PJ</i>	Identificación y Firma	Identificación y Firma			
2.9.6. semnaticsllegal	0.4.0.194121.1.2				Para indicar semántica de persona jurídica definida por la EN 319 412-1
2.10. Basic Constraints			Sí	Sí	
2.10.1. cA	FALSE		Sí		

7. Certificado de SELLO IoT

Existe un único perfil emitido en software.

Este perfil no se gestiona desde la plataforma NebulaCert.

Campo	Emitido en Software	Oblig	Crít	Observaciones
<i>SELLO-E de IOT</i>	Identificación y Firma			
1. Basic structure				
1.1. Version	"2"	Sí		Integer=2 [RFC5280] El literal "2" corresponde a la versión 3.
1.2. Serial Number	Establecido automáticamente por la CA. Número identificativo único del certificado.	Sí		Integer. SerialNumber = ej: 111222. // [RFC5280] No superior a 20 octetos y no puede ser un número negativo ni 0.
1.3. Signature Algorithm	SHA-256 with RSA Signature	Sí		1.2.840.113549.1.1.11
1.4. Issuer		Sí		Todos los campos tienen que

Campo	Emitido en Software	Oblig	Crít	Observaciones
<i>SELLO-E de IOT</i>	Identificación y Firma			
Distinguished Name				estar codificados en UTF8
1.4.1. Country (C)	"ES"	Sí		OID 2.5.4.6 Size [RFC 5280] 2 (PrintableString)
1.4.2. Organization (O)	"VINTEGRIS SL"	Sí		OID 2.5.4.10 Size [RFC 5280] 128 (String UTF8)
1.4.3. Locality (L)	"Barcelona"			OID 2.5.4.7 Size [RFC 5280] 128 (String UTF8)
1.4.4. Organizational Unit (OU)	"EC-VINTEGRIS"			OID 2.5.4.11 Size [RFC 5280] 64 (String UTF8)
1.4.5. Organizational Unit (OU)	"see current address at https://www.vincasign.net/contact "			OID 2.5.4.11 Size [RFC 5280] 64 (String UTF8)
1.4.6. Serial Number	"B62913926"	Sí		OID 2.5.4.5 (Printable String) Size = 9

Campo	Emitido en Software	Oblig	Crít	Observaciones
SELLO-E de IOT	Identificación y Firma			
1.4.7. OrganizationalIdentifier	"VATES-B62913926"			OID 2.5.4.97 (String UTF8)
1.4.8. Common Name (CN)	"vinCAsign NEBULASUITE Authority"	Sí		Size [RFC 5280] 80 (String UTF8)
1.5. Validity		Sí		
1.5.1. Not Before	Fecha de inicio de validez	Sí		UTCTime YYMMDDHHMMSSZ
1.5.2. Not After	Fecha de expiración	Sí		UTCTime YYMMDDHHMMSSZ
1.6. Subject		Sí		Todos los campos tienen que estar codificados en UTF8
1.6.1. Country (C)	"ES"	Sí		OID 2.5.4.6 (PrintableString)
1.6.2. Organization (O)	Denominación (nombre "oficial" de la persona jurídica) del creador del sello (Empresa, Organización, Entidad)	Sí		OID 2.5.4.10
1.6.3. Organizational Unit (OU)	Id de la cosa, que permita identificar únicamente su ubicación.	Sí		OID 2.5.4.11 Size [RFC 5280] 64 (String UTF8)
1.6.4. OrganizationIdentifier	NIF de la persona jurídica a la que está vinculado este sello, en formato ETSI EN 319412-1 (Ejemplo: "VATES-Q0000000J)	Sí		OID 2.5.4.97

Campo	Emitido en Software	Oblig	Crít	Observaciones
SELLO-E de IOT	Identificación y Firma			
1.6.5. Serial Number	NIF de la persona jurídica	Sí		OID 2.5.4.5 (PrintableString)
1.6.6. Common Name (CN)	Nombre descriptivo de la cosa. Asegurando que dicho nombre tenga sentido y no dé lugar a ambigüedades.	Sí		OID 2.5.4.3
1.7. Subject Public Key Info	Clave pública del firmante, codificada en RSA encryption (2048 bits)	Sí		OID 1.2.840.113549.1.1.1
2. Extensions				
2.1. Authority Key Identifier	Presente	Sí	No	OID 2.5.29.35 (Marcado como NO crítico según EN 319412-2)
2.2. Subject Key Identifier	Presente	Sí	No	OID 2.5.29.14 Identificador de la clave pública del suscriptor (derivada hash clave pub subj). (Marcado como NO crítico según EN 319412-2)
2.3. Key Usage		Sí	Sí	OID 2.5.29.15
2.3.1. Digital Signature	Seleccionado "1"	Sí		Se utiliza cuando se realiza la función de autenticación de

Campo	Emitido en Software	Oblig	Crít	Observaciones
<i>SELLO-E de IOT</i>	Identificación y Firma			
				activo digital de la persona jurídica
2.3.2. Content commintment	Seleccionado "1"	Sí		Se utiliza cuando se realiza la función de sello electrónico de documento expedido por persona jurídica
2.3.3. Key Encipherment	Seleccionado "1"	Sí		Se utiliza para gestión y transporte de claves
2.3.4. Data Encipherment	No seleccionado. "0"			
2.3.5. Key Agreement	No seleccionado. "0"			
2.3.6. Key Certificate Signature	No seleccionado. "0"			
2.3.7. CRL Signature	No seleccionado. "0"			
2.4. Certificate Policies		Si	No	OID 2.5.29.32 (Marcado como NO crítico según EN 319412-2)

Campo	Emitido en Software	Oblig	Crít	Observaciones
SELLO-E de IOT	Identificación y Firma			
2.4.1. Policy Identifier ²⁴	1.3.6.1.4.1.47155.1.7.2			
2.4.2. Policy Identifier ²⁵	0.4.0.194112.1.1	Sí		
2.4.3. Policy Qualifier ID		Sí		
2.4.3.1. CPS Pointer	https://policy.vincasign.net	Sí		
2.4.3.2. Use r Notice	“Certificado cualificado de sello electrónico para IoT emitido en software. Ver https://policy.vincasign.net “	Sí		
2.5. Subject Alternative Names		Sí	No	Este apartado puede disponer de más campos (Marcado como NO crítico según EN 319412-2).
2.5.1. rfc822Name	Correo electrónico de la entidad suscriptora del sello electrónico			
2.6. Extended Key		Sí	No	OID 2.5.29.37

²⁴ Política perteneciente a vinCAsign

²⁵ QCP-I, política para los certificados EU cualificados emitidos a personas jurídicas en software, **SIN** EL USO de un QSCD o dispositivo cualificado de creación de firma (DCCF).

Campo	Emitido en Software	Oblig	Crít	Observaciones
SELLO-E de IOT	Identificación y Firma			
Usage				(Marcado como NO crítico según EN 319412-2)
2.6.1. clientAuth	Presente (1.3.6.1.5.5.7.3.2)			Protección de mail
2.6.2. Email protection	Presente (1.3.6.1.5.5.7.3.4)			Autenticación cliente
2.6.3.				
2.6.4.				
2.7. cRLDistributionPoint		Sí	No	OID 2.5.29.31 Este apartado no es obligatorio siempre que exista la funcionalidad de OCSP. (Marcado como NO crítico según EN 319412-2)
2.7.1. distributionPoint	http://crl3.vincasign.net/casub.crl	Sí		
2.7.2. distributionPoint	http://crl4.vincasign.net/casub.crl			
2.8. Authority Info Acces		Sí	No	OID 1.3.6.1.5.5.7.1.1 (Marcado como NO crítico según EN 319412-2)
2.8.1. OCSP Access	Id-ad-ocsp	Sí		

Campo	Emitido en Software	Oblig	Crít	Observaciones
SELLO-E de IOT	Identificación y Firma			
Method				
2.8.1.1. Acc es Location	http://ocsp3.vincasign.net	Sí		
2.8.1.2. Acc es Location	http://ocsp4.vincasign.net			
2.8.2. calssuersAccessM ethod	id-ad-calssuers	Sí		
2.8.2.1. Acc es Location	http://www.vincasign.net/publickeys/casub.crt	Si		
2.9. Qualified Certificate Statements		Sí	No	
2.9.1. qCCompliance	id-etsi-qcs-QcCompliance	Sí		OID 0.4.0.1862.1.1 id-etsi-qcs-QcCompliance
2.9.2. QcEuRetentionPer iod	"15"	Sí		OID 0.4.0.1862.1.3 id-etsi-qcs- QcRetentionPeriod
2.9.3. QcPDS	{ https://www.vincasign.net/policy/es/PDS-SELLOIoT-soft/pds-selloIoT-soft-es.pdf,es },{ https://www.vincasign.net/policy/en/PDS-SELLOIoT-soft/pds-selloIoT-soft-en.pdf,en }	Sí		OID 0.4.0.1862.1.5 id-etsi-qcs-QcPDS PdsLocation ::= SEQUENCE {

Campo	Emitido en Software	Oblig	Crít	Observaciones
<i>SELLO-E de IOT</i>	Identificación y Firma			
				url IA5String, language PrintableString (SIZE(2))} -- ISO 639-1 language code
2.9.4. QcType	id-etsi-qct-eseal (0.4.0.1862.1.6.2)	Sí		OID 0.4.0.1862.1.6.2 id-etsi-qct-eseal OBJECT IDENTIFIER ::= { id-etsi-qcs- QcType 2 } -- Certificate for electronic signatures as defined in Regulation (EU) No 910/2014
2.9.5. semnaticsllegal	0.4.0.194121.1.2			Para indicar semántica de persona jurídica definida por la EN 319 412-1
2.10. Basic Constraints		Sí	Sí	
2.10.1. cA	FALSE	Sí		