Perfiles de Certificados

ENTIDAD FINAL

Versión 2.2

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
2.0		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
2.1		Se añade extensión en perfiles de PF Empleado Público	vinCAsign	12/05/2017
2.2		Se añaden los cambios de nebulaSUITE2	vinCAsign	21/10/2017

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....14
4. Certificado de PERSONA FÍSICA REPRESENTANTE de una ENTIDAD SIN PERSONALIDAD JURÍDICA....25
5. Certificado de PERSONA FÍSICA EMPLEADO PÚBLICO de una AAPP....38
6. Certificado de SELLO DE ÓRGANO para una Administración Pública....50
7. Certificado de SELLO ELECTRÓNICO de persona jurídica....62
8. Certificado de SELLO IoT....72

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 *PERSONA FÍSICA vinculada*	Emitido en HSM **Identificación y Firma**	Emitido en Software **Identificación y Firma**	Oblig	Crít	Observaciones
1. Basic estructure					
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

Campo *PERSONA FÍSICA vinculada*	**Emitido en HSM** **Identificación y Firma**	**Emitido en Software** **Identificación y Firma**	Oblig	Crít	Observaciones
1.4. Issuer Distinguished Name			Sí		Todos los campos tienen que 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*
1.4.7. OrganizationalIdentifier	"VATES-B62913926"				*OID 2.5.4.97* *(String UTF8)*

Campo *PERSONA FÍSICA vinculada*	**Emitido en HSM** **Identificación y Firma**	**Emitido en Software** **Identificación y Firma**	Oblig	Crít	Observaciones
1.4.8. Common Name (CN)	"vinCAsign NEBULASUITE2 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 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*** *(String UTF8)*
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

Campo *PERSONA FÍSICA vinculada*	Emitido en HSM **Identificación y Firma**	Emitido en Software **Identificación y Firma**	Oblig	Crít	Observaciones
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[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

[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 *PERSONA FÍSICA vinculada*	**Emitido en HSM** **Identificación y Firma**	**Emitido en Software** **Identificación y Firma**	Oblig	Crít	Observaciones
					(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"**	**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"			

Campo *PERSONA FÍSICA vinculada*	Emitido en HSM Identificación y Firma	Emitido en Software Identificación y Firma	Oblig	Crít	Observaciones
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)
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		

[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 *PERSONA FÍSICA vinculada*	**Emitido en HSM** **Identificación y Firma**	**Emitido en Software** **Identificación y Firma**	Oblig	Crít	Observaciones
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 (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

Campo *PERSONA FÍSICA vinculada*	Emitido en HSM Identificación y Firma	Emitido en Software Identificación y Firma	Oblig	Crít	Observaciones
					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://crl1.vincasign.net/canebula2.crl		Sí		
2.7.2. distributionPoint	http://crl2.vincasign.net/canebula2.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. OCSP Access Method	Id-ad-ocsp		Sí		
2.8.1.1. Acces Location	http://ocsp.vincasign.net		Sí		
2.8.2. caIssuersAccessMethod	id-ad-caIssuers		Sí		
2.8.2.1. Acces Location	http://www.vincasign.net/publickeys/casub.crt		Si		

Campo *PERSONA FÍSICA vinculada*	**Emitido en HSM** **Identificación y Firma**	**Emitido en Software** **Identificación y Firma**	Oblig	Crít	Observaciones
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
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 }

Campo *PERSONA FÍSICA vinculada*	Emitido en HSM **Identificación y Firma**	Emitido en Software **Identificación y Firma**	Oblig	Crít	Observaciones
					-- Certificate for electronic signatures as defined in Regulation (EU) No 910/2014
2.9.6. semnaticsIdNatural	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 *P. Física REPRESENTANTE*	Emitido en HSM Identificación y Firma	Emitido en Software Identificación y Firma	Oblig	Crít	Observaciones
1. Basic estructure					
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

Campo *P. Física REPRESENTANTE*	Emitido en HSM Identificación y Firma	Emitido en Software Identificación y Firma	Oblig	Crít	Observaciones
1.4. Issuer Distinguished Name			Sí		Todos los campos tienen que 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 *P. Física REPRESENTANTE*	Emitido en HSM Identificación y Firma	Emitido en Software Identificación y Firma	Oblig	Crít	Observaciones
1.4.7. OrganizationalIdentifier	"VATES-B62913926"				*OID 2.5.4.97* *(String UTF8)*
1.4.8. Common Name (CN)	"vinCAsign NEBULASUITE2 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 *P. Física REPRESENTANTE*	Emitido en HSM Identificación y Firma	Emitido en Software Identificación y Firma	Oblig	Crít	Observaciones
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]	• 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 carácteres 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 *P. Física REPRESENTANTE*	Emitido en HSM Identificación y Firma	Emitido en Software Identificación y Firma	Oblig	Crít	Observaciones
	• 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 *P. Física REPRESENTANTE*	Emitido en HSM Identificación y Firma	Emitido en Software Identificación y Firma	Oblig	Crít	Observaciones
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 HSM	Emitido en Software	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 *P. Física REPRESENTANTE*	Emitido en HSM Identificación y Firma	Emitido en Software Identificación y Firma	Oblig	Crít	Observaciones
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 *P. Física REPRESENTANTE*	Emitido en HSM Identificación y Firma	Emitido en Software Identificación y Firma	Oblig	Crít	Observaciones
					OCSP. (Marcado como NO crítico según EN 319412-2
2.7.1. distributionPoint	http://crl1.vincasign.net/canebula2.crl		Sí		
2.7.2. distributionPoint	http://crl2.vincasign.net/canebula2.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. OCSP Access Method	Id-ad-ocsp		Sí		
2.8.1.1. Acces Location	http://ocsp.vincasign.net		Sí		
2.8.2. caIssuersAccessMethod	id-ad-caIssuers		Sí		
2.8.2.1. Acces Location	http://www.vincasign.net/publickeys/casub.crt		Si		
2.9. Qualified Certificate Statements			Sí	No	

Campo *P. Física REPRESENTANTE*	Emitido en HSM Identificación y Firma	Emitido en Software Identificación y Firma	Oblig	Crít	Observaciones
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

Campo	Emitido en HSM	Emitido en Software	Oblig	Crít	Observaciones
P. Física REPRESENTANTE	**Identificación y Firma**	**Identificación y Firma**			
2.9.6. semnaticsIdNatural	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		

4. Certificado de PERSONA FÍSICA REPRESENTANTE de una ENTIDAD SIN PERSONALIDAD JURÍDICA

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

Ambos perfiles se gestionan desde la aplicación NebulaCert.

Campo *P. Física REPR. ESPJ*	**Emitido en HSM** **Identificación y Firma**	**Emitido en Software** **Identificación y Firma**	Oblig	Crít	Observaciones
1. Basic estructure					
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

Campo *P. Física REPR. ESPJ*	Emitido en HSM Identificación y Firma	Emitido en Software Identificación y Firma	Oblig	Crít	Observaciones
					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
1.4.1. Country (C)	”ES”		Sí		*OID 2.5.4.6* *Size [RFC 5280] 2 (PrintableString)*
1.4.2. Organization (O)	“Víntegris SL”		Sí		*OID 2.5.4.10* *Size [RFC 5280] 128 (String UTF8)*
1.4.3. Locality (L)	“Hospitalet de Llobregat”				*OID 2.5.4.7*

Campo *P. Física REPR. ESPJ*	Emitido en HSM Identificación y Firma	Emitido en Software Identificación y Firma	Oblig	Crít	Observaciones
					Size [RFC 5280] 128 (String UTF8)
1.4.4. OrganizationalIdentifier	"VATES-B62913926"				*OID 2.5.4.97 (String UTF8)*
1.4.5. Common Name (CN)	"vinCAsign nebulaSUITE2 Authority"		Sí		Size [RFC 5280] 80 *(String UTF8)*
1.4.6. stateOrProvinceName	"Barcelona"		Sí		*OID 2.5.4.8*
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

Campo *P. Física REPR. ESPJ*	**Emitido en HSM** **Identificación y Firma**	**Emitido en Software** **Identificación y Firma**	Oblig	Crít	Observaciones
					codificados en UTF8
1.6.1. Country (C)	"ES"		Sí		OID 2.5.4.6 *(PrintableString)*
1.6.2. Organization (O)	Entidad sin personalidad jurídica a la que pertenece el representante, como figura en los registros oficiales.		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.		No		OID 2.5.4.11 ***Size [RFC 5280] 64*** *(String UTF8)*
1.6.4. OrganizationIdentifier	NIF de la Entidad Sin Personalidad 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
1.6.5. Title	{Representante de …/ Presidente de … / …}				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 *P. Física REPR. ESPJ*	Emitido en HSM Identificación y Firma	Emitido en Software Identificación y Firma	Oblig	Crít	Observaciones
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]	123456789Z Antonio Casas (R: Q0000000J)		Sí		OID 2.5.4.3
1.6.10. Description[15]	Codificación del documento público que acredita las facultades del firmante o los datos registrales		Sí		OID 2.5.4.13
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

[13] 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.

[14] 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 carácteres según la RFC 5280

[15] 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 *P. Física REPR. ESPJ*	Emitido en HSM Identificación y Firma	Emitido en Software Identificación y Firma	Oblig	Crít	Observaciones
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"**	**Seleccionado "1"**	Sí		
2.3.2. Content commintment	**Seleccionado "1"**	**Seleccionado "1"**	Sí		

Campo *P. Física REPR. ESPJ*	Emitido en HSM Identificación y Firma	Emitido en Software Identificación y Firma	Oblig	Crít	Observaciones
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)
2.4.1. Policy Identifier[16]	1.3.6.1.4.1.47155.1.2.11	1.3.6.1.4.1.47155.1.2.12	Sí		

[16] Política perteneciente a vinCAsign

Campo	Emitido en HSM	Emitido en Software	Oblig	Crít	Observaciones
P. Física REPR. ESPJ	**Identificación y Firma**	**Identificación y Firma**			
2.4.2. Policy Identifier[17]	0.4.0.194112.1.2		Sí		
2.4.3. Policy Identifier[18]		0.4.0.194112.1.0	Sí		
2.4.4. Policy Identifier[19]	2.16.724.1.3.5.9				
2.4.5. Policy Qualifier ID			Sí		

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

[18] 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).

[19] 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 = **2.16.724.1.3.5.9**. Indica que el certificado es un certificado de representante de "**Entidad sin personalidad jurídica**", con poderes totales, administrador único o solidario de la organización, o al menos con poderes específicos generales para actuar ante las AAPP".

Campo *P. Física REPR. ESPJ*	Emitido en HSM Identificación y Firma	Emitido en Software Identificación y Firma	Oblig	Crít	Observaciones
2.4.5.1. CPS Pointer	https://policy.vincasign.net		Sí		
2.4.5.2. User Notice	"Certificado cualificado de representante de entidad sin personalidad jurídica en DCCF. Ver https://policy.vincasign.net "	"Certificado cualificado de representante de entidad sin personalidad jurídica 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		

Campo *P. Física REPR. ESPJ*	Emitido en HSM Identificación y Firma	Emitido en Software Identificación y Firma	Oblig	Crít	Observaciones
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://crl1.vincasign.net/canebula2.crl		Sí		
2.7.2. distributionPoint	http://crl2.vincasign.net/canebula2.crl		Sí		
2.8. Authority Info Acces			Sí	No	OID 1.3.6.1.5.5.7.1.1 (Marcado como

Campo *P. Física REPR. ESPJ*	**Emitido en HSM** **Identificación y Firma**	**Emitido en Software** **Identificación y Firma**	Oblig	Crít	Observaciones
					NO crítico según EN 319412-2)
2.8.1. OCSP Access Method	Id-ad-ocsp		Sí		
2.8.1.1. Acces Location	http://ocsp.vincasign.net		Sí		
2.8.2. caIssuersAccess Method	id-ad-caIssuers		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. QcEuRetention Period	"15"		Sí		OID 0.4.0.1862.1.3 id-etsi-qcs-

Campo *P. Física REPR. ESPJ*	**Emitido en HSM** **Identificación y Firma**	**Emitido en Software** **Identificación y Firma**	Oblig	Crít	Observaciones
					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-REPESPJ-hard/pds-repespj-hard-es.pdf,es},{https://www.vincasign.net/policy/en/PDS-REPESPJ-hard/pds-repespj-hard-en.pdf,en}	{https://www.vincasign.net/policy/es/PDS-REPESPJ-soft/pds-repespj-soft-es.pdf,es},{https://www.vincasign.net/policy/en/PDS-REPESPJ-soft/pds-repespj-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

Campo *P. Física REPR. ESPJ*	Emitido en HSM Identificación y Firma	Emitido en Software Identificación y Firma	Oblig	Crít	Observaciones
					IDENTIFIER::= { id-etsi-qcs-QcType 1 } -- Certificate for electronic signatures as defined in Regulation (EU) No 910/2014
2.9.6. semnaticsIdNatural	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 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 *P.F. EMPLEADO PÚBLICO*	**Nivel ALTO** **Identificación y Firma**	**Nivel MEDIO** **Identificación y Firma**	Oblig	Crít	Observaciones
1. Basic estructure					
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*

Campo *P.F. EMPLEADO PÚBLICO*	Nivel ALTO **Identificación y Firma**	Nivel MEDIO **Identificación y Firma**	Oblig	Crít	Observaciones
1.4.7. Organization alIdentifier	"VATES-B62913926"				*OID 2.5.4.97* *(String UTF8)*
1.4.8. Common Name (CN)	"vinCAsign NEBULASUITE2 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)*

Campo *P.F. EMPLEADO PÚBLICO*	Nivel ALTO **Identificación y Firma**	Nivel MEDIO **Identificación y Firma**	Oblig	Crít	Observaciones
1.6.4. Organizational Unit (OU)	Código DIR3 de la unidad (Ejemplo: E04976701)				OID 2.5.4.1 ***Size [RFC 5280] 64*** *[String UTF8]*
1.6.5. 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
1.6.6. 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
1.6.7. Surname	Apellidos de la persona física (como consta en el DNI/NIE)		Sí		OID 2.5.4.4
1.6.8. Given Name	Nombre de la persona física (como consta en el DNI/NIE)		Sí		OID 2.5.4.42
1.6.9. Serial Number[20]	NIF del titular acorde a ETSI EN 319 412-1 "IDCES-123456789Z")		Sí		OID 2.5.4.5 *(PrintableString)*
1.6.10. Common Name (CN)[21]	Nombre Apellido1 Apellido2 – DNI 00000000G		Sí		OID 2.5.4.3

[20] Se recomienda codificación acorde a ETSI EN 319 412-1

[21] 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 *P.F. EMPLEADO PÚBLICO*	Nivel ALTO **Identificación y Firma**	Nivel MEDIO **Identificación y Firma**	Oblig	Crít	Observaciones
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	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		

Campo *P.F. EMPLEADO PÚBLICO*	Nivel ALTO **Identificación y Firma**	Nivel MEDIO **Identificación y Firma**	Oblig	Crít	Observaciones
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)
2.4.1. Policy Identifier[22]	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[23]	0.4.0.194112.1.2		Sí		

[22] Política perteneciente a vinCAsign

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

Campo *P.F. EMPLEADO PÚBLICO*	Nivel ALTO **Identificación y Firma**	Nivel MEDIO **Identificación y Firma**	Oblig	Crít	Observaciones
2.4.3. Policy Identifier[24]		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		
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		

[24] 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 *P.F. EMPLEADO PÚBLICO*	Nivel ALTO **Identificación y Firma**	Nivel MEDIO **Identificación y Firma**	Oblig	Crít	Observaciones
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 subscriptora	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
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

Campo *P.F. EMPLEADO PÚBLICO*	Nivel ALTO **Identificación y Firma**	Nivel MEDIO **Identificación y Firma**	Oblig	Crít	Observaciones
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
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		

Campo *P.F. EMPLEADO PÚBLICO*	Nivel ALTO **Identificación y Firma**	Nivel MEDIO **Identificación y Firma**	Oblig	Crít	Observaciones
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://crl1.vincasign.net/canebula2.crl		Sí		
2.7.2. distributionPoint	http://crl2.vincasign.net/canebula2.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. OCSP Access Method	Id-ad-ocsp		Sí		
2.8.1.1. Acces Location	http://ocsp.vincasign.net		Sí		
2.8.2. caIssuersAccessMethod	id-ad-caIssuers		Sí		

Campo *P.F. EMPLEADO PÚBLICO*	Nivel ALTO Identificación y Firma	Nivel MEDIO Identificación y Firma	Oblig	Crít	Observaciones
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
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

Campo *P.F. EMPLEADO PÚBLICO*	Nivel ALTO **Identificación y Firma**	Nivel MEDIO **Identificación y Firma**	Oblig	Crít	Observaciones
					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. semnaticsIdNatural	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		

6. 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 *SELLO-E ÓRGANO AAPP*	**Nivel ALTO** **Identificación y Firma**	**Nivel MEDIO** **Identificación y Firma**	Oblig	Crít	Observaciones
1. Basic estructure					
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 *SELLO-E ÓRGANO AAPP*	Nivel ALTO **Identificación y Firma**	Nivel MEDIO **Identificación y Firma**	Oblig	Crít	Observaciones
1.4.8. Common Name (CN)	"vinCAsign NEBULASUITE2 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 *SELLO-E ÓRGANO AAPP*	Nivel ALTO **Identificación y Firma**	Nivel MEDIO **Identificación y Firma**	Oblig	Crít	Observaciones
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 *SELLO-E ÓRGANO AAPP*	Nivel ALTO **Identificación y Firma**	Nivel MEDIO **Identificación y Firma**	Oblig	Crít	Observaciones
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

Campo *SELLO-E ÓRGANO AAPP*	Nivel ALTO **Identificación y Firma**	Nivel MEDIO **Identificación y Firma**	Oblig	Crít	Observaciones
					(Marcado como NO crítico según EN 319412-2)
2.4.1. Policy Identifier[25]	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[26]	0.4.0.194112.1.3		Sí		
2.4.3. Policy Identifier[27]		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	"Certificado cualificado de sello electrónico para la	Sí		

[25] Política perteneciente a vinCAsign

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

[27] QCP-l, 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 *SELLO-E ÓRGANO AAPP*	Nivel ALTO **Identificación y Firma**	Nivel MEDIO **Identificación y Firma**	Oblig	Crít	Observaciones
	Pública, Órgano o Entidad de Derecho Público, nivel alto. Ver https://policy.vincasign.net "	Administración Pública, 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 subscriptora	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

Campo	Nivel ALTO	Nivel MEDIO	Oblig	Crít	Observaciones
SELLO-E ÓRGANO AAPP	**Identificación y Firma**	**Identificación y Firma**			
2.5.2.3. NIF de la entidad subscriptora	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 Responsable	DNI o NIE del responsable del sello				OID ALTO: 2.16.724.1.3.5.6.1.4 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

Campo *SELLO-E ÓRGANO AAPP*	Nivel ALTO **Identificación y Firma**	Nivel MEDIO **Identificación y Firma**	Oblig	Crít	Observaciones
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)
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://crl1.vincasign.net/canebula2crl		Sí		

Campo *SELLO-E ÓRGANO AAPP*	Nivel ALTO **Identificación y Firma**	Nivel MEDIO **Identificación y Firma**	Oblig	Crít	Observaciones
2.7.2. distributionPoint	http://crl2.vincasign.net/canebula.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://ocsp.vincasign.net		Sí		
2.8.2. caIssuersAccessMethod	id-ad-caIssuers		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

Campo *SELLO-E ÓRGANO AAPP*	Nivel ALTO **Identificación y Firma**	Nivel MEDIO **Identificación y Firma**	Oblig	Crít	Observaciones
					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-es.pdf,es},{https://www.vincasign.net/policy/en/PDS-SELLO-ALTO/pds-sello-alto-en.pdf,en}	{https://www.vincasign.net/policy/es/PDS-SELLO-MEDIO/pds-sello-medio-es.pdf,es},{https://www.vincasign.net/policy/en/PDS-SELLO-MEDIO/pds-sello-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	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. semnaticsIdlegal	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	

Campo	Nivel ALTO	Nivel MEDIO	Oblig	Crít	Observaciones
SELLO-E ÓRGANO AAPP	**Identificación y Firma**	**Identificación y Firma**			
2.10.1. cA	FALSE		Sí		

7. 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 *SELLO-E de PJ*	Emitido en HSM **Identificación y Firma**	Emitido en Software **Identificación y Firma**	Oblig	Crít	Observaciones
1. Basic estructure					
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 *SELLO-E de PJ*	Emitido en HSM **Identificación y Firma**	Emitido en Software **Identificación y Firma**	Oblig	Crít	Observaciones
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 *SELLO-E de PJ*	Emitido en HSM **Identificación y Firma**	Emitido en Software **Identificación y Firma**	Oblig	Crít	Observaciones
1.4.8. Common Name (CN)	"vinCAsign NEBULASUITE2 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 *SELLO-E de PJ*	Emitido en HSM **Identificación y Firma**	Emitido en Software **Identificación y Firma**	Oblig	Crít	Observaciones
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 *SELLO-E de PJ*	Emitido en HSM **Identificación y Firma**	Emitido en Software **Identificación y Firma**	Oblig	Crít	Observaciones
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

Campo *SELLO-E de PJ*	Emitido en HSM Identificación y Firma	Emitido en Software Identificación y Firma	Oblig	Crít	Observaciones
					(Marcado como NO crítico según EN 319412-2)
2.4.1. Policy Identifier[28]	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[29]	0.4.0.194112.1.3		Sí		
2.4.3. Policy Identifier[30]		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		

[28] Política perteneciente a vinCAsign

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

[30] QCP-l, 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 *SELLO-E de PJ*	Emitido en HSM **Identificación y Firma**	Emitido en Software **Identificación y Firma**	Oblig	Crít	Observaciones
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 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

Campo *SELLO-E de PJ*	Emitido en HSM **Identificación y Firma**	Emitido en Software **Identificación y Firma**	Oblig	Crít	Observaciones
					OCSP. (Marcado como NO crítico según EN 319412-2
2.7.1. distributionPoint	http://crl1.vincasign.net/canebula2.crl		Sí		
2.7.2. distributionPoint	http://crl2.vincasign.net/canebula2.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://ocsp.vincasign.net		Sí		
2.8.2. caIssuersAccessMethod	id-ad-caIssuers		Sí		
2.8.2.1. Acces Location	http://www.vincasign.net/publickeys/casub.crt		Si		
2.9. Qualified Certificate Statements			Sí	No	

Campo *SELLO-E de PJ*	Emitido en HSM Identificación y Firma	Emitido en Software Identificación y Firma	Oblig	Crít	Observaciones
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 *SELLO-E de PJ*	Emitido en HSM **Identificación y Firma**	Emitido en Software **Identificación y Firma**	Oblig	Crít	Observaciones
2.9.6. semnaticsIdlegal	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		

8. Certificado de SELLO IoT

Existe un único perfil emitido en software.

Este perfil no se gestiona desde la plataforma NebulaCert.

Campo *SELLO-E de IOT*	Emitido en Software **Identificación y Firma**	Oblig	Crít	Observaciones
1. Basic estructure				
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

Campo *SELLO-E de IOT*	Emitido en Software **Identificación y Firma**	Oblig	Crít	Observaciones
1.4. Issuer Distinguished Name		Sí		Todos los campos tienen que 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 NEBULASUITE2 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 *SELLO-E de IOT*	Emitido en Software **Identificación y Firma**	Oblig	Crít	Observaciones
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 *SELLO-E de IOT*	Emitido en Software **Identificación y Firma**	Oblig	Crít	Observaciones
				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[31]	1.3.6.1.4.1.47155.1.7.2			
2.4.2. Policy Identifier[32]	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. User 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			

[31] Política perteneciente a vinCAsign

[32] QCP-l, 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 *SELLO-E de IOT*	Emitido en Software **Identificación y Firma**	Oblig	Crít	Observaciones
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
2.7.1. distributionPoint	http://crl1.vincasign.net/canebula2.crl	Sí		
2.7.2. distributionPoint	http://crl2.vincasign.net/canebula2.crl			

Campo *SELLO-E de IOT*	Emitido en Software Identificación y Firma	Oblig	Crít	Observaciones
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://ocsp.vincasign.net	Sí		
2.8.2. caIssuersAccessMethod	id-ad-caIssuers	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
2.9.3. QcPDS	{https://www.vincasign.net/policy/es/PDS-SELLOIoT-soft/pds-selloIoT-soft-	Sí		OID 0.4.0.1862.1.5 id-etsi-qcs-QcPDS

Campo	Emitido en Software	Oblig	Crít	Observaciones
SELLO-E de IOT	**Identificación y Firma**			
	es.pdf,es},{https://www.vincasign.net/policy/en/PDS-SELLOIoT-soft/pds-selloIoT-soft-en.pdf,en}			PdsLocation::= SEQUENCE { 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. semnaticsIdlegal	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		