Perfiles de Certificados

ENTIDAD FINAL

Versión 3.0

PERFILES DE CERTIFICADOS v1r12 - 02022020		Política	OID ETSI	OID vinCAsign	OID HACIENDA ESP
De PERSONA FÍSICA VINCULADA a Empresa/Organización					
1	Cert Corporativo de PF en DCCF	QCP-n-qscd	0.4.0.194112.1.2	**1.3.6.1.4.1.47155.1.1.1**	
2	Cert Corporativo de PF en SOFT	QCP-n	0.4.0.194112.1.0	**1.3.6.1.4.1.47155.1.1.2**	
3	Cert Corporativo y Efímero de PF en DCCF	QCP-n-qscd	0.4.0.194112.1.2	**1.3.6.1.4.1.47155.1.1.51**	
4	Cert Corporativo y Efímero de PF en SOFT	QCP-n	0.4.0.194112.1.0	**1.3.6.1.4.1.47155.1.1.52**	
De PERSONA FÍSICA REPRESENTANTE LEGAL de Empresa/Organización ante las AAPP españolas					
5	Cert Corporativo de PF REP de PJ en DCCF	QCP-n-qscd	0.4.0.194112.1.2	**1.3.6.1.4.1.47155.1.2.1**	2.16.724.1.3.5.8
6	Cert Corporativo de PF REP de PJ en SOFT	QCP-n	0.4.0.194112.1.0	**1.3.6.1.4.1.47155.1.2.2**	2.16.724.1.3.5.8
7	Cert Corporativo y Efímero de PF REP de PJ en DCCF	QCP-n-qscd	0.4.0.194112.1.2	**1.3.6.1.4.1.47155.1.2.51**	2.16.724.1.3.5.8
8	Cert Corporativo y Efímero de PF REP de PJ en SOFT	QCP-n	0.4.0.194112.1.0	**1.3.6.1.4.1.47155.1.2.52**	2.16.724.1.3.5.8
De PERSONA FÍSICA REPRESENTANTE LEGAL de Entidad Sin Personalidad Jurídica ante las AAPP españolas					
9	Cert Corporativo de PF REP de ESPJ en DCCF	QCP-n-qscd	0.4.0.194112.1.2	**1.3.6.1.4.1.47155.1.2.11**	2.16.724.1.3.5.9
10	Cert Corporativo de PF REP de ESPJ en SOFT	QCP-n	0.4.0.194112.1.0	**1.3.6.1.4.1.47155.1.2.12**	2.16.724.1.3.5.9
11	Cert Corporativo y Efímero de PF REP de ESPJ en DCCF	QCP-n-qscd	0.4.0.194112.1.2	**1.3.6.1.4.1.47155.1.2.151**	2.16.724.1.3.5.9
12	Cert Corporativo y Efímero de PF REP de ESPJ en SOFT	QCP-n	0.4.0.194112.1.0	**1.3.6.1.4.1.47155.1.2.152**	2.16.724.1.3.5.9
De PERSONA FÍSICA EMPLEADO PÚBLICO español					
13	Cert de Empleado Público nivel ALTO	QCP-n-qscd	0.4.0.194112.1.2	**1.3.6.1.4.1.47155.1.4.1**	2.16.724.1.3.5.7.1
14	Cert de Empleado Público nivel MEDIO	QCP-n	0.4.0.194112.1.0	**1.3.6.1.4.1.47155.1.4.2**	2.16.724.1.3.5.7.2
15	Cert de Empleado Público con seudónimo nivel ALTO	QCP-n-qscd	0.4.0.194112.1.2	**1.3.6.1.4.1.47155.1.4.11**	2.16.724.1.3.5.4.1
16	Cert de Empleado Público con seudónimo nivel MEDIO	QCP-n	0.4.0.194112.1.0	**1.3.6.1.4.1.47155.1.4.12**	2.16.724.1.3.5.4.2
SELLO ELECTRÓNICO de Administración Pública española					
17	Cert de Sello de AAPP nivel ALTO	QCP-l-qscd	0.4.0.194112.1.3	**1.3.6.1.4.1.47155.1.5.1**	2.16.724.1.3.5.6.1
18	Cert de Sello de AAPP nivel MEDIO	QCP-l	0.4.0.194112.1.1	**1.3.6.1.4.1.47155.1.5.2**	2.16.724.1.3.5.6.2
SELLO ELECTRÓNICO de Persona JURÍDICA					
19	Cert de Sello de Empresa en DCCF	QCP-l-qscd	0.4.0.194112.1.3	**1.3.6.1.4.1.47155.1.6.1**	
20	Cert de Sello de Empresa en SOFT	QCP-l	0.4.0.194112.1.1	**1.3.6.1.4.1.47155.1.6.2**	
21	Cert Efímero de Sello de Empresa en DCCF	QCP-l-qscd	0.4.0.194112.1.3	**1.3.6.1.4.1.47155.1.6.51**	
22	Cert Efímero de Sello de Empresa en SOFT	QCP-l	0.4.0.194112.1.1	**1.3.6.1.4.1.47155.1.6.52**	
SELLO ELECTRÓNICO para Internet of Things					
23	Cert de Sello para IoT	QCP-l	0.4.0.194112.1.1	**1.3.6.1.4.1.47155.1.7.2**	
SELLO ELECTRÓNICO para Tiempo Electrónico					
24	Cert Corporativo de Sello de Tiempo Electrónico	QCP-l	0.4.0.194112.1.1	**1.3.6.1.4.1.47155.1.9.1**	
De PERSONA FÍSICA - INDIVIDUAL					
25	Cert Individual de PF en DCCF	QCP-n-qscd	0.4.0.194112.1.2	**1.3.6.1.4.1.47155.1.10.1**	
26	Cert Individual de PF en SOFT	QCP-n	0.4.0.194112.1.0	**1.3.6.1.4.1.47155.1.10.2**	
27	Cert Individual y Efímero de PF en DCCF	QCP-n-qscd	0.4.0.194112.1.2	**1.3.6.1.4.1.47155.1.10.51**	
28	Cert Individual y Efímero de PF en SOFT	QCP-n	0.4.0.194112.1.0	**1.3.6.1.4.1.47155.1.10.52**	
De PERSONA FÍSICA - INDIVIDUAL					
29	Cert Persona física Representante AGIF en DCCF	QCP-n-qscd	0.4.0.194112.1.2	**1.3.6.1.4.1.47155.1.11.1**	
30	Cert Persona física Representante AGIF en SOFT	QCP-n	0.4.0.194112.1.0	**1.3.6.1.4.1.47155.1.11.2**	

1. Cert Corporativo de PF en DCCF

Campo PERSONA FÍSICA · DCCF	Gestión CENTRALIZADA Identificación y Firma	Oblig.	Crít.	Longitud máxima	Codif	Observaciones OID 1.3.6.1.4.1.47155.1.1.1
1. Basic estructure						
1.1. Version	"2"	Sí		1	Integer	El literal "2" corresponde a la versión 3.
1.2. Serial Number	Establecido automáticamente por la CA. Número identificativo único del certificado.	Sí		20 octetos	Integer	No puede ser un número negativo ni 0.
1.3. Signature Algorithm		Sí				
1.3.1. Algorithm	SHA-256 with RSA Signature	Sí			OID	1.2.840.113549.1.1.11
1.3.2. Parameters	No aplicable	No				
1.4. Issuer		Sí				
1.4.1. Country Name (C)	"ES"	Sí		2 caracteres	PrintableString	OID 2.5.4.6
1.4.2. Organization Name (O)	"VINTEGRIS SL"	Sí		64 caracteres	UTF8String	OID 2.5.4.10
1.4.3. organizationalUnitName (OU)	"vinCAsign"	Sí				OID 2.5.4.11
1.4.4. Locality Name (L)	"HOSPITALET DE LLOBREGAT"	Sí		128 caracteres	UTF8String	OID 2.5.4.7
1.4.5. Organization Identifier	"VATES-B62913926"	Sí		Ilimitado	UTF8String	OID 2.5.4.97
1.4.6. Common Name (CN)	"vinCAsign nebulaSUITE2 Authority"	Sí		64 caracteres	UTF8String	OID 2.5.4.3
1.4.7. stateOrProvinceName	"BARCELONA"	Sí			UTF8String	OID 2.5.4.8
1.5. Validity		Sí				3 YEAR
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				
1.6.1. Country Name	"ES"	Sí		2 caracteres	PrintableString	OID 2.5.4.6
1.6.2. Organization (O)	Organización a la que pertenece el firmante.	Sí		40 caracteres	UTF8String	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		16 caracteres	UTF8String	OID 2.5.4.11
1.6.4. Organization Identifier	NIF de la persona jurídica a la que está vinculado el titular del certificado, en formato ETSI EN 319412-1	Sí		64 caracteres	PrintableString	OID 2.5.4.97
1.6.5. Title	Cargo del firmante en la organización			64 caracteres	UTF8String	OID 2.5.4.12
1.6.6. Serial Number	NIF del titular acorde a ETSI EN 319 412-1 "IDCES-123456789Z")	Sí			PrintableString	OID 2.5.4.5
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. Common Name	APELLIDO1 APELLIDO2 NOMBRE – DNI 1234567892	Sí				OID 2.5.4.3
1.6.10. emailAddress	Correo electrónico del firmante	Sí			IA5String	

1.7. Subject Public Key Info	Clave pública del firmante, codificada en RSA encryption (2048 bits)	Sí				
1.7.1. AlgorithmIdentifier						
1.7.1.1. Algorithm	RSA encryption	Sí			OID	OID 1.2.840.113549.1.1.1
1.7.1.2. Parameters	No aplicable	No				
1.7.2. SubjectPublicKey	Clave pública del firmante	Sí			Bit String	
2. Extensions						
2.1. Authority Key Identifier	Identificador de la clave del emisor	Sí	No			OID 2.5.29.35 (Marcado como NO crítico según EN 319412-2)
2.1.1. KeyIdentifier		Sí			Octet string	Derivado de la clave pública
2.1.2. AuthorityCertIssuer	Nombre de la CA a la que corresponde la clave identificada en keyIdentifier					(String UTF8) Size 12
2.1.3. AuthorityCertSerialNumber	Número de serie del certificado de CA					
2.2. Subject Key Identifier	Identificador de la clave del firmante	Sí	No			OID 2.5.29.14 (Marcado como NO crítico según EN 319412-2)
2.2.1. KeyIdentifier		Sí			Octet string	Derivado de la clave pública
2.3. Key Usage		Sí	Sí		Bit String	OID 2.5.29.15
2.3.1. Digital Signature	**Seleccionado "1"**	Sí				Bit para autenticación
2.3.2. Content commintment	**Seleccionado "1"**	Sí				Bit para firma
2.3.3. Key Encipherment	No seleccionado. "0"					
2.3.4. Data Encipherment	No seleccionado. "0"					
2.3.5. Key Agreement	No seleccionado. "0"					
2.3.6. Key Certificate Signature	No seleccionado. "0"					
2.3.7. CRL Signature	No seleccionado. "0"					
2.3.8. Encipher Only	No seleccionado. "0"					
2.3.9. Decipher Only	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 Information		Sí				
2.4.1.1. Policy Identifier	**1.3.6.1.4.1.47155.1.1.1**	Sí			OID	Identificador de la política de Logalty
2.4.1.2. Policy Qualifiers		Sí				
2.4.1.1.1 CPS URI	https://policy.vincasign.net				IA5String	URL de la DPC (opcional por CAB FORUM)
2.4.1.1.2. User Notice/Explicit text	"Certificado cualificado de persona física vinculada emitido en un DCCF. Ver https://policy.vincasign.net "	Sí		200 caracteres	UTF8String y NFC	Texto indicativo
2.4.2. Policy Information		Sí				

	2.4.2.1. Policy Identifier	**0.4.0.194112.1.2**	Sí			OID	QCP-n-qscd. Identificador de la política de certificado cualificado de persona física con dispositivo seguro
	2.5. Subject Alternative Names		Sí	No			OID 2.5.29.17 (Marcado como NO crítico según EN 319412-2)
	2.5.1. DirectoryName	Nombre de la persona física (como consta en el DNI/NIE)	Sí				OID 1.3.6.1.4.1.47155.1.1
		Apellido primero de la persona física (como consta en el DNI/NIE)	Sí				OID 1.3.6.1.4.1.47155.1.2
		Apellido segundo de la persona física (como consta en el DNI/NIE)	Sí				OID 1.3.6.1.4.1.47155.1.3
		NIF del titular acorde a ETSI EN 319 412-1 "IDCES-1234567890Z")	Sí			PrintableString	OID 1.3.6.1.4.1.47155.1.4
		Organización a la que pertenece el representante.	Sí		40 caracteres	UTF8String	OID 1.3.6.1.4.1.47155.1.6
		NIF de la persona jurídica de la que es representante el titular del certificado, en formato ETSI EN 319412-1 (Ejemplo: "VATES-Q0000000J)	Sí		64 caracteres	PrintableString	OID 1.3.6.1.4.1.47155.1.7
	2.5.1. rfc822Name	Correo electrónico de la persona física	Sí			rfc822Name	
	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			OID	
	2.6.2. Email protection	Presente (1.3.6.1.5.5.7.3.4)	Sí			OID	Sólo se activa si se incluye el correo electrónico del firmante
	2.7. cRLDistributionPoint		No	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			IA5String	uniformResourceIdentifier **(NO HTTPS)**
	2.7.2. distributionPoint	http://crl2.vincasing.net/canebula2.crl	Sí			IA5String	uniformResourceIdentifier **(NO HTTPS)**
	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. Access Description		Sí				
	2.8.1.1. Acces Method	id-ad-ocsp	Sí			OID	OID 1.3.6.1.5.5.7.48.1
	2.8.1.2. Acces Location	http://ocsp.vincasign.net	Sí			IA5String	URL de acceso al OCSP **(NO HTTPS)** uniformResourceIdentifier
	2.8.2. Access Description		Sí				
	2.8.2.1. Acces Method	id-ad-calssuers	Sí			OID	OID 1.3.6.1.5.5.7.48.2
	2.8.2.1. Acces Location	http://www.vincasign.net/publickeys/casub.crt	Si			IA5String	URL acceso a certificado de la CA (NO HTTPS) uniformResourceIdentifier
	2.9. Qualified Certificate Statements		Sí	No			OID 1.3.6.1.5.5.7.1.3
	2.9.1. qCCompliance	id-etsi-qcs-QcCompliance	Sí				OID 0.4.0.1862.1.1 Indicación de certificado cualificado

	2.9.2. QcEuRetentionPeriod	"15"	Sí				OID 0.4.0.1862.1.3 Plazo de retención de registros
	2.9.3. QcSSCD	id-etsi-qcs-QcSSCD	Sí				OID 0.4.0.1862.1.4 Dispositivo cualificado de creación de 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}	Sí				OID 0.4.0.1862.1.5 **(SÍ HTTPS)** URLs de acceso al texto divulgativo en inglés (obligatorio) y en castellano
	2.9.5. QcType	id-etsi-qct-esign	Sí				OID 0.4.0.1862.1.6.1 Certificado de firma electrónica conforme al Reglamento (UE) Nº 910/2014
	2.9.6. qcStatement-2						OID 1.3.6.1.5.5.7.11.2 (RFC 3739)
	2.9.6.1. SemanticsInformation						
	2.9.6.1.1. semanticsIdNatural	0.4.0.194121.1.1					Semántica de persona fisica conforme a EN 319 412-1, en serial number
	2.10. Basic Constraints		Sí	Sí			OID 2.5.29.19
	2.10.1. cA	FALSO	Sí			Boolean	

2. Cert Corporativo de PF en SOFT

Campo PERSONA FÍSICA · SOFT	Gestión CENTRALIZADA Identificación y Firma	Oblig.	Crít.	Longitud máxima	Codif	Observaciones OID 1.3.6.1.4.1.47155.1.1.2
1. Basic estructure						
1.1. Version	"2"	Sí		1	Integer	El literal "2" corresponde a la versión 3.
1.2. Serial Number	Establecido automáticamente por la CA. Número identificativo único del certificado.	Sí		20 octetos	Integer	No puede ser un número negativo ni 0.
1.3. Signature Algorithm		Sí				
1.3.1. Algorithm	SHA-256 with RSA Signature	Sí			OID	1.2.840.113549.1.1.11
1.3.2. Parameters	No aplicable	No				
1.4. Issuer		Sí				
1.4.1. Country Name (C)	"ES"	Sí		2 caracteres	PrintableString	OID 2.5.4.6
1.4.2. Organization Name (O)	"VINTEGRIS SL"	Sí		64 caracteres	UTF8String	OID 2.5.4.10
1.4.3. organizationalUnitName (OU)	"vinCAsign"	Sí				OID 2.5.4.11
1.4.4. Locality Name (L)	"HOSPITALET DE LLOBREGAT"	Sí		128 caracteres	UTF8String	OID 2.5.4.7
1.4.5. Organization Identifier	"VATES-B62913926"	Sí		Ilimitado	UTF8String	OID 2.5.4.97
1.4.6. Common Name (CN)	"vinCAsign nebulaSUITE2 Authority"	Sí		64 caracteres	UTF8String	OID 2.5.4.3
1.4.7. stateOrProvinceName	"BARCELONA"	Sí			UTF8String	OID 2.5.4.8
1.5. Validity		Sí				3 YEAR
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				
1.6.1. Country Name	"ES"	Sí		2 caracteres	PrintableString	OID 2.5.4.6
1.6.2. Organization (O)	Organización a la que pertenece el firmante.	Sí		40 caracteres	UTF8String	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		16 caracteres	UTF8String	OID 2.5.4.11
1.6.4. Organization Identifier	NIF de la persona jurídica a la que está vinculado el titular del certificado, en formato ETSI EN 319412-1	Sí		64 caracteres	PrintableString	OID 2.5.4.97
1.6.5. Title	Cargo del firmante en la organización			64 caracteres	UTF8String	OID 2.5.4.12
1.6.6. Serial Number	NIF del titular acorde a ETSI EN 319 412-1 "IDCES-123456789Z")	Sí			PrintableString	OID 2.5.4.5
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. Common Name	APELLIDO1 APELLIDO2 NOMBRE – DNI 123456789Z	Sí				OID 2.5.4.3
1.6.10. emailAddress	Correo electrónico del firmante	Sí			IA5String	

1.7. Subject Public Key Info	Clave pública del firmante, codificada en RSA encryption (2048 bits)	Sí				
1.7.1. AlgorithmIdentifier						
1.7.1.1. Algorithm	RSA encryption	Sí			OID	OID 1.2.840.113549.1.1.1
1.7.1.2. Parameters	No aplicable	No				
1.7.2. SubjectPublicKey	Clave pública del firmante	Sí			Bit String	
2. Extensions						
2.1. Authority Key Identifier	Identificador de la clave del emisor	Sí	No			OID 2.5.29.35 (Marcado como NO crítico según EN 319412-2)
2.1.1. KeyIdentifier		Sí			Octet string	Derivado de la clave pública
2.1.2. AuthorityCertIssuer	Nombre de la CA a la que corresponde la clave identificada en keyIdentifier					(String UTF8) Size 12
2.1.3. AuthorityCertSerialNumber	Número de serie del certificado de CA					
2.2. Subject Key Identifier	Identificador de la clave del firmante	Sí	No			OID 2.5.29.14 (Marcado como NO crítico según EN 319412-2)
2.2.1. KeyIdentifier		Sí			Octet string	Derivado de la clave pública
2.3. Key Usage		Sí	Sí		Bit String	OID 2.5.29.15
2.3.1. Digital Signature	**Seleccionado "1"**	Sí				Bit para autenticación
2.3.2. Content commintment	**Seleccionado "1"**	Sí				Bit para firma
2.3.3. Key Encipherment	No seleccionado. "0"					
2.3.4. Data Encipherment	No seleccionado. "0"					
2.3.5. Key Agreement	No seleccionado. "0"					
2.3.6. Key Certificate Signature	No seleccionado. "0"					
2.3.7. CRL Signature	No seleccionado. "0"					
2.3.8. Encipher Only	No seleccionado. "0"					
2.3.9. Decipher Only	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 Information		Sí				
2.4.1.1. Policy Identifier	**1.3.6.1.4.1.47155.1.1.2**	Sí			OID	Identificador de la política de Logalty
2.4.1.2. Policy Qualifiers		Sí				
2.4.1.1.1 CPS URI	https://policy.vincasign.net				IA5String	URL de la DPC (opcional por CAB FORUM)
2.4.1.1.2. User Notice/Explicit text	"Certificado cualificado de persona física vinculada emitido en software. Ver https://policy.vincasign.net "	Sí		200 caracteres	UTF8String y NFC	Texto indicativo
2.4.2. Policy Information		Sí				

	2.4.2.1. Policy Identifier	**0.4.0.194112.1.0**	Sí			OID	QCP-n. Identificador de la política de certificado cualificado de persona física sin uso de dispositivo seguro
	2.5. Subject Alternative Names		Sí	No			OID 2.5.29.17 (Marcado como NO crítico según EN 319412-2)
	2.5.1. DirectoryName	Nombre de la persona física (como consta en el DNI/NIE)	Sí				OID 1.3.6.1.4.1.47155.1.1
		Apellido primero de la persona física (como consta en el DNI/NIE)	Sí				OID 1.3.6.1.4.1.47155.1.2
		Apellido segundo de la persona física (como consta en el DNI/NIE)	Sí				OID 1.3.6.1.4.1.47155.1.3
		NIF del titular acorde a ETSI EN 319 412-1 "IDCES-123456789Z")	Sí			PrintableString	OID 1.3.6.1.4.1.47155.1.4
		Organización a la que pertenece el representante.	Sí		40 caracteres	UTF8String	OID 1.3.6.1.4.1.47155.1.6
		NIF de la persona jurídica de la que es representante el titular del certificado, en formato ETSI EN 319412-1 (Ejemplo: "VATES-Q0000000J)	Sí		64 caracteres	PrintableString	OID 1.3.6.1.4.1.47155.1.7
	2.5.2. rfc822Name	Correo electrónico de la persona física	Sí			rfc822Name	
	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			OID	
	2.6.2. Email protection	Presente (1.3.6.1.5.5.7.3.4)	Sí			OID	Sólo se activa si se incluye el correo electrónico del firmante
	2.7. cRLDistributionPoint		No	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			IA5String	uniformResourceIdentifier **(NO HTTPS)**
	2.7.2. distributionPoint	http://crl2.vincasing.net/canebula2.crl	Sí			IA5String	uniformResourceIdentifier **(NO HTTPS)**
	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. Access Description		Sí				
	2.8.1.1. Acces Method	id-ad-ocsp	Sí			OID	OID 1.3.6.1.5.5.7.48.1
	2.8.1.2. Acces Location	http://ocsp.vincasign.net	Sí			IA5String	URL de acceso al OCSP **(NO HTTPS)** uniformResourceIdentifier
	2.8.2. Access Description		Sí				
	2.8.2.1. Acces Method	id-ad-caIssuers	Sí			OID	OID 1.3.6.1.5.5.7.48.2
	2.8.2.1. Acces Location	http://www.vincasign.net/publickeys/casub.crt	Si			IA5String	URL acceso a certificado de la CA (NO HTTPS) uniformResourceIdentifier
	2.9. Qualified Certificate Statements		Sí	No			OID 1.3.6.1.5.5.7.1.3
	2.9.1. qCCompliance	id-etsi-qcs-QcCompliance	Sí				OID 0.4.0.1862.1.1 Indicación de certificado cualificado

	2.9.2. QcEuRetentionPeriod	"15"	Sí				OID 0.4.0.1862.1.3 Plazo de retención de registros
	2.9.4. QcPDS	{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 **(SÍ HTTPS)** URLs de acceso al texto divulgativo en inglés (obligatorio) y en castellano
	2.9.5. QcType	id-etsi-qct-esign	Sí				OID 0.4.0.1862.1.6.1 Certificado de firma electrónica conforme al Reglamento (UE) Nº 910/2014
	2.9.6. qcStatement-2						OID 1.3.6.1.5.5.7.11.2 (RFC 3739)
	2.9.6.1. SemanticsInformation						
	2.9.6.1.1. semanticsIdNatural	0.4.0.194121.1.1					Semántica de persona fisica conforme a EN 319 412-1, en serial number
	2.10. Basic Constraints		Sí	Sí			OID 2.5.29.19
	2.10.1. cA	FALSO	Sí			Boolean	

3. Cert Corporativo y Efímero de PF en DCCF

Campo EFÍMERO DE PERSONA FÍSICA · DCCF	Gestión CENTRALIZADA Identificación y Firma	Oblig.	Crít.	Longitud máxima	Codif	Observaciones OID 1.3.6.1.4.1.47155.1.1.51
1. Basic estructure						
1.1. Version	"2"	Sí		1	Integer	El literal "2" corresponde a la versión 3.
1.2. Serial Number	Establecido automáticamente por la CA. Número identificativo único del certificado.	Sí		20 octetos	Integer	No puede ser un número negativo ni 0.
1.3. Signature Algorithm		Sí				
1.3.1. Algorithm	SHA-256 with RSA Signature	Sí			OID	1.2.840.113549.1.1.11
1.3.2. Parameters	No aplicable	No				
1.4. Issuer		Sí				
1.4.1. Country Name (C)	"ES"	Sí		2 caracteres	PrintableString	OID 2.5.4.6
1.4.2. Organization Name (O)	"VINTEGRIS SL"	Sí		64 caracteres	UTF8String	OID 2.5.4.10
1.4.3. organizationalUnitName (OU)	"vinCAsign"	Sí				OID 2.5.4.11
1.4.4. Locality Name (L)	"HOSPITALET DE LLOBREGAT"	Sí		128 caracteres	UTF8String	OID 2.5.4.7
1.4.5. Organization Identifier	"VATES-B62913926"	Sí		Ilimitado	UTF8String	OID 2.5.4.97
1.4.6. Common Name (CN)	"vinCAsign nebulaSUITE2 Authority"	Sí		64 caracteres	UTF8String	OID 2.5.4.3
1.4.7. stateOrProvinceName	"BARCELONA"	Sí			UTF8String	OID 2.5.4.8
1.5. Validity	MENOR DE 1 HORA	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				
1.6.1. Country Name	"ES"	Sí		2 caracteres	PrintableString	OID 2.5.4.6
1.6.2. Organization (O)	Organización a la que pertenece el firmante.	Sí		40 caracteres	UTF8String	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		16 caracteres	UTF8String	OID 2.5.4.11
1.6.4. Organization Identifier	NIF de la persona jurídica a la que está vinculado el titular del certificado, en formato ETSI EN 319412-1	Sí		64 caracteres	PrintableString	OID 2.5.4.97
1.6.5. Title	Cargo del firmante en la organización			64 caracteres	UTF8String	OID 2.5.4.12
1.6.6. Serial Number	NIF del titular acorde a ETSI EN 319 412-1 "IDCES-123456789Z")	Sí			PrintableString	OID 2.5.4.5
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. Common Name	APELLIDO1 APELLIDO2 NOMBRE – DNI 1234567892	Sí				OID 2.5.4.3
1.6.10. emailAddress	Correo electrónico del firmante	Sí			IA5String	

1.7. Subject Public Key Info	Clave pública del firmante, codificada en RSA encryption (2048 bits)	Sí				
1.7.1. AlgorithmIdentifier						
1.7.1.1. Algorithm	RSA encryption	Sí			OID	OID 1.2.840.113549.1.1.1
1.7.1.2. Parameters	No aplicable	No				
1.7.2. SubjectPublicKey	Clave pública del firmante	Sí			Bit String	
2. Extensions						
2.1. Authority Key Identifier	Identificador de la clave del emisor	Sí	No			OID 2.5.29.35 (Marcado como NO crítico según EN 319412-2)
2.1.1. KeyIdentifier		Sí			Octet string	Derivado de la clave pública
2.1.2. AuthorityCertIssuer	Nombre de la CA a la que corresponde la clave identificada en keyIdentifier					(String UTF8) Size 12
2.1.3. AuthorityCertSerialNumber	Número de serie del certificado de CA					
2.2. Subject Key Identifier	Identificador de la clave del firmante	Sí	No			OID 2.5.29.14 (Marcado como NO crítico según EN 319412-2)
2.2.1. KeyIdentifier		Sí			Octet string	Derivado de la clave pública
2.3. Key Usage		Sí	Sí		Bit String	OID 2.5.29.15
2.3.1. Digital Signature	**Seleccionado "1"**	Sí				Bit para autenticación
2.3.2. Content commintment	**Seleccionado "1"**	Sí				Bit para firma
2.3.3. Key Encipherment	No seleccionado. "0"					
2.3.4. Data Encipherment	No seleccionado. "0"					
2.3.5. Key Agreement	No seleccionado. "0"					
2.3.6. Key Certificate Signature	No seleccionado. "0"					
2.3.7. CRL Signature	No seleccionado. "0"					
2.3.8. Encipher Only	No seleccionado. "0"					
2.3.9. Decipher Only	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 Information		Sí				
2.4.1.1. Policy Identifier	**1.3.6.1.4.1.47155.1.1.51**	Sí			OID	Identificador de la política de Logalty
2.4.1.2. Policy Qualifiers		Sí				
2.4.1.1.1 CPS URI	https://policy.vincasign.net				IA5String	URL de la DPC (opcional por CAB FORUM)
2.4.1.1.2. User Notice/Explicit text	"Certificado cualificado y efímero de persona física vinculada emitido en DCCF. Ver https://policy.vincasign.net "	Sí		200 caracteres	UTF8String y NFC	Texto indicativo
2.4.2. Policy Information		Sí				

	2.4.2.1. Policy Identifier	**0.4.0.194112.1.2**	Sí			OID	QCP-n-qscd. Identificador de la política de certificado cualificado de persona física con dispositivo seguro
	2.5. Subject Alternative Names		Sí	No			OID 2.5.29.17 (Marcado como NO crítico según EN 319412-2)
	2.5.1. DirectoryName	Nombre de la persona física (como consta en el DNI/NIE)	Sí				OID 1.3.6.1.4.1.47155.1.1
		Apellido primero de la persona física (como consta en el DNI/NIE)	Sí				OID 1.3.6.1.4.1.47155.1.2
		Apellido segundo de la persona física (como consta en el DNI/NIE)	Sí				OID 1.3.6.1.4.1.47155.1.3
		NIF del titular acorde a ETSI EN 319 412-1 "IDCES-123456789Z")	Sí			PrintableString	OID 1.3.6.1.4.1.47155.1.4
		Organización a la que pertenece el representante.	Sí		40 caracteres	UTF8String	OID 1.3.6.1.4.1.47155.1.6
		NIF de la persona jurídica de la que es representante el titular del certificado, en formato ETSI EN 319412-1 (Ejemplo: "VATES-Q0000000J)	Sí		64 caracteres	PrintableString	OID 1.3.6.1.4.1.47155.1.7
	2.5.2. rfc822Name	Correo electrónico de la persona física	Sí			rfc822Name	
	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			OID	
	2.6.2. Email protection	Presente (1.3.6.1.5.5.7.3.4)	Sí			OID	Sólo se activa si se incluye el correo electrónico del firmante
	2.7. cRLDistributionPoint		No	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			IA5String	uniformResourceIdentifier **(NO HTTPS)**
	2.7.2. distributionPoint	http://crl2.vincasing.net/canebula2.crl	Sí			IA5String	uniformResourceIdentifier **(NO HTTPS)**
	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. Access Description		Sí				
	2.8.1.1. Acces Method	id-ad-ocsp	Sí			OID	OID 1.3.6.1.5.5.7.48.1
	2.8.1.2. Acces Location	http://ocsp.vincasign.net	Sí			IA5String	URL de acceso al OCSP **(NO HTTPS)** uniformResourceIdentifier
	2.8.2. Access Description		Sí				
	2.8.2.1. Acces Method	id-ad-calssuers	Sí			OID	OID 1.3.6.1.5.5.7.48.2
	2.8.2.1. Acces Location	http://www.vincasign.net/publickeys/casub.crt	Si			IA5String	URL acceso a certificado de la CA (NO HTTPS) uniformResourceIdentifier
	2.9. Qualified Certificate Statements		Sí	No			OID 1.3.6.1.5.5.7.1.3
	2.9.1. qCCompliance	id-etsi-qcs-QcCompliance	Sí				OID 0.4.0.1862.1.1 Indicación de certificado cualificado

	2.9.2. QcEuRetentionPeriod	"15"	Sí				OID 0.4.0.1862.1.3 Plazo de retención de registros
	2.9.3. QcSSCD	id-etsi-qcs-QcSSCD	Sí				OID 0.4.0.1862.1.4 Dispositivo cualificado de creación de firma
	2.9.4. QcPDS	{https://www.vincasign.net/policy/es/PDS-PF1u-hard/pds-pf1u-hard-es.pdf,es},{https://www.vincasign.net/policy/en/PDS-PF1u-hard/pds-pf1u-hard-en.pdf,en}	Sí				OID 0.4.0.1862.1.5 **(SÍ HTTPS)** URLs de acceso al texto divulgativo en inglés (obligatorio) y en castellano
	2.9.5. QcType	id-etsi-qct-esign	Sí				OID 0.4.0.1862.1.6.1 Certificado de firma electrónica conforme al Reglamento (UE) Nº 910/2014
	2.9.6. qcStatement-2						OID 1.3.6.1.5.5.7.11.2 (RFC 3739)
	2.9.6.1. SemanticsInformation						
	2.9.6.1.1. semanticsIdNatural	0.4.0.194121.1.1					Semántica de persona fisica conforme a EN 319 412-1, en serial number
	2.10. Basic Constraints		Sí	Sí			OID 2.5.29.19
	2.10.1. cA	FALSO	Sí			Boolean	

4. Cert Corporativo y Efímero de PF en SOFT

Campo	Gestión CENTRALIZADA	Oblig.	Crít.	Longitud máxima	Codif	Observaciones OID 1.3.6.1.4.1.47155.1.1.52
EFÍMERO DE PERSONA FÍSICA · SOFT	Identificación y Firma					
1. Basic estructure						
1.1. Version	"2"	Sí		1	Integer	El literal "2" corresponde a la versión 3.
1.2. Serial Number	Establecido automáticamente por la CA. Número identificativo único del certificado.	Sí		20 octetos	Integer	No puede ser un número negativo ni 0.
1.3. Signature Algorithm		Sí				
1.3.1. Algorithm	SHA-256 with RSA Signature	Sí			OID	1.2.840.113549.1.1.11
1.3.2. Parameters	No aplicable	No				
1.4. Issuer		Sí				
1.4.1. Country Name (C)	"ES"	Sí		2 caracteres	PrintableString	OID 2.5.4.6
1.4.2. Organization Name (O)	"VINTEGRIS SL"	Sí		64 caracteres	UTF8String	OID 2.5.4.10
1.4.3. organizationalUnitName (OU)	"vinCAsign"	Sí				OID 2.5.4.11
1.4.4. Locality Name (L)	"HOSPITALET DE LLOBREGAT"	Sí		128 caracteres	UTF8String	OID 2.5.4.7
1.4.5. Organization Identifier	"VATES-B62913926"	Sí		Ilimitado	UTF8String	OID 2.5.4.97
1.4.6. Common Name (CN)	"vinCAsign nebulaSUITE2 Authority"	Sí		64 caracteres	UTF8String	OID 2.5.4.3
1.4.7. stateOrProvinceName	"BARCELONA"	Sí			UTF8String	OID 2.5.4.8
1.5. Validity	MENOR DE 1 HORA	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				
1.6.1. Country Name	"ES"	Sí		2 caracteres	PrintableString	OID 2.5.4.6
1.6.2. Organization (O)	Organización a la que pertenece el firmante.	Sí		40 caracteres	UTF8String	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		16 caracteres	UTF8String	OID 2.5.4.11
1.6.4. Organization Identifier	NIF de la persona jurídica a la que está vinculado el titular del certificado, en formato ETSI EN 319412-1	Sí		64 caracteres	PrintableString	OID 2.5.4.97
1.6.5. Title	Cargo del firmante en la organización			64 caracteres	UTF8String	OID 2.5.4.12
1.6.6. Serial Number	NIF del titular acorde a ETSI EN 319 412-1 "IDCES-123456789Z")	Sí			PrintableString	OID 2.5.4.5
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. Common Name	APELLIDO1 APELLIDO2 NOMBRE – DNI 1234567892	Sí				OID 2.5.4.3
1.6.10. emailAddress	Correo electrónico del firmante	Sí			IA5String	

1.7. Subject Public Key Info	Clave pública del firmante, codificada en RSA encryption (2048 bits)	Sí				
1.7.1. AlgorithmIdentifier						
1.7.1.1. Algorithm	RSA encryption	Sí			OID	OID 1.2.840.113549.1.1.1
1.7.1.2. Parameters	No aplicable	No				
1.7.2. SubjectPublicKey	Clave pública del firmante	Sí			Bit String	
2. Extensions						
2.1. Authority Key Identifier	Identificador de la clave del emisor	Sí	No			OID 2.5.29.35 (Marcado como NO crítico según EN 319412-2)
2.1.1. KeyIdentifier		Sí			Octet string	Derivado de la clave pública
2.1.2. AuthorityCertIssuer	Nombre de la CA a la que corresponde la clave identificada en keyIdentifier					(String UTF8) Size 12
2.1.3. AuthorityCertSerialNumber	Número de serie del certificado de CA					
2.2. Subject Key Identifier	Identificador de la clave del firmante	Sí	No			OID 2.5.29.14 (Marcado como NO crítico según EN 319412-2)
2.2.1. KeyIdentifier		Sí			Octet string	Derivado de la clave pública
2.3. Key Usage		Sí	Sí		Bit String	OID 2.5.29.15
2.3.1. Digital Signature	**Seleccionado "1"**	Sí				Bit para autenticación
2.3.2. Content commintment	**Seleccionado "1"**	Sí				Bit para firma
2.3.3. Key Encipherment	**Seleccionado "1"**	Sí				
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"					
2.3.8. Encipher Only	No seleccionado. "0"					
2.3.9. Decipher Only	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 Information		Sí				
2.4.1.1. Policy Identifier	**1.3.6.1.4.1.47155.1.1.52**	Sí			OID	Identificador de la política de Logalty
2.4.1.2. Policy Qualifiers		Sí				
2.4.1.1.1 CPS URI	https://policy.vincasign.net				IA5String	URL de la DPC (opcional por CAB FORUM)
2.4.1.1.2. User Notice/Explicit text	"Certificado cualificado y efímero de persona física vinculada emitido en software. Ver https://policy.vincasign.net "	Sí		200 caracteres	UTF8String y NFC	Texto indicativo
2.4.2. Policy Information		Sí				

	2.4.2.1. Policy Identifier	**0.4.0.194112.1.0**	Sí			OID	QCP-n. Identificador de la política de certificado cualificado de persona física sin uso de dispositivo seguro
	2.5. Subject Alternative Names		Sí	No			OID 2.5.29.17 (Marcado como NO crítico según EN 319412-2)
	2.5.1. DirectoryName	Nombre de la persona física (como consta en el DNI/NIE)	Sí				OID 1.3.6.1.4.1.47155.1.1
		Apellido primero de la persona física (como consta en el DNI/NIE)	Sí				OID 1.3.6.1.4.1.47155.1.2
		Apellido segundo de la persona física (como consta en el DNI/NIE)	Sí				OID 1.3.6.1.4.1.47155.1.3
		NIF del titular acorde a ETSI EN 319 412-1 "IDCES-123456789Z")	Sí			PrintableString	OID 1.3.6.1.4.1.47155.1.4
		Organización a la que pertenece el representante.	Sí		40 caracteres	UTF8String	OID 1.3.6.1.4.1.47155.1.6
		NIF de la persona jurídica de la que es representante el titular del certificado, en formato ETSI EN 319412-1 (Ejemplo: "VATES-Q0000000J)	Sí		64 caracteres	PrintableString	OID 1.3.6.1.4.1.47155.1.7
	2.5.2. rfc822Name	Correo electrónico de la persona física	Sí			rfc822Name	
	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			OID	
	2.6.2. Email protection	Presente (1.3.6.1.5.5.7.3.4)	Sí			OID	Sólo se activa si se incluye el correo electrónico del firmante
	2.7. cRLDistributionPoint		No	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			IA5String	uniformResourceIdentifier **(NO HTTPS)**
	2.7.2. distributionPoint	http://crl2.vincasing.net/canebula2.crl	Sí			IA5String	uniformResourceIdentifier **(NO HTTPS)**
	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. Access Description		Sí				
	2.8.1.1. Acces Method	id-ad-ocsp	Sí			OID	OID 1.3.6.1.5.5.7.48.1
	2.8.1.2. Acces Location	http://ocsp.vincasign.net	Sí			IA5String	URL de acceso al OCSP **(NO HTTPS)** uniformResourceIdentifier
	2.8.2. Access Description		Sí				
	2.8.2.1. Acces Method	id-ad-calssuers	Sí			OID	OID 1.3.6.1.5.5.7.48.2
	2.8.2.1. Acces Location	http://www.vincasign.net/publickeys/casub.crt	Si			IA5String	URL acceso a certificado de la CA (NO HTTPS) uniformResourceIdentifier
	2.9. Qualified Certificate Statements		Sí	No			OID 1.3.6.1.5.5.7.1.3
	2.9.1. qCCompliance	id-etsi-qcs-QcCompliance	Sí				OID 0.4.0.1862.1.1 Indicación de certificado cualificado

	2.9.2. QcEuRetentionPeriod	"15"	Sí				OID 0.4.0.1862.1.3 Plazo de retención de registros
	2.9.4. QcPDS	{https://www.vincasign.net/policy/es/PDS-PF1u-soft/pds-pf1u-soft-es.pdf,es},{https://www.vincasign.net/policy/en/PDS-PF1u-soft/pds-pf1u-soft-en.pdf,en}	Sí				OID 0.4.0.1862.1.5 **(SÍ HTTPS)** URLs de acceso al texto divulgativo en inglés (obligatorio) y en castellano
	2.9.5. QcType	id-etsi-qct-esign	Sí				OID 0.4.0.1862.1.6.1 Certificado de firma electrónica conforme al Reglamento (UE) Nº 910/2014
	2.9.6. qcStatement-2						OID 1.3.6.1.5.5.7.11.2 (RFC 3739)
	2.9.6.1. SemanticsInformation						
	2.9.6.1.1. semanticsIdNatural	0.4.0.194121.1.1					Semántica de persona fisica conforme a EN 319 412-1, en serial number
	2.10. Basic Constraints		Sí	Sí			OID 2.5.29.19
	2.10.1. cA	FALSO	Sí			Boolean	

5. Cert Corporativo de PF REP de PJ en DCCF

Campo	Gestión CENTRALIZADA	Oblig.	Crít.	Longitud máxima	Codif	Observaciones OID 1.3.6.1.4.1.47155.1.2.1
REPRESENTANT PJ · DCCF	Identificación y Firma					
1. Basic estructure						
1.1. Version	"2"	Sí		1	Integer	El literal "2" corresponde a la versión 3.
1.2. Serial Number	Establecido automáticamente por la CA. Número identificativo único del certificado.	Sí		20 octetos	Integer	No puede ser un número negativo ni 0.
1.3. Signature Algorithm		Sí				
1.3.1. Algorithm	SHA-256 with RSA Signature	Sí			OID	1.2.840.113549.1.1.11
1.3.2. Parameters	No aplicable	No				
1.4. Issuer		Sí				
1.4.1. Country Name (C)	"ES"	Sí		2 caracteres	PrintableString	OID 2.5.4.6
1.4.2. Organization Name (O)	"VINTEGRIS SL"	Sí		64 caracteres	UTF8String	OID 2.5.4.10
1.4.3. organizationalUnitName (OU)	"vinCAsign"	Sí				OID 2.5.4.11
1.4.4. Locality Name (L)	"HOSPITALET DE LLOBREGAT"	Sí		128 caracteres	UTF8String	OID 2.5.4.7
1.4.5. Organization Identifier	"VATES-B62913926"	Sí		Ilimitado	UTF8String	OID 2.5.4.97
1.4.6. Common Name (CN)	"vinCAsign nebulaSUITE2 Authority"	Sí		64 caracteres	UTF8String	OID 2.5.4.3
1.4.7. stateOrProvinceName	"BARCELONA"	Sí			UTF8String	OID 2.5.4.8
1.5. Validity		Sí				3 YEAR
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				
1.6.1. Country Name	"ES"	Sí		2 caracteres	PrintableString	OID 2.5.4.6
1.6.2. Organization (O)	Organización a la que pertenece el representante.	Sí		40 caracteres	UTF8String	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		16 caracteres	UTF8String	OID 2.5.4.11
1.6.4. Organization Identifier	NIF de la persona jurídica de la que es representante el titular del certificado, en formato ETSI EN 319412-1 (Ejemplo: "VATES-Q0000000J)	Sí		64 caracteres	PrintableString	OID 2.5.4.97
1.6.5. Title	Representante legal ...			64 caracteres	UTF8String	OID 2.5.4.12
1.6.6. Serial Number	NIF del titular acorde a ETSI EN 319 412-1 "IDCES-123456789Z")	Sí			PrintableString	OID 2.5.4.5
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. Common Name	123456789Z Nombre Apellido (R: Q0000000J)	Sí				OID 2.5.4.3

1.6.10. emailAddress	Correo electrónico del firmante	Sí			IA5String	
1.6.11. Description	• Reg: XXX /Hoja: XXX /Tomo:XXX /Sección:XXX /Libro:XXX /Folio:XXX /Fecha: dd-mm-aaaa /Inscripción: XXX • Notario: Nombre Apellido1 Apellido2 /Núm Protocolo: XXX /Fecha Otorgamiento: dd-mm-aaaa • En Boletines Oficiales: Boletín: XXX/ /Fecha: dd-mm-aaaa /Numero resolución: XXX	Sí				OID 2.5.4.13
1.7. Subject Public Key Info	Clave pública del firmante, codificada en RSA encryption (2048 bits)	Sí				
1.7.1. AlgorithmIdentifier						
1.7.1.1. Algorithm	RSA encryption	Sí			OID	OID 1.2.840.113549.1.1.1
1.7.1.2. Parameters	No aplicable	No				
1.7.2. SubjectPublicKey	Clave pública del firmante	Sí			Bit String	
2. Extensions						
2.1. Authority Key Identifier	Identificador de la clave del emisor	Sí	No			OID 2.5.29.35 (Marcado como NO crítico según EN 319412-2)
2.1.1. KeyIdentifier		Sí			Octet string	Derivado de la clave pública
2.1.2. AuthorityCertIssuer	Nombre de la CA a la que corresponde la clave identificada en keyIdentifier					(String UTF8) Size 12
2.1.3. AuthorityCertSerialNumber	Número de serie del certificado de CA					
2.2. Subject Key Identifier	Identificador de la clave del firmante	Sí	No			OID 2.5.29.14 (Marcado como NO crítico según EN 319412-2)
2.2.1. KeyIdentifier		Sí			Octet string	Derivado de la clave pública
2.3. Key Usage		Sí	Sí		Bit String	OID 2.5.29.15
2.3.1. Digital Signature	**Seleccionado "1"**	Sí				Bit para autenticación
2.3.2. Content commintment	**Seleccionado "1"**	Sí				Bit para firma
2.3.3. Key Encipherment	No seleccionado. "0"					
2.3.4. Data Encipherment	No seleccionado. "0"					
2.3.5. Key Agreement	No seleccionado. "0"					
2.3.6. Key Certificate Signature	No seleccionado. "0"					
2.3.7. CRL Signature	No seleccionado. "0"					
2.3.8. Encipher Only	No seleccionado. "0"					
2.3.9. Decipher Only	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 Information		Sí				
2.4.1.1. Policy Identifier	**1.3.6.1.4.1.47155.1.2.1**	Sí			OID	Identificador de la política de Logalty
2.4.1.2. Policy Qualifiers		Sí				

2.4.1.1.1 CPS URI	https://policy.vincasign.net				IA5String	URL de la DPC (opcional por CAB FORUM)
2.4.1.1.2. User Notice/Explicit text	"Certificado cualificado de persona física representante emitido en un DCCF. Ver https://policy.vincasign.net "	Sí		200 caracteres	UTF8String y NFC	Texto indicativo
2.4.2. Policy Information		Sí				
2.4.2.1. Policy Identifier	**0.4.0.194112.1.2**	Sí			OID	QCP-n-qscd. Identificador de la política de certificado cualificado de persona física con dispositivo seguro
2.4.3. Policy Information		Sí				
2.4.3.1. Policy Identifier	**2.16.724.1.3.5.8**	Sí			OID	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".
2.5. Subject Alternative Names		Sí	No			OID 2.5.29.17 (Marcado como NO crítico según EN 319412-2)
2.5.1. DirectoryName	Nombre de la persona física (como consta en el DNI/NIE)	Sí				OID 1.3.6.1.4.1.47155.1.1
	Apellido primero de la persona física (como consta en el DNI/NIE)	Sí				OID 1.3.6.1.4.1.47155.1.2
	Apellido segundo de la persona física (como consta en el DNI/NIE)	Sí				OID 1.3.6.1.4.1.47155.1.3
	NIF del titular acorde a ETSI EN 319 412-1 "IDCES-1234567892")	Sí			PrintableString	OID 1.3.6.1.4.1.47155.1.4
	Organización a la que pertenece el representante.	Sí		40 caracteres	UTF8String	OID 1.3.6.1.4.1.47155.1.6
	NIF de la persona jurídica de la que es representante el titular del certificado, en formato ETSI EN 319412-1 (Ejemplo: "VATES-Q0000000J)	Sí		64 caracteres	PrintableString	OID 1.3.6.1.4.1.47155.1.7
2.5.2. rfc822Name	Correo electrónico de la persona física	Sí			rfc822Name	
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			OID	
2.6.2. Email protection	Presente (1.3.6.1.5.5.7.3.4)	Sí			OID	Sólo se activa si se incluye el correo electrónico del firmante
2.7. cRLDistributionPoint		No	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			IA5String	uniformResourceIdentifier **(NO HTTPS)**
2.7.2. distributionPoint	http://crl2.vincasing.net/canebula2.crl	Sí			IA5String	uniformResourceIdentifier **(NO HTTPS)**

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. Access Description		Sí				
2.8.1.1. Acces Method	id-ad-ocsp	Sí			OID	OID 1.3.6.1.5.5.7.48.1
2.8.1.2. Acces Location	http://ocsp.vincasign.net	Sí			IA5String	URL de acceso al OCSP **(NO HTTPS)** uniformResourceIdentifier
2.8.2. Access Description		Sí				
2.8.2.1. Acces Method	id-ad-calssuers	Sí			OID	OID 1.3.6.1.5.5.7.48.2
2.8.2.1. Acces Location	http://www.vincasign.net/publickeys/casub.crt	Si			IA5String	URL acceso a certificado de la CA (NO HTTPS) uniformResourceIdentifier
2.9. Qualified Certificate Statements		Sí	No			OID 1.3.6.1.5.5.7.1.3
2.9.1. qCCompliance	id-etsi-qcs-QcCompliance	Sí				OID 0.4.0.1862.1.1 Indicación de certificado cualificado
2.9.2. QcEuRetentionPeriod	"15"	Sí				OID 0.4.0.1862.1.3 Plazo de retención de registros
2.9.3. QcSSCD	id-etsi-qcs-QcSSCD	Sí				OID 0.4.0.1862.1.4 Dispositivo cualificado de creación de firma
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}	Sí				OID 0.4.0.1862.1.5 **(SÍ HTTPS)** URLs de acceso al texto divulgativo en inglés (obligatorio) y en castellano
2.9.5. QcType	id-etsi-qct-esign	Sí				OID 0.4.0.1862.1.6.1 Certificado de firma electrónica conforme al Reglamento (UE) Nº 910/2014
2.9.6. qcStatement-2						OID 1.3.6.1.5.5.7.11.2 (RFC 3739)
2.9.6.1. SemanticsInformation						
2.9.6.1.1. semanticsIdNatural	0.4.0.194121.1.1					Semántica de persona fisica conforme a EN 319 412-1, en serial number
2.10. Basic Constraints		Sí	Sí			OID 2.5.29.19
2.10.1. cA	FALSO	Sí			Boolean	

6. Cert Corporativo de PF REP de PJ en SOFT

Campo	Gestión CENTRALIZADA	Oblig.	Crít.	Longitud máxima	Codif	Observaciones OID 1.3.6.1.4.1.47155.1.2.2
REPRESENTANT PJ · SOFT	Identificación y Firma					
1. Basic estructure						
1.1. Version	"2"	Sí		1	Integer	El literal "2" corresponde a la versión 3.
1.2. Serial Number	Establecido automáticamente por la CA. Número identificativo único del certificado.	Sí		20 octetos	Integer	No puede ser un número negativo ni 0.
1.3. Signature Algorithm		Sí				
1.3.1. Algorithm	SHA-256 with RSA Signature	Sí			OID	1.2.840.113549.1.1.11
1.3.2. Parameters	No aplicable	No				
1.4. Issuer		Sí				
1.4.1. Country Name (C)	"ES"	Sí		2 caracteres	PrintableString	OID 2.5.4.6
1.4.2. Organization Name (O)	"VINTEGRIS SL"	Sí		64 caracteres	UTF8String	OID 2.5.4.10
1.4.3. organizationalUnitName (OU)	"vinCAsign"	Sí				OID 2.5.4.11
1.4.4. Locality Name (L)	"HOSPITALET DE LLOBREGAT"	Sí		128 caracteres	UTF8String	OID 2.5.4.7
1.4.5. Organization Identifier	"VATES-B62913926"	Sí		Ilimitado	UTF8String	OID 2.5.4.97
1.4.6. Common Name (CN)	"vinCAsign nebulaSUITE2 Authority"	Sí		64 caracteres	UTF8String	OID 2.5.4.3
1.4.7. stateOrProvinceName	"BARCELONA"	Sí			UTF8String	OID 2.5.4.8
1.5. Validity		Sí				3 YEAR
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				
1.6.1. Country Name	"ES"	Sí		2 caracteres	PrintableString	OID 2.5.4.6
1.6.2. Organization (O)	Organización a la que pertenece el representante.	Sí		40 caracteres	UTF8String	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		16 caracteres	UTF8String	OID 2.5.4.11
1.6.4. Organization Identifier	NIF de la persona jurídica de la que es representante el titular del certificado, en formato ETSI EN 319412-1 (Ejemplo: "VATES-Q0000000J)	Sí		64 caracteres	PrintableString	OID 2.5.4.97
1.6.5. Title	Representante legal ...			64 caracteres	UTF8String	OID 2.5.4.12
1.6.6. Serial Number	NIF del titular acorde a ETSI EN 319 412-1 "IDCES-123456789Z")	Sí			PrintableString	OID 2.5.4.5
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. Common Name	123456789Z Nombre Apellido (R: Q0000000J)	Sí				OID 2.5.4.3

	1.6.10. emailAddress	Correo electrónico del firmante	Sí			IA5String	
	1.6.11. Description	• Reg: XXX /Hoja: XXX /Tomo:XXX /Sección:XXX /Libro:XXX /Folio:XXX /Fecha: dd-mm-aaaa /Inscripción: XXX • Notario: Nombre Apellido1 Apellido2 /Núm Protocolo: XXX /Fecha Otorgamiento: dd-mm-aaaa • En Boletines Oficiales: Boletín: XXX/ /Fecha: dd-mm-aaaa /Numero resolución: XXX	Sí				OID 2.5.4.13
	1.7. Subject Public Key Info	Clave pública del firmante, codificada en RSA encryption (2048 bits)	Sí				
	1.7.1. AlgorithmIdentifier						
	1.7.1.1. Algorithm	RSA encryption	Sí			OID	OID 1.2.840.113549.1.1.1
	1.7.1.2. Parameters	No aplicable	No				
	1.7.2. SubjectPublicKey	Clave pública del firmante	Sí			Bit String	
2. Extensions							
	2.1. Authority Key Identifier	Identificador de la clave del emisor	Sí	No			OID 2.5.29.35 (Marcado como NO crítico según EN 319412-2)
	2.1.1. KeyIdentifier		Sí			Octet string	Derivado de la clave pública
	2.1.2. AuthorityCertIssuer	Nombre de la CA a la que corresponde la clave identificada en keyIdentifier					(String UTF8) Size 12
	2.1.3. AuthorityCertSerialNumber	Número de serie del certificado de CA					
	2.2. Subject Key Identifier	Identificador de la clave del firmante	Sí	No			OID 2.5.29.14 (Marcado como NO crítico según EN 319412-2)
	2.2.1. KeyIdentifier		Sí			Octet string	Derivado de la clave pública
	2.3. Key Usage		Sí	Sí		Bit String	OID 2.5.29.15
	2.3.1. Digital Signature	**Seleccionado "1"**	Sí				Bit para autenticación
	2.3.2. Content commintment	**Seleccionado "1"**	Sí				Bit para firma
	2.3.3. Key Encipherment	No seleccionado. "0"					
	2.3.4. Data Encipherment	No seleccionado. "0"					
	2.3.5. Key Agreement	No seleccionado. "0"					
	2.3.6. Key Certificate Signature	No seleccionado. "0"					
	2.3.7. CRL Signature	No seleccionado. "0"					
	2.3.8. Encipher Only	No seleccionado. "0"					
	2.3.9. Decipher Only	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 Information		Sí				
	2.4.1.1. Policy Identifier	**1.3.6.1.4.1.47155.1.2.2**	Sí			OID	Identificador de la política de Logalty
	2.4.1.2. Policy Qualifiers		Sí				

	2.4.1.1.1 CPS URI	https://policy.vincasign.net				IA5String	URL de la DPC (opcional por CAB FORUM)
	2.4.1.1.2. User Notice/Explicit text	"Certificado cualificado de persona física representante emitido en software. Ver https://policy.vincasign.net "	Sí		200 caracteres	UTF8String y NFC	Texto indicativo
	2.4.2. Policy Information		Sí				
	2.4.2.1. Policy Identifier	**0.4.0.194112.1.0**	Sí			OID	QCP-n-qscd. Identificador de la política de certificado cualificado de persona física sin uso de dispositivo seguro
	2.4.3. Policy Information		Sí				
	2.4.3.1. Policy Identifier	**2.16.724.1.3.5.8**	Sí			OID	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".
	2.5. Subject Alternative Names		Sí	No			OID 2.5.29.17 (Marcado como NO crítico según EN 319412-2)
	2.5.1. DirectoryName	Nombre de la persona física (como consta en el DNI/NIE)	Sí				OID 1.3.6.1.4.1.47155.1.1
		Apellido primero de la persona física (como consta en el DNI/NIE)	Sí				OID 1.3.6.1.4.1.47155.1.2
		Apellido segundo de la persona física (como consta en el DNI/NIE)	Sí				OID 1.3.6.1.4.1.47155.1.3
		NIF del titular acorde a ETSI EN 319 412-1 "IDCES-123456789Z")	Sí			PrintableString	OID 1.3.6.1.4.1.47155.1.4
		Organización a la que pertenece el representante.	Sí		40 caracteres	UTF8String	OID 1.3.6.1.4.1.47155.1.6
		NIF de la persona jurídica de la que es representante el titular del certificado, en formato ETSI EN 319412-1 (Ejemplo: "VATES-Q0000000J)	Sí		64 caracteres	PrintableString	OID 1.3.6.1.4.1.47155.1.7
	2.5.1. rfc822Name	Correo electrónico de la persona física	Sí			rfc822Name	
	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			OID	
	2.6.2. Email protection	Presente (1.3.6.1.5.5.7.3.4)	Sí			OID	Sólo se activa si se incluye el correo electrónico del firmante
	2.7. cRLDistributionPoint		No	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			IA5String	uniformResourceIdentifier **(NO HTTPS)**
	2.7.2. distributionPoint	http://crl2.vincasing.net/canebula2.crl	Sí			IA5String	uniformResourceIdentifier **(NO HTTPS)**

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. Access Description			Sí				
2.8.1.1. Acces Method	id-ad-ocsp		Sí			OID	OID 1.3.6.1.5.5.7.48.1
2.8.1.2. Acces Location	http://ocsp.vincasign.net		Sí			IA5String	URL de acceso al OCSP **(NO HTTPS)** uniformResourceIdentifier
2.8.2. Access Description			Sí				
2.8.2.1. Acces Method	id-ad-calssuers		Sí			OID	OID 1.3.6.1.5.5.7.48.2
2.8.2.1. Acces Location	http://www.vincasign.net/publickeys/casub.crt		Si			IA5String	URL acceso a certificado de la CA (NO HTTPS) uniformResourceIdentifier
2.9. Qualified Certificate Statements			Sí	No			OID 1.3.6.1.5.5.7.1.3
2.9.1. qCCompliance	id-etsi-qcs-QcCompliance		Sí				OID 0.4.0.1862.1.1 Indicación de certificado cualificado
2.9.2. QcEuRetentionPeriod	"15"		Sí				OID 0.4.0.1862.1.3 Plazo de retención de registros
2.9.4. QcPDS	{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 **(SÍ HTTPS)** URLs de acceso al texto divulgativo en inglés (obligatorio) y en castellano
2.9.5. QcType	id-etsi-qct-esign		Sí				OID 0.4.0.1862.1.6.1 Certificado de firma electrónica conforme al Reglamento (UE) Nº 910/2014
2.9.6. qcStatement-2							OID 1.3.6.1.5.5.7.11.2 (RFC 3739)
2.9.6.1. SemanticsInformation							
2.9.6.1.1. semanticsIdNatural	0.4.0.194121.1.1						Semántica de persona fisica conforme a EN 319 412-1, en serial number
2.10. Basic Constraints			Sí	Sí			OID 2.5.29.19
2.10.1. cA	FALSO		Sí			Boolean	

7. Cert Corporativo y Efímero de PF REP de PJ en DCCF

Campo	Gestión CENTRALIZADA	Oblig.	Crít.	Longitud máxima	Codif	Observaciones OID 1.3.6.1.4.1.47155.1.2.51
EFÍMERO REPRESENTANT PJ · DCCF	Identificación y Firma					
1. Basic estructure						
1.1. Version	"2"	Sí		1	Integer	El literal "2" corresponde a la versión 3.
1.2. Serial Number	Establecido automáticamente por la CA. Número identificativo único del certificado.	Sí		20 octetos	Integer	No puede ser un número negativo ni 0.
1.3. Signature Algorithm		Sí				
1.3.1. Algorithm	SHA-256 with RSA Signature	Sí			OID	1.2.840.113549.1.1.11
1.3.2. Parameters	No aplicable	No				
1.4. Issuer		Sí				
1.4.1. Country Name (C)	"ES"	Sí		2 caracteres	PrintableString	OID 2.5.4.6
1.4.2. Organization Name (O)	"VINTEGRIS SL"	Sí		64 caracteres	UTF8String	OID 2.5.4.10
1.4.3. organizationalUnitName (OU)	"vinCAsign"	Sí				OID 2.5.4.11
1.4.4. Locality Name (L)	"HOSPITALET DE LLOBREGAT"	Sí		128 caracteres	UTF8String	OID 2.5.4.7
1.4.5. Organization Identifier	"VATES-B62913926"	Sí		Ilimitado	UTF8String	OID 2.5.4.97
1.4.6. Common Name (CN)	"vinCAsign nebulaSUITE2 Authority"	Sí		64 caracteres	UTF8String	OID 2.5.4.3
1.4.7. stateOrProvinceName	"BARCELONA"	Sí			UTF8String	OID 2.5.4.8
1.5. Validity	MENOR DE 1 HORA	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				
1.6.1. Country Name	"ES"	Sí		2 caracteres	PrintableString	OID 2.5.4.6
1.6.2. Organization (O)	Organización a la que pertenece el representante.	Sí		40 caracteres	UTF8String	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		16 caracteres	UTF8String	OID 2.5.4.11
1.6.4. Organization Identifier	NIF de la persona jurídica de la que es representante el titular del certificado, en formato ETSI EN 319412-1 (Ejemplo: "VATES-Q0000000J)	Sí		64 caracteres	PrintableString	OID 2.5.4.97
1.6.5. Title	Representante legal ...			64 caracteres	UTF8String	OID 2.5.4.12
1.6.6. Serial Number	NIF del titular acorde a ETSI EN 319 412-1 "IDCES-123456789Z")	Sí			PrintableString	OID 2.5.4.5
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. Common Name	123456789Z Nombre Apellido (R: Q0000000J)	Sí				OID 2.5.4.3

1.6.10. emailAddress	Correo electrónico del firmante	Sí			IA5String	
1.6.11. Description	• Reg: XXX /Hoja: XXX /Tomo:XXX /Sección:XXX /Libro:XXX /Folio:XXX /Fecha: dd-mm-aaaa /Inscripción: XXX • Notario: Nombre Apellido1 Apellido2 /Núm Protocolo: XXX /Fecha Otorgamiento: dd-mm-aaaa • En Boletines Oficiales: Boletín: XXX/ /Fecha: dd-mm-aaaa /Numero resolución: XXX	Sí				OID 2.5.4.13
1.7. Subject Public Key Info	Clave pública del firmante, codificada en RSA encryption (2048 bits)	Sí				
1.7.1. AlgorithmIdentifier						
1.7.1.1. Algorithm	RSA encryption	Sí			OID	OID 1.2.840.113549.1.1.1
1.7.1.2. Parameters	No aplicable	No				
1.7.2. SubjectPublicKey	Clave pública del firmante	Sí			Bit String	
2. Extensions						
2.1. Authority Key Identifier	Identificador de la clave del emisor	Sí	No			OID 2.5.29.35 (Marcado como NO crítico según EN 319412-2)
2.1.1. KeyIdentifier		Sí			Octet string	Derivado de la clave pública
2.1.2. AuthorityCertIssuer	Nombre de la CA a la que corresponde la clave identificada en keyIdentifier					(String UTF8) Size 12
2.1.3. AuthorityCertSerialNumber	Número de serie del certificado de CA					
2.2. Subject Key Identifier	Identificador de la clave del firmante	Sí	No			OID 2.5.29.14 (Marcado como NO crítico según EN 319412-2)
2.2.1. KeyIdentifier		Sí			Octet string	Derivado de la clave pública
2.3. Key Usage		Sí	Sí		Bit String	OID 2.5.29.15
2.3.1. Digital Signature	**Seleccionado "1"**	Sí				Bit para autenticación
2.3.2. Content commintment	**Seleccionado "1"**	Sí				Bit para firma
2.3.3. Key Encipherment	No seleccionado. "0"					
2.3.4. Data Encipherment	No seleccionado. "0"					
2.3.5. Key Agreement	No seleccionado. "0"					
2.3.6. Key Certificate Signature	No seleccionado. "0"					
2.3.7. CRL Signature	No seleccionado. "0"					
2.3.8. Encipher Only	No seleccionado. "0"					
2.3.9. Decipher Only	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 Information		Sí				
2.4.1.1. Policy Identifier	**1.3.6.1.4.1.47155.1.2.51**	Sí			OID	Identificador de la política de Logalty

	2.4.1.2. Policy Qualifiers		Sí				
	2.4.1.1.1 CPS URI	https://policy.vincasign.net				IA5String	URL de la DPC (opcional por CAB FORUM)
	2.4.1.1.2. User Notice/Explicit text	"Certificado cualificado y efímero de persona física representante emitido en un DCCF. Ver https://policy.vincasign.net "	Sí		200 caracteres	UTF8String y NFC	Texto indicativo
	2.4.2. Policy Information		Sí				
	2.4.2.1. Policy Identifier	**0.4.0.194112.1.2**	Sí			OID	QCP-n-qscd. Identificador de la política de certificado cualificado de persona física con dispositivo seguro
	2.4.3. Policy Information		Sí				
	2.4.3.1. Policy Identifier	**2.16.724.1.3.5.8**	Sí			OID	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".
	2.5. Subject Alternative Names		Sí	No			OID 2.5.29.17 (Marcado como NO crítico según EN 319412-2)
	2.5.1. DirectoryName	Nombre de la persona física (como consta en el DNI/NIE)	Sí				OID 1.3.6.1.4.1.47155.1.1
		Apellido primero de la persona física (como consta en el DNI/NIE)	Sí				OID 1.3.6.1.4.1.47155.1.2
		Apellido segundo de la persona física (como consta en el DNI/NIE)	Sí				OID 1.3.6.1.4.1.47155.1.3
		NIF del titular acorde a ETSI EN 319 412-1 "IDCES-1234567892")	Sí			PrintableString	OID 1.3.6.1.4.1.47155.1.4
		Organización a la que pertenece el representante.	Sí		40 caracteres	UTF8String	OID 1.3.6.1.4.1.47155.1.6
		NIF de la persona jurídica de la que es representante el titular del certificado, en formato ETSI EN 319412-1 (Ejemplo: "VATES-Q0000000J)	Sí		64 caracteres	PrintableString	OID 1.3.6.1.4.1.47155.1.7
	2.5.2. rfc822Name	Correo electrónico de la persona física	Sí			rfc822Name	
	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			OID	
	2.6.2. Email protection	Presente (1.3.6.1.5.5.7.3.4)	Sí			OID	Sólo se activa si se incluye el correo electrónico del firmante
	2.7. cRLDistributionPoint		No	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			IA5String	uniformResourceIdentifier **(NO HTTPS)**

	2.7.2. distributionPoint	http://crl2.vincasing.net/canebula2.crl	Sí			IA5String	uniformResourceIdentifier **(NO HTTPS)**
	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. Access Description		Sí				
	2.8.1.1. Acces Method	id-ad-ocsp	Sí			OID	OID 1.3.6.1.5.5.7.48.1
	2.8.1.2. Acces Location	http://ocsp.vincasign.net	Sí			IA5String	URL de acceso al OCSP **(NO HTTPS)** uniformResourceIdentifier
	2.8.2. Access Description		Sí				
	2.8.2.1. Acces Method	id-ad-calssuers	Sí			OID	OID 1.3.6.1.5.5.7.48.2
	2.8.2.1. Acces Location	http://www.vincasign.net/publickeys/casub.crt	Si			IA5String	URL acceso a certificado de la CA (NO HTTPS) uniformResourceIdentifier
	2.9. Qualified Certificate Statements		Sí	No			OID 1.3.6.1.5.5.7.1.3
	2.9.1. qCCompliance	id-etsi-qcs-QcCompliance	Sí				OID 0.4.0.1862.1.1 Indicación de certificado cualificado
	2.9.2. QcEuRetentionPeriod	"15"	Sí				OID 0.4.0.1862.1.3 Plazo de retención de registros
	2.9.3. QcSSCD	id-etsi-qcs-QcSSCD	Sí				OID 0.4.0.1862.1.4 Dispositivo cualificado de creación de firma
	2.9.4. QcPDS	{https://www.vincasign.net/policy/es/PDS-REP1u-hard/pds-rep1u-hard-es.pdf,es},{https://www.vincasign.net/policy/en/PDS-REP1u-hard/pds-rep1u-hard-en.pdf,en}	Sí				OID 0.4.0.1862.1.5 **(SÍ HTTPS)** URLs de acceso al texto divulgativo en inglés (obligatorio) y en castellano
	2.9.5. QcType	id-etsi-qct-esign	Sí				OID 0.4.0.1862.1.6.1 Certificado de firma electrónica conforme al Reglamento (UE) Nº 910/2014
	2.9.6. qcStatement-2						OID 1.3.6.1.5.5.7.11.2 (RFC 3739)
	2.9.6.1. SemanticsInformation						
	2.9.6.1.1. semanticsIdNatural	0.4.0.194121.1.1					Semántica de persona fisica conforme a EN 319 412-1, en serial number
	2.10. Basic Constraints		Sí	Sí			OID 2.5.29.19
	2.10.1. cA	FALSO	Sí			Boolean	

8. Cert Corporativo y Efímero de PF REP de PJ en SOFT

Campo EFIMERO REPRESENTANT PJ · SOFT	Gestión CENTRALIZADA Identificación y Firma	Oblig.	Crít.	Longitud máxima	Codif	Observaciones OID 1.3.6.1.4.1.47155.1.2.52
1. Basic estructure						
1.1. Version	"2"	Sí		1	Integer	El literal "2" corresponde a la versión 3.
1.2. Serial Number	Establecido automáticamente por la CA. Número identificativo único del certificado.	Sí		20 octetos	Integer	No puede ser un número negativo ni 0.
1.3. Signature Algorithm		Sí				
1.3.1. Algorithm	SHA-256 with RSA Signature	Sí			OID	1.2.840.113549.1.1.11
1.3.2. Parameters	No aplicable	No				
1.4. Issuer		Sí				
1.4.1. Country Name (C)	"ES"	Sí		2 caracteres	PrintableString	OID 2.5.4.6
1.4.2. Organization Name (O)	"VINTEGRIS SL"	Sí		64 caracteres	UTF8String	OID 2.5.4.10
1.4.3. organizationalUnitName (OU)	"vinCAsign"	Sí				OID 2.5.4.11
1.4.4. Locality Name (L)	"HOSPITALET DE LLOBREGAT"	Sí		128 caracteres	UTF8String	OID 2.5.4.7
1.4.5. Organization Identifier	"VATES-B62913926"	Sí		Ilimitado	UTF8String	OID 2.5.4.97
1.4.6. Common Name (CN)	"vinCAsign nebulaSUITE2 Authority"	Sí		64 caracteres	UTF8String	OID 2.5.4.3
1.4.7. stateOrProvinceName	"BARCELONA"	Sí			UTF8String	OID 2.5.4.8
1.5. Validity	MENOR DE 1 HORA	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				
1.6.1. Country Name	"ES"	Sí		2 caracteres	PrintableString	OID 2.5.4.6
1.6.2. Organization (O)	Organización a la que pertenece el representante.	Sí		40 caracteres	UTF8String	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		16 caracteres	UTF8String	OID 2.5.4.11
1.6.4. Organization Identifier	NIF de la persona jurídica de la que es representante el titular del certificado, en formato ETSI EN 319412-1 (Ejemplo: "VATES-Q0000000J)	Sí		64 caracteres	PrintableString	OID 2.5.4.97
1.6.5. Title	Representante legal ...			64 caracteres	UTF8String	OID 2.5.4.12
1.6.6. Serial Number	NIF del titular acorde a ETSI EN 319 412-1 "IDCES-123456789Z")	Sí			PrintableString	OID 2.5.4.5
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. Common Name	123456789Z Nombre Apellido (R: Q0000000J)	Sí				OID 2.5.4.3

1.6.10. emailAddress	Correo electrónico del firmante	Sí			IA5String	
1.6.11. Description	• Reg: XXX /Hoja: XXX /Tomo:XXX /Sección:XXX /Libro:XXX /Folio:XXX /Fecha: dd-mm-aaaa /Inscripción: XXX • Notario: Nombre Apellido1 Apellido2 /Núm Protocolo: XXX /Fecha Otorgamiento: dd-mm-aaaa • En Boletines Oficiales: Boletín: XXX/ /Fecha: dd-mm-aaaa /Numero resolución: XXX	Sí				OID 2.5.4.13
1.7. Subject Public Key Info	Clave pública del firmante, codificada en RSA encryption (2048 bits)	Sí				
1.7.1. AlgorithmIdentifier						
1.7.1.1. Algorithm	RSA encryption	Sí			OID	OID 1.2.840.113549.1.1.1
1.7.1.2. Parameters	No aplicable	No				
1.7.2. SubjectPublicKey	Clave pública del firmante	Sí			Bit String	
2. Extensions						
2.1. Authority Key Identifier	Identificador de la clave del emisor	Sí	No			OID 2.5.29.35 (Marcado como NO crítico según EN 319412-2)
2.1.1. KeyIdentifier		Sí			Octet string	Derivado de la clave pública
2.1.2. AuthorityCertIssuer	Nombre de la CA a la que corresponde la clave identificada en keyIdentifier					(String UTF8) Size 12
2.1.3. AuthorityCertSerialNumber	Número de serie del certificado de CA					
2.2. Subject Key Identifier	Identificador de la clave del firmante	Sí	No			OID 2.5.29.14 (Marcado como NO crítico según EN 319412-2)
2.2.1. KeyIdentifier		Sí			Octet string	Derivado de la clave pública
2.3. Key Usage		Sí	Sí		Bit String	OID 2.5.29.15
2.3.1. Digital Signature	**Seleccionado "1"**	Sí				Bit para autenticación
2.3.2. Content commintment	**Seleccionado "1"**	Sí				Bit para firma
2.3.3. Key Encipherment	No seleccionado. "0"					
2.3.4. Data Encipherment	No seleccionado. "0"					
2.3.5. Key Agreement	No seleccionado. "0"					
2.3.6. Key Certificate Signature	No seleccionado. "0"					
2.3.7. CRL Signature	No seleccionado. "0"					
2.3.8. Encipher Only	No seleccionado. "0"					
2.3.9. Decipher Only	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 Information		Sí				
2.4.1.1. Policy Identifier	**1.3.6.1.4.1.47155.1.2.2**	Sí			OID	Identificador de la política de Logalty
2.4.1.2. Policy Qualifiers		Sí				

2.4.1.1.1 CPS URI	https://policy.vincasign.net				IA5String	URL de la DPC (opcional por CAB FORUM)
2.4.1.1.2. User Notice/Explicit text	"Certificado cualificado y efímero de persona física representante emitido en software. Ver https://policy.vincasign.net "	Sí		200 caracteres	UTF8String y NFC	Texto indicativo
2.4.2. Policy Information		Sí				
2.4.2.1. Policy Identifier	**0.4.0.194112.1.0**	Sí			OID	QCP-n-qscd. Identificador de la política de certificado cualificado de persona física sin uso de dispositivo seguro
2.4.3. Policy Information		Sí				
2.4.3.1. Policy Identifier	**2.16.724.1.3.5.8**	Sí			OID	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".
2.5. Subject Alternative Names		Sí	No			OID 2.5.29.17 (Marcado como NO crítico según EN 319412-2)
2.5.1. DirectoryName	Nombre de la persona física (como consta en el DNI/NIE)	Sí				OID 1.3.6.1.4.1.47155.1.1
	Apellido primero de la persona física (como consta en el DNI/NIE)	Sí				OID 1.3.6.1.4.1.47155.1.2
	Apellido segundo de la persona física (como consta en el DNI/NIE)	Sí				OID 1.3.6.1.4.1.47155.1.3
	NIF del titular acorde a ETSI EN 319 412-1 "IDCES-1234567892")	Sí			PrintableString	OID 1.3.6.1.4.1.47155.1.4
	Organización a la que pertenece el representante.	Sí		40 caracteres	UTF8String	OID 1.3.6.1.4.1.47155.1.6
	NIF de la persona jurídica de la que es representante el titular del certificado, en formato ETSI EN 319412-1 (Ejemplo: "VATES-Q0000000J)	Sí		64 caracteres	PrintableString	OID 1.3.6.1.4.1.47155.1.7
2.5.2. rfc822Name	Correo electrónico de la persona física	Sí			rfc822Name	
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			OID	
2.6.2. Email protection	Presente (1.3.6.1.5.5.7.3.4)	Sí			OID	Sólo se activa si se incluye el correo electrónico del firmante
2.7. cRLDistributionPoint		No	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			IA5String	uniformResourceIdentifier **(NO HTTPS)**
2.7.2. distributionPoint	http://crl2.vincasing.net/canebula2.crl	Sí			IA5String	uniformResourceIdentifier **(NO HTTPS)**

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. Access Description		Sí				
2.8.1.1. Acces Method	id-ad-ocsp	Sí			OID	OID 1.3.6.1.5.5.7.48.1
2.8.1.2. Acces Location	http://ocsp.vincasign.net	Sí			IA5String	URL de acceso al OCSP **(NO HTTPS)** uniformResourceIdentifier
2.8.2. Access Description		Sí				
2.8.2.1. Acces Method	id-ad-calssuers	Sí			OID	OID 1.3.6.1.5.5.7.48.2
2.8.2.1. Acces Location	http://www.vincasign.net/publickeys/casub.crt	Si			IA5String	URL acceso a certificado de la CA (NO HTTPS) uniformResourceIdentifier
2.9. Qualified Certificate Statements		Sí	No			OID 1.3.6.1.5.5.7.1.3
2.9.1. qCCompliance	id-etsi-qcs-QcCompliance	Sí				OID 0.4.0.1862.1.1 Indicación de certificado cualificado
2.9.2. QcEuRetentionPeriod	"15"	Sí				OID 0.4.0.1862.1.3 Plazo de retención de registros
2.9.4. QcPDS	{https://www.vincasign.net/policy/es/PDS-REP1u-soft/pds-rep1u-soft-es.pdf,es},{https://www.vincasign.net/policy/en/PDS-REP1u-soft/pds-rep1u-soft-en.pdf,en}	Sí				OID 0.4.0.1862.1.5 **(SÍ HTTPS)** URLs de acceso al texto divulgativo en inglés (obligatorio) y en castellano
2.9.5. QcType	id-etsi-qct-esign	Sí				OID 0.4.0.1862.1.6.1 Certificado de firma electrónica conforme al Reglamento (UE) Nº 910/2014
2.9.6. qcStatement-2						OID 1.3.6.1.5.5.7.11.2 (RFC 3739)
2.9.6.1. SemanticsInformation						
2.9.6.1.1. semanticsIdNatural	0.4.0.194121.1.1					Semántica de persona fisica conforme a EN 319 412-1, en serial number
2.10. Basic Constraints		Sí	Sí			OID 2.5.29.19
2.10.1. cA	FALSO	Sí			Boolean	

9. Cert Corporativo de PF REP de ESPJ en DCCF

Campo	Gestión CENTRALIZADA	Oblig.	Crít.	Longitud máxima	Codif	Observaciones OID 1.3.6.1.4.1.47155.1.2.11
REPRESENTANT ESPJ · DCCF	Identificación y Firma					
1. Basic estructure						
1.1. Version	"2"	Sí		1	Integer	El literal "2" corresponde a la versión 3.
1.2. Serial Number	Establecido automáticamente por la CA. Número identificativo único del certificado.	Sí		20 octetos	Integer	No puede ser un número negativo ni 0.
1.3. Signature Algorithm		Sí				
1.3.1. Algorithm	SHA-256 with RSA Signature	Sí			OID	1.2.840.113549.1.1.11
1.3.2. Parameters	No aplicable	No				
1.4. Issuer		Sí				
1.4.1. Country Name (C)	"ES"	Sí		2 caracteres	PrintableString	OID 2.5.4.6
1.4.2. Organization Name (O)	"VINTEGRIS SL"	Sí		64 caracteres	UTF8String	OID 2.5.4.10
1.4.3. organizationalUnitName (OU)	"vinCAsign"	Sí				OID 2.5.4.11
1.4.4. Locality Name (L)	"HOSPITALET DE LLOBREGAT"	Sí		128 caracteres	UTF8String	OID 2.5.4.7
1.4.5. Organization Identifier	"VATES-B62913926"	Sí		Ilimitado	UTF8String	OID 2.5.4.97
1.4.6. Common Name (CN)	"vinCAsign nebulaSUITE2 Authority"	Sí		64 caracteres	UTF8String	OID 2.5.4.3
1.4.7. stateOrProvinceName	"BARCELONA"	Sí			UTF8String	OID 2.5.4.8
1.5. Validity		Sí				3 YEAR
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				
1.6.1. Country Name	"ES"	Sí		2 caracteres	PrintableString	OID 2.5.4.6
1.6.2. Organization (O)	Organización a la que pertenece el representante.	Sí		40 caracteres	UTF8String	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		16 caracteres	UTF8String	OID 2.5.4.11
1.6.4. Organization Identifier	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		64 caracteres	PrintableString	OID 2.5.4.97
1.6.5. Title	Representante de... / Presidente de ...			64 caracteres	UTF8String	OID 2.5.4.12
1.6.6. Serial Number	NIF del titular acorde a ETSI EN 319 412-1 "IDCES-123456789Z")	Sí			PrintableString	OID 2.5.4.5
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. Common Name	123456789Z Nombre Apellido (R: Q0000000J)	Sí				OID 2.5.4.3

1.6.10. emailAddress	Correo electrónico del firmante	Sí			IA5String	
1.6.11. Description	Codificación del documento público que acredita las facultades del firmante o los datos registrales	Sí				OID 2.5.4.13
1.7. Subject Public Key Info	Clave pública del firmante, codificada en RSA encryption (2048 bits)	Sí				
1.7.1. AlgorithmIdentifier						
1.7.1.1. Algorithm	RSA encryption	Sí			OID	OID 1.2.840.113549.1.1.1
1.7.1.2. Parameters	No aplicable	No				
1.7.2. SubjectPublicKey	Clave pública del firmante	Sí			Bit String	
2. Extensions						
2.1. Authority Key Identifier	Identificador de la clave del emisor	Sí	No			OID 2.5.29.35 (Marcado como NO crítico según EN 319412-2)
2.1.1. KeyIdentifier		Sí			Octet string	Derivado de la clave pública
2.1.2. AuthorityCertIssuer	Nombre de la CA a la que corresponde la clave identificada en keyIdentifier					(String UTF8) Size 12
2.1.3. AuthorityCertSerialNumber	Número de serie del certificado de CA					
2.2. Subject Key Identifier	Identificador de la clave del firmante	Sí	No			OID 2.5.29.14 (Marcado como NO crítico según EN 319412-2)
2.2.1. KeyIdentifier		Sí			Octet string	Derivado de la clave pública
2.3. Key Usage		Sí	Sí		Bit String	OID 2.5.29.15
2.3.1. Digital Signature	**Seleccionado "1"**	Sí				Bit para autenticación
2.3.2. Content commintment	**Seleccionado "1"**	Sí				Bit para firma
2.3.3. Key Encipherment	No seleccionado. "0"					
2.3.4. Data Encipherment	No seleccionado. "0"					
2.3.5. Key Agreement	No seleccionado. "0"					
2.3.6. Key Certificate Signature	No seleccionado. "0"					
2.3.7. CRL Signature	No seleccionado. "0"					
2.3.8. Encipher Only	No seleccionado. "0"					
2.3.9. Decipher Only	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 Information		Sí				
2.4.1.1. Policy Identifier	**1.3.6.1.4.1.47155.1.2.11**	Sí			OID	Identificador de la política de Logalty
2.4.1.2. Policy Qualifiers		Sí				
2.4.1.1.1 CPS URI	https://policy.vincasign.net				IA5String	URL de la DPC (opcional por CAB FORUM)

	2.4.1.1.2. User Notice/Explicit text	"Certificado cualificado de persona física representante de ESPJ emitido en un DCCF. Ver https://policy.vincasign.net "	Sí		200 caracteres	UTF8String y NFC	Texto indicativo
	2.4.2. Policy Information		Sí				
	2.4.2.1. Policy Identifier	**0.4.0.194112.1.2**	Sí			OID	QCP-n-qscd. Identificador de la política de certificado cualificado de persona física con dispositivo seguro
	2.4.3. Policy Information		Sí				
	2.4.3.1. Policy Identifier	**2.16.724.1.3.5.9**	Sí			OID	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".
	2.5. Subject Alternative Names		Sí	No			OID 2.5.29.17 (Marcado como NO crítico según EN 319412-2)
	2.5.1. DirectoryName	Nombre de la persona física (como consta en el DNI/NIE)	Sí				OID 1.3.6.1.4.1.47155.1.1
		Apellido primero de la persona física (como consta en el DNI/NIE)	Sí				OID 1.3.6.1.4.1.47155.1.2
		Apellido segundo de la persona física (como consta en el DNI/NIE)	Sí				OID 1.3.6.1.4.1.47155.1.3
		NIF del titular acorde a ETSI EN 319 412-1 "IDCES-1234567892")	Sí			PrintableString	OID 1.3.6.1.4.1.47155.1.4
		Organización a la que pertenece el representante.	Sí		40 caracteres	UTF8String	OID 1.3.6.1.4.1.47155.1.6
		NIF de la persona jurídica de la que es representante el titular del certificado, en formato ETSI EN 319412-1 (Ejemplo: "VATES-Q0000000J)	Sí		64 caracteres	PrintableString	OID 1.3.6.1.4.1.47155.1.7
	2.5.2. rfc822Name	Correo electrónico de la persona física	Sí			rfc822Name	
	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			OID	
	2.6.2. Email protection	Presente (1.3.6.1.5.5.7.3.4)	Sí			OID	Sólo se activa si se incluye el correo electrónico del firmante
	2.7. cRLDistributionPoint		No	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			IA5String	uniformResourceIdentifier **(NO HTTPS)**
	2.7.2. distributionPoint	http://crl2.vincasing.net/canebula2.crl	Sí			IA5String	uniformResourceIdentifier **(NO HTTPS)**
	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. Access Description		Sí				

	2.8.1.1. Acces Method	id-ad-ocsp	Sí			OID	OID 1.3.6.1.5.5.7.48.1
	2.8.1.2. Acces Location	http://ocsp.vincasign.net	Sí			IA5String	URL de acceso al OCSP **(NO HTTPS)** uniformResourceIdentifier
	2.8.2. Access Description		Sí				
	2.8.2.1. Acces Method	id-ad-calssuers	Sí			OID	OID 1.3.6.1.5.5.7.48.2
	2.8.2.1. Acces Location	http://www.vincasign.net/publickeys/casub.crt	Si			IA5String	URL acceso a certificado de la CA (NO HTTPS) uniformResourceIdentifier
	2.9. Qualified Certificate Statements		Sí	No			OID 1.3.6.1.5.5.7.1.3
	2.9.1. qCCompliance	id-etsi-qcs-QcCompliance	Sí				OID 0.4.0.1862.1.1 Indicación de certificado cualificado
	2.9.2. QcEuRetentionPeriod	"15"	Sí				OID 0.4.0.1862.1.3 Plazo de retención de registros
	2.9.3. QcSSCD	id-etsi-qcs-QcSSCD	Sí				OID 0.4.0.1862.1.4 Dispositivo cualificado de creación de firma
	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}	Sí				OID 0.4.0.1862.1.5 **(SÍ HTTPS)** URLs de acceso al texto divulgativo en inglés (obligatorio) y en castellano
	2.9.5. QcType	id-etsi-qct-esign	Sí				OID 0.4.0.1862.1.6.1 Certificado de firma electrónica conforme al Reglamento (UE) Nº 910/2014
	2.9.6. qcStatement-2						OID 1.3.6.1.5.5.7.11.2 (RFC 3739)
	2.9.6.1. SemanticsInformation						
	2.9.6.1.1. semanticsIdNatural	0.4.0.194121.1.1					Semántica de persona fisica conforme a EN 319 412-1, en serial number
	2.10. Basic Constraints		Sí	Sí			OID 2.5.29.19
	2.10.1. cA	FALSO	Sí			Boolean	

10. Cert Corporativo de PF REP de ESPJ en SOFT

Campo	Gestión CENTRALIZADA	Oblig.	Crít.	Longitud máxima	Codif	Observaciones OID 1.3.6.1.4.1.47155.1.2.12
REPRESENTANT ESPJ · SOFT	Identificación y Firma					
1. Basic estructure						
1.1. Version	"2"	Sí		1	Integer	El literal "2" corresponde a la versión 3.
1.2. Serial Number	Establecido automáticamente por la CA. Número identificativo único del certificado.	Sí		20 octetos	Integer	No puede ser un número negativo ni 0.
1.3. Signature Algorithm		Sí				
1.3.1. Algorithm	SHA-256 with RSA Signature	Sí			OID	1.2.840.113549.1.1.11
1.3.2. Parameters	No aplicable	No				
1.4. Issuer		Sí				
1.4.1. Country Name (C)	"ES"	Sí		2 caracteres	PrintableString	OID 2.5.4.6
1.4.2. Organization Name (O)	"VINTEGRIS SL"	Sí		64 caracteres	UTF8String	OID 2.5.4.10
1.4.3. organizationalUnitName (OU)	"vinCAsign"	Sí				OID 2.5.4.11
1.4.4. Locality Name (L)	"HOSPITALET DE LLOBREGAT"	Sí		128 caracteres	UTF8String	OID 2.5.4.7
1.4.5. Organization Identifier	"VATES-B62913926"	Sí		Ilimitado	UTF8String	OID 2.5.4.97
1.4.6. Common Name (CN)	"vinCAsign nebulaSUITE2 Authority"	Sí		64 caracteres	UTF8String	OID 2.5.4.3
1.4.7. stateOrProvinceName	"BARCELONA"	Sí			UTF8String	OID 2.5.4.8
1.5. Validity		Sí				3 YEAR
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				
1.6.1. Country Name	"ES"	Sí		2 caracteres	PrintableString	OID 2.5.4.6
1.6.2. Organization (O)	Organización a la que pertenece el representante.	Sí		40 caracteres	UTF8String	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		16 caracteres	UTF8String	OID 2.5.4.11
1.6.4. Organization Identifier	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		64 caracteres	PrintableString	OID 2.5.4.97
1.6.5. Title	Representante de... / Presidente de ...			64 caracteres	UTF8String	OID 2.5.4.12
1.6.6. Serial Number	NIF del titular acorde a ETSI EN 319 412-1 "IDCES-123456789Z")	Sí			PrintableString	OID 2.5.4.5
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. Common Name	123456789Z Nombre Apellido (R: Q0000000J)	Sí				OID 2.5.4.3

1.6.10. emailAddress	Correo electrónico del firmante	Sí			IA5String	
1.6.11. Description	Codificación del documento público que acredita las facultades del firmante o los datos registrales	Sí				OID 2.5.4.13
1.7. Subject Public Key Info	Clave pública del firmante, codificada en RSA encryption (2048 bits)	Sí				
1.7.1. AlgorithmIdentifier						
1.7.1.1. Algorithm	RSA encryption	Sí			OID	OID 1.2.840.113549.1.1.1
1.7.1.2. Parameters	No aplicable	No				
1.7.2. SubjectPublicKey	Clave pública del firmante	Sí			Bit String	
2. Extensions						
2.1. Authority Key Identifier	Identificador de la clave del emisor	Sí	No			OID 2.5.29.35 (Marcado como NO crítico según EN 319412-2)
2.1.1. KeyIdentifier		Sí			Octet string	Derivado de la clave pública
2.1.2. AuthorityCertIssuer	Nombre de la CA a la que corresponde la clave identificada en keyIdentifier					(String UTF8) Size 12
2.1.3. AuthorityCertSerialNumber	Número de serie del certificado de CA					
2.2. Subject Key Identifier	Identificador de la clave del firmante	Sí	No			OID 2.5.29.14 (Marcado como NO crítico según EN 319412-2)
2.2.1. KeyIdentifier		Sí			Octet string	Derivado de la clave pública
2.3. Key Usage		Sí	Sí		Bit String	OID 2.5.29.15
2.3.1. Digital Signature	**Seleccionado "1"**	Sí				Bit para autenticación
2.3.2. Content commintment	**Seleccionado "1"**	Sí				Bit para firma
2.3.3. Key Encipherment	No seleccionado. "0"					
2.3.4. Data Encipherment	No seleccionado. "0"					
2.3.5. Key Agreement	No seleccionado. "0"					
2.3.6. Key Certificate Signature	No seleccionado. "0"					
2.3.7. CRL Signature	No seleccionado. "0"					
2.3.8. Encipher Only	No seleccionado. "0"					
2.3.9. Decipher Only	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 Information		Sí				
2.4.1.1. Policy Identifier	**1.3.6.1.4.1.47155.1.2.12**	Sí			OID	Identificador de la política de Logalty
2.4.1.2. Policy Qualifiers		Sí				
2.4.1.1.1 CPS URI	https://policy.vincasign.net				IA5String	URL de la DPC (opcional por CAB FORUM)

2.4.1.1.2. User Notice/Explicit text	"Certificado cualificado de persona física representante de ESPJ emitido en software. Ver https://policy.vincasign.net "	Sí		200 caracteres	UTF8String y NFC	Texto indicativo
2.4.2. Policy Information		Sí				
2.4.2.1. Policy Identifier	**0.4.0.194112.1.0**	Sí			OID	QCP-n-qscd. Identificador de la política de certificado cualificado de persona física con dispositivo seguro
2.4.3. Policy Information		Sí				
2.4.3.1. Policy Identifier	**2.16.724.1.3.5.9**	Sí			OID	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".
2.5. Subject Alternative Names		Sí	No			OID 2.5.29.17 (Marcado como NO crítico según EN 319412-2)
2.5.1. DirectoryName	Nombre de la persona física (como consta en el DNI/NIE)	Sí				OID 1.3.6.1.4.1.47155.1.1
	Apellido primero de la persona física (como consta en el DNI/NIE)	Sí				OID 1.3.6.1.4.1.47155.1.2
	Apellido segundo de la persona física (como consta en el DNI/NIE)	Sí				OID 1.3.6.1.4.1.47155.1.3
	NIF del titular acorde a ETSI EN 319 412-1 "IDCES-1234567892")	Sí			PrintableString	OID 1.3.6.1.4.1.47155.1.4
	Organización a la que pertenece el representante.	Sí		40 caracteres	UTF8String	OID 1.3.6.1.4.1.47155.1.6
	NIF de la persona jurídica de la que es representante el titular del certificado, en formato ETSI EN 319412-1 (Ejemplo: "VATES-Q0000000J)	Sí		64 caracteres	PrintableString	OID 1.3.6.1.4.1.47155.1.7
2.5.2. rfc822Name	Correo electrónico de la persona física	Sí			rfc822Name	
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			OID	
2.6.2. Email protection	Presente (1.3.6.1.5.5.7.3.4)	Sí			OID	Sólo se activa si se incluye el correo electrónico del firmante
2.7. cRLDistributionPoint		No	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			IA5String	uniformResourceIdentifier **(NO HTTPS)**
2.7.2. distributionPoint	http://crl2.vincasing.net/canebula2.crl	Sí			IA5String	uniformResourceIdentifier **(NO HTTPS)**
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. Access Description		Sí				

	2.8.1.1. Acces Method	id-ad-ocsp	Sí			OID	OID 1.3.6.1.5.5.7.48.1
	2.8.1.2. Acces Location	http://ocsp.vincasign.net	Sí			IA5String	URL de acceso al OCSP **(NO HTTPS)** uniformResourceIdentifier
	2.8.2. Access Description		Sí				
	2.8.2.1. Acces Method	id-ad-caIssuers	Sí			OID	OID 1.3.6.1.5.5.7.48.2
	2.8.2.1. Acces Location	http://www.vincasign.net/publickeys/casub.crt	Si			IA5String	URL acceso a certificado de la CA (NO HTTPS) uniformResourceIdentifier
	2.9. Qualified Certificate Statements		Sí	No			OID 1.3.6.1.5.5.7.1.3
	2.9.1. qCCompliance	id-etsi-qcs-QcCompliance	Sí				OID 0.4.0.1862.1.1 Indicación de certificado cualificado
	2.9.2. QcEuRetentionPeriod	"15"	Sí				OID 0.4.0.1862.1.3 Plazo de retención de registros
	2.9.4. QcPDS	{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 **(SÍ HTTPS)** URLs de acceso al texto divulgativo en inglés (obligatorio) y en castellano
	2.9.5. QcType	id-etsi-qct-esign	Sí				OID 0.4.0.1862.1.6.1 Certificado de firma electrónica conforme al Reglamento (UE) Nº 910/2014
	2.9.6. qcStatement-2						OID 1.3.6.1.5.5.7.11.2 (RFC 3739)
	2.9.6.1. SemanticsInformation						
	2.9.6.1.1. semanticsIdNatural	0.4.0.194121.1.1					Semántica de persona fisica conforme a EN 319 412-1, en serial number
	2.10. Basic Constraints		Sí	Sí			OID 2.5.29.19
	2.10.1. cA	FALSO	Sí			Boolean	

11. Cert Corporativo y Efímero de PF REP de ESPJ en DCCF

Campo EFÍMERO REPRESENTANT ESPJ · DCCF	Gestión CENTRALIZADA Identificación y Firma	Oblig.	Crít.	Longitud máxima	Codif	Observaciones OID 1.3.6.1.4.1.47155.1.2.151
1. Basic estructure						
1.1. Version	"2"	Sí		1	Integer	El literal "2" corresponde a la versión 3.
1.2. Serial Number	Establecido automáticamente por la CA. Número identificativo único del certificado.	Sí		20 octetos	Integer	No puede ser un número negativo ni 0.
1.3. Signature Algorithm		Sí				
1.3.1. Algorithm	SHA-256 with RSA Signature	Sí			OID	1.2.840.113549.1.1.11
1.3.2. Parameters	No aplicable	No				
1.4. Issuer		Sí				
1.4.1. Country Name (C)	"ES"	Sí		2 caracteres	PrintableString	OID 2.5.4.6
1.4.2. Organization Name (O)	"VINTEGRIS SL"	Sí		64 caracteres	UTF8String	OID 2.5.4.10
1.4.3. organizationalUnitName (OU)	"vinCAsign"	Sí				OID 2.5.4.11
1.4.4. Locality Name (L)	"HOSPITALET DE LLOBREGAT"	Sí		128 caracteres	UTF8String	OID 2.5.4.7
1.4.5. Organization Identifier	"VATES-B62913926"	Sí		Ilimitado	UTF8String	OID 2.5.4.97
1.4.6. Common Name (CN)	"vinCAsign nebulaSUITE2 Authority"	Sí		64 caracteres	UTF8String	OID 2.5.4.3
1.4.7. stateOrProvinceName	"BARCELONA"	Sí			UTF8String	OID 2.5.4.8
1.5. Validity	MENOR DE 1 HORA	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				
1.6.1. Country Name	"ES"	Sí		2 caracteres	PrintableString	OID 2.5.4.6
1.6.2. Organization (O)	Organización a la que pertenece el representante.	Sí		40 caracteres	UTF8String	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		16 caracteres	UTF8String	OID 2.5.4.11
1.6.4. Organization Identifier	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		64 caracteres	PrintableString	OID 2.5.4.97
1.6.5. Title	Representante de... / Presidente de ...			64 caracteres	UTF8String	OID 2.5.4.12
1.6.6. Serial Number	NIF del titular acorde a ETSI EN 319 412-1 "IDCES-123456789Z")	Sí			PrintableString	OID 2.5.4.5
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. Common Name	123456789Z Nombre Apellido (R: Q0000000J)	Sí				OID 2.5.4.3

1.6.10. emailAddress	Correo electrónico del firmante	Sí			IA5String	
1.6.11. Description	Codificación del documento público que acredita las facultades del firmante o los datos registrales	Sí				OID 2.5.4.13
1.7. Subject Public Key Info	Clave pública del firmante, codificada en RSA encryption (2048 bits)	Sí				
1.7.1. AlgorithmIdentifier						
1.7.1.1. Algorithm	RSA encryption	Sí			OID	OID 1.2.840.113549.1.1.1
1.7.1.2. Parameters	No aplicable	No				
1.7.2. SubjectPublicKey	Clave pública del firmante	Sí			Bit String	
2. Extensions						
2.1. Authority Key Identifier	Identificador de la clave del emisor	Sí	No			OID 2.5.29.35 (Marcado como NO crítico según EN 319412-2)
2.1.1. KeyIdentifier		Sí			Octet string	Derivado de la clave pública
2.1.2. AuthorityCertIssuer	Nombre de la CA a la que corresponde la clave identificada en keyIdentifier					(String UTF8) Size 12
2.1.3. AuthorityCertSerialNumber	Número de serie del certificado de CA					
2.2. Subject Key Identifier	Identificador de la clave del firmante	Sí	No			OID 2.5.29.14 (Marcado como NO crítico según EN 319412-2)
2.2.1. KeyIdentifier		Sí			Octet string	Derivado de la clave pública
2.3. Key Usage		Sí	Sí		Bit String	OID 2.5.29.15
2.3.1. Digital Signature	**Seleccionado "1"**	Sí				Bit para autenticación
2.3.2. Content commintment	**Seleccionado "1"**	Sí				Bit para firma
2.3.3. Key Encipherment	No seleccionado. "0"					
2.3.4. Data Encipherment	No seleccionado. "0"					
2.3.5. Key Agreement	No seleccionado. "0"					
2.3.6. Key Certificate Signature	No seleccionado. "0"					
2.3.7. CRL Signature	No seleccionado. "0"					
2.3.8. Encipher Only	No seleccionado. "0"					
2.3.9. Decipher Only	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 Information		Sí				
2.4.1.1. Policy Identifier	**1.3.6.1.4.1.47155.1.2.151**	Sí			OID	Identificador de la política de Logalty
2.4.1.2. Policy Qualifiers		Sí				
2.4.1.1.1 CPS URI	https://policy.vincasign.net				IA5String	URL de la DPC (opcional por CAB FORUM)

2.4.1.1.2. User Notice/Explicit text	"Certificado cualificado y efímero de persona física representante de ESPJ emitido en un DCCF. Ver https://policy.vincasign.net "	Sí		200 caracteres	UTF8String y NFC	Texto indicativo
2.4.2. Policy Information		Sí				
2.4.2.1. Policy Identifier	**0.4.0.194112.1.2**	Sí			OID	QCP-n-qscd. Identificador de la política de certificado cualificado de persona física con dispositivo seguro
2.4.3. Policy Information		Sí				
2.4.3.1. Policy Identifier	**2.16.724.1.3.5.9**	Sí			OID	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".
2.5. Subject Alternative Names		Sí	No			OID 2.5.29.17 (Marcado como NO crítico según EN 319412-2)
2.5.1. DirectoryName	Nombre de la persona física (como consta en el DNI/NIE)	Sí				OID 1.3.6.1.4.1.47155.1.1
	Apellido primero de la persona física (como consta en el DNI/NIE)	Sí				OID 1.3.6.1.4.1.47155.1.2
	Apellido segundo de la persona física (como consta en el DNI/NIE)	Sí				OID 1.3.6.1.4.1.47155.1.3
	NIF del titular acorde a ETSI EN 319 412-1 "IDCES-1234567892")	Sí			PrintableString	OID 1.3.6.1.4.1.47155.1.4
	Organización a la que pertenece el representante.	Sí		40 caracteres	UTF8String	OID 1.3.6.1.4.1.47155.1.6
	NIF de la persona jurídica de la que es representante el titular del certificado, en formato ETSI EN 319412-1 (Ejemplo: "VATES-Q0000000J)	Sí		64 caracteres	PrintableString	OID 1.3.6.1.4.1.47155.1.7
2.5.2. rfc822Name	Correo electrónico de la persona física	Sí			rfc822Name	
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			OID	
2.6.2. Email protection	Presente (1.3.6.1.5.5.7.3.4)	Sí			OID	Sólo se activa si se incluye el correo electrónico del firmante
2.7. cRLDistributionPoint		No	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			IA5String	uniformResourceIdentifier **(NO HTTPS)**
2.7.2. distributionPoint	http://crl2.vincasing.net/canebula2.crl	Sí			IA5String	uniformResourceIdentifier **(NO HTTPS)**
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. Access Description		Sí				

	2.8.1.1. Acces Method	id-ad-ocsp	Sí			OID	OID 1.3.6.1.5.5.7.48.1
	2.8.1.2. Acces Location	http://ocsp.vincasign.net	Sí			IA5String	URL de acceso al OCSP **(NO HTTPS)** uniformResourceIdentifier
	2.8.2. Access Description		Sí				
	2.8.2.1. Acces Method	id-ad-caIssuers	Sí			OID	OID 1.3.6.1.5.5.7.48.2
	2.8.2.1. Acces Location	http://www.vincasign.net/publickeys/casub.crt	Si			IA5String	URL acceso a certificado de la CA (NO HTTPS) uniformResourceIdentifier
	2.9. Qualified Certificate Statements		Sí	No			OID 1.3.6.1.5.5.7.1.3
	2.9.1. qCCompliance	id-etsi-qcs-QcCompliance	Sí				OID 0.4.0.1862.1.1 Indicación de certificado cualificado
	2.9.2. QcEuRetentionPeriod	"15"	Sí				OID 0.4.0.1862.1.3 Plazo de retención de registros
	2.9.3. QcSSCD	id-etsi-qcs-QcSSCD	Sí				OID 0.4.0.1862.1.4 Dispositivo cualificado de creación de firma
	2.9.4. QcPDS	{https://www.vincasign.net/policy/es/PDS-REPESPJ1u-hard/pds-repespj1u-hard-es.pdf,es},{https://www.vincasign.net/policy/en/PDS-REPESPJ1u-hard/pds-repespj1u-hard-en.pdf,en}	Sí				OID 0.4.0.1862.1.5 **(SÍ HTTPS)** URLs de acceso al texto divulgativo en inglés (obligatorio) y en castellano
	2.9.5. QcType	id-etsi-qct-esign	Sí				OID 0.4.0.1862.1.6.1 Certificado de firma electrónica conforme al Reglamento (UE) Nº 910/2014
	2.9.6. qcStatement-2						OID 1.3.6.1.5.5.7.11.2 (RFC 3739)
	2.9.6.1. SemanticsInformation						
	2.9.6.1.1. semanticsIdNatural	0.4.0.194121.1.1					Semántica de persona fisica conforme a EN 319 412-1, en serial number
	2.10. Basic Constraints		Sí	Sí			OID 2.5.29.19
	2.10.1. cA	FALSO	Sí			Boolean	

12. Cert Corporativo y Efímero de PF REP de ESPJ en SOFT

Campo EFÍMERO REPRESENTANT ESPJ · SOFT	Gestión CENTRALIZADA Identificación y Firma	Oblig.	Crít.	Longitud máxima	Codif	Observaciones OID 1.3.6.1.4.1.47155.1.2.152
1. Basic estructure						
1.1. Version	"2"	Sí		1	Integer	El literal "2" corresponde a la versión 3.
1.2. Serial Number	Establecido automáticamente por la CA. Número identificativo único del certificado.	Sí		20 octetos	Integer	No puede ser un número negativo ni 0.
1.3. Signature Algorithm		Sí				
1.3.1. Algorithm	SHA-256 with RSA Signature	Sí			OID	1.2.840.113549.1.1.11
1.3.2. Parameters	No aplicable	No				
1.4. Issuer		Sí				
1.4.1. Country Name (C)	"ES"	Sí		2 caracteres	PrintableString	OID 2.5.4.6
1.4.2. Organization Name (O)	"VINTEGRIS SL"	Sí		64 caracteres	UTF8String	OID 2.5.4.10
1.4.3. organizationalUnitName (OU)	"vinCAsign"	Sí				OID 2.5.4.11
1.4.4. Locality Name (L)	"HOSPITALET DE LLOBREGAT"	Sí		128 caracteres	UTF8String	OID 2.5.4.7
1.4.5. Organization Identifier	"VATES-B62913926"	Sí		Ilimitado	UTF8String	OID 2.5.4.97
1.4.6. Common Name (CN)	"vinCAsign nebulaSUITE2 Authority"	Sí		64 caracteres	UTF8String	OID 2.5.4.3
1.4.7. stateOrProvinceName	"BARCELONA"	Sí			UTF8String	OID 2.5.4.8
1.5. Validity	MENOR DE 1 HORA	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				
1.6.1. Country Name	"ES"	Sí		2 caracteres	PrintableString	OID 2.5.4.6
1.6.2. Organization (O)	Organización a la que pertenece el representante.	Sí		40 caracteres	UTF8String	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		16 caracteres	UTF8String	OID 2.5.4.11
1.6.4. Organization Identifier	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		64 caracteres	PrintableString	OID 2.5.4.97
1.6.5. Title	Representante de... / Presidente de ...			64 caracteres	UTF8String	OID 2.5.4.12
1.6.6. Serial Number	NIF del titular acorde a ETSI EN 319 412-1 "IDCES-123456789Z")	Sí			PrintableString	OID 2.5.4.5
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. Common Name	123456789Z Nombre Apellido (R: Q0000000J)	Sí				OID 2.5.4.3

	1.6.10. emailAddress	Correo electrónico del firmante	Sí			IA5String	
	1.6.11. Description	Codificación del documento público que acredita las facultades del firmante o los datos registrales	Sí				OID 2.5.4.13
	1.7. Subject Public Key Info	Clave pública del firmante, codificada en RSA encryption (2048 bits)	Sí				
	1.7.1. AlgorithmIdentifier						
	1.7.1.1. Algorithm	RSA encryption	Sí			OID	OID 1.2.840.113549.1.1.1
	1.7.1.2. Parameters	No aplicable	No				
	1.7.2. SubjectPublicKey	Clave pública del firmante	Sí			Bit String	
2. Extensions							
	2.1. Authority Key Identifier	Identificador de la clave del emisor	Sí	No			OID 2.5.29.35 (Marcado como NO crítico según EN 319412-2)
	2.1.1. KeyIdentifier		Sí			Octet string	Derivado de la clave pública
	2.1.2. AuthorityCertIssuer	Nombre de la CA a la que corresponde la clave identificada en keyIdentifier					(String UTF8) Size 12
	2.1.3. AuthorityCertSerialNumber	Número de serie del certificado de CA					
	2.2. Subject Key Identifier	Identificador de la clave del firmante	Sí	No			OID 2.5.29.14 (Marcado como NO crítico según EN 319412-2)
	2.2.1. KeyIdentifier		Sí			Octet string	Derivado de la clave pública
	2.3. Key Usage		Sí	Sí		Bit String	OID 2.5.29.15
	2.3.1. Digital Signature	**Seleccionado "1"**	Sí				Bit para autenticación
	2.3.2. Content commintment	**Seleccionado "1"**	Sí				Bit para firma
	2.3.3. Key Encipherment	No seleccionado. "0"					
	2.3.4. Data Encipherment	No seleccionado. "0"					
	2.3.5. Key Agreement	No seleccionado. "0"					
	2.3.6. Key Certificate Signature	No seleccionado. "0"					
	2.3.7. CRL Signature	No seleccionado. "0"					
	2.3.8. Encipher Only	No seleccionado. "0"					
	2.3.9. Decipher Only	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 Information		Sí				
	2.4.1.1. Policy Identifier	**1.3.6.1.4.1.47155.1.2.152**	Sí			OID	Identificador de la política de Logalty
	2.4.1.2. Policy Qualifiers		Sí				
	2.4.1.1.1 CPS URI	https://policy.vincasign.net				IA5String	URL de la DPC (opcional por CAB FORUM)

	2.4.1.1.2. User Notice/Explicit text	"Certificado cualificado y efímero de persona física representante de ESPJ emitido en software. Ver https://policy.vincasign.net "	Sí		200 caracteres	UTF8String y NFC	Texto indicativo
	2.4.2. Policy Information		Sí				
	2.4.2.1. Policy Identifier	**0.4.0.194112.1.0**	Sí			OID	QCP-n-qscd. Identificador de la política de certificado cualificado de persona física con dispositivo seguro
	2.4.3. Policy Information		Sí				
	2.4.3.1. Policy Identifier	**2.16.724.1.3.5.9**	Sí			OID	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".
	2.5. Subject Alternative Names		Sí	No			OID 2.5.29.17 (Marcado como NO crítico según EN 319412-2)
	2.5.1. DirectoryName	Nombre de la persona física (como consta en el DNI/NIE)	Sí				OID 1.3.6.1.4.1.47155.1.1
		Apellido primero de la persona física (como consta en el DNI/NIE)	Sí				OID 1.3.6.1.4.1.47155.1.2
		Apellido segundo de la persona física (como consta en el DNI/NIE)	Sí				OID 1.3.6.1.4.1.47155.1.3
		NIF del titular acorde a ETSI EN 319 412-1 "IDCES-1234567892")	Sí			PrintableString	OID 1.3.6.1.4.1.47155.1.4
		Organización a la que pertenece el representante.	Sí		40 caracteres	UTF8String	OID 1.3.6.1.4.1.47155.1.6
		NIF de la persona jurídica de la que es representante el titular del certificado, en formato ETSI EN 319412-1 (Ejemplo: "VATES-Q0000000J)	Sí		64 caracteres	PrintableString	OID 1.3.6.1.4.1.47155.1.7
	2.5.2. rfc822Name	Correo electrónico de la persona física	Sí			rfc822Name	
	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			OID	
	2.6.2. Email protection	Presente (1.3.6.1.5.5.7.3.4)	Sí			OID	Sólo se activa si se incluye el correo electrónico del firmante
	2.7. cRLDistributionPoint		No	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			IA5String	uniformResourceIdentifier **(NO HTTPS)**
	2.7.2. distributionPoint	http://crl2.vincasing.net/canebula2.crl	Sí			IA5String	uniformResourceIdentifier **(NO HTTPS)**
	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. Access Description		Sí				

	2.8.1.1. Acces Method	id-ad-ocsp	Sí			OID	OID 1.3.6.1.5.5.7.48.1
	2.8.1.2. Acces Location	http://ocsp.vincasign.net	Sí			IA5String	URL de acceso al OCSP **(NO HTTPS)** uniformResourceIdentifier
	2.8.2. Access Description		Sí				
	2.8.2.1. Acces Method	id-ad-caIssuers	Sí			OID	OID 1.3.6.1.5.5.7.48.2
	2.8.2.1. Acces Location	http://www.vincasign.net/publickeys/casub.crt	Si			IA5String	URL acceso a certificado de la CA (NO HTTPS) uniformResourceIdentifier
	2.9. Qualified Certificate Statements		Sí	No			OID 1.3.6.1.5.5.7.1.3
	2.9.1. qCCompliance	id-etsi-qcs-QcCompliance	Sí				OID 0.4.0.1862.1.1 Indicación de certificado cualificado
	2.9.2. QcEuRetentionPeriod	"15"	Sí				OID 0.4.0.1862.1.3 Plazo de retención de registros
	2.9.4. QcPDS	{https://www.vincasign.net/policy/es/PDS-REPESPJ1u-soft/pds-repespj1u-soft-es.pdf,es},{https://www.vincasign.net/policy/en/PDS-REPESPJ1u-soft/pds-repespj1u-soft-en.pdf,en}	Sí				OID 0.4.0.1862.1.5 **(SÍ HTTPS)** URLs de acceso al texto divulgativo en inglés (obligatorio) y en castellano
	2.9.5. QcType	id-etsi-qct-esign	Sí				OID 0.4.0.1862.1.6.1 Certificado de firma electrónica conforme al Reglamento (UE) Nº 910/2014
	2.9.6. qcStatement-2						OID 1.3.6.1.5.5.7.11.2 (RFC 3739)
	2.9.6.1. SemanticsInformation						
	2.9.6.1.1. semanticsIdNatural	0.4.0.194121.1.1					Semántica de persona fisica conforme a EN 319 412-1, en serial number
	2.10. Basic Constraints		Sí	Sí			OID 2.5.29.19
	2.10.1. cA	FALSO	Sí			Boolean	

13. Cert de Empleado Público nivel ALTO

Campo PF Empleado Público · ALTO	Gestión CENTRALIZADA Identificación y Firma	Oblig.	Crít.	Longitud máxima	Codif	Observaciones OID 1.3.6.1.4.1.47155.1.4.1
1. Basic estructure						
1.1. Version	"2"	Sí		1	Integer	El literal "2" corresponde a la versión 3.
1.2. Serial Number	Establecido automáticamente por la CA. Número identificativo único del certificado.	Sí		20 octetos	Integer	No puede ser un número negativo ni 0.
1.3. Signature Algorithm		Sí				
1.3.1. Algorithm	SHA-256 with RSA Signature	Sí			OID	1.2.840.113549.1.1.11
1.3.2. Parameters	No aplicable	No				
1.4. Issuer		Sí				
1.4.1. Country Name (C)	"ES"	Sí		2 caracteres	PrintableString	OID 2.5.4.6
1.4.2. Organization Name (O)	"VINTEGRIS SL"	Sí		64 caracteres	UTF8String	OID 2.5.4.10
1.4.3. organizationalUnitName (OU)	"vinCAsign"	Sí				OID 2.5.4.11
1.4.4. Locality Name (L)	"HOSPITALET DE LLOBREGAT"	Sí		128 caracteres	UTF8String	OID 2.5.4.7
1.4.5. Organization Identifier	"VATES-B62913926"	Sí		Ilimitado	UTF8String	OID 2.5.4.97
1.4.6. Common Name (CN)	"vinCAsign nebulaSUITE2 Authority"	Sí		64 caracteres	UTF8String	OID 2.5.4.3
1.4.7. stateOrProvinceName	"BARCELONA"	Sí			UTF8String	OID 2.5.4.8
1.5. Validity		Sí				3 YEAR
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				
1.6.1. Country Name	"ES"	Sí		2 caracteres	PrintableString	OID 2.5.4.6
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		40 caracteres	UTF8String	OID 2.5.4.10
1.6.3. Organizational Unit (OU)	"Certificado electrónico de empleado público nivel Alto"	Sí		16 caracteres	UTF8String	OID 2.5.4.11
1.6.4. Organization Identifier	NIF de la AAPP a la que está vinculado el empleado público titular del certificado, en formato ETSI EN 319412-1 (Ejemplo: "VATES-Q0000000J)			64 caracteres	PrintableString	OID 2.5.4.97
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			64 caracteres	UTF8String	OID 2.5.4.12
1.6.6. Serial Number	NIF del titular acorde a ETSI EN 319 412-1 "IDCES-1234567892")	Sí			PrintableString	OID 2.5.4.5

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. Common Name	Nombre Apellido1 Apellido2 – DNI 00000000G	Sí				OID 2.5.4.3
1.6.10. emailAddress	Correo electrónico del firmante	Sí			IA5String	
1.7. Subject Public Key Info	Clave pública del firmante, codificada en RSA encryption (2048 bits)	Sí				
1.7.1. AlgorithmIdentifier						
1.7.1.1. Algorithm	RSA encryption	Sí			OID	OID 1.2.840.113549.1.1.1
1.7.1.2. Parameters	No aplicable	No				
1.7.2. SubjectPublicKey	Clave pública del firmante	Sí			Bit String	
2. Extensions						
2.1. Authority Key Identifier	Identificador de la clave del emisor	Sí	No			OID 2.5.29.35 (Marcado como NO crítico según EN 319412-2)
2.1.1. KeyIdentifier		Sí			Octet string	Derivado de la clave pública
2.1.2. AuthorityCertIssuer	Nombre de la CA a la que corresponde la clave identificada en keyIdentifier					(String UTF8) Size 12
2.1.3. AuthorityCertSerialNumber	Número de serie del certificado de CA					
2.2. Subject Key Identifier	Identificador de la clave del firmante	Sí	No			OID 2.5.29.14 (Marcado como NO crítico según EN 319412-2)
2.2.1. KeyIdentifier		Sí			Octet string	Derivado de la clave pública
2.3. Key Usage		Sí	Sí		Bit String	OID 2.5.29.15
2.3.1. Digital Signature	**Seleccionado "1"**	Sí				Bit para autenticación
2.3.2. Content commintment	**Seleccionado "1"**	Sí				Bit para firma
2.3.3. Key Encipherment	No seleccionado. "0"					
2.3.4. Data Encipherment	No seleccionado. "0"					
2.3.5. Key Agreement	No seleccionado. "0"					
2.3.6. Key Certificate Signature	No seleccionado. "0"					
2.3.7. CRL Signature	No seleccionado. "0"					
2.3.8. Encipher Only	No seleccionado. "0"					
2.3.9. Decipher Only	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 Information		Sí				
2.4.1.1. Policy Identifier	**1.3.6.1.4.1.47155.1.4.1**	Sí			OID	Identificador de la política de Logalty
2.4.1.2. Policy Qualifiers		Sí				

2.4.1.1.1 CPS URI	https://policy.vincasign.net				IA5String	URL de la DPC (opcional por CAB FORUM)
2.4.1.1.2. User Notice/Explicit text	"Certificado cualificado de persona física empleado público de nivel alto. Ver https://policy.vincasign.net "	Sí		200 caracteres	UTF8String y NFC	Texto indicativo
2.4.2. Policy Information		Sí				
2.4.2.1. Policy Identifier	**0.4.0.194112.1.2**	Sí			OID	QCP-n-qscd. Identificador de la política de certificado cualificado de persona física con dispositivo seguro
2.4.2. Policy Information		Sí				
2.4.2.1. Policy Identifier	**2.16.724.1.3.5.7.1**	Sí			OID	OID asociado a certificado de empleado público
2.5. Subject Alternative Names		Sí	No			OID 2.5.29.17 (Marcado como NO crítico según EN 319412-2)
2.5.1. rfc822Name	Correo electrónico de la persona física	Sí			rfc822Name	
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
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
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
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
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
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
2.5.2.7. Primer apellido	Primer apellido del responsable del certificado	Sí				OID ALTO: 2.16.724.1.3.5.7.1.7
2.5.2.8. Segundo apellido	Segundo apellido del responsable del certificado	Sí				OID ALTO: 2.16.724.1.3.5.7.1.8
2.5.2.9. Correo electrónico	Correo electrónico del responsable del certificado					OID ALTO: 2.16.724.1.3.5.7.1.9
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
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
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			OID	
2.6.2. Email protection	Presente (1.3.6.1.5.5.7.3.4)	Sí			OID	Sólo se activa si se incluye el correo electrónico del firmante

2.7. cRLDistributionPoint		No	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			IA5String	uniformResourceIdentifier **(NO HTTPS)**
2.7.2. distributionPoint	http://crl2.vincasing.net/canebula2.crl	Sí			IA5String	uniformResourceIdentifier **(NO HTTPS)**
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. Access Description		Sí				
2.8.1.1. Acces Method	id-ad-ocsp	Sí			OID	OID 1.3.6.1.5.5.7.48.1
2.8.1.2. Acces Location	http://ocsp.vincasign.net	Sí			IA5String	URL de acceso al OCSP **(NO HTTPS)** uniformResourceIdentifier
2.8.2. Access Description		Sí				
2.8.2.1. Acces Method	id-ad-caIssuers	Sí			OID	OID 1.3.6.1.5.5.7.48.2
2.8.2.1. Acces Location	http://www.vincasign.net/publickeys/casub.crt	Si			IA5String	URL acceso a certificado de la CA (NO HTTPS) uniformResourceIdentifier
2.9. Qualified Certificate Statements		Sí	No			OID 1.3.6.1.5.5.7.1.3
2.9.1. qCCompliance	id-etsi-qcs-QcCompliance	Sí				OID 0.4.0.1862.1.1 Indicación de certificado cualificado
2.9.2. QcEuRetentionPeriod	"15"	Sí				OID 0.4.0.1862.1.3 Plazo de retención de registros
2.9.3. QcSSCD	id-etsi-qcs-QcSSCD	Sí				OID 0.4.0.1862.1.4 Dispositivo cualificado de creación de 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}	Sí				OID 0.4.0.1862.1.5 **(SÍ HTTPS)** URLs de acceso al texto divulgativo en inglés (obligatorio) y en castellano
2.9.5. QcType	id-etsi-qct-esign	Sí				OID 0.4.0.1862.1.6.1 Certificado de firma electrónica conforme al Reglamento (UE) Nº 910/2014
2.9.6. qcStatement-2						OID 1.3.6.1.5.5.7.11.2 (RFC 3739)
2.9.6.1. SemanticsInformation						
2.9.6.1.1. semanticsIdNatural	0.4.0.194121.1.1					Semántica de persona fisica conforme a EN 319 412-1, en serial number
2.10. Basic Constraints		Sí	Sí			OID 2.5.29.19
2.10.1. cA	FALSO	Sí			Boolean	

14. Cert de Empleado Público nivel MEDIO

Campo PF Empleado Público · MEDIO	Gestión CENTRALIZADA Identificación y Firma	Oblig.	Crít.	Longitud máxima	Codif	Observaciones OID 1.3.6.1.4.1.47155.1.4.2
1. Basic estructure						
1.1. Version	"2"	Sí		1	Integer	El literal "2" corresponde a la versión 3.
1.2. Serial Number	Establecido automáticamente por la CA. Número identificativo único del certificado.	Sí		20 octetos	Integer	No puede ser un número negativo ni 0.
1.3. Signature Algorithm		Sí				
1.3.1. Algorithm	SHA-256 with RSA Signature	Sí			OID	1.2.840.113549.1.1.11
1.3.2. Parameters	No aplicable	No				
1.4. Issuer		Sí				
1.4.1. Country Name (C)	"ES"	Sí		2 caracteres	PrintableString	OID 2.5.4.6
1.4.2. Organization Name (O)	"VINTEGRIS SL"	Sí		64 caracteres	UTF8String	OID 2.5.4.10
1.4.3. organizationalUnitName (OU)	"vinCAsign"	Sí				OID 2.5.4.11
1.4.4. Locality Name (L)	"HOSPITALET DE LLOBREGAT"	Sí		128 caracteres	UTF8String	OID 2.5.4.7
1.4.5. Organization Identifier	"VATES-B62913926"	Sí		Ilimitado	UTF8String	OID 2.5.4.97
1.4.6. Common Name (CN)	"vinCAsign nebulaSUITE2 Authority"	Sí		64 caracteres	UTF8String	OID 2.5.4.3
1.4.7. stateOrProvinceName	"BARCELONA"	Sí			UTF8String	OID 2.5.4.8
1.5. Validity		Sí				3 YEAR
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				
1.6.1. Country Name	"ES"	Sí		2 caracteres	PrintableString	OID 2.5.4.6
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		40 caracteres	UTF8String	OID 2.5.4.10
1.6.3. Organizational Unit (OU)	"Certificado electrónico de empleado público nivel Medio"	Sí		16 caracteres	UTF8String	OID 2.5.4.11
1.6.4. Organization Identifier	NIF de la AAPP a la que está vinculado el empleado público titular del certificado, en formato ETSI EN 319412-1 (Ejemplo: "VATES-Q0000000J)			64 caracteres	PrintableString	OID 2.5.4.97
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			64 caracteres	UTF8String	OID 2.5.4.12
1.6.6. Serial Number	NIF del titular acorde a ETSI EN 319 412-1 "IDCES-1234567892")	Sí			PrintableString	OID 2.5.4.5

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. Common Name	Nombre Apellido1 Apellido2 – DNI 00000000G	Sí				OID 2.5.4.3
1.6.10. emailAddress	Correo electrónico del firmante	Sí			IA5String	
1.7. Subject Public Key Info	Clave pública del firmante, codificada en RSA encryption (2048 bits)	Sí				
1.7.1. AlgorithmIdentifier						
1.7.1.1. Algorithm	RSA encryption	Sí			OID	OID 1.2.840.113549.1.1.1
1.7.1.2. Parameters	No aplicable	No				
1.7.2. SubjectPublicKey	Clave pública del firmante	Sí			Bit String	
2. Extensions						
2.1. Authority Key Identifier	Identificador de la clave del emisor	Sí	No			OID 2.5.29.35 (Marcado como NO crítico según EN 319412-2)
2.1.1. KeyIdentifier		Sí			Octet string	Derivado de la clave pública
2.1.2. AuthorityCertIssuer	Nombre de la CA a la que corresponde la clave identificada en keyIdentifier					(String UTF8) Size 12
2.1.3. AuthorityCertSerialNumber	Número de serie del certificado de CA					
2.2. Subject Key Identifier	Identificador de la clave del firmante	Sí	No			OID 2.5.29.14 (Marcado como NO crítico según EN 319412-2)
2.2.1. KeyIdentifier		Sí			Octet string	Derivado de la clave pública
2.3. Key Usage		Sí	Sí		Bit String	OID 2.5.29.15
2.3.1. Digital Signature	**Seleccionado "1"**	Sí				Bit para autenticación
2.3.2. Content commintment	**Seleccionado "1"**	Sí				Bit para firma
2.3.3. Key Encipherment	**Seleccionado "1"**	Sí				
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"					
2.3.8. Encipher Only	No seleccionado. "0"					
2.3.9. Decipher Only	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 Information		Sí				
2.4.1.1. Policy Identifier	**1.3.6.1.4.1.47155.1.4.2**	Sí			OID	Identificador de la política de Logalty
2.4.1.2. Policy Qualifiers		Sí				

2.4.1.1.1 CPS URI	https://policy.vincasign.net				IA5String	URL de la DPC (opcional por CAB FORUM)
2.4.1.1.2. User Notice/Explicit text	"Certificado cualificado de persona física empleado público de nivel medio. Ver https://policy.vincasign.net "	Sí		200 caracteres	UTF8String y NFC	Texto indicativo
2.4.2. Policy Information		Sí				
2.4.2.1. Policy Identifier	**0.4.0.194112.1.0**	Sí			OID	QCP-n-qscd. Identificador de la política de certificado cualificado de persona física sin uso de dispositivo seguro
2.4.2. Policy Information		Sí				
2.4.2.1. Policy Identifier	**2.16.724.1.3.5.7.2**	Sí			OID	OID asociado a certificado de empleado público
2.5. Subject Alternative Names		Sí	No			OID 2.5.29.17 (Marcado como NO crítico según EN 319412-2)
2.5.1. rfc822Name	Correo electrónico de la persona física	Sí			rfc822Name	
2.5.2. Directory Name	Identidad administrativa	Sí				
2.5.2.1. Tipo de certificado	"certificado electrónico de empleado público"	Sí				OID ALTO: 2.16.724.1.3.5.7.2.1
2.5.2.2. Nombre de la entidad subscriptora	Entidad propietaria del certificado	Sí				OID ALTO: 2.16.724.1.3.5.7.2.2
2.5.2.3. NIF de la entidad subscriptora	Número de identificación fiscal de la entidad propietaria del certificado	Sí				OID ALTO: 2.16.724.1.3.5.7.2.3
2.5.2.4. DNI/NIE del Responsable	DNI o NIE del responsable	Sí				OID ALTO: 2.16.724.1.3.5.7.2.4
2.5.2.5. Número de identificación personal	NRP o NIP del responsable del suscriptor del certificado					OID ALTO: 2.16.724.1.3.5.7.2.5
2.5.2.6. Nombre de pila	Nombre de pila del responsable del certificado	Sí				OID ALTO: 2.16.724.1.3.5.7.2.6
2.5.2.7. Primer apellido	Primer apellido del responsable del certificado	Sí				OID ALTO: 2.16.724.1.3.5.7.2.7
2.5.2.8. Segundo apellido	Segundo apellido del responsable del certificado	Sí				OID ALTO: 2.16.724.1.3.5.7.2.8
2.5.2.9. Correo electrónico	Correo electrónico del responsable del certificado					OID ALTO: 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: 2.16.724.1.3.5.7.2.10
2.5.2.11. Puesto o cargo	Puesto desempeñado por el suscriptor del certificado dentro de la Administración					OID ALTO: 2.16.724.1.3.5.7.2.11
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			OID	
2.6.2. Email protection	Presente (1.3.6.1.5.5.7.3.4)	Sí			OID	Sólo se activa si se incluye el correo electrónico del firmante

2.7. cRLDistributionPoint		No	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			IA5String	uniformResourceIdentifier **(NO HTTPS)**
2.7.2. distributionPoint	http://crl2.vincasing.net/canebula2.crl	Sí			IA5String	uniformResourceIdentifier **(NO HTTPS)**
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. Access Description		Sí				
2.8.1.1. Acces Method	id-ad-ocsp	Sí			OID	OID 1.3.6.1.5.5.7.48.1
2.8.1.2. Acces Location	http://ocsp.vincasign.net	Sí			IA5String	URL de acceso al OCSP **(NO HTTPS)** uniformResourceIdentifier
2.8.2. Access Description		Sí				
2.8.2.1. Acces Method	id-ad-caIssuers	Sí			OID	OID 1.3.6.1.5.5.7.48.2
2.8.2.1. Acces Location	http://www.vincasign.net/publickeys/casub.crt	Si			IA5String	URL acceso a certificado de la CA (NO HTTPS) uniformResourceIdentifier
2.9. Qualified Certificate Statements		Sí	No			OID 1.3.6.1.5.5.7.1.3
2.9.1. qCCompliance	id-etsi-qcs-QcCompliance	Sí				OID 0.4.0.1862.1.1 Indicación de certificado cualificado
2.9.2. QcEuRetentionPeriod	"15"	Sí				OID 0.4.0.1862.1.3 Plazo de retención de registros
2.9.4. QcPDS	{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 **(SÍ HTTPS)** URLs de acceso al texto divulgativo en inglés (obligatorio) y en castellano
2.9.5. QcType	id-etsi-qct-esign	Sí				OID 0.4.0.1862.1.6.1 Certificado de firma electrónica conforme al Reglamento (UE) Nº 910/2014
2.9.6. qcStatement-2						OID 1.3.6.1.5.5.7.11.2 (RFC 3739)
2.9.6.1. SemanticsInformation						
2.9.6.1.1. semanticsIdNatural	0.4.0.194121.1.1					Semántica de persona fisica conforme a EN 319 412-1, en serial number
2.10. Basic Constraints		Sí	Sí			OID 2.5.29.19
2.10.1. cA	FALSO	Sí			Boolean	

15. Cert de Empleado Público con seudónimo nivel ALTO

Campo Empleado Público Seudónimo · ALTO	Gestión CENTRALIZADA Identificación y Firma	Oblig.	Crít.	Longitud máxima	Codif	Observaciones OID 1.3.6.1.4.1.47155.1.4.11
1. Basic estructure						
1.1. Version	"2"	Sí		1	Integer	El literal "2" corresponde a la versión 3.
1.2. Serial Number	Establecido automáticamente por la CA. Número identificativo único del certificado.	Sí		20 octetos	Integer	No puede ser un número negativo ni 0.
1.3. Signature Algorithm		Sí				
1.3.1. Algorithm	SHA-256 with RSA Signature	Sí			OID	1.2.840.113549.1.1.11
1.3.2. Parameters	No aplicable	No				
1.4. Issuer		Sí				
1.4.1. Country Name (C)	"ES"	Sí		2 caracteres	PrintableString	OID 2.5.4.6
1.4.2. Organization Name (O)	"VINTEGRIS SL"	Sí		64 caracteres	UTF8String	OID 2.5.4.10
1.4.3. organizationalUnitName (OU)	"vinCAsign"	Sí				OID 2.5.4.11
1.4.4. Locality Name (L)	"HOSPITALET DE LLOBREGAT"	Sí		128 caracteres	UTF8String	OID 2.5.4.7
1.4.5. Organization Identifier	"VATES-B62913926"	Sí		Ilimitado	UTF8String	OID 2.5.4.97
1.4.6. Common Name (CN)	"vinCAsign nebulaSUITE2 Authority"	Sí		64 caracteres	UTF8String	OID 2.5.4.3
1.4.7. stateOrProvinceName	"BARCELONA"	Sí			UTF8String	OID 2.5.4.8
1.5. Validity		Sí				3 YEAR
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				
1.6.1. Country Name	"ES"	Sí		2 caracteres	PrintableString	OID 2.5.4.6
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		40 caracteres	UTF8String	OID 2.5.4.10
1.6.3. Organizational Unit (OU)	"CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO CON SEUDONIMO"	Sí			UTF8String	OID 2.5.4.11
1.6.4. Organizational Unit (OU)	Unidad, dentro de la Administración, en la que está incluida el suscriptor del certificado	No			UTF8String	OID 2.5.4.11
1.6.5. Organizational Unit (OU)	Código DIR3 de la unidad	No			UTF8String	OID 2.5.4.11
1.6.6. pseudonym	NIP 111111111	Sí				OID 2.5.4.65 Obligatorio según ETSI EN 319 412-2

1.6.7. Organization Identifier	NIF de la AAPP a la que está vinculado el empleado público titular del certificado, en formato ETSI EN 319412-1 (Ejemplo: "VATES-Q0000000J)			64 caracteres	PrintableString	OID 2.5.4.97
1.6.8. 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			64 caracteres	UTF8String	OID 2.5.4.12
1.6.9. Common Name	CARGO/SEUDONIMO – NIP 11111111 – NOMBRE ORGANISMO	Sí				OID 2.5.4.3 Si existe TITLE = CARGO Sinó indicar "SEUDONIMO"
1.7. Subject Public Key Info	Clave pública del firmante, codificada en RSA encryption (2048 bits)	Sí				
1.7.1. AlgorithmIdentifier						
1.7.1.1. Algorithm	RSA encryption	Sí			OID	OID 1.2.840.113549.1.1.1
1.7.1.2. Parameters	No aplicable	No				
1.7.2. SubjectPublicKey	Clave pública del firmante	Sí			Bit String	
2. Extensions						
2.1. Authority Key Identifier	Identificador de la clave del emisor	Sí	No			OID 2.5.29.35 (Marcado como NO crítico según EN 319412-2)
2.1.1. KeyIdentifier		Sí			Octet string	Derivado de la clave pública
2.1.2. AuthorityCertIssuer	Nombre de la CA a la que corresponde la clave identificada en keyIdentifier					(String UTF8) Size 12
2.1.3. AuthorityCertSerialNumber	Número de serie del certificado de CA					
2.2. Subject Key Identifier	Identificador de la clave del firmante	Sí	No			OID 2.5.29.14 (Marcado como NO crítico según EN 319412-2)
2.2.1. KeyIdentifier		Sí			Octet string	Derivado de la clave pública
2.3. Key Usage		Sí	Sí		Bit String	OID 2.5.29.15
2.3.1. Digital Signature	**Seleccionado "1"**	Sí				Bit para autenticación
2.3.2. Content commintment	**Seleccionado "1"**	Sí				Bit para firma
2.3.3. Key Encipherment	No seleccionado. "0"					
2.3.4. Data Encipherment	No seleccionado. "0"					
2.3.5. Key Agreement	No seleccionado. "0"					
2.3.6. Key Certificate Signature	No seleccionado. "0"					
2.3.7. CRL Signature	No seleccionado. "0"					
2.3.8. Encipher Only	No seleccionado. "0"					
2.3.9. Decipher Only	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 Information		Sí				
2.4.1.1. Policy Identifier	**1.3.6.1.4.1.47155.1.4.11**	Sí			OID	Identificador de la política de Logalty
2.4.1.2. Policy Qualifiers		Sí				
2.4.1.1.1 CPS URI	https://policy.vincasign.net				IA5String	URL de la DPC (opcional por CAB FORUM)
2.4.1.1.2. User Notice/Explicit text	"CERTIFICADO CUALIFICADO DE EMPLEADO PUBLICO CON SEUDONIMO DE NIVEL ALTO. Ver https://policy.vincasign.net "	Sí		200 caracteres	UTF8String y NFC	Texto indicativo
2.4.2. Policy Information		Sí				
2.4.2.1. Policy Identifier	**0.4.0.194112.1.2**	Sí			OID	QCP-n-qscd. Identificador de la política de certificado cualificado de persona física con dispositivo seguro
2.4.2. Policy Information		Sí				
2.4.2.1. Policy Identifier	**2.16.724.1.3.5.4.1**	Sí			OID	OID asociado a certificado de empleado público con seudónimo
2.5. Subject Alternative Names		Sí	No			OID 2.5.29.17 (Marcado como NO crítico según EN 319412-2)
2.5.1. rfc822Name	Correo electrónico de contacto				rfc822Name	
2.5.2. Directory Name	Identidad administrativa	Sí				
2.5.2.1. Tipo de certificado	"CERTIFICADO CUALIFICADO DE EMPLEADO PUBLICO CON SEUDONIMO, DE NIVEL ALTO"	Sí				OID ALTO: 2.16.724.1.3.5.4.1.1
2.5.2.2. Nombre de la entidad subscriptora	Entidad propietaria del certificado	Sí				OID ALTO: 2.16.724.1.3.5.4.1.2
2.5.2.3. NIF de la entidad subscriptora	Número de identificación fiscal de la entidad propietaria del certificado	Sí				OID ALTO: 2.16.724.1.3.5.4.1.3
2.5.2.4. Correo electrónico	Correo electrónico de contacto					OID ALTO: 2.16.724.1.3.5.4.1.9
2.5.2.5. Unidad organizativa	Unidad, dentro de la Administración, en la que está incluido el suscriptor del certificado					OID ALTO: 2.16.724.1.3.5.4.1.10
2.5.2.6. Puesto o cargo	Puesto desempeñado por el suscriptor del certificado dentro de la Administración					OID ALTO: 2.16.724.1.3.5.4.1.11
2.5.2.7. Seudónimo	NIP 1111					OID ALTO: 2.16.724.1.3.5.4.1.12
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			OID	
2.6.2. Email protection	Presente (1.3.6.1.5.5.7.3.4)	Sí			OID	Sólo se activa si se incluye el correo electrónico del firmante

2.7. cRLDistributionPoint		No	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			IA5String	uniformResourceIdentifier **(NO HTTPS)**	
2.7.2. distributionPoint	http://crl2.vincasing.net/canebula2.crl	Sí			IA5String	uniformResourceIdentifier **(NO HTTPS)**	
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. Access Description		Sí					
2.8.1.1. Acces Method	id-ad-ocsp	Sí			OID	OID 1.3.6.1.5.5.7.48.1	
2.8.1.2. Acces Location	http://ocsp.vincasign.net	Sí			IA5String	URL de acceso al OCSP **(NO HTTPS)** uniformResourceIdentifier	
2.8.2. Access Description		Sí					
2.8.2.1. Acces Method	id-ad-calssuers	Sí			OID	OID 1.3.6.1.5.5.7.48.2	
2.8.2.1. Acces Location	http://www.vincasign.net/publickeys/casub.crt	Si			IA5String	URL acceso a certificado de la CA (NO HTTPS) uniformResourceIdentifier	
2.9. Qualified Certificate Statements		Sí	No			OID 1.3.6.1.5.5.7.1.3	
2.9.1. qCCompliance	id-etsi-qcs-QcCompliance	Sí				OID 0.4.0.1862.1.1 Indicación de certificado cualificado	
2.9.2. QcEuRetentionPeriod	"15"	Sí				OID 0.4.0.1862.1.3 Plazo de retención de registros	
2.9.3. QcSSCD	id-etsi-qcs-QcSSCD	Sí				OID 0.4.0.1862.1.4 Dispositivo cualificado de creación de firma	
2.9.4. QcPDS	{https://www.vincasign.net/policy/es/PDS-EPS-ALTO/pds-eps-alto-es.pdf,es},{https://www.vincasign.net/policy/en/PDS-EPS-ALTO/pds-eps-alto-en.pdf,en}	Sí				OID 0.4.0.1862.1.5 **(SÍ HTTPS)** URLs de acceso al texto divulgativo en inglés (obligatorio) y en castellano	
2.9.5. QcType	id-etsi-qct-esign	Sí				OID 0.4.0.1862.1.6.1 Certificado de firma electrónica conforme al Reglamento (UE) Nº 910/2014	
2.9.6. qcStatement-2						OID 1.3.6.1.5.5.7.11.2 (RFC 3739)	
2.9.6.1. SemanticsInformation							
2.9.6.1.1. semanticsIdNatural	0.4.0.194121.1.1					Semántica de persona fisica conforme a EN 319 412-1, en serial number	
2.10. Basic Constraints		Sí	Sí			OID 2.5.29.19	
2.10.1. cA	FALSO	Sí			Boolean		

16. Cert de Empleado Público con seudónimo nivel MEDIO

Campo	Gestión CENTRALIZADA	Oblig.	Crít.	Longitud máxima	Codif	Observaciones OID 1.3.6.1.4.1.47155.1.4.12
Empleado Público Seudónimo MEDIO	Identificación y Firma					
1. Basic estructure						
1.1. Version	"2"	Sí		1	Integer	El literal "2" corresponde a la versión 3.
1.2. Serial Number	Establecido automáticamente por la CA. Número identificativo único del certificado.	Sí		20 octetos	Integer	No puede ser un número negativo ni 0.
1.3. Signature Algorithm		Sí				
1.3.1. Algorithm	SHA-256 with RSA Signature	Sí			OID	1.2.840.113549.1.1.11
1.3.2. Parameters	No aplicable	No				
1.4. Issuer		Sí				
1.4.1. Country Name (C)	"ES"	Sí		2 caracteres	PrintableString	OID 2.5.4.6
1.4.2. Organization Name (O)	"VINTEGRIS SL"	Sí		64 caracteres	UTF8String	OID 2.5.4.10
1.4.3. organizationalUnitName (OU)	"vinCAsign"	Sí				OID 2.5.4.11
1.4.4. Locality Name (L)	"HOSPITALET DE LLOBREGAT"	Sí		128 caracteres	UTF8String	OID 2.5.4.7
1.4.5. Organization Identifier	"VATES-B62913926"	Sí		Ilimitado	UTF8String	OID 2.5.4.97
1.4.6. Common Name (CN)	"vinCAsign nebulaSUITE2 Authority"	Sí		64 caracteres	UTF8String	OID 2.5.4.3
1.4.7. stateOrProvinceName	"BARCELONA"	Sí			UTF8String	OID 2.5.4.8
1.5. Validity		Sí				3 YEAR
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				
1.6.1. Country Name	"ES"	Sí		2 caracteres	PrintableString	OID 2.5.4.6
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		40 caracteres	UTF8String	OID 2.5.4.10
1.6.3. Organizational Unit (OU)	"CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO CON SEUDONIMO"	Sí			UTF8String	OID 2.5.4.11
1.6.4. Organizational Unit (OU)	Unidad, dentro de la Administración, en la que está incluida el suscriptor del certificado	No			UTF8String	OID 2.5.4.11
1.6.5. Organizational Unit (OU)	Código DIR3 de la unidad	No			UTF8String	OID 2.5.4.11
1.6.6. pseudonym	NIP 111111111	Sí				OID 2.5.4.65 Obligatorio según ETSI EN 319 412-2

1.6.7. Organization Identifier	NIF de la AAPP a la que está vinculado el empleado público titular del certificado, en formato ETSI EN 319412-1 (Ejemplo: "VATES-Q0000000J)			64 caracteres	PrintableString	OID 2.5.4.97
1.6.8. 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			64 caracteres	UTF8String	OID 2.5.4.12
1.6.9. Common Name	CARGO/SEUDONIMO – NIP 11111111 – NOMBRE ORGANISMO	Sí				OID 2.5.4.3 Si existe TITLE = CARGO Sinó indicar "SEUDONIMO"
1.7. Subject Public Key Info	Clave pública del firmante, codificada en RSA encryption (2048 bits)	Sí				
1.7.1. AlgorithmIdentifier						
1.7.1.1. Algorithm	RSA encryption	Sí			OID	OID 1.2.840.113549.1.1.1
1.7.1.2. Parameters	No aplicable	No				
1.7.2. SubjectPublicKey	Clave pública del firmante	Sí			Bit String	
2. Extensions						
2.1. Authority Key Identifier	Identificador de la clave del emisor	Sí	No			OID 2.5.29.35 (Marcado como NO crítico según EN 319412-2)
2.1.1. KeyIdentifier		Sí			Octet string	Derivado de la clave pública
2.1.2. AuthorityCertIssuer	Nombre de la CA a la que corresponde la clave identificada en keyIdentifier					(String UTF8) Size 12
2.1.3. AuthorityCertSerialNumber	Número de serie del certificado de CA					
2.2. Subject Key Identifier	Identificador de la clave del firmante	Sí	No			OID 2.5.29.14 (Marcado como NO crítico según EN 319412-2)
2.2.1. KeyIdentifier		Sí			Octet string	Derivado de la clave pública
2.3. Key Usage		Sí	Sí		Bit String	OID 2.5.29.15
2.3.1. Digital Signature	**Seleccionado "1"**	Sí				Bit para autenticación
2.3.2. Content commintment	**Seleccionado "1"**	Sí				Bit para firma
2.3.3. Key Encipherment	**Seleccionado "1"**	Sí				
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"					
2.3.8. Encipher Only	No seleccionado. "0"					
2.3.9. Decipher Only	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 Information		Sí				
2.4.1.1. Policy Identifier	**1.3.6.1.4.1.47155.1.4.12**	Sí			OID	Identificador de la política de Logalty
2.4.1.2. Policy Qualifiers		Sí				
2.4.1.1.1 CPS URI	https://policy.vincasign.net				IA5String	URL de la DPC (opcional por CAB FORUM)
2.4.1.1.2. User Notice/Explicit text	"CERTIFICADO CUALIFICADO DE EMPLEADO PUBLICO CON SEUDONIMO DE NIVEL MEDIO. Ver https://policy.vincasign.net "	Sí		200 caracteres	UTF8String y NFC	Texto indicativo
2.4.2. Policy Information		Sí				
2.4.2.1. Policy Identifier	**0.4.0.194112.1.0**	Sí			OID	QCP-n-qscd. Identificador de la política de certificado cualificado de persona física sin uso de dispositivo seguro
2.4.2. Policy Information		Sí				
2.4.2.1. Policy Identifier	**2.16.724.1.3.5.4.2**	Sí			OID	OID asociado a certificado de empleado público con seudónimo
2.5. Subject Alternative Names		Sí	No			OID 2.5.29.17 (Marcado como NO crítico según EN 319412-2)
2.5.1. rfc822Name	Correo electrónico de contacto				rfc822Name	
2.5.2. Directory Name	Identidad administrativa	Sí				
2.5.2.1. Tipo de certificado	"CERTIFICADO CUALIFICADO DE EMPLEADO PUBLICO CON SEUDONIMO, DE NIVEL MEDIO"	Sí				OID ALTO: 2.16.724.1.3.5.4.2.1
2.5.2.2. Nombre de la entidad subscriptora	Entidad propietaria del certificado	Sí				OID ALTO: 2.16.724.1.3.5.4.2.2
2.5.2.3. NIF de la entidad subscriptora	Número de identificación fiscal de la entidad propietaria del certificado	Sí				OID ALTO: 2.16.724.1.3.5.4.2.3
2.5.2.4. Correo electrónico	Correo electrónico de contacto					OID ALTO: 2.16.724.1.3.5.4.2.9
2.5.2.5. Unidad organizativa	Unidad, dentro de la Administración, en la que está incluido el suscriptor del certificado					OID ALTO: 2.16.724.1.3.5.4.2.10
2.5.2.6. Puesto o cargo	Puesto desempeñado por el suscriptor del certificado dentro de la Administración					OID ALTO: 2.16.724.1.3.5.4.2.11
2.5.2.7. Seudónimo	NIP 1111					OID ALTO: 2.16.724.1.3.5.4.2.12
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			OID	
2.6.2. Email protection	Presente (1.3.6.1.5.5.7.3.4)	Sí			OID	Sólo se activa si se incluye el correo electrónico del firmante

2.7. cRLDistributionPoint		No	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			IA5String	uniformResourceIdentifier **(NO HTTPS)**
2.7.2. distributionPoint	http://crl2.vincasing.net/canebula2.crl	Sí			IA5String	uniformResourceIdentifier **(NO HTTPS)**
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. Access Description		Sí				
2.8.1.1. Acces Method	id-ad-ocsp	Sí			OID	OID 1.3.6.1.5.5.7.48.1
2.8.1.2. Acces Location	http://ocsp.vincasign.net	Sí			IA5String	URL de acceso al OCSP **(NO HTTPS)** uniformResourceIdentifier
2.8.2. Access Description		Sí				
2.8.2.1. Acces Method	id-ad-calssuers	Sí			OID	OID 1.3.6.1.5.5.7.48.2
2.8.2.1. Acces Location	http://www.vincasign.net/publickeys/casub.crt	Si			IA5String	URL acceso a certificado de la CA (NO HTTPS) uniformResourceIdentifier
2.9. Qualified Certificate Statements		Sí	No			OID 1.3.6.1.5.5.7.1.3
2.9.1. qCCompliance	id-etsi-qcs-QcCompliance	Sí				OID 0.4.0.1862.1.1 Indicación de certificado cualificado
2.9.2. QcEuRetentionPeriod	"15"	Sí				OID 0.4.0.1862.1.3 Plazo de retención de registros
2.9.4. QcPDS	{https://www.vincasign.net/policy/es/PDS-EPS-MEDIO/pds-eps-medio-es.pdf,es},{https://www.vincasign.net/policy/en/PDS-EPS-MEDIO/pds-eps-medio-en.pdf,en}	Sí				OID 0.4.0.1862.1.5 **(SÍ HTTPS)** URLs de acceso al texto divulgativo en inglés (obligatorio) y en castellano
2.9.5. QcType	id-etsi-qct-esign	Sí				OID 0.4.0.1862.1.6.1 Certificado de firma electrónica conforme al Reglamento (UE) Nº 910/2014
2.9.6. qcStatement-2						OID 1.3.6.1.5.5.7.11.2 (RFC 3739)
2.9.6.1. SemanticsInformation						
2.9.6.1.1. semanticsIdNatural	0.4.0.194121.1.1					Semántica de persona fisica conforme a EN 319 412-1, en serial number
2.10. Basic Constraints		Sí	Sí			OID 2.5.29.19
2.10.1. cA	FALSO	Sí			Boolean	

17. Cert de Sello de AAPP nivel ALTO

Campo	Gestión CENTRALIZADA	Oblig.	Crít.	Longitud máxima	Codif	Observaciones OID 1.3.6.1.4.1.47155.1.5.1
SELLO de AAPP · ALTO	Identificación y Firma					
1. Basic estructure						
1.1. Version	"2"	Sí		1	Integer	El literal "2" corresponde a la versión 3.
1.2. Serial Number	Establecido automáticamente por la CA. Número identificativo único del certificado.	Sí		20 octetos	Integer	No puede ser un número negativo ni 0.
1.3. Signature Algorithm		Sí				
1.3.1. Algorithm	SHA-256 with RSA Signature	Sí			OID	1.2.840.113549.1.1.11
1.3.2. Parameters	No aplicable	No				
1.4. Issuer		Sí				
1.4.1. Country Name (C)	"ES"	Sí		2 caracteres	PrintableString	OID 2.5.4.6
1.4.2. Organization Name (O)	"VINTEGRIS SL"	Sí		64 caracteres	UTF8String	OID 2.5.4.10
1.4.3. organizationalUnitName (OU)	"vinCAsign"	Sí				OID 2.5.4.11
1.4.4. Locality Name (L)	"HOSPITALET DE LLOBREGAT"	Sí		128 caracteres	UTF8String	OID 2.5.4.7
1.4.5. Organization Identifier	"VATES-B62913926"	Sí		Ilimitado	UTF8String	OID 2.5.4.97
1.4.6. Common Name (CN)	"vinCAsign nebulaSUITE2 Authority"	Sí		64 caracteres	UTF8String	OID 2.5.4.3
1.4.7. stateOrProvinceName	"BARCELONA"	Sí			UTF8String	OID 2.5.4.8
1.5. Validity		Sí				3 YEAR
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				
1.6.1. Country Name	"ES"	Sí		2 caracteres	PrintableString	OID 2.5.4.6
1.6.2. Organization (O)	Denominación (nombre "oficial") de la Administración, organismo o entidad de derecho público suscriptora del certificado.	Sí		40 caracteres	UTF8String	OID 2.5.4.10
1.6.3. Organizational Unit (OU)	"SELLO ELECTRONICO"	Sí			UTF8String	OID 2.5.4.11
1.6.4. Organizational Unit (OU)	Código DIR3 de la unidad de la AAPP (p. ej: E04976701)				UTF8String	OID 2.5.4.11
1.6.5. Organization Identifier	NIF de la AAPP a la que está vinculado el sello, en formato ETSI EN 319412-1 (Ejemplo: "VATES-Q0000000J)	Sí		64 caracteres	PrintableString	OID 2.5.4.97
1.6.6. Serial Number	NIF de la entidad	Sí			PrintableString	OID 2.5.4.5
1.6.7. Surname	Apellidos de la persona física (como consta en el DNI/NIE)					OID 2.5.4.4

1.6.8. Given Name	Nombre de la persona física (como consta en el DNI/NIE)					OID 2.5.4.42
1.6.9. Common Name	Nombre descriptivo del sistema automático. Asegurando que dicho nombre tenga sentido y no dé lugar a ambigüedades.	Sí				OID 2.5.4.3
1.6.10. emailAddress	Correo electrónico del firmante	Sí			IA5String	
1.7. Subject Public Key Info	Clave pública del firmante, codificada en RSA encryption (2048 bits)	Sí				
1.7.1. AlgorithmIdentifier						
1.7.1.1. Algorithm	RSA encryption	Sí			OID	OID 1.2.840.113549.1.1.1
1.7.1.2. Parameters	No aplicable	No				
1.7.2. SubjectPublicKey	Clave pública del firmante	Sí			Bit String	
2. Extensions						
2.1. Authority Key Identifier	Identificador de la clave del emisor	Sí	No			OID 2.5.29.35 (Marcado como NO crítico según EN 319412-2)
2.1.1. KeyIdentifier		Sí			Octet string	Derivado de la clave pública
2.1.2. AuthorityCertIssuer	Nombre de la CA a la que corresponde la clave identificada en keyIdentifier					(String UTF8) Size 12
2.1.3. AuthorityCertSerialNumber	Número de serie del certificado de CA					
2.2. Subject Key Identifier	Identificador de la clave del firmante	Sí	No			OID 2.5.29.14 (Marcado como NO crítico según EN 319412-2)
2.2.1. KeyIdentifier		Sí			Octet string	Derivado de la clave pública
2.3. Key Usage		Sí	Sí		Bit String	OID 2.5.29.15
2.3.1. Digital Signature	**Seleccionado "1"**	Sí				Bit para autenticación
2.3.2. Content commintment	**Seleccionado "1"**	Sí				Bit para firma
2.3.3. Key Encipherment	No seleccionado. "0"					
2.3.4. Data Encipherment	No seleccionado. "0"					
2.3.5. Key Agreement	No seleccionado. "0"					
2.3.6. Key Certificate Signature	No seleccionado. "0"					
2.3.7. CRL Signature	No seleccionado. "0"					
2.3.8. Encipher Only	No seleccionado. "0"					
2.3.9. Decipher Only	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 Information		Sí				
2.4.1.1. Policy Identifier	**1.3.6.1.4.1.47155.1.5.1**	Sí			OID	Identificador de la política de Logalty
2.4.1.2. Policy Qualifiers		Sí				

	2.4.1.1.1 CPS URI	https://policy.vincasign.net				IA5String	URL de la DPC (opcional por CAB FORUM)
	2.4.1.1.2. User Notice/Explicit text	"Certificado cualificado de sello electrónico para la Administración Pública, Órgano o Entidad de Derecho Público, nivel alto. Ver https://policy.vincasign.net "	Sí		200 caracteres	UTF8String y NFC	Texto indicativo
	2.4.2. Policy Information		Sí				
	2.4.2.1. Policy Identifier	**0.4.0.194112.1.3**	Sí			OID	QCP-l-qscd. Identificador de la política de certificado cualificado de sello de persona jurídica con dispositivo seguro
	2.4.2. Policy Information		Sí				
	2.4.2.1. Policy Identifier	**2.16.724.1.3.5.6.1**	Sí			OID	OID asociado a certificado de sello electrónico de órgano para AAPP
	2.5. Subject Alternative Names		Sí	No			OID 2.5.29.17 (Marcado como NO crítico según EN 319412-2)
	2.5.1. rfc822Name	Correo electrónico de la persona física	Sí			rfc822Name	
	2.5.2. Directory Name	Identidad administrativa	Sí				
	2.5.2.1. Tipo de certificado	"SELLO ELECTRONICO DE NIVEL ALTO"	Sí				OID ALTO: 2.16.724.1.3.5.6.1.1
	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
	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
	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
	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
	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
	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
	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
	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
	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			OID	
	2.6.2. Email protection	Presente (1.3.6.1.5.5.7.3.4)	Sí			OID	Sólo se activa si se incluye el correo electrónico del firmante
	2.7. cRLDistributionPoint		No	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			IA5String	uniformResourceIdentifier **(NO HTTPS)**

	2.7.2. distributionPoint	http://crl2.vincasing.net/canebula2.crl	Sí			IA5String	uniformResourceIdentifier **(NO HTTPS)**
	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. Access Description		Sí				
	2.8.1.1. Acces Method	id-ad-ocsp	Sí			OID	OID 1.3.6.1.5.5.7.48.1
	2.8.1.2. Acces Location	http://ocsp.vincasign.net	Sí			IA5String	URL de acceso al OCSP **(NO HTTPS)** uniformResourceIdentifier
	2.8.2. Access Description		Sí				
	2.8.2.1. Acces Method	id-ad-calssuers	Sí			OID	OID 1.3.6.1.5.5.7.48.2
	2.8.2.1. Acces Location	http://www.vincasign.net/publickeys/casub.crt	Si			IA5String	URL acceso a certificado de la CA (NO HTTPS) uniformResourceIdentifier
	2.9. Qualified Certificate Statements		Sí	No			OID 1.3.6.1.5.5.7.1.3
	2.9.1. qCCompliance	id-etsi-qcs-QcCompliance	Sí				OID 0.4.0.1862.1.1 Indicación de certificado cualificado
	2.9.2. QcEuRetentionPeriod	"15"	Sí				OID 0.4.0.1862.1.3 Plazo de retención de registros
	2.9.3. QcSSCD	id-etsi-qcs-QcSSCD	Sí				OID 0.4.0.1862.1.4 Dispositivo cualificado de creación de firma
	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}	Sí				OID 0.4.0.1862.1.5 **(SÍ HTTPS)** URLs de acceso al texto divulgativo en inglés (obligatorio) y en castellano
	2.9.5. QcType	id-etsi-qct-eseal	Sí				OID 0.4.0.1862.1.6.2 Certificado de sello-e conforme al Reglamento (UE) Nº 910/2014
	2.9.6. qcStatement-2						OID 1.3.6.1.5.5.7.11.2 (RFC 3739)
	2.9.6.1. SemanticsInformation						
	2.9.6.1.1. semanticsIdNatural	0.4.0.194121.1.2					Semántica de persona jurídica conforme a EN 319 412-1, en serial number
	2.10. Basic Constraints		Sí	Sí			OID 2.5.29.19
	2.10.1. cA	FALSO	Sí			Boolean	

18. Cert de Sello de AAPP nivel MEDIO

Campo SELLO de AAPP · MEDIO	Gestión CENTRALIZADA Identificación y Firma	Oblig.	Crít.	Longitud máxima	Codif	Observaciones OID 1.3.6.1.4.1.47155.1.5.2
1. Basic estructure						
1.1. Version	"2"	Sí		1	Integer	El literal "2" corresponde a la versión 3.
1.2. Serial Number	Establecido automáticamente por la CA. Número identificativo único del certificado.	Sí		20 octetos	Integer	No puede ser un número negativo ni 0.
1.3. Signature Algorithm		Sí				
1.3.1. Algorithm	SHA-256 with RSA Signature	Sí			OID	1.2.840.113549.1.1.11
1.3.2. Parameters	No aplicable	No				
1.4. Issuer		Sí				
1.4.1. Country Name (C)	"ES"	Sí		2 caracteres	PrintableString	OID 2.5.4.6
1.4.2. Organization Name (O)	"VINTEGRIS SL"	Sí		64 caracteres	UTF8String	OID 2.5.4.10
1.4.3. organizationalUnitName (OU)	"vinCAsign"	Sí				OID 2.5.4.11
1.4.4. Locality Name (L)	"HOSPITALET DE LLOBREGAT"	Sí		128 caracteres	UTF8String	OID 2.5.4.7
1.4.5. Organization Identifier	"VATES-B62913926"	Sí		Ilimitado	UTF8String	OID 2.5.4.97
1.4.6. Common Name (CN)	"vinCAsign nebulaSUITE2 Authority"	Sí		64 caracteres	UTF8String	OID 2.5.4.3
1.4.7. stateOrProvinceName	"BARCELONA"	Sí			UTF8String	OID 2.5.4.8
1.5. Validity		Sí				3 YEAR
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				
1.6.1. Country Name	"ES"	Sí		2 caracteres	PrintableString	OID 2.5.4.6
1.6.2. Organization (O)	Denominación (nombre "oficial") de la Administración, organismo o entidad de derecho público suscriptora del certificado.	Sí		40 caracteres	UTF8String	OID 2.5.4.10
1.6.3. Organizational Unit (OU)	"SELLO ELECTRONICO"	Sí			UTF8String	OID 2.5.4.11
1.6.4. Organizational Unit (OU)	Código DIR3 de la unidad de la AAPP (p. ej: E04976701)				UTF8String	OID 2.5.4.11
1.6.5. Organization Identifier	NIF de la AAPP a la que está vinculado el sello, en formato ETSI EN 319412-1 (Ejemplo: "VATES-Q0000000J)	Sí		64 caracteres	PrintableString	OID 2.5.4.97
1.6.6. Serial Number	NIF de la entidad	Sí			PrintableString	OID 2.5.4.5
1.6.7. Surname	Apellidos de la persona física (como consta en el DNI/NIE)					OID 2.5.4.4

1.6.8. Given Name	Nombre de la persona física (como consta en el DNI/NIE)					OID 2.5.4.42
1.6.9. Common Name	Nombre descriptivo del sistema automático. Asegurando que dicho nombre tenga sentido y no dé lugar a ambigüedades.	Sí				OID 2.5.4.3
1.6.10. emailAddress	Correo electrónico del firmante	Sí			IA5String	
1.7. Subject Public Key Info	Clave pública del firmante, codificada en RSA encryption (2048 bits)	Sí				
1.7.1. AlgorithmIdentifier						
1.7.1.1. Algorithm	RSA encryption	Sí			OID	OID 1.2.840.113549.1.1.1
1.7.1.2. Parameters	No aplicable	No				
1.7.2. SubjectPublicKey	Clave pública del firmante	Sí			Bit String	
2. Extensions						
2.1. Authority Key Identifier	Identificador de la clave del emisor	Sí	No			OID 2.5.29.35 (Marcado como NO crítico según EN 319412-2)
2.1.1. KeyIdentifier		Sí			Octet string	Derivado de la clave pública
2.1.2. AuthorityCertIssuer	Nombre de la CA a la que corresponde la clave identificada en keyIdentifier					(String UTF8) Size 12
2.1.3. AuthorityCertSerialNumber	Número de serie del certificado de CA					
2.2. Subject Key Identifier	Identificador de la clave del firmante	Sí	No			OID 2.5.29.14 (Marcado como NO crítico según EN 319412-2)
2.2.1. KeyIdentifier		Sí			Octet string	Derivado de la clave pública
2.3. Key Usage		Sí	Sí		Bit String	OID 2.5.29.15
2.3.1. Digital Signature	**Seleccionado "1"**	Sí				Bit para autenticación
2.3.2. Content commintment	**Seleccionado "1"**	Sí				Bit para firma
2.3.3. Key Encipherment	**Seleccionado "1"**	Sí				
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"					
2.3.8. Encipher Only	No seleccionado. "0"					
2.3.9. Decipher Only	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 Information		Sí				
2.4.1.1. Policy Identifier	**1.3.6.1.4.1.47155.1.5.2**	Sí			OID	Identificador de la política de Logalty
2.4.1.2. Policy Qualifiers		Sí				

	2.4.1.1.1 CPS URI	https://policy.vincasign.net				IA5String	URL de la DPC (opcional por CAB FORUM)
	2.4.1.1.2. User Notice/Explicit text	"Certificado cualificado de sello electrónico para la Administración Pública, Órgano o Entidad de Derecho Público, nivel medio. Ver https://policy.vincasign.net "	Sí		200 caracteres	UTF8String y NFC	Texto indicativo
	2.4.2. Policy Information		Sí				
	2.4.2.1. Policy Identifier	**0.4.0.194112.1.1**	Sí			OID	QCP-l. Identificador de la política de certificado cualificado de sello de persona jurídica sin uso de dispositivo seguro
	2.4.2. Policy Information		Sí				
	2.4.2.1. Policy Identifier	**2.16.724.1.3.5.6.2**	Sí			OID	OID asociado a certificado de sello electrónico de órgano para AAPP
	2.5. Subject Alternative Names		Sí	No			OID 2.5.29.17 (Marcado como NO crítico según EN 319412-2)
	2.5.1. rfc822Name	Correo electrónico de la persona física	Sí			rfc822Name	
	2.5.2. Directory Name	Identidad administrativa	Sí				
	2.5.2.1. Tipo de certificado	"SELLO ELECTRONICO DE NIVEL MEDIO"	Sí				OID ALTO: 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: 2.16.724.1.3.5.6.2.2
	2.5.2.3. NIF de la entidad subscriptora	Número de identificación fiscal de la entidad propietaria del certificado	Sí				OID ALTO: 2.16.724.1.3.5.6.2.3
	2.5.2.4. DNI/NIE del Responsable	DNI o NIE del responsable del sello					OID ALTO: 2.16.724.1.3.5.6.2.4
	2.5.2.5 Denominación de sistema o componente	Breve descripción del componente que posee el certificado de sello					OID ALTO: 2.16.724.1.3.5.6.2.5
	2.5.2.6. Nombre de pila (titular del órgano)	Nombre de pila del responsable del certificado de sello					OID ALTO: 2.16.724.1.3.5.6.2.6
	2.5.2.7. Primer apellido (titular del órgano)	Primer apellido del responsable del certificado de sello					OID ALTO: 2.16.724.1.3.5.6.2.7
	2.5.2.8 Segundo apellido (titular del órgano)	Segundo apellido del responsable del certificado de sello					OID ALTO: 2.16.724.1.3.5.6.2.8
	2.5.2.9. Correo electrónico	Correo electrónico de la persona responsable del certificado de sello					OID ALTO: 2.16.724.1.3.5.6.2.9
	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)	Sí			OID	
	2.6.2. Email protection	Presente (1.3.6.1.5.5.7.3.4)	Sí			OID	Sólo se activa si se incluye el correo electrónico del firmante
	2.7. cRLDistributionPoint		No	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			IA5String	uniformResourceIdentifier **(NO HTTPS)**

	2.7.2. distributionPoint	http://crl2.vincasing.net/canebula2.crl	Sí			IA5String	uniformResourceIdentifier **(NO HTTPS)**
	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. Access Description		Sí				
	2.8.1.1. Acces Method	id-ad-ocsp	Sí			OID	OID 1.3.6.1.5.5.7.48.1
	2.8.1.2. Acces Location	http://ocsp.vincasign.net	Sí			IA5String	URL de acceso al OCSP **(NO HTTPS)** uniformResourceIdentifier
	2.8.2. Access Description		Sí				
	2.8.2.1. Acces Method	id-ad-calssuers	Sí			OID	OID 1.3.6.1.5.5.7.48.2
	2.8.2.1. Acces Location	http://www.vincasign.net/publickeys/casub.crt	Si			IA5String	URL acceso a certificado de la CA (NO HTTPS) uniformResourceIdentifier
	2.9. Qualified Certificate Statements		Sí	No			OID 1.3.6.1.5.5.7.1.3
	2.9.1. qCCompliance	id-etsi-qcs-QcCompliance	Sí				OID 0.4.0.1862.1.1 Indicación de certificado cualificado
	2.9.2. QcEuRetentionPeriod	"15"	Sí				OID 0.4.0.1862.1.3 Plazo de retención de registros
	2.9.4. QcPDS	{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 **(SÍ HTTPS)** URLs de acceso al texto divulgativo en inglés (obligatorio) y en castellano
	2.9.5. QcType	id-etsi-qct-eseal	Sí				OID 0.4.0.1862.1.6.2 Certificado de sello-e conforme al Reglamento (UE) Nº 910/2014
	2.9.6. qcStatement-2						OID 1.3.6.1.5.5.7.11.2 (RFC 3739)
	2.9.6.1. SemanticsInformation						
	2.9.6.1.1. semanticsIdNatural	0.4.0.194121.1.2					Semántica de persona jurídica conforme a EN 319 412-1, en serial number
	2.10. Basic Constraints		Sí	Sí			OID 2.5.29.19
	2.10.1. cA	FALSO	Sí			Boolean	

19. Cert de Sello de Empresa en DCCF

Campo	Gestión CENTRALIZADA	Oblig.	Crít.	Longitud máxima	Codif	Observaciones OID 1.3.6.1.4.1.47155.1.6.1
SELLO de Empresa en DCCF	Identificación y Firma					
1. Basic estructure						
1.1. Version	"2"	Sí		1	Integer	El literal "2" corresponde a la versión 3.
1.2. Serial Number	Establecido automáticamente por la CA. Número identificativo único del certificado.	Sí		20 octetos	Integer	No puede ser un número negativo ni 0.
1.3. Signature Algorithm		Sí				
1.3.1. Algorithm	SHA-256 with RSA Signature	Sí			OID	1.2.840.113549.1.1.11
1.3.2. Parameters	No aplicable	No				
1.4. Issuer		Sí				
1.4.1. Country Name (C)	"ES"	Sí		2 caracteres	PrintableString	OID 2.5.4.6
1.4.2. Organization Name (O)	"VINTEGRIS SL"	Sí		64 caracteres	UTF8String	OID 2.5.4.10
1.4.3. organizationalUnitName (OU)	"vinCAsign"	Sí				OID 2.5.4.11
1.4.4. Locality Name (L)	"HOSPITALET DE LLOBREGAT"	Sí		128 caracteres	UTF8String	OID 2.5.4.7
1.4.5. Organization Identifier	"VATES-B62913926"	Sí		Ilimitado	UTF8String	OID 2.5.4.97
1.4.6. Common Name (CN)	"vinCAsign nebulaSUITE2 Authority"	Sí		64 caracteres	UTF8String	OID 2.5.4.3
1.4.7. stateOrProvinceName	"BARCELONA"	Sí			UTF8String	OID 2.5.4.8
1.5. Validity		Sí				3 YEAR
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				
1.6.1. Country Name	"ES"	Sí		2 caracteres	PrintableString	OID 2.5.4.6
1.6.2. Organization (O)	Denominación (nombre "oficial" de la persona jurídica) del creador del sello (Empresa, Organización, Entidad)	Sí		40 caracteres	UTF8String	OID 2.5.4.10
1.6.3. Organizational Unit (OU)	"SELLO ELECTRONICO"	Sí			UTF8String	OID 2.5.4.11
1.6.5. Organization Identifier	NIF de la persona jurídica a la que está vinculado este sello, en formato ETSI EN 319412-1 (Ejemplo: "VATES-Q0000000J)	Sí		64 caracteres	PrintableString	OID 2.5.4.97
1.6.6. Serial Number	NIF de la PERSONA JURÍDICA	Sí			PrintableString	OID 2.5.4.5
1.6.9. Common Name	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				

1.7.1. AlgorithmIdentifier						
1.7.1.1. Algorithm	RSA encryption	Sí			OID	OID 1.2.840.113549.1.1.1
1.7.1.2. Parameters	No aplicable	No				
1.7.2. SubjectPublicKey	Clave pública del firmante	Sí			Bit String	
2. Extensions						
2.1. Authority Key Identifier	Identificador de la clave del emisor	Sí	No			OID 2.5.29.35 (Marcado como NO crítico según EN 319412-2)
2.1.1. KeyIdentifier		Sí			Octet string	Derivado de la clave pública
2.1.2. AuthorityCertIssuer	Nombre de la CA a la que corresponde la clave identificada en keyIdentifier					(String UTF8) Size 12
2.1.3. AuthorityCertSerialNumber	Número de serie del certificado de CA					
2.2. Subject Key Identifier	Identificador de la clave del firmante	Sí	No			OID 2.5.29.14 (Marcado como NO crítico según EN 319412-2)
2.2.1. KeyIdentifier		Sí			Octet string	Derivado de la clave pública
2.3. Key Usage		Sí	Sí		Bit String	OID 2.5.29.15
2.3.1. Digital Signature	**Seleccionado "1"**	Sí				Bit para autenticación
2.3.2. Content commintment	**Seleccionado "1"**	Sí				Bit para firma
2.3.3. Key Encipherment	**Seleccionado "1"**	Sí				
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"					
2.3.8. Encipher Only	No seleccionado. "0"					
2.3.9. Decipher Only	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 Information		Sí				
2.4.1.1. Policy Identifier	**1.3.6.1.4.1.47155.1.6.1**	Sí			OID	Identificador de la política de Logalty
2.4.1.2. Policy Qualifiers		Sí				
2.4.1.1.1 CPS URI	https://policy.vincasign.net				IA5String	URL de la DPC (opcional por CAB FORUM)
2.4.1.1.2. User Notice/Explicit text	"Certificado cualificado de sello electrónico de persona jurídica emitido en HSM-QSCD. Ver https://policy.vincasign.net "	Sí		200 caracteres	UTF8String y NFC	Texto indicativo
2.4.2. Policy Information		Sí				

	2.4.2.1. Policy Identifier	**0.4.0.194112.1.3**	Sí			OID	QCP-l-qscd. Identificador de la política de certificado cualificado de sello de persona jurídica con dispositivo seguro
	2.5. Subject Alternative Names		Sí	No			OID 2.5.29.17 (Marcado como NO crítico según EN 319412-2)
	2.5.1. DirectoryName	Organización a la que pertenece el representante.	Sí		40 caracteres	UTF8String	OID 1.3.6.1.4.1.47155.1.6
		NIF de la persona jurídica de la que es representante el titular del certificado, en formato ETSI EN 319412-1 (Ejemplo: "VATES-Q0000000J)	Sí		64 caracteres	PrintableString	OID 1.3.6.1.4.1.47155.1.7
	2.5.2. rfc822Name	Correo electrónico de la persona física	Sí			rfc822Name	
	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			OID	
	2.6.2. Email protection	Presente (1.3.6.1.5.5.7.3.4)	Sí			OID	Sólo se activa si se incluye el correo electrónico del firmante
	2.7. cRLDistributionPoint		No	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			IA5String	uniformResourceIdentifier **(NO HTTPS)**
	2.7.2. distributionPoint	http://crl2.vincasing.net/canebula2.crl	Sí			IA5String	uniformResourceIdentifier **(NO HTTPS)**
	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. Access Description		Sí				
	2.8.1.1. Acces Method	id-ad-ocsp	Sí			OID	OID 1.3.6.1.5.5.7.48.1
	2.8.1.2. Acces Location	http://ocsp.vincasign.net	Sí			IA5String	URL de acceso al OCSP **(NO HTTPS)** uniformResourceIdentifier
	2.8.2. Access Description		Sí				
	2.8.2.1. Acces Method	id-ad-calssuers	Sí			OID	OID 1.3.6.1.5.5.7.48.2
	2.8.2.1. Acces Location	http://www.vincasign.net/publickeys/casub.crt	Si			IA5String	URL acceso a certificado de la CA (NO HTTPS) uniformResourceIdentifier
	2.9. Qualified Certificate Statements		Sí	No			OID 1.3.6.1.5.5.7.1.3
	2.9.1. qCCompliance	id-etsi-qcs-QcCompliance	Sí				OID 0.4.0.1862.1.1 Indicación de certificado cualificado
	2.9.2. QcEuRetentionPeriod	"15"	Sí				OID 0.4.0.1862.1.3 Plazo de retención de registros
	2.9.3. QcSSCD	id-etsi-qcs-QcSSCD	Sí				OID 0.4.0.1862.1.4 Dispositivo cualificado de creación de firma

	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}	Sí				OID 0.4.0.1862.1.5 **(SÍ HTTPS)** URLs de acceso al texto divulgativo en inglés (obligatorio) y en castellano
	2.9.5. QcType	id-etsi-qct-eseal	Sí				OID 0.4.0.1862.1.6.2 Certificado de sello-e conforme al Reglamento (UE) Nº 910/2014
	2.9.6. qcStatement-2						OID 1.3.6.1.5.5.7.11.2 (RFC 3739)
	2.9.6.1. SemanticsInformation						
	2.9.6.1.1. semanticsIdNatural	0.4.0.194121.1.2					Semántica de persona jurídica conforme a EN 319 412-1, en serial number
	2.10. Basic Constraints		Sí	Sí			OID 2.5.29.19
	2.10.1. cA	FALSO	Sí			Boolean	

20. Cert de Sello de Empresa en SOFT

Campo SELLO de Empresa - SOFT	Gestión CENTRALIZADA Identificación y Firma	Oblig.	Crít.	Longitud máxima	Codif	Observaciones OID 1.3.6.1.4.1.47155.1.6.2
1. Basic estructure						
1.1. Version	"2"	Sí		1	Integer	El literal "2" corresponde a la versión 3.
1.2. Serial Number	Establecido automáticamente por la CA. Número identificativo único del certificado.	Sí		20 octetos	Integer	No puede ser un número negativo ni 0.
1.3. Signature Algorithm		Sí				
1.3.1. Algorithm	SHA-256 with RSA Signature	Sí			OID	1.2.840.113549.1.1.11
1.3.2. Parameters	No aplicable	No				
1.4. Issuer		Sí				
1.4.1. Country Name (C)	"ES"	Sí		2 caracteres	PrintableString	OID 2.5.4.6
1.4.2. Organization Name (O)	"VINTEGRIS SL"	Sí		64 caracteres	UTF8String	OID 2.5.4.10
1.4.3. organizationalUnitName (OU)	"vinCAsign"	Sí				OID 2.5.4.11
1.4.4. Locality Name (L)	"HOSPITALET DE LLOBREGAT"	Sí		128 caracteres	UTF8String	OID 2.5.4.7
1.4.5. Organization Identifier	"VATES-B62913926"	Sí		Ilimitado	UTF8String	OID 2.5.4.97
1.4.6. Common Name (CN)	"vinCAsign nebulaSUITE2 Authority"	Sí		64 caracteres	UTF8String	OID 2.5.4.3
1.4.7. stateOrProvinceName	"BARCELONA"	Sí			UTF8String	OID 2.5.4.8
1.5. Validity		Sí				3 YEAR
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				
1.6.1. Country Name	"ES"	Sí		2 caracteres	PrintableString	OID 2.5.4.6
1.6.2. Organization (O)	Denominación (nombre "oficial" de la persona jurídica) del creador del sello (Empresa, Organización, Entidad)	Sí		40 caracteres	UTF8String	OID 2.5.4.10
1.6.3. Organizational Unit (OU)	"SELLO ELECTRONICO"	Sí			UTF8String	OID 2.5.4.11
1.6.5. Organization Identifier	NIF de la persona jurídica a la que está vinculado este sello, en formato ETSI EN 319412-1 (Ejemplo: "VATES-Q0000000J)	Sí		64 caracteres	PrintableString	OID 2.5.4.97
1.6.6. Serial Number	NIF de la PERSONA JURÍDICA	Sí			PrintableString	OID 2.5.4.5
1.6.9. Common Name	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				

1.7.1. AlgorithmIdentifier						
1.7.1.1. Algorithm	RSA encryption	Sí			OID	OID 1.2.840.113549.1.1.1
1.7.1.2. Parameters	No aplicable	No				
1.7.2. SubjectPublicKey	Clave pública del firmante	Sí			Bit String	
2. Extensions						
2.1. Authority Key Identifier	Identificador de la clave del emisor	Sí	No			OID 2.5.29.35 (Marcado como NO crítico según EN 319412-2)
2.1.1. KeyIdentifier		Sí			Octet string	Derivado de la clave pública
2.1.2. AuthorityCertIssuer	Nombre de la CA a la que corresponde la clave identificada en keyIdentifier					(String UTF8) Size 12
2.1.3. AuthorityCertSerialNumber	Número de serie del certificado de CA					
2.2. Subject Key Identifier	Identificador de la clave del firmante	Sí	No			OID 2.5.29.14 (Marcado como NO crítico según EN 319412-2)
2.2.1. KeyIdentifier		Sí			Octet string	Derivado de la clave pública
2.3. Key Usage		Sí	Sí		Bit String	OID 2.5.29.15
2.3.1. Digital Signature	**Seleccionado "1"**	Sí				Bit para autenticación
2.3.2. Content commintment	**Seleccionado "1"**	Sí				Bit para firma
2.3.3. Key Encipherment	**Seleccionado "1"**	Sí				
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"					
2.3.8. Encipher Only	No seleccionado. "0"					
2.3.9. Decipher Only	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 Information		Sí				
2.4.1.1. Policy Identifier	**1.3.6.1.4.1.47155.1.6.2**	Sí			OID	Identificador de la política de Logalty
2.4.1.2. Policy Qualifiers		Sí				
2.4.1.1.1 CPS URI	https://policy.vincasign.net				IA5String	URL de la DPC (opcional por CAB FORUM)
2.4.1.1.2. User Notice/Explicit text	"Certificado cualificado de sello electrónico de persona jurídica emitido en software. Ver https://policy.vincasign.net "	Sí		200 caracteres	UTF8String y NFC	Texto indicativo
2.4.2. Policy Information		Sí				

	2.4.2.1. Policy Identifier	**0.4.0.194112.1.1**	Sí			OID	QCP-l. Identificador de la política de certificado cualificado de sello de persona jurídica sin uso de dispositivo seguro
	2.5. Subject Alternative Names		Sí	No			OID 2.5.29.17 (Marcado como NO crítico según EN 319412-2)
	2.5.1. DirectoryName	Organización a la que pertenece el representante.	Sí		40 caracteres	UTF8String	OID 1.3.6.1.4.1.47155.1.6
		NIF de la persona jurídica de la que es representante el titular del certificado, en formato ETSI EN 319412-1 (Ejemplo: "VATES-Q0000000J)	Sí		64 caracteres	PrintableString	OID 1.3.6.1.4.1.47155.1.7
	2.5.2. rfc822Name	Correo electrónico de la persona física	Sí			rfc822Name	
	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			OID	
	2.6.2. Email protection	Presente (1.3.6.1.5.5.7.3.4)	Sí			OID	Sólo se activa si se incluye el correo electrónico del firmante
	2.7. cRLDistributionPoint		No	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			IA5String	uniformResourceIdentifier **(NO HTTPS)**
	2.7.2. distributionPoint	http://crl2.vincasing.net/canebula2.crl	Sí			IA5String	uniformResourceIdentifier **(NO HTTPS)**
	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. Access Description		Sí				
	2.8.1.1. Acces Method	id-ad-ocsp	Sí			OID	OID 1.3.6.1.5.5.7.48.1
	2.8.1.2. Acces Location	http://ocsp.vincasign.net	Sí			IA5String	URL de acceso al OCSP **(NO HTTPS)** uniformResourceIdentifier
	2.8.2. Access Description		Sí				
	2.8.2.1. Acces Method	id-ad-caIssuers	Sí			OID	OID 1.3.6.1.5.5.7.48.2
	2.8.2.1. Acces Location	http://www.vincasign.net/publickeys/casub.crt	Si			IA5String	URL acceso a certificado de la CA (NO HTTPS) uniformResourceIdentifier
	2.9. Qualified Certificate Statements		Sí	No			OID 1.3.6.1.5.5.7.1.3
	2.9.1. qCCompliance	id-etsi-qcs-QcCompliance	Sí				OID 0.4.0.1862.1.1 Indicación de certificado cualificado
	2.9.2. QcEuRetentionPeriod	"15"	Sí				OID 0.4.0.1862.1.3 Plazo de retención de registros

	2.9.4. QcPDS	{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 **(SÍ HTTPS)** URLs de acceso al texto divulgativo en inglés (obligatorio) y en castellano
	2.9.5. QcType	id-etsi-qct-eseal	Sí				OID 0.4.0.1862.1.6.2 Certificado de sello-e conforme al Reglamento (UE) Nº 910/2014
	2.9.6. qcStatement-2						OID 1.3.6.1.5.5.7.11.2 (RFC 3739)
	2.9.6.1. SemanticsInformation						
	2.9.6.1.1. semanticsIdNatural	0.4.0.194121.1.2					Semántica de persona jurídica conforme a EN 319 412-1, en serial number
	2.10. Basic Constraints		Sí	Sí			OID 2.5.29.19
	2.10.1. cA	FALSO	Sí			Boolean	

21. Cert Efímero de Sello de Empresa en DCCF

Campo EFÍMERO de SELLO de Empresa en DCCF	Gestión CENTRALIZADA Identificación y Firma	Oblig.	Crít.	Longitud máxima	Codif	Observaciones OID 1.3.6.1.4.1.47155.1.6.51
1. Basic estructure						
1.1. Version	"2"	Sí		1	Integer	El literal "2" corresponde a la versión 3.
1.2. Serial Number	Establecido automáticamente por la CA. Número identificativo único del certificado.	Sí		20 octetos	Integer	No puede ser un número negativo ni 0.
1.3. Signature Algorithm		Sí				
1.3.1. Algorithm	SHA-256 with RSA Signature	Sí			OID	1.2.840.113549.1.1.11
1.3.2. Parameters	No aplicable	No				
1.4. Issuer		Sí				
1.4.1. Country Name (C)	"ES"	Sí		2 caracteres	PrintableString	OID 2.5.4.6
1.4.2. Organization Name (O)	"VINTEGRIS SL"	Sí		64 caracteres	UTF8String	OID 2.5.4.10
1.4.3. organizationalUnitName (OU)	"vinCAsign"	Sí				OID 2.5.4.11
1.4.4. Locality Name (L)	"HOSPITALET DE LLOBREGAT"	Sí		128 caracteres	UTF8String	OID 2.5.4.7
1.4.5. Organization Identifier	"VATES-B62913926"	Sí		Ilimitado	UTF8String	OID 2.5.4.97
1.4.6. Common Name (CN)	"vinCAsign nebulaSUITE2 Authority"	Sí		64 caracteres	UTF8String	OID 2.5.4.3
1.4.7. stateOrProvinceName	"BARCELONA"	Sí			UTF8String	OID 2.5.4.8
1.5. Validity	MENOR DE 1 HORA	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				
1.6.1. Country Name	"ES"	Sí		2 caracteres	PrintableString	OID 2.5.4.6
1.6.2. Organization (O)	Denominación (nombre "oficial" de la persona jurídica) del creador del sello (Empresa, Organización, Entidad)	Sí		40 caracteres	UTF8String	OID 2.5.4.10
1.6.3. Organizational Unit (OU)	"SELLO ELECTRONICO"	Sí			UTF8String	OID 2.5.4.11
1.6.5. Organization Identifier	NIF de la persona jurídica a la que está vinculado este sello, en formato ETSI EN 319412-1 (Ejemplo: "VATES-Q0000000J)	Sí		64 caracteres	PrintableString	OID 2.5.4.97
1.6.6. Serial Number	NIF de la PERSONA JURÍDICA	Sí			PrintableString	OID 2.5.4.5
1.6.9. Common Name	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				

1.7.1. AlgorithmIdentifier						
1.7.1.1. Algorithm	RSA encryption	Sí			OID	OID 1.2.840.113549.1.1.1
1.7.1.2. Parameters	No aplicable	No				
1.7.2. SubjectPublicKey	Clave pública del firmante	Sí			Bit String	
2. Extensions						
2.1. Authority Key Identifier	Identificador de la clave del emisor	Sí	No			OID 2.5.29.35 (Marcado como NO crítico según EN 319412-2)
2.1.1. KeyIdentifier		Sí			Octet string	Derivado de la clave pública
2.1.2. AuthorityCertIssuer	Nombre de la CA a la que corresponde la clave identificada en keyIdentifier					(String UTF8) Size 12
2.1.3. AuthorityCertSerialNumber	Número de serie del certificado de CA					
2.2. Subject Key Identifier	Identificador de la clave del firmante	Sí	No			OID 2.5.29.14 (Marcado como NO crítico según EN 319412-2)
2.2.1. KeyIdentifier		Sí			Octet string	Derivado de la clave pública
2.3. Key Usage		Sí	Sí		Bit String	OID 2.5.29.15
2.3.1. Digital Signature	**Seleccionado "1"**	Sí				Bit para autenticación
2.3.2. Content commintment	**Seleccionado "1"**	Sí				Bit para firma
2.3.3. Key Encipherment	**Seleccionado "1"**	Sí				
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"					
2.3.8. Encipher Only	No seleccionado. "0"					
2.3.9. Decipher Only	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 Information		Sí				
2.4.1.1. Policy Identifier	**1.3.6.1.4.1.47155.1.6.51**	Sí			OID	Identificador de la política de Logalty
2.4.1.2. Policy Qualifiers		Sí				
2.4.1.1.1 CPS URI	https://policy.vincasign.net				IA5String	URL de la DPC (opcional por CAB FORUM)
2.4.1.1.2. User Notice/Explicit text	"Certificado cualificado y efímero de sello electrónico de persona jurídica emitido en HSM-QSCD. Ver https://policy.vincasign.net "	Sí		200 caracteres	UTF8String y NFC	Texto indicativo
2.4.2. Policy Information		Sí				

	2.4.2.1. Policy Identifier	**0.4.0.194112.1.3**	Sí			OID	QCP-l-qscd. Identificador de la política de certificado cualificado de sello de persona jurídica con dispositivo seguro
	2.5. Subject Alternative Names		Sí	No			OID 2.5.29.17 (Marcado como NO crítico según EN 319412-2)
	2.5.1. DirectoryName	Organización a la que pertenece el representante.	Sí		40 caracteres	UTF8String	OID 1.3.6.1.4.1.47155.1.6
		NIF de la persona jurídica de la que es representante el titular del certificado, en formato ETSI EN 319412-1 (Ejemplo: "VATES-Q0000000J)	Sí		64 caracteres	PrintableString	OID 1.3.6.1.4.1.47155.1.7
	2.5.2. rfc822Name	Correo electrónico de la persona física	Sí			rfc822Name	
	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			OID	
	2.6.2. Email protection	Presente (1.3.6.1.5.5.7.3.4)	Sí			OID	Sólo se activa si se incluye el correo electrónico del firmante
	2.7. cRLDistributionPoint		No	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			IA5String	uniformResourceIdentifier **(NO HTTPS)**
	2.7.2. distributionPoint	http://crl2.vincasing.net/canebula2.crl	Sí			IA5String	uniformResourceIdentifier **(NO HTTPS)**
	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. Access Description		Sí				
	2.8.1.1. Acces Method	id-ad-ocsp	Sí			OID	OID 1.3.6.1.5.5.7.48.1
	2.8.1.2. Acces Location	http://ocsp.vincasign.net	Sí			IA5String	URL de acceso al OCSP **(NO HTTPS)** uniformResourceIdentifier
	2.8.2. Access Description		Sí				
	2.8.2.1. Acces Method	id-ad-calssuers	Sí			OID	OID 1.3.6.1.5.5.7.48.2
	2.8.2.1. Acces Location	http://www.vincasign.net/publickeys/casub.crt	Si			IA5String	URL acceso a certificado de la CA (NO HTTPS) uniformResourceIdentifier
	2.9. Qualified Certificate Statements		Sí	No			OID 1.3.6.1.5.5.7.1.3
	2.9.1. qCCompliance	id-etsi-qcs-QcCompliance	Sí				OID 0.4.0.1862.1.1 Indicación de certificado cualificado
	2.9.2. QcEuRetentionPeriod	"15"	Sí				OID 0.4.0.1862.1.3 Plazo de retención de registros
	2.9.3. QcSSCD	id-etsi-qcs-QcSSCD	Sí				OID 0.4.0.1862.1.4 Dispositivo cualificado de creación de firma

	2.9.4. QcPDS	{https://www.vincasign.net/policy/es/PDS-SELLOPJ1u-HSM/pds-sellopj1u-hsm-es.pdf,es},{https://www.vincasign.net/policy/en/PDS-SELLOPJ1u-HSM/pds-sellopj1u-hsm-en.pdf,en}	Sí				OID 0.4.0.1862.1.5 **(SÍ HTTPS)** URLs de acceso al texto divulgativo en inglés (obligatorio) y en castellano
	2.9.5. QcType	id-etsi-qct-eseal	Sí				OID 0.4.0.1862.1.6.2 Certificado de sello-e conforme al Reglamento (UE) Nº 910/2014
	2.9.6. qcStatement-2						OID 1.3.6.1.5.5.7.11.2 (RFC 3739)
	2.9.6.1. SemanticsInformation						
	2.9.6.1.1. semanticsIdNatural	0.4.0.194121.1.2					Semántica de persona jurídica conforme a EN 319 412-1, en serial number
	2.10. Basic Constraints		Sí	Sí			OID 2.5.29.19
	2.10.1. cA	FALSO	Sí			Boolean	

22. Cert Efímero de Sello de Empresa en SOFT

Campo EFÍMERO de SELLO de Empresa en SOFT	Gestión CENTRALIZADA Identificación y Firma	Oblig.	Crít.	Longitud máxima	Codif	Observaciones OID 1.3.6.1.4.1.47155.1.6.52
1. Basic estructure						
1.1. Version	"2"	Sí		1	Integer	El literal "2" corresponde a la versión 3.
1.2. Serial Number	Establecido automáticamente por la CA. Número identificativo único del certificado.	Sí		20 octetos	Integer	No puede ser un número negativo ni 0.
1.3. Signature Algorithm		Sí				
1.3.1. Algorithm	SHA-256 with RSA Signature	Sí			OID	1.2.840.113549.1.1.11
1.3.2. Parameters	No aplicable	No				
1.4. Issuer		Sí				
1.4.1. Country Name (C)	"ES"	Sí		2 caracteres	PrintableString	OID 2.5.4.6
1.4.2. Organization Name (O)	"VINTEGRIS SL"	Sí		64 caracteres	UTF8String	OID 2.5.4.10
1.4.3. organizationalUnitName (OU)	"vinCAsign"	Sí				OID 2.5.4.11
1.4.4. Locality Name (L)	"HOSPITALET DE LLOBREGAT"	Sí		128 caracteres	UTF8String	OID 2.5.4.7
1.4.5. Organization Identifier	"VATES-B62913926"	Sí		Ilimitado	UTF8String	OID 2.5.4.97
1.4.6. Common Name (CN)	"vinCAsign nebulaSUITE2 Authority"	Sí		64 caracteres	UTF8String	OID 2.5.4.3
1.4.7. stateOrProvinceName	"BARCELONA"	Sí			UTF8String	OID 2.5.4.8
1.5. Validity	MENOR DE 1 HORA	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				
1.6.1. Country Name	"ES"	Sí		2 caracteres	PrintableString	OID 2.5.4.6
1.6.2. Organization (O)	Denominación (nombre "oficial" de la persona jurídica) del creador del sello (Empresa, Organización, Entidad)	Sí		40 caracteres	UTF8String	OID 2.5.4.10
1.6.3. Organizational Unit (OU)	"SELLO ELECTRONICO"	Sí			UTF8String	OID 2.5.4.11
1.6.5. Organization Identifier	NIF de la persona jurídica a la que está vinculado este sello, en formato ETSI EN 319412-1 (Ejemplo: "VATES-Q0000000J)	Sí		64 caracteres	PrintableString	OID 2.5.4.97
1.6.6. Serial Number	NIF de la PERSONA JURÍDICA	Sí			PrintableString	OID 2.5.4.5
1.6.9. Common Name	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				

1.7.1. AlgorithmIdentifier						
1.7.1.1. Algorithm	RSA encryption	Sí			OID	OID 1.2.840.113549.1.1.1
1.7.1.2. Parameters	No aplicable	No				
1.7.2. SubjectPublicKey	Clave pública del firmante	Sí			Bit String	
2. Extensions						
2.1. Authority Key Identifier	Identificador de la clave del emisor	Sí	No			OID 2.5.29.35 (Marcado como NO crítico según EN 319412-2)
2.1.1. KeyIdentifier		Sí			Octet string	Derivado de la clave pública
2.1.2. AuthorityCertIssuer	Nombre de la CA a la que corresponde la clave identificada en keyIdentifier					(String UTF8) Size 12
2.1.3. AuthorityCertSerialNumber	Número de serie del certificado de CA					
2.2. Subject Key Identifier	Identificador de la clave del firmante	Sí	No			OID 2.5.29.14 (Marcado como NO crítico según EN 319412-2)
2.2.1. KeyIdentifier		Sí			Octet string	Derivado de la clave pública
2.3. Key Usage		Sí	Sí		Bit String	OID 2.5.29.15
2.3.1. Digital Signature	**Seleccionado "1"**	Sí				Bit para autenticación
2.3.2. Content commintment	**Seleccionado "1"**	Sí				Bit para firma
2.3.3. Key Encipherment	**Seleccionado "1"**	Sí				
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"					
2.3.8. Encipher Only	No seleccionado. "0"					
2.3.9. Decipher Only	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 Information		Sí				
2.4.1.1. Policy Identifier	**1.3.6.1.4.1.47155.1.6.52**	Sí			OID	Identificador de la política de Logalty
2.4.1.2. Policy Qualifiers		Sí				
2.4.1.1.1 CPS URI	https://policy.vincasign.net				IA5String	URL de la DPC (opcional por CAB FORUM)
2.4.1.1.2. User Notice/Explicit text	"Certificado cualificado y efímero de sello electrónico de persona jurídica emitido en software. Ver https://policy.vincasign.net "	Sí		200 caracteres	UTF8String y NFC	Texto indicativo
2.4.2. Policy Information		Sí				

2.4.2.1. Policy Identifier	**0.4.0.194112.1.1**	Sí			OID	QCP-l. Identificador de la política de certificado cualificado de sello de persona jurídica sin uso de dispositivo seguro
2.5. Subject Alternative Names		Sí	No			OID 2.5.29.17 (Marcado como NO crítico según EN 319412-2)
2.5.1. DirectoryName	Organización a la que pertenece el representante.	Sí		40 caracteres	UTF8String	OID 1.3.6.1.4.1.47155.1.6
	NIF de la persona jurídica de la que es representante el titular del certificado, en formato ETSI EN 319412-1 (Ejemplo: "VATES-Q0000000J)	Sí		64 caracteres	PrintableString	OID 1.3.6.1.4.1.47155.1.7
2.5.2. rfc822Name	Correo electrónico de la persona física	Sí			rfc822Name	
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			OID	
2.6.2. Email protection	Presente (1.3.6.1.5.5.7.3.4)	Sí			OID	Sólo se activa si se incluye el correo electrónico del firmante
2.7. cRLDistributionPoint		No	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			IA5String	uniformResourceIdentifier **(NO HTTPS)**
2.7.2. distributionPoint	http://crl2.vincasing.net/canebula2.crl	Sí			IA5String	uniformResourceIdentifier **(NO HTTPS)**
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. Access Description		Sí				
2.8.1.1. Acces Method	id-ad-ocsp	Sí			OID	OID 1.3.6.1.5.5.7.48.1
2.8.1.2. Acces Location	http://ocsp.vincasign.net	Sí			IA5String	URL de acceso al OCSP **(NO HTTPS)** uniformResourceIdentifier
2.8.2. Access Description		Sí				
2.8.2.1. Acces Method	id-ad-calssuers	Sí			OID	OID 1.3.6.1.5.5.7.48.2
2.8.2.1. Acces Location	http://www.vincasign.net/publickeys/casub.crt	Si			IA5String	URL acceso a certificado de la CA (NO HTTPS) uniformResourceIdentifier
2.9. Qualified Certificate Statements		Sí	No			OID 1.3.6.1.5.5.7.1.3
2.9.1. qCCompliance	id-etsi-qcs-QcCompliance	Sí				OID 0.4.0.1862.1.1 Indicación de certificado cualificado
2.9.2. QcEuRetentionPeriod	"15"	Sí				OID 0.4.0.1862.1.3 Plazo de retención de registros

	2.9.4. QcPDS	{https://www.vincasign.net/policy/es/PDS-SELLOPJ1u-SOFT/pds-sellopj1u-soft-es.pdf,es},{https://www.vincasign.net/policy/en/PDS-SELLOPJ1u-SOFT/pds-sellopj1u-soft-en.pdf,en}	Sí				OID 0.4.0.1862.1.5 **(SÍ HTTPS)** URLs de acceso al texto divulgativo en inglés (obligatorio) y en castellano
	2.9.5. QcType	id-etsi-qct-eseal	Sí				OID 0.4.0.1862.1.6.2 Certificado de sello-e conforme al Reglamento (UE) Nº 910/2014
	2.9.6. qcStatement-2						OID 1.3.6.1.5.5.7.11.2 (RFC 3739)
	2.9.6.1. SemanticsInformation						
	2.9.6.1.1. semanticsIdNatural	0.4.0.194121.1.2					Semántica de persona jurídica conforme a EN 319 412-1, en serial number
	2.10. Basic Constraints		Sí	Sí			OID 2.5.29.19
	2.10.1. cA	FALSO	Sí			Boolean	

23. Cert de Sello para IoT

Campo	Gestión CENTRALIZADA	Oblig.	Crít.	Longitud máxima	Codif	Observaciones OID 1.3.6.1.4.1.47155.1.7.2
SELLO para IoT	Identificación y Firma					
1. Basic estructure						
1.1. Version	"2"	Sí		1	Integer	El literal "2" corresponde a la versión 3.
1.2. Serial Number	Establecido automáticamente por la CA. Número identificativo único del certificado.	Sí		20 octetos	Integer	No puede ser un número negativo ni 0.
1.3. Signature Algorithm		Sí				
1.3.1. Algorithm	SHA-256 with RSA Signature	Sí			OID	1.2.840.113549.1.1.11
1.3.2. Parameters	No aplicable	No				
1.4. Issuer		Sí				
1.4.1. Country Name (C)	"ES"	Sí		2 caracteres	PrintableString	OID 2.5.4.6
1.4.2. Organization Name (O)	"VINTEGRIS SL"	Sí		64 caracteres	UTF8String	OID 2.5.4.10
1.4.3. organizationalUnitName (OU)	"vinCAsign"	Sí				OID 2.5.4.11
1.4.4. Locality Name (L)	"HOSPITALET DE LLOBREGAT"	Sí		128 caracteres	UTF8String	OID 2.5.4.7
1.4.5. Organization Identifier	"VATES-B62913926"	Sí		Ilimitado	UTF8String	OID 2.5.4.97
1.4.6. Common Name (CN)	"vinCAsign nebulaSUITE2 Authority"	Sí		64 caracteres	UTF8String	OID 2.5.4.3
1.4.7. stateOrProvinceName	"BARCELONA"	Sí			UTF8String	OID 2.5.4.8
1.5. Validity		Sí				3 YEAR
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				
1.6.1. Country Name	"ES"	Sí		2 caracteres	PrintableString	OID 2.5.4.6
1.6.2. Organization (O)	Denominación (nombre "oficial" de la persona jurídica) del creador del sello (Empresa, Organización, Entidad)	Sí		40 caracteres	UTF8String	OID 2.5.4.10
1.6.3. Organizational Unit (OU)	Id de la cosa, que permita identificar únicamente su ubicación.	Sí			UTF8String	OID 2.5.4.11
1.6.5. Organization Identifier	NIF de la persona jurídica a la que está vinculado este sello, en formato ETSI EN 319412-1 (Ejemplo: "VATES-Q0000000J)	Sí		64 caracteres	PrintableString	OID 2.5.4.97
1.6.6. Serial Number	NIF de la PERSONA JURÍDICA	Sí			PrintableString	OID 2.5.4.5
1.6.9. Common Name	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				

1.7.1. AlgorithmIdentifier						
1.7.1.1. Algorithm	RSA encryption	Sí			OID	OID 1.2.840.113549.1.1.1
1.7.1.2. Parameters	No aplicable	No				
1.7.2. SubjectPublicKey	Clave pública del firmante	Sí			Bit String	
2. Extensions						
2.1. Authority Key Identifier	Identificador de la clave del emisor	Sí	No			OID 2.5.29.35 (Marcado como NO crítico según EN 319412-2)
2.1.1. KeyIdentifier		Sí			Octet string	Derivado de la clave pública
2.1.2. AuthorityCertIssuer	Nombre de la CA a la que corresponde la clave identificada en keyIdentifier					(String UTF8) Size 12
2.1.3. AuthorityCertSerialNumber	Número de serie del certificado de CA					
2.2. Subject Key Identifier	Identificador de la clave del firmante	Sí	No			OID 2.5.29.14 (Marcado como NO crítico según EN 319412-2)
2.2.1. KeyIdentifier		Sí			Octet string	Derivado de la clave pública
2.3. Key Usage		Sí	Sí		Bit String	OID 2.5.29.15
2.3.1. Digital Signature	**Seleccionado "1"**	Sí				Bit para autenticación
2.3.2. Content commintment	**Seleccionado "1"**	Sí				Bit para firma
2.3.3. Key Encipherment	**Seleccionado "1"**	Sí				
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"					
2.3.8. Encipher Only	No seleccionado. "0"					
2.3.9. Decipher Only	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 Information		Sí				
2.4.1.1. Policy Identifier	**1.3.6.1.4.1.47155.1.7.2**	Sí			OID	Identificador de la política de Logalty
2.4.1.2. Policy Qualifiers		Sí				
2.4.1.1.1 CPS URI	https://policy.vincasign.net				IA5String	URL de la DPC (opcional por CAB FORUM)
2.4.1.1.2. User Notice/Explicit text	"Certificado cualificado de sello electrónico para IoT emitido en software. Ver https://policy.vincasign.net "	Sí		200 caracteres	UTF8String y NFC	Texto indicativo
2.4.2. Policy Information		Sí				

2.4.2.1. Policy Identifier	**0.4.0.194112.1.1**	Sí			OID	QCP-l. Identificador de la política de certificado cualificado de sello de persona jurídica sin uso de dispositivo seguro
2.5. Subject Alternative Names		Sí	No			OID 2.5.29.17 (Marcado como NO crítico según EN 319412-2)
2.5.1. rfc822Name	Correo electrónico de contacto	Sí			rfc822Name	
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			OID	
2.6.2. Email protection	Presente (1.3.6.1.5.5.7.3.4)	Sí			OID	Sólo se activa si se incluye el correo electrónico del firmante
2.7. cRLDistributionPoint		No	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			IA5String	uniformResourceIdentifier **(NO HTTPS)**
2.7.2. distributionPoint	http://crl2.vincasing.net/canebula2.crl	Sí			IA5String	uniformResourceIdentifier **(NO HTTPS)**
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. Access Description		Sí				
2.8.1.1. Acces Method	id-ad-ocsp	Sí			OID	OID 1.3.6.1.5.5.7.48.1
2.8.1.2. Acces Location	http://ocsp.vincasign.net	Sí			IA5String	URL de acceso al OCSP **(NO HTTPS)** uniformResourceIdentifier
2.8.2. Access Description		Sí				
2.8.2.1. Acces Method	id-ad-calssuers	Sí			OID	OID 1.3.6.1.5.5.7.48.2
2.8.2.1. Acces Location	http://www.vincasign.net/publickeys/casub.crt	Si			IA5String	URL acceso a certificado de la CA (NO HTTPS) uniformResourceIdentifier
2.9. Qualified Certificate Statements		Sí	No			OID 1.3.6.1.5.5.7.1.3
2.9.1. qCCompliance	id-etsi-qcs-QcCompliance	Sí				OID 0.4.0.1862.1.1 Indicación de certificado cualificado
2.9.2. QcEuRetentionPeriod	"15"	Sí				OID 0.4.0.1862.1.3 Plazo de retención de registros
2.9.4. 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 **(SÍ HTTPS)** URLs de acceso al texto divulgativo en inglés (obligatorio) y en castellano
2.9.5. QcType	id-etsi-qct-eseal	Sí				OID 0.4.0.1862.1.6.2 Certificado de sello-e conforme al Reglamento (UE) Nº 910/2014

	2.9.6. qcStatement-2						OID 1.3.6.1.5.5.7.11.2 (RFC 3739)
	2.9.6.1. SemanticsInformation						
	2.9.6.1.1. semanticsIdNatural	0.4.0.194121.1.2					Semántica de persona jurídica conforme a EN 319 412-1, en serial number
	2.10. Basic Constraints		Sí	Sí			OID 2.5.29.19
	2.10.1. cA	FALSO	Sí			Boolean	

24. Cert Corporativo de Sello de Tiempo Electrónico

Campo TSA - TSU	Gestión CENTRALIZADA SELLADO DE TIEMPO ELECTRÓNICO	Oblig.	Crít.	Longitud máxima	Codif	Observaciones OID 1.3.6.1.4.1.47155.1.9.1
1. Basic estructure						
1.1. Version	"2"	Sí		1	Integer	El literal "2" corresponde a la versión 3.
1.2. Serial Number	Establecido automáticamente por la CA. Número identificativo único del certificado.	Sí		20 octetos	Integer	No puede ser un número negativo ni 0.
1.3. Signature Algorithm		Sí				
1.3.1. Algorithm	SHA-512 with RSA Signature	Sí			OID	1.2.840.113549.1.1.13
1.3.2. Parameters	No aplicable	No				
1.4. Issuer		Sí				
1.4.1. Country Name (C)	"ES"	Sí		2 caracteres	PrintableString	OID 2.5.4.6
1.4.2. Organization Name (O)	"VINTEGRIS SL"	Sí		64 caracteres	UTF8String	OID 2.5.4.10
1.4.3. organizationalUnitName (OU)	"vinCAsign"	Sí				OID 2.5.4.11
1.4.4. Locality Name (L)	"HOSPITALET DE LLOBREGAT"	Sí		128 caracteres	UTF8String	OID 2.5.4.7
1.4.5. Organization Identifier	"VATES-B62913926"	Sí		Ilimitado	UTF8String	OID 2.5.4.97
1.4.6. Common Name (CN)	"vinCAsign nebulaSUITE2 Authority"	Sí		64 caracteres	UTF8String	OID 2.5.4.3
1.4.7. stateOrProvinceName	"BARCELONA"	Sí			UTF8String	OID 2.5.4.8
1.5. Validity		Sí				1 YEAR
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				
1.6.1. Country Name	"ES"	Sí		2 caracteres	PrintableString	OID 2.5.4.6
1.6.2. Organization (O)	"VINTEGRIS SL"	Sí		40 caracteres	UTF8String	OID 2.5.4.10
1.6.3. Organizational Unit (OU)	"vinCAsign"	Sí			UTF8String	OID 2.5.4.11
1.6.4 Locality Name (L)	"HOSPITALET DE LLOBREGAT"					OID 2.5.4.7
1.6.5. Organization Identifier	"VATES-B62913926"	Sí		64 caracteres	PrintableString	OID 2.5.4.97
1.6.6. stateOrProvinceName	"BARCELONA"	Sí			PrintableString	OID 2.5.4.8

1.6.7. Common Name	vinCAsign qualified TSA TSU01	Sí				OID 2.5.4.3
1.7. Subject Public Key Info	Clave pública del firmante, codificada en RSA encryption (2048 bits)	Sí				
1.7.1. AlgorithmIdentifier						
1.7.1.1. Algorithm	RSA encryption	Sí			OID	OID 1.2.840.113549.1.1.1
1.7.1.2. Parameters	No aplicable	No				
1.7.2. SubjectPublicKey	Clave pública del firmante	Sí			Bit String	
2. Extensions						
2.1. Authority Key Identifier	Identificador de la clave del emisor	Sí	No			OID 2.5.29.35 (Marcado como NO crítico según EN 319412-2)
2.1.1. KeyIdentifier		Sí			Octet string	Derivado de la clave pública
2.1.2. AuthorityCertIssuer	Nombre de la CA a la que corresponde la clave identificada en keyIdentifier					(String UTF8) Size 12
2.1.3. AuthorityCertSerialNumber	Número de serie del certificado de CA					
2.2. Subject Key Identifier	Identificador de la clave del firmante	Sí	No			OID 2.5.29.14 (Marcado como NO crítico según EN 319412-2)
2.2.1. KeyIdentifier		Sí			Octet string	Derivado de la clave pública
2.3. Key Usage		Sí	Sí		Bit String	OID 2.5.29.15
2.3.1. Digital Signature	**Seleccionado "1"**	Sí				Bit para autenticación
2.3.2. Content commintment	**Seleccionado "1"**	Sí				Bit para firma
2.3.3. Key Encipherment	No seleccionado. "0"					
2.3.4. Data Encipherment	No seleccionado. "0"					
2.3.5. Key Agreement	No seleccionado. "0"					
2.3.6. Key Certificate Signature	No seleccionado. "0"					
2.3.7. CRL Signature	No seleccionado. "0"					
2.3.8. Encipher Only	No seleccionado. "0"					
2.3.9. Decipher Only	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 Information		Sí				
2.4.1.1. Policy Identifier	**1.3.6.1.4.1.47155.1.9.1**	Sí			OID	Identificador de la política de Logalty
2.4.1.2. Policy Qualifiers		Sí				
2.4.1.1.1 CPS URI	https://policy.vincasign.net				IA5String	URL de la DPC (opcional por CAB FORUM)

	2.4.1.1.2. User Notice/Explicit text	"Certificado cualificado de sello electrónico de persona jurídica para la expedición de sellos cualificados de tiempo electrónico"	Sí		200 caracteres	UTF8String y NFC	Texto indicativo
	2.4.2. Policy Information		Sí				
	2.4.2.1. Policy Identifier	**0.4.0.194112.1.1**	Sí			OID	QCP-l. Identificador de la política de certificado cualificado de sello de persona jurídica sin uso de dispositivo seguro
	2.6. Extended Key Usage		Sí	No			OID 2.5.29.37 (Marcado como NO crítico según EN 319412-2)
	2.6.1. timeStamping	Presente (1.3.6.1.5.5.7.3.8)	Sí			OID	
	2.7. cRLDistributionPoint		No	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			IA5String	uniformResourceIdentifier **(NO HTTPS)**
	2.7.2. distributionPoint	http://crl2.vincasing.net/canebula2.crl	Sí			IA5String	uniformResourceIdentifier **(NO HTTPS)**
	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. Access Description		Sí				
	2.8.1.1. Acces Method	id-ad-ocsp	Sí			OID	OID 1.3.6.1.5.5.7.48.1
	2.8.1.2. Acces Location	http://ocsp.vincasign.net	Sí			IA5String	URL de acceso al OCSP **(NO HTTPS)** uniformResourceIdentifier
	2.8.2. Access Description		Sí				
	2.8.2.1. Acces Method	id-ad-calssuers	Sí			OID	OID 1.3.6.1.5.5.7.48.2
	2.8.2.1. Acces Location	http://www.vincasign.net/publickeys/casub.crt	Si			IA5String	URL acceso a certificado de la CA (NO HTTPS) uniformResourceIdentifier
	2.9. Qualified Certificate Statements		Sí	No			OID 1.3.6.1.5.5.7.1.3
	2.9.1. qCCompliance	id-etsi-qcs-QcCompliance	Sí				OID 0.4.0.1862.1.1 Indicación de certificado cualificado
	2.9.2. QcEuRetentionPeriod	"15"	Sí				OID 0.4.0.1862.1.3 Plazo de retención de registros
	2.9.4. QcPDS	{https://www.vincasign.net/policy/es/PDS-TSA/pds-tsa-es.pdf,es},{https://www.vincasign.net/policy/en/PDS-TSA/pds-tsa-en.pdf,en}	Sí				OID 0.4.0.1862.1.5 **(SÍ HTTPS)** URLs de acceso al texto divulgativo en inglés (obligatorio) y en castellano

	2.9.5. QcType	id-etsi-qct-eseal	Sí				OID 0.4.0.1862.1.6.2 Certificado de sello-e conforme al Reglamento (UE) Nº 910/2014
	2.10. Basic Constraints		Sí	Sí			OID 2.5.29.19
	2.10.1. cA	FALSO	Sí			Boolean	

25 Cert Individual de PF en DCCF

Campo Individual de PF · DCCF	Gestión CENTRALIZADA Identificación y Firma	Oblig.	Crít.	Longitud máxima	Codif	Observaciones OID 1.3.6.1.4.1.47155.1.10.1
1. Basic estructure						
1.1. Version	"2"	Sí		1	Integer	El literal "2" corresponde a la versión 3.
1.2. Serial Number	Establecido automáticamente por la CA. Número identificativo único del certificado.	Sí		20 octetos	Integer	No puede ser un número negativo ni 0.
1.3. Signature Algorithm		Sí				
1.3.1. Algorithm	SHA-256 with RSA Signature	Sí			OID	1.2.840.113549.1.1.11
1.3.2. Parameters	No aplicable	No				
1.4. Issuer		Sí				
1.4.1. Country Name (C)	"ES"	Sí		2 caracteres	PrintableString	OID 2.5.4.6
1.4.2. Organization Name (O)	"VINTEGRIS SL"	Sí		64 caracteres	UTF8String	OID 2.5.4.10
1.4.3. organizationalUnitName (OU)	"vinCAsign"	Sí				OID 2.5.4.11
1.4.4. Locality Name (L)	"HOSPITALET DE LLOBREGAT"	Sí		128 caracteres	UTF8String	OID 2.5.4.7
1.4.5. Organization Identifier	"VATES-B62913926"	Sí		Ilimitado	UTF8String	OID 2.5.4.97
1.4.6. Common Name (CN)	"vinCAsign nebulaSUITE2 Authority"	Sí		64 caracteres	UTF8String	OID 2.5.4.3
1.4.7. stateOrProvinceName	"BARCELONA"	Sí			UTF8String	OID 2.5.4.8
1.5. Validity		Sí				3 years
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				
1.6.1. Country Name	"ES"	Sí		2 caracteres	PrintableString	OID 2.5.4.6
1.6.3. Organizational Unit (OU)	Indicación opcional			16 caracteres	UTF8String	OID 2.5.4.11
1.6.6. Serial Number	NIF del titular acorde a ETSI EN 319 412-1 "IDCES-123456789Z")	Sí			PrintableString	OID 2.5.4.5
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. Common Name	APELLIDO1 APELLIDO2 NOMBRE – DNI 123456789Z	Sí				OID 2.5.4.3
1.6.10. emailAddress	Correo electrónico del firmante	Sí			IA5String	

1.7. Subject Public Key Info	Clave pública del firmante, codificada en RSA encryption (2048 bits)	Sí				
1.7.1. AlgorithmIdentifier						
1.7.1.1. Algorithm	RSA encryption	Sí			OID	OID 1.2.840.113549.1.1.1
1.7.1.2. Parameters	No aplicable	No				
1.7.2. SubjectPublicKey	Clave pública del firmante	Sí			Bit String	
2. Extensions						
2.1. Authority Key Identifier	Identificador de la clave del emisor	Sí	No			OID 2.5.29.35 (Marcado como NO crítico según EN 319412-2)
2.1.1. KeyIdentifier		Sí			Octet string	Derivado de la clave pública
2.1.2. AuthorityCertIssuer	Nombre de la CA a la que corresponde la clave identificada en keyIdentifier					(String UTF8) Size 12
2.1.3. AuthorityCertSerialNumber	Número de serie del certificado de CA					
2.2. Subject Key Identifier	Identificador de la clave del firmante	Sí	No			OID 2.5.29.14 (Marcado como NO crítico según EN 319412-2)
2.2.1. KeyIdentifier		Sí			Octet string	Derivado de la clave pública
2.3. Key Usage		Sí	Sí		Bit String	OID 2.5.29.15
2.3.1. Digital Signature	**Seleccionado "1"**	Sí				Bit para autenticación
2.3.2. Content commintment	**Seleccionado "1"**	Sí				Bit para firma
2.3.3. Key Encipherment	No seleccionado. "0"					
2.3.4. Data Encipherment	No seleccionado. "0"					
2.3.5. Key Agreement	No seleccionado. "0"					
2.3.6. Key Certificate Signature	No seleccionado. "0"					
2.3.7. CRL Signature	No seleccionado. "0"					
2.3.8. Encipher Only	No seleccionado. "0"					
2.3.9. Decipher Only	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 Information		Sí				
2.4.1.1. Policy Identifier	**1.3.6.1.4.1.47155.1.10.1**	Sí			OID	Identificador de la política de Logalty
2.4.1.2. Policy Qualifiers		Sí				
2.4.1.1.1 CPS URI	https://policy.vincasign.net				IA5String	URL de la DPC (opcional por CAB FORUM)
2.4.1.1.2. User Notice/Explicit text	"Certificado cualificado de persona física emitido en un DCCF. Ver https://policy.vincasign.net "	Sí		200 caracteres	UTF8String y NFC	Texto indicativo
2.4.2. Policy Information		Sí				

2.4.2.1. Policy Identifier	**0.4.0.194112.1.2**	Sí			OID	QCP-n-qscd. Identificador de la política de certificado cualificado de persona física con dispositivo seguro
2.5. Subject Alternative Names		Sí	No			OID 2.5.29.17 (Marcado como NO crítico según EN 319412-2)
2.5.1. DirectoryName	Nombre de la persona física (como consta en el DNI/NIE)	Sí				OID 1.3.6.1.4.1.47155.1.1
	Apellido primero de la persona física (como consta en el DNI/NIE)	Sí				OID 1.3.6.1.4.1.47155.1.2
	Apellido segundo de la persona física (como consta en el DNI/NIE)	Sí				OID 1.3.6.1.4.1.47155.1.3
	NIF del titular acorde a ETSI EN 319 412-1 "IDCES-123456789Z")	Sí			PrintableString	OID 1.3.6.1.4.1.47155.1.4
2.5.2. rfc822Name	Correo electrónico de la persona física	Sí			rfc822Name	
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			OID	
2.6.2. Email protection	Presente (1.3.6.1.5.5.7.3.4)	Sí			OID	Sólo se activa si se incluye el correo electrónico del firmante
2.7. cRLDistributionPoint		No	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			IA5String	uniformResourceIdentifier **(NO HTTPS)**
2.7.2. distributionPoint	http://crl2.vincasing.net/canebula2.crl	Sí			IA5String	uniformResourceIdentifier **(NO HTTPS)**
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. Access Description		Sí				
2.8.1.1. Acces Method	id-ad-ocsp	Sí			OID	OID 1.3.6.1.5.5.7.48.1
2.8.1.2. Acces Location	http://ocsp.vincasign.net	Sí			IA5String	URL de acceso al OCSP **(NO HTTPS)** uniformResourceIdentifier
2.8.2. Access Description		Sí				
2.8.2.1. Acces Method	id-ad-calssuers	Sí			OID	OID 1.3.6.1.5.5.7.48.2
2.8.2.1. Acces Location	http://www.vincasign.net/publickeys/casub.crt	Si			IA5String	URL acceso a certificado de la CA (NO HTTPS) uniformResourceIdentifier
2.9. Qualified Certificate Statements		Sí	No			OID 1.3.6.1.5.5.7.1.3
2.9.1. qCCompliance	id-etsi-qcs-QcCompliance	Sí				OID 0.4.0.1862.1.1 Indicación de certificado cualificado
2.9.2. QcEuRetentionPeriod	"15"	Sí				OID 0.4.0.1862.1.3 Plazo de retención de registros
2.9.3. QcSSCD	id-etsi-qcs-QcSSCD	Sí				OID 0.4.0.1862.1.4 Dispositivo cualificado de creación de firma

	2.9.4. QcPDS	{https://www.vincasign.net/policy/es/PDS-PF-hard-IND/pds-pf-hard-ind-es.pdf,es},{https://www.vincasign.net/policy/en/PDS-PF-hard-IND/pds-pf-hard-ind-en.pdf,en}	Sí				OID 0.4.0.1862.1.5 **(SÍ HTTPS)** URLs de acceso al texto divulgativo en inglés (obligatorio) y en castellano
	2.9.5. QcType	id-etsi-qct-esign	Sí				OID 0.4.0.1862.1.6.1 Certificado de firma electrónica conforme al Reglamento (UE) Nº 910/2014
	2.9.6. qcStatement-2						OID 1.3.6.1.5.5.7.11.2 (RFC 3739)
	2.9.6.1. SemanticsInformation						
	2.9.6.1.1. semanticsIdNatural	0.4.0.194121.1.1					Semántica de persona fisica conforme a EN 319 412-1, en serial number
	2.10. Basic Constraints		Sí	Sí			OID 2.5.29.19
	2.10.1. cA	FALSO	Sí			Boolean	

26. Cert Individual de PF en SOFT

Campo Individual de PF · SOFT	Gestión CENTRALIZADA Identificación, Firma	Oblig.	Crít.	Longitud máxima	Codif	Observaciones OID 1.3.6.1.4.1.47155.1.10.2
1. Basic estructure						
1.1. Version	"2"	Sí		1	Integer	El literal "2" corresponde a la versión 3.
1.2. Serial Number	Establecido automáticamente por la CA. Número identificativo único del certificado.	Sí		20 octetos	Integer	No puede ser un número negativo ni 0.
1.3. Signature Algorithm		Sí				
1.3.1. Algorithm	SHA-256 with RSA Signature	Sí			OID	1.2.840.113549.1.1.11
1.3.2. Parameters	No aplicable	No				
1.4. Issuer		Sí				
1.4.1. Country Name (C)	"ES"	Sí		2 caracteres	PrintableString	OID 2.5.4.6
1.4.2. Organization Name (O)	"VINTEGRIS SL"	Sí		64 caracteres	UTF8String	OID 2.5.4.10
1.4.3. organizationalUnitName (OU)	"vinCAsign"	Sí				OID 2.5.4.11
1.4.4. Locality Name (L)	"HOSPITALET DE LLOBREGAT"	Sí		128 caracteres	UTF8String	OID 2.5.4.7
1.4.5. Organization Identifier	"VATES-B62913926"	Sí		Ilimitado	UTF8String	OID 2.5.4.97
1.4.6. Common Name (CN)	"vinCAsign nebulaSUITE2 Authority"	Sí		64 caracteres	UTF8String	OID 2.5.4.3
1.4.7. stateOrProvinceName	"BARCELONA"	Sí			UTF8String	OID 2.5.4.8
1.5. Validity		Sí				3 years
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				
1.6.1. Country Name	"ES"	Sí		2 caracteres	PrintableString	OID 2.5.4.6
1.6.3. Organizational Unit (OU)	Indicación opcional			16 caracteres	UTF8String	OID 2.5.4.11
1.6.6. Serial Number	NIF del titular acorde a ETSI EN 319 412-1 "IDCES-123456789Z")	Sí			PrintableString	OID 2.5.4.5
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. Common Name	APELLIDO1 APELLIDO2 NOMBRE – DNI 123456789Z	Sí				OID 2.5.4.3
1.6.10. emailAddress	Correo electrónico del firmante	Sí			IA5String	

1.7. Subject Public Key Info	Clave pública del firmante, codificada en RSA encryption (2048 bits)	Sí				
1.7.1. AlgorithmIdentifier						
1.7.1.1. Algorithm	RSA encryption	Sí			OID	OID 1.2.840.113549.1.1.1
1.7.1.2. Parameters	No aplicable	No				
1.7.2. SubjectPublicKey	Clave pública del firmante	Sí			Bit String	
2. Extensions						
2.1. Authority Key Identifier	Identificador de la clave del emisor	Sí	No			OID 2.5.29.35 (Marcado como NO crítico según EN 319412-2)
2.1.1. KeyIdentifier		Sí			Octet string	Derivado de la clave pública
2.1.2. AuthorityCertIssuer	Nombre de la CA a la que corresponde la clave identificada en keyIdentifier					(String UTF8) Size 12
2.1.3. AuthorityCertSerialNumber	Número de serie del certificado de CA					
2.2. Subject Key Identifier	Identificador de la clave del firmante	Sí	No			OID 2.5.29.14 (Marcado como NO crítico según EN 319412-2)
2.2.1. KeyIdentifier		Sí			Octet string	Derivado de la clave pública
2.3. Key Usage		Sí	Sí		Bit String	OID 2.5.29.15
2.3.1. Digital Signature	**Seleccionado "1"**	Sí				Bit para autenticación
2.3.2. Content commintment	**Seleccionado "1"**	Sí				Bit para firma
2.3.3. Key Encipherment	**Seleccionado "1"**	Sí				
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"					
2.3.8. Encipher Only	No seleccionado. "0"					
2.3.9. Decipher Only	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 Information		Sí				
2.4.1.1. Policy Identifier	**1.3.6.1.4.1.47155.1.10.2**	Sí			OID	Identificador de la política de Logalty
2.4.1.2. Policy Qualifiers		Sí				
2.4.1.1.1 CPS URI	https://policy.vincasign.net				IA5String	URL de la DPC (opcional por CAB FORUM)
2.4.1.1.2. User Notice/Explicit text	"Certificado cualificado de persona física emitido en SOFT. Ver https://policy.vincasign.net "	Sí		200 caracteres	UTF8String y NFC	Texto indicativo
2.4.2. Policy Information		Sí				

2.4.2.1. Policy Identifier	**0.4.0.194112.1.0**	Sí			OID	QCP-n. Identificador de la política de certificado cualificado de persona física sin uso de dispositivo seguro
2.5. Subject Alternative Names		Sí	No			OID 2.5.29.17 (Marcado como NO crítico según EN 319412-2)
2.5.1. DirectoryName	Nombre de la persona física (como consta en el DNI/NIE)	Sí				OID 1.3.6.1.4.1.47155.1.1
	Apellido primero de la persona física (como consta en el DNI/NIE)	Sí				OID 1.3.6.1.4.1.47155.1.2
	Apellido segundo de la persona física (como consta en el DNI/NIE)	Sí				OID 1.3.6.1.4.1.47155.1.3
	NIF del titular acorde a ETSI EN 319 412-1 "IDCES-123456789Z")	Sí			PrintableString	OID 1.3.6.1.4.1.47155.1.4
2.5.2. rfc822Name	Correo electrónico de la persona física	Sí			rfc822Name	
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			OID	
2.6.2. Email protection	Presente (1.3.6.1.5.5.7.3.4)	Sí			OID	Sólo se activa si se incluye el correo electrónico del firmante
2.7. cRLDistributionPoint		No	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			IA5String	uniformResourceIdentifier **(NO HTTPS)**
2.7.2. distributionPoint	http://crl2.vincasing.net/canebula2.crl	Sí			IA5String	uniformResourceIdentifier **(NO HTTPS)**
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. Access Description		Sí				
2.8.1.1. Acces Method	id-ad-ocsp	Sí			OID	OID 1.3.6.1.5.5.7.48.1
2.8.1.2. Acces Location	http://ocsp.vincasign.net	Sí			IA5String	URL de acceso al OCSP **(NO HTTPS)** uniformResourceIdentifier
2.8.2. Access Description		Sí				
2.8.2.1. Acces Method	id-ad-calssuers	Sí			OID	OID 1.3.6.1.5.5.7.48.2
2.8.2.1. Acces Location	http://www.vincasign.net/publickeys/casub.crt	Si			IA5String	URL acceso a certificado de la CA (NO HTTPS) uniformResourceIdentifier
2.9. Qualified Certificate Statements		Sí	No			OID 1.3.6.1.5.5.7.1.3
2.9.1. qCCompliance	id-etsi-qcs-QcCompliance	Sí				OID 0.4.0.1862.1.1 Indicación de certificado cualificado
2.9.2. QcEuRetentionPeriod	"15"	Sí				OID 0.4.0.1862.1.3 Plazo de retención de registros

	2.9.4. QcPDS	{https://www.vincasign.net/policy/es/PDS-PF-soft-IND/pds-pf-soft-ind-es.pdf,es},{https://www.vincasign.net/policy/en/PDS-PF-soft-IND/pds-pf-soft-ind-en.pdf,en}	Sí				OID 0.4.0.1862.1.5 **(SÍ HTTPS)** URLs de acceso al texto divulgativo en inglés (obligatorio) y en castellano
	2.9.5. QcType	id-etsi-qct-esign	Sí				OID 0.4.0.1862.1.6.1 Certificado de firma electrónica conforme al Reglamento (UE) Nº 910/2014
	2.9.6. qcStatement-2						OID 1.3.6.1.5.5.7.11.2 (RFC 3739)
	2.9.6.1. SemanticsInformation						
	2.9.6.1.1. semanticsIdNatural	0.4.0.194121.1.1					Semántica de persona fisica conforme a EN 319 412-1, en serial number
	2.10. Basic Constraints		Sí	Sí			OID 2.5.29.19
	2.10.1. cA	FALSO	Sí			Boolean	

27. Cert Individual y Efímero de PF en DCCF

Campo Individual y efímero de PF · DCCF	Gestión CENTRALIZADA Identificación y Firma	Oblig.	Crít.	Longitud máxima	Codif	Observaciones OID 1.3.6.1.4.1.47155.1.10.51
1. Basic estructure						
1.1. Version	"2"	Sí		1	Integer	El literal "2" corresponde a la versión 3.
1.2. Serial Number	Establecido automáticamente por la CA. Número identificativo único del certificado.	Sí		20 octetos	Integer	No puede ser un número negativo ni 0.
1.3. Signature Algorithm		Sí				
1.3.1. Algorithm	SHA-256 with RSA Signature	Sí			OID	1.2.840.113549.1.1.11
1.3.2. Parameters	No aplicable	No				
1.4. Issuer		Sí				
1.4.1. Country Name (C)	"ES"	Sí		2 caracteres	PrintableString	OID 2.5.4.6
1.4.2. Organization Name (O)	"VINTEGRIS SL"	Sí		64 caracteres	UTF8String	OID 2.5.4.10
1.4.3. organizationalUnitName (OU)	"vinCAsign"	Sí				OID 2.5.4.11
1.4.4. Locality Name (L)	"HOSPITALET DE LLOBREGAT"	Sí		128 caracteres	UTF8String	OID 2.5.4.7
1.4.5. Organization Identifier	"VATES-B62913926"	Sí		Ilimitado	UTF8String	OID 2.5.4.97
1.4.6. Common Name (CN)	"vinCAsign nebulaSUITE2 Authority"	Sí		64 caracteres	UTF8String	OID 2.5.4.3
1.4.7. stateOrProvinceName	"BARCELONA"	Sí			UTF8String	OID 2.5.4.8
1.5. Validity		Sí				60 minutos
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				
1.6.1. Country Name	"ES"	Sí		2 caracteres	PrintableString	OID 2.5.4.6
1.6.3. Organizational Unit (OU)	Indicación opcional			16 caracteres	UTF8String	OID 2.5.4.11
1.6.6. Serial Number	NIF del titular acorde a ETSI EN 319 412-1 "IDCES-123456789Z")	Sí			PrintableString	OID 2.5.4.5
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. Common Name	APELLIDO1 APELLIDO2 NOMBRE – DNI 123456789Z	Sí				OID 2.5.4.3
1.6.10. emailAddress	Correo electrónico del firmante	Sí			IA5String	

1.7. Subject Public Key Info	Clave pública del firmante, codificada en RSA encryption (2048 bits)	Sí				
1.7.1. AlgorithmIdentifier						
1.7.1.1. Algorithm	RSA encryption	Sí			OID	OID 1.2.840.113549.1.1.1
1.7.1.2. Parameters	No aplicable	No				
1.7.2. SubjectPublicKey	Clave pública del firmante	Sí			Bit String	
2. Extensions						
2.1. Authority Key Identifier	Identificador de la clave del emisor	Sí	No			OID 2.5.29.35 (Marcado como NO crítico según EN 319412-2)
2.1.1. KeyIdentifier		Sí			Octet string	Derivado de la clave pública
2.1.2. AuthorityCertIssuer	Nombre de la CA a la que corresponde la clave identificada en keyIdentifier					(String UTF8) Size 12
2.1.3. AuthorityCertSerialNumber	Número de serie del certificado de CA					
2.2. Subject Key Identifier	Identificador de la clave del firmante	Sí	No			OID 2.5.29.14 (Marcado como NO crítico según EN 319412-2)
2.2.1. KeyIdentifier		Sí			Octet string	Derivado de la clave pública
2.3. Key Usage		Sí	Sí		Bit String	OID 2.5.29.15
2.3.1. Digital Signature	**Seleccionado "1"**	Sí				Bit para autenticación
2.3.2. Content commintment	**Seleccionado "1"**	Sí				Bit para firma
2.3.3. Key Encipherment	No seleccionado. "0"					
2.3.4. Data Encipherment	No seleccionado. "0"					
2.3.5. Key Agreement	No seleccionado. "0"					
2.3.6. Key Certificate Signature	No seleccionado. "0"					
2.3.7. CRL Signature	No seleccionado. "0"					
2.3.8. Encipher Only	No seleccionado. "0"					
2.3.9. Decipher Only	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 Information		Sí				
2.4.1.1. Policy Identifier	**1.3.6.1.4.1.47155.1.10.51**	Sí			OID	Identificador de la política de Logalty
2.4.1.2. Policy Qualifiers		Sí				
2.4.1.1.1 CPS URI	https://policy.vincasign.net				IA5String	URL de la DPC (opcional por CAB FORUM)
2.4.1.1.2. User Notice/Explicit text	"Certificado cualificado y efimero de persona fisica emitido en un DCCF. Ver https://policy.vincasign.net "	Sí		200 caracteres	UTF8String y NFC	Texto indicativo
2.4.2. Policy Information		Sí				

2.4.2.1. Policy Identifier	**0.4.0.194112.1.2**	Sí			OID	QCP-n-qscd. Identificador de la política de certificado cualificado de persona física con dispositivo seguro
2.5. Subject Alternative Names		Sí	No			OID 2.5.29.17 (Marcado como NO crítico según EN 319412-2)
2.5.1. DirectoryName	Nombre de la persona física (como consta en el DNI/NIE)	Sí				OID 1.3.6.1.4.1.47155.1.1
	Apellido primero de la persona física (como consta en el DNI/NIE)	Sí				OID 1.3.6.1.4.1.47155.1.2
	Apellido segundo de la persona física (como consta en el DNI/NIE)	Sí				OID 1.3.6.1.4.1.47155.1.3
	NIF del titular acorde a ETSI EN 319 412-1 "IDCES-123456789Z")	Sí			PrintableString	OID 1.3.6.1.4.1.47155.1.4
2.5.2. rfc822Name	Correo electrónico de la persona física	Sí			rfc822Name	
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			OID	
2.6.2. Email protection	Presente (1.3.6.1.5.5.7.3.4)	Sí			OID	Sólo se activa si se incluye el correo electrónico del firmante
2.7. cRLDistributionPoint		No	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			IA5String	uniformResourceIdentifier **(NO HTTPS)**
2.7.2. distributionPoint	http://crl2.vincasing.net/canebula2.crl	Sí			IA5String	uniformResourceIdentifier **(NO HTTPS)**
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. Access Description		Sí				
2.8.1.1. Acces Method	id-ad-ocsp	Sí			OID	OID 1.3.6.1.5.5.7.48.1
2.8.1.2. Acces Location	http://ocsp.vincasign.net	Sí			IA5String	URL de acceso al OCSP **(NO HTTPS)** uniformResourceIdentifier
2.8.2. Access Description		Sí				
2.8.2.1. Acces Method	id-ad-calssuers	Sí			OID	OID 1.3.6.1.5.5.7.48.2
2.8.2.1. Acces Location	http://www.vincasign.net/publickeys/casub.crt	Si			IA5String	URL acceso a certificado de la CA (NO HTTPS) uniformResourceIdentifier
2.9. Qualified Certificate Statements		Sí	No			OID 1.3.6.1.5.5.7.1.3
2.9.1. qCCompliance	id-etsi-qcs-QcCompliance	Sí				OID 0.4.0.1862.1.1 Indicación de certificado cualificado
2.9.2. QcEuRetentionPeriod	"15"	Sí				OID 0.4.0.1862.1.3 Plazo de retención de registros
2.9.3. QcSSCD	id-etsi-qcs-QcSSCD	Sí				OID 0.4.0.1862.1.4 Dispositivo cualificado de creación de firma

	2.9.4. QcPDS	{https://www.vincasign.net/policy/es/PDS-PF-hard-IND-EFIM/pds-pf-hard-ind-efim-es.pdf,es},{https://www.vincasign.net/policy/en/PDS-PF-hard-IND-EFIM/pds-pf-hard-ind-efim-en.pdf,en}	Sí				OID 0.4.0.1862.1.5 **(SÍ HTTPS)** URLs de acceso al texto divulgativo en inglés (obligatorio) y en castellano
	2.9.5. QcType	id-etsi-qct-esign	Sí				OID 0.4.0.1862.1.6.1 Certificado de firma electrónica conforme al Reglamento (UE) Nº 910/2014
	2.9.6. qcStatement-2						OID 1.3.6.1.5.5.7.11.2 (RFC 3739)
	2.9.6.1. SemanticsInformation						
	2.9.6.1.1. semanticsIdNatural	0.4.0.194121.1.1					Semántica de persona fisica conforme a EN 319 412-1, en serial number
	2.10. Basic Constraints		Sí	Sí			OID 2.5.29.19
	2.10.1. cA	FALSO	Sí			Boolean	

28. Cert Individual y Efímero de PF en SOFT

Campo Individual y efímero de PF · SOFT	Gestión CENTRALIZADA Identificación, Firma	Oblig.	Crít.	Longitud máxima	Codif	Observaciones OID 1.3.6.1.4.1.47155.1.10.52
1. Basic estructure						
1.1. Version	"2"	Sí		1	Integer	El literal "2" corresponde a la versión 3.
1.2. Serial Number	Establecido automáticamente por la CA. Número identificativo único del certificado.	Sí		20 octetos	Integer	No puede ser un número negativo ni 0.
1.3. Signature Algorithm		Sí				
1.3.1. Algorithm	SHA-256 with RSA Signature	Sí			OID	1.2.840.113549.1.1.11
1.3.2. Parameters	No aplicable	No				
1.4. Issuer		Sí				
1.4.1. Country Name (C)	"ES"	Sí		2 caracteres	PrintableString	OID 2.5.4.6
1.4.2. Organization Name (O)	"VINTEGRIS SL"	Sí		64 caracteres	UTF8String	OID 2.5.4.10
1.4.3. organizationalUnitName (OU)	"vinCAsign"	Sí				OID 2.5.4.11
1.4.4. Locality Name (L)	"HOSPITALET DE LLOBREGAT"	Sí		128 caracteres	UTF8String	OID 2.5.4.7
1.4.5. Organization Identifier	"VATES-B62913926"	Sí		Ilimitado	UTF8String	OID 2.5.4.97
1.4.6. Common Name (CN)	"vinCAsign nebulaSUITE2 Authority"	Sí		64 caracteres	UTF8String	OID 2.5.4.3
1.4.7. stateOrProvinceName	"BARCELONA"	Sí			UTF8String	OID 2.5.4.8
1.5. Validity		Sí				60 minutos
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				
1.6.1. Country Name	"ES"	Sí		2 caracteres	PrintableString	OID 2.5.4.6
1.6.3. Organizational Unit (OU)	Indicación opcional			16 caracteres	UTF8String	OID 2.5.4.11
1.6.6. Serial Number	NIF del titular acorde a ETSI EN 319 412-1 "IDCES-123456789Z")	Sí			PrintableString	OID 2.5.4.5
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. Common Name	APELLIDO1 APELLIDO2 NOMBRE – DNI 1234567892	Sí				OID 2.5.4.3
1.6.10. emailAddress	Correo electrónico del firmante	Sí			IA5String	

1.7. Subject Public Key Info	Clave pública del firmante, codificada en RSA encryption (2048 bits)	Sí				
1.7.1. AlgorithmIdentifier						
1.7.1.1. Algorithm	RSA encryption	Sí			OID	OID 1.2.840.113549.1.1.1
1.7.1.2. Parameters	No aplicable	No				
1.7.2. SubjectPublicKey	Clave pública del firmante	Sí			Bit String	
2. Extensions						
2.1. Authority Key Identifier	Identificador de la clave del emisor	Sí	No			OID 2.5.29.35 (Marcado como NO crítico según EN 319412-2)
2.1.1. KeyIdentifier		Sí			Octet string	Derivado de la clave pública
2.1.2. AuthorityCertIssuer	Nombre de la CA a la que corresponde la clave identificada en keyIdentifier					(String UTF8) Size 12
2.1.3. AuthorityCertSerialNumber	Número de serie del certificado de CA					
2.2. Subject Key Identifier	Identificador de la clave del firmante	Sí	No			OID 2.5.29.14 (Marcado como NO crítico según EN 319412-2)
2.2.1. KeyIdentifier		Sí			Octet string	Derivado de la clave pública
2.3. Key Usage		Sí	Sí		Bit String	OID 2.5.29.15
2.3.1. Digital Signature	**Seleccionado "1"**	Sí				Bit para autenticación
2.3.2. Content commintment	**Seleccionado "1"**	Sí				Bit para firma
2.3.3. Key Encipherment	**Seleccionado "1"**	Sí				
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"					
2.3.8. Encipher Only	No seleccionado. "0"					
2.3.9. Decipher Only	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 Information		Sí				
2.4.1.1. Policy Identifier	**1.3.6.1.4.1.47155.1.10.52**	Sí			OID	Identificador de la política de Logalty
2.4.1.2. Policy Qualifiers		Sí				
2.4.1.1.1 CPS URI	https://policy.vincasign.net				IA5String	URL de la DPC (opcional por CAB FORUM)
2.4.1.1.2. User Notice/Explicit text	"Certificado cualificado y efimero de persona física emitido en SOFT. Ver https://policy.vincasign.net "	Sí		200 caracteres	UTF8String y NFC	Texto indicativo
2.4.2. Policy Information		Sí				

2.4.2.1. Policy Identifier	**0.4.0.194112.1.0**	Sí			OID	QCP-n. Identificador de la política de certificado cualificado de persona física sin uso de dispositivo seguro
2.5. Subject Alternative Names		Sí	No			OID 2.5.29.17 (Marcado como NO crítico según EN 319412-2)
2.5.1. DirectoryName	Nombre de la persona física (como consta en el DNI/NIE)	Sí				OID 1.3.6.1.4.1.47155.1.1
	Apellido primero de la persona física (como consta en el DNI/NIE)	Sí				OID 1.3.6.1.4.1.47155.1.2
	Apellido segundo de la persona física (como consta en el DNI/NIE)	Sí				OID 1.3.6.1.4.1.47155.1.3
	NIF del titular acorde a ETSI EN 319 412-1 "IDCES-123456789Z")	Sí			PrintableString	OID 1.3.6.1.4.1.47155.1.4
2.5.2. rfc822Name	Correo electrónico de la persona física	Sí			rfc822Name	
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			OID	
2.6.2. Email protection	Presente (1.3.6.1.5.5.7.3.4)	Sí			OID	Sólo se activa si se incluye el correo electrónico del firmante
2.7. cRLDistributionPoint		No	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			IA5String	uniformResourceIdentifier **(NO HTTPS)**
2.7.2. distributionPoint	http://crl2.vincasing.net/canebula2.crl	Sí			IA5String	uniformResourceIdentifier **(NO HTTPS)**
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. Access Description		Sí				
2.8.1.1. Acces Method	id-ad-ocsp	Sí			OID	OID 1.3.6.1.5.5.7.48.1
2.8.1.2. Acces Location	http://ocsp.vincasign.net	Sí			IA5String	URL de acceso al OCSP **(NO HTTPS)** uniformResourceIdentifier
2.8.2. Access Description		Sí				
2.8.2.1. Acces Method	id-ad-calssuers	Sí			OID	OID 1.3.6.1.5.5.7.48.2
2.8.2.1. Acces Location	http://www.vincasign.net/publickeys/casub.crt	Si			IA5String	URL acceso a certificado de la CA (NO HTTPS) uniformResourceIdentifier
2.9. Qualified Certificate Statements		Sí	No			OID 1.3.6.1.5.5.7.1.3
2.9.1. qCCompliance	id-etsi-qcs-QcCompliance	Sí				OID 0.4.0.1862.1.1 Indicación de certificado cualificado
2.9.2. QcEuRetentionPeriod	"15"	Sí				OID 0.4.0.1862.1.3 Plazo de retención de registros

	2.9.4. QcPDS	{https://www.vincasign.net/policy/es/PDS-PF-soft-IND-EFIM/pds-pf-soft-ind-efim-es.pdf,es},{https://www.vincasign.net/policy/en/PDS-PF-soft-IND-EFIM/pds-pf-soft-ind-efim-en.pdf,en}	Sí				OID 0.4.0.1862.1.5 **(SÍ HTTPS)** URLs de acceso al texto divulgativo en inglés (obligatorio) y en castellano
	2.9.5. QcType	id-etsi-qct-esign	Sí				OID 0.4.0.1862.1.6.1 Certificado de firma electrónica conforme al Reglamento (UE) Nº 910/2014
	2.9.6. qcStatement-2						OID 1.3.6.1.5.5.7.11.2 (RFC 3739)
	2.9.6.1. SemanticsInformation						
	2.9.6.1.1. semanticsIdNatural	0.4.0.194121.1.1					Semántica de persona fisica conforme a EN 319 412-1, en serial number
	2.10. Basic Constraints		Sí	Sí			OID 2.5.29.19
	2.10.1. cA	FALSO	Sí			Boolean	

29. Cert Persona física Representante AGIF en DCCF

Campo REPRESENTANT AGID · DCCF	Gestión CENTRALIZADA Identificación y Firma	Oblig.	Crít.	Longitud máxima	Codif	Observaciones OID 1.3.6.1.4.1.47155.1.11.1
1. Basic estructure						
1.1. Version	"2"	Sí		1	Integer	El literal "2" corresponde a la versión 3.
1.2. Serial Number	Establecido automáticamente por la CA. Número identificativo único del certificado.	Sí		20 octetos	Integer	No puede ser un número negativo ni 0.
1.3. Signature Algorithm		Sí				
1.3.1. Algorithm	SHA-256 with RSA Signature	Sí			OID	1.2.840.113549.1.1.11
1.3.2. Parameters	No aplicable	No				
1.4. Issuer		Sí				
1.4.1. Country Name (C)	"ES"	Sí		2 caracteres	PrintableString	OID 2.5.4.6
1.4.2. Organization Name (O)	"VINTEGRIS SL"	Sí		64 caracteres	UTF8String	OID 2.5.4.10
1.4.3. organizationalUnitName (OU)	"vinCAsign"	Sí				OID 2.5.4.11
1.4.4. Locality Name (L)	"HOSPITALET DE LLOBREGAT"	Sí		128 caracteres	UTF8String	OID 2.5.4.7
1.4.5. Organization Identifier	"VATES-B62913926"	Sí		Ilimitado	UTF8String	OID 2.5.4.97
1.4.6. Common Name (CN)	"vinCAsign nebulaSUITE2 Authority"	Sí		64 caracteres	UTF8String	OID 2.5.4.3
1.4.7. stateOrProvinceName	"BARCELONA"	Sí			UTF8String	OID 2.5.4.8
1.5. Validity		Sí				3 YEAR
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				
1.6.1. Country Name	"ES"	Sí		2 caracteres	PrintableString	OID 2.5.4.6
1.6.2. Organization (O)	Organización a la que pertenece el representante.	Sí		40 caracteres	UTF8String	OID 2.5.4.10
1.6.6. Serial Number	NIF del titular acorde a ETSI EN 319 412-1 "IDCES-123456789Z")	Sí			PrintableString	OID 2.5.4.5
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. Common Name	123456789Z Nombre Apellido (R: Q0000000J)	Sí				OID 2.5.4.3
1.6.10. Description	Codificación del documento público que acredita las facultades del firmante o los datos registrales	Sí				OID 2.5.4.13
1.7. Subject Public Key Info	Clave pública del firmante, codificada en RSA encryption (2048 bits)	Sí				

1.7.1. AlgorithmIdentifier						
1.7.1.1. Algorithm	RSA encryption	Sí			OID	OID 1.2.840.113549.1.1.1
1.7.1.2. Parameters	No aplicable	No				
1.7.2. SubjectPublicKey	Clave pública del firmante	Sí			Bit String	
2. Extensions						
2.1. Authority Key Identifier	Identificador de la clave del emisor	Sí	No			OID 2.5.29.35 (Marcado como NO crítico según EN 319412-2)
2.1.1. KeyIdentifier		Sí			Octet string	Derivado de la clave pública
2.1.2. AuthorityCertIssuer	Nombre de la CA a la que corresponde la clave identificada en keyIdentifier					(String UTF8) Size 12
2.1.3. AuthorityCertSerialNumber	Número de serie del certificado de CA					
2.2. Subject Key Identifier	Identificador de la clave del firmante	Sí	No			OID 2.5.29.14 (Marcado como NO crítico según EN 319412-2)
2.2.1. KeyIdentifier		Sí			Octet string	Derivado de la clave pública
2.3. Key Usage		Sí	Sí		Bit String	OID 2.5.29.15
2.3.1. Digital Signature	**Seleccionado "1"**	Sí				Bit para autenticación
2.3.2. Content commintment	**Seleccionado "1"**	Sí				Bit para firma
2.3.3. Key Encipherment	No seleccionado. "0"					
2.3.4. Data Encipherment	No seleccionado. "0"					
2.3.5. Key Agreement	No seleccionado. "0"					
2.3.6. Key Certificate Signature	No seleccionado. "0"					
2.3.7. CRL Signature	No seleccionado. "0"					
2.3.8. Encipher Only	No seleccionado. "0"					
2.3.9. Decipher Only	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 Information		Sí				
2.4.1.1. Policy Identifier	**1.3.6.1.4.1.47155.1.11.1**	Sí			OID	Identificador de la política de Vintegris
2.4.1.2. Policy Qualifiers		Sí				
2.4.1.1.1 CPS URI	https://policy.vincasign.net				IA5String	URL de la DPC (opcional por CAB FORUM)
2.4.1.1.2. User Notice/Explicit text	"Certificado cualificado europeo de persona física representante emitido en un DCCF. Ver https://policy.vincasign.net "	Sí		200 caracteres	UTF8String y NFC	Texto indicativo
2.4.2. Policy Information		Sí				
2.4.2.1. Policy Identifier	**0.4.0.194112.1.2**	Sí			OID	QCP-n-qscd. Identificador de la política de certificado cualificado de persona física con dispositivo seguro
2.5. Subject Alternative Names		Sí	No			OID 2.5.29.17 (Marcado como NO crítico según EN 319412-2)

2.5.1. rfc822Name	Correo electrónico de la persona física	Sí			rfc822Name	
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			OID	
2.6.2. Email protection	Presente (1.3.6.1.5.5.7.3.4)	Sí			OID	Sólo se activa si se incluye el correo electrónico del firmante
2.7. cRLDistributionPoint		No	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			IA5String	uniformResourceIdentifier **(NO HTTPS)**
2.7.2. distributionPoint	http://crl2.vincasing.net/canebula2.crl	Sí			IA5String	uniformResourceIdentifier **(NO HTTPS)**
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. Access Description		Sí				
2.8.1.1. Acces Method	id-ad-ocsp	Sí			OID	OID 1.3.6.1.5.5.7.48.1
2.8.1.2. Acces Location	http://ocsp.vincasign.net	Sí			IA5String	URL de acceso al OCSP **(NO HTTPS)** uniformResourceIdentifier
2.8.2. Access Description		Sí				
2.8.2.1. Acces Method	id-ad-caIssuers	Sí			OID	OID 1.3.6.1.5.5.7.48.2
2.8.2.1. Acces Location	http://www.vincasign.net/publickeys/casub.crt	Si			IA5String	URL acceso a certificado de la CA (NO HTTPS) uniformResourceIdentifier
2.9. Qualified Certificate Statements		Sí	No			OID 1.3.6.1.5.5.7.1.3
2.9.1. qCCompliance	id-etsi-qcs-QcCompliance	Sí				OID 0.4.0.1862.1.1 Indicación de certificado cualificado
2.9.2. QcEuRetentionPeriod	"15"	Sí				OID 0.4.0.1862.1.3 Plazo de retención de registros
2.9.3. QcSSCD	id-etsi-qcs-QcSSCD	Sí				OID 0.4.0.1862.1.4 Dispositivo cualificado de creación de firma
2.9.4. QcPDS	{https://www.vincasign.net/policy/es/PDS-REPAGID-hard/pds-rep-hard-es.pdf,es},{https://www.vincasign.net/policy/en/PDS-REPAGID-hard/pds-rep-hard-en.pdf,en}	Sí				OID 0.4.0.1862.1.5 **(SÍ HTTPS)** URLs de acceso al texto divulgativo en inglés (obligatorio) y en castellano
2.9.5. QcType	id-etsi-qct-esign	Sí				OID 0.4.0.1862.1.6.1 Certificado de firma electrónica conforme al Reglamento (UE) Nº 910/2014
2.9.6. qcStatement-2						OID 1.3.6.1.5.5.7.11.2 (RFC 3739)
2.9.6.1. SemanticsInformation						
2.9.6.1.1. semanticsIdNatural	0.4.0.194121.1.1					Semántica de persona fisica conforme a EN 319 412-1, en serial number
2.10. Basic Constraints		Sí	Sí			OID 2.5.29.19
2.10.1. cA	FALSO	Sí			Boolean	

30. Cert Persona física Representante AGIF en SOFT

Campo REPRESENTANT AGID · SOFT	Gestión CENTRALIZADA Identificación y Firma	Oblig.	Crít.	Longitud máxima	Codif	Observaciones OID 1.3.6.1.4.1.47155.1.11.2
1. Basic estructure						
1.1. Version	"2"	Sí		1	Integer	El literal "2" corresponde a la versión 3.
1.2. Serial Number	Establecido automáticamente por la CA. Número identificativo único del certificado.	Sí		20 octetos	Integer	No puede ser un número negativo ni 0.
1.3. Signature Algorithm		Sí				
1.3.1. Algorithm	SHA-256 with RSA Signature	Sí			OID	1.2.840.113549.1.1.11
1.3.2. Parameters	No aplicable	No				
1.4. Issuer		Sí				
1.4.1. Country Name (C)	"ES"	Sí		2 caracteres	PrintableString	OID 2.5.4.6
1.4.2. Organization Name (O)	"VINTEGRIS SL"	Sí		64 caracteres	UTF8String	OID 2.5.4.10
1.4.3. organizationalUnitName (OU)	"vinCAsign"	Sí				OID 2.5.4.11
1.4.4. Locality Name (L)	"HOSPITALET DE LLOBREGAT"	Sí		128 caracteres	UTF8String	OID 2.5.4.7
1.4.5. Organization Identifier	"VATES-B62913926"	Sí		Ilimitado	UTF8String	OID 2.5.4.97
1.4.6. Common Name (CN)	"vinCAsign nebulaSUITE2 Authority"	Sí		64 caracteres	UTF8String	OID 2.5.4.3
1.4.7. stateOrProvinceName	"BARCELONA"	Sí			UTF8String	OID 2.5.4.8
1.5. Validity		Sí				3 YEAR
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				
1.6.1. Country Name	"ES"	Sí		2 caracteres	PrintableString	OID 2.5.4.6
1.6.2. Organization (O)	Organización a la que pertenece el representante.	Sí		40 caracteres	UTF8String	OID 2.5.4.10
1.6.6. Serial Number	NIF del titular acorde a ETSI EN 319 412-1 "IDCES-123456789Z")	Sí			PrintableString	OID 2.5.4.5
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. Common Name	123456789Z Nombre Apellido (R: Q0000000J)	Sí				OID 2.5.4.3
1.6.10. Description	Codificación del documento público que acredita las facultades del firmante o los datos registrales	Sí				OID 2.5.4.13
1.7. Subject Public Key Info	Clave pública del firmante, codificada en RSA encryption (2048 bits)	Sí				
1.7.1. AlgorithmIdentifier						
1.7.1.1. Algorithm	RSA encryption	Sí			OID	OID 1.2.840.113549.1.1.1
1.7.1.2. Parameters	No aplicable	No				
1.7.2. SubjectPublicKey	Clave pública del firmante	Sí			Bit String	

2. Extensions						
2.1. Authority Key Identifier	Identificador de la clave del emisor	Sí	No			OID 2.5.29.35 (Marcado como NO crítico según EN 319412-2)
2.1.1. KeyIdentifier		Sí			Octet string	Derivado de la clave pública
2.1.2. AuthorityCertIssuer	Nombre de la CA a la que corresponde la clave identificada en keyIdentifier					(String UTF8) Size 12
2.1.3. AuthorityCertSerialNumber	Número de serie del certificado de CA					
2.2. Subject Key Identifier	Identificador de la clave del firmante	Sí	No			OID 2.5.29.14 (Marcado como NO crítico según EN 319412-2)
2.2.1. KeyIdentifier		Sí			Octet string	Derivado de la clave pública
2.3. Key Usage		Sí	Sí		Bit String	OID 2.5.29.15
2.3.1. Digital Signature	**Seleccionado "1"**	Sí				Bit para autenticación
2.3.2. Content commintment	**Seleccionado "1"**	Sí				Bit para firma
2.3.3. Key Encipherment	No seleccionado. "0"					
2.3.4. Data Encipherment	No seleccionado. "0"					
2.3.5. Key Agreement	No seleccionado. "0"					
2.3.6. Key Certificate Signature	No seleccionado. "0"					
2.3.7. CRL Signature	No seleccionado. "0"					
2.3.8. Encipher Only	No seleccionado. "0"					
2.3.9. Decipher Only	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 Information		Sí				
2.4.1.1. Policy Identifier	**1.3.6.1.4.1.47155.1.2.2**	Sí			OID	Identificador de la política de Vintegirs
2.4.1.2. Policy Qualifiers		Sí				
2.4.1.1.1 CPS URI	https://policy.vincasign.net				IA5String	URL de la DPC (opcional por CAB FORUM)
2.4.1.1.2. User Notice/Explicit text	"Certificado cualificado europeo de persona física representante emitido en software. Ver https://policy.vincasign.net "	Sí		200 caracteres	UTF8String y NFC	Texto indicativo
2.4.2. Policy Information		Sí				
2.4.2.1. Policy Identifier	**0.4.0.194112.1.0**	Sí			OID	QCP-n-qscd. Identificador de la política de certificado cualificado de persona física sin uso de dispositivo seguro
2.5. Subject Alternative Names		Sí	No			OID 2.5.29.17 (Marcado como NO crítico según EN 319412-2)
2.5.1. rfc822Name	Correo electrónico de la persona física	Sí			rfc822Name	
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			OID	

2.6.2. Email protection	Presente (1.3.6.1.5.5.7.3.4)	Sí			OID	Sólo se activa si se incluye el correo electrónico del firmante
2.7. cRLDistributionPoint		No	No			OID 2.5.29.31 Este apartado no es obligatorio siempre que exista la funcionalidad de
2.7.1. distributionPoint	http://crl1.vincasign.net/canebula2.crl	Sí			IA5String	uniformResourceIdentifier **(NO HTTPS)**
2.7.2. distributionPoint	http://crl2.vincasing.net/canebula2.crl	Sí			IA5String	uniformResourceIdentifier **(NO HTTPS)**
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. Access Description		Sí				
2.8.1.1. Acces Method	id-ad-ocsp	Sí			OID	OID 1.3.6.1.5.5.7.48.1
2.8.1.2. Acces Location	http://ocsp.vincasign.net	Sí			IA5String	URL de acceso al OCSP **(NO HTTPS)** uniformResourceIdentifier
2.8.2. Access Description		Sí				
2.8.2.1. Acces Method	id-ad-calssuers	Sí			OID	OID 1.3.6.1.5.5.7.48.2
2.8.2.1. Acces Location	http://www.vincasign.net/publickeys/casub.crt	Si			IA5String	URL acceso a certificado de la CA (NO HTTPS) uniformResourceIdentifier
2.9. Qualified Certificate Statements		Sí	No			OID 1.3.6.1.5.5.7.1.3
2.9.1. qCCompliance	id-etsi-qcs-QcCompliance	Sí				OID 0.4.0.1862.1.1 Indicación de certificado cualificado
2.9.2. QcEuRetentionPeriod	"15"	Sí				OID 0.4.0.1862.1.3 Plazo de retención de registros
2.9.4. QcPDS	{https://www.vincasign.net/policy/es/PDS-REPAGID-soft/pds-rep-soft-es.pdf,es},{https://www.vincasign.net/policy/en/PDS-REPAGID-soft/pds-rep-soft-en.pdf,en}	Sí				OID 0.4.0.1862.1.5 **(SÍ HTTPS)** URLs de acceso al texto divulgativo en inglés (obligatorio) y en castellano
2.9.5. QcType	id-etsi-qct-esign	Sí				OID 0.4.0.1862.1.6.1 Certificado de firma electrónica conforme al Reglamento (UE) Nº
2.9.6. qcStatement-2						OID 1.3.6.1.5.5.7.11.2 (RFC 3739)
2.9.6.1. SemanticsInformation						
2.9.6.1.1. semanticsIdNatural	0.4.0.194121.1.1					Semántica de persona física conforme a EN 319 412-1, en serial number
2.10. Basic Constraints		Sí	Sí			OID 2.5.29.19
2.10.1. cA	FALSO	Sí			Boolean	