Perfiles de Certificados ENTIDAD

FINAL

Control de versiones

Versión	Partes que cambian	Descripción del cambio	Autor del cambio	Fecha del cambio
1.0		Creación documento	vinCAsign	08/03/2016
1.1		Revisión perfiles de REPRESENTANTE para @firma	vinCAsign	27/07/2016

1. Índice

2. Certificado de PERSONA FÍSICA vinculada a una Organización (en DSCF)

2.1. Perfil único para firma y autenticación.

Campo	Contenido	Obligatorio	Crítico
1. Basic estructure			
1.1. Version	"2"	Sí	
1.2. Serial Number	Establecido automáticamente por la CA. Número identificativo **único** del certificado.	Sí	
1.3. Signature Algorithm		Sí	
1.3.1. Identifier	1.2.840.113549.1.1.11	Sí	
1.3.2. Description	SHA-2 with RSA Signature[1]	Sí	
1.4. **Issuer Distinguished Name**		Sí	
1.4.1. Country (C)	"ES"	Sí	
1.4.2. Organization (O)	"VINTEGRIS SL"	Si	

[1] No usar el algoritmo SHA-1 por recomendación de la ETSI TS 119 312.

Campo	Contenido	Obligatorio	Crítico
1.4.3. Locality (L)	"Barcelona (see current address at https://www.vincasign.net/contact)"		
1.4.4. Organizational Unit (OU)	"EC-VINTEGRIS"		
1.4.5. Serial Number	"B62913926"	Sí	
1.4.6. Common Name (CN)	"vinCAsign Global Authority"	Sí	
1.5. Validity		Sí	
1.5.1. Not Before	Fecha de inicio de la validez	Si	
1.5.2. Not After	Fecha de expiración	Si	
1.6. Subject		Sí	
1.6.1. Country (C)	"ES"	Sí	
1.6.2. Organization (O)	Organización a la que pertenece el suscriptor.	Si	
1.6.3. organizationalUnitName (OU)	Primera Indicación del Departamento en la Organización a la que pertenece el firmante u otra información sobre la Organización.	Sí	
1.6.4. organizationalUnitName (OU)	Segunda Indicación del Departamento en la Organización a la que pertenece el firmante u otra información sobre la Organización..		

Campo	Contenido	Obligatorio	Crítico
1.6.5. Surname	Apellido/s de la persona física firmante	Sí	
1.6.6. Given Name	Nombre de la persona física firmante	Sí	
1.6.7. Title	Cargo del firmante en la organización		
1.6.8. Serial Number	Número de identificación de la persona física firmante	Sí	
1.6.9. Common Name (CN)		Sí	
1.6.10. emailAddress (EA)	Correo electrónico del firmante	Sí	
1.7. Subject Public Key Info	2048-Bit Public key encoded in accordance with RFC3279	Sí	
2. Extensions			
2.1. Authority Key Identifier	Presente	Sí	No
2.1.1. Key Identifier			
2.2. Subject Key Identifier	Presente	Sí	NO
2.3. Key Usage		Sí	Sí
2.3.1. Digital Signature	Seleccionado. “1”	Sí	
2.3.2. contentCommitment	Seleccionado. “1”	Sí	

Campo	Contenido	Obligatorio	Crítico
2.3.3. Key Encipherment	No seleccionado. "0"	Sí	
2.3.4. Data Encipherment	No seleccionado. "0"	Sí	
2.3.5. Key Agreement	No seleccionado. "0"		
2.3.6. Key Certificate Signature	No seleccionado. "0"		
2.3.7. CRL Signature	No seleccionado. "0"		
2.4. Certificate Policies		Sí	NO
2.4.1. Policy Identifier	1.3.6.1.4.1.**47155.1.1.1**	Sí	
2.4.2. Policy Qualifier ID		Sí	
2.4.2.1. CPS Pointer	https://policy.vincasign.net	Sí	
2.4.2.2. User Notice	"Certificado reconocido de persona física vinculada emitido en DSCF. Ver https://policy.vincasign.net"	Sí	
2.5. Subject Alternative Names		Sí	NO
2.5.1. rfc822Name	Correo electrónico de la persona física		
2.6. Issuer Alternative Name			NO

Campo	Contenido	Obligatorio	Crítico
2.7. Extended Key Usages		Sí	NO
2.7.1. emailProtection	Presente	Sí	
2.7.2. clientAuth	Presente	Sí	
2.8. cRLDistributionPoint			NO
2.8.1. distributionPoint	http://crl1.vincasign.net/casub.crl	Sí	
2.8.2. distributionPoint	http://crl2.vincasign.net/casub.crl	Sí	
2.9. Authority Info Acces		Sí	NO
2.9.1. Access Method	Id-ad-ocsp	Sí	
2.9.1.1. Acces Location	http://ocsp1.vincasign.net	Sí	
2.9.1.2. Acces Location	http://ocsp2.vincasign.net		
2.9.2. calssuersAccessMethod	id-ad-calssuers	Sí	
2.9.2.1. Acces Location	http://www.vincasign.net/publickeys/casub.crt	Sí	
2.10. NetscapeCertType	"SSL client", "S/MIME"		
2.11. Qualified Certificate Statements		Sí	No
2.11.1. esi4-qcStatement-1	Presente	Sí	

Campo		Contenido	Obligatorio	Crítico
2.11.2.	esi4-qcStatement-3	"15"	Sí	
2.11.3.	esi4-qcStatement-4	Presente	Sí	
2.11.4.	esi4-qcStatement-5	https://www.vincasign.net/policy/PDS-en-PF-hard/	Sí	
2.12.	Subject Directory Attributes			NO
2.12.1.	Country of Citizenship	Nacionalidad		
2.12.2.	Country of Residence	País de residencia		

3. Certificado de PERSONA FÍSICA vinculada a una Organización (en software)

3.1. Perfil único para firma y autenticación.

Campo	Contenido	Obligatorio	Crítico
1. Basic estructure			
1.1. Version	"2"	Sí	
1.2. Serial Number	Establecido automáticamente por la CA. Número identificativo **único** del certificado.	Sí	
1.3. Signature Algorithm		Sí	
1.3.1. Identifier	1.2.840.113549.1.1.11	Sí	
1.3.2. Description	SHA-2 with RSA Signature[2]	Sí	
1.4. **Issuer Distinguished Name**		Sí	
1.4.1. Country (C)	"ES"	Sí	
1.4.2. Organization (O)	"VINTEGRIS SL"	Si	

[2] No usar el algoritmo SHA-1 por recomendación de la ETSI TS 119 312.

Campo	Contenido	Obligatorio	Crítico
1.4.3. Locality (L)	"Barcelona (see current address at https://www.vincasign.net/contact)"		
1.4.4. Organizational Unit (OU)	"EC-VINTEGRIS"		
1.4.5. Serial Number	"B62913926"	Sí	
1.4.6. Common Name (CN)	"vinCAsign Global Authority"	Sí	
1.5. Validity		Sí	
1.5.1. Not Before	Fecha de inicio de la validez	Si	
1.5.2. Not After	Fecha de expiración	Si	
1.6. Subject		Sí	
1.6.1. Country (C)	"ES"	Sí	
1.6.2. Organization (O)	Organización a la que pertenece el suscriptor.	Si	
1.6.3. organizationalUnitName (OU)	Primera Indicación del Departamento en la Organización a la que pertenece el firmante u otra información sobre la Organización.	Sí	
1.6.4. organizationalUnitName (OU)	Segunda Indicación del Departamento en la Organización a la que pertenece el firmante u otra información sobre la Organización..		

Campo	Contenido	Obligatorio	Crítico
1.6.5. Surname	Apellido/s de la persona física firmante	Sí	
1.6.6. Given Name	Nombre de la persona física firmante	Sí	
1.6.7. Title	Cargo del firmante en la organización		
1.6.8. Serial Number	Número de identificación de la persona física firmante	Sí	
1.6.9. Common Name (CN)		Sí	
1.6.10. emailAddress (EA)	Correo electrónico del firmante	Sí	
1.7. Subject Public Key Info	2048-Bit Public key encoded in accordance with RFC3279	Sí	
2. Extensions			
2.1. Authority Key Identifier	Presente	Sí	No
2.1.1. Key Identifier			
2.2. Subject Key Identifier	Presente	Sí	NO
2.3. Key Usage		Sí	Sí
2.3.1. Digital Signature	Seleccionado. “1”	Sí	
2.3.2. contentCommitment	Seleccionado. “1”	Sí	

Campo	Contenido	Obligatorio	Crítico
2.3.3. Key Encipherment	No seleccionado. "0"	Sí	
2.3.4. Data Encipherment	No seleccionado. "0"	Sí	
2.3.5. Key Agreement	No seleccionado. "0"		
2.3.6. Key Certificate Signature	No seleccionado. "0"		
2.3.7. CRL Signature	No seleccionado. "0"		
2.4. Certificate Policies		Sí	NO
2.4.1. Policy Identifier	1.3.6.1.4.1.**47155.1.1.2**	Sí	
2.4.2. Policy Qualifier ID		Sí	
2.4.2.1. CPS Pointer	https://policy.vincasign.net	Sí	
2.4.2.2. User Notice	"Certificado reconocido de persona física vinculada emitido en software. Ver https://policy.vincasign.net"	Sí	
2.5. Subject Alternative Names		Sí	NO
2.5.1. rfc822Name	Correo electrónico de la persona física		
2.6. Issuer Alternative Name			NO

Campo	Contenido	Obligatorio	Crítico
2.7. Extended Key Usages		Sí	NO
2.7.1. emailProtection	Presente	Sí	
2.7.2. clientAuth	Presente	Sí	
2.8. cRLDistributionPoint			NO
2.8.1. distributionPoint	http://crl1.vincasign.net/casub.crl	Sí	
2.8.2. distributionPoint	http://crl2.vincasign.net/casub.crl	Sí	
2.9. Authority Info Acces		Sí	NO
2.9.1. Access Method	Id-ad-ocsp	Sí	
2.9.1.1. Acces Location	http://ocsp1.vincasign.net	Sí	
2.9.1.2. Acces Location	http://ocsp2.vincasign.net		
2.9.2. caIssuersAccessMethod	id-ad-caIssuers	Sí	
2.9.2.1. Acces Location	http://www.vincasign.net/publickeys/casub.crt	Sí	
2.10. NetscapeCertType	"SSL client", "S/MIME"		
2.11. Qualified Certificate Statements		Sí	No
2.11.1. esi4-qcStatement-1	Presente	Sí	

Campo		Contenido	Obligatorio	Crítico
2.11.2.	esi4-qcStatement-3	"15"	Sí	
2.11.3.	esi4-qcStatement-5	https://www.vincasign.net/policy/PDS-en-PF-soft/	Sí	
2.12.	Subject Directory Attributes			NO
2.12.1.	Country of Citizenship	Nacionalidad		
2.12.2.	Country of Residence	País de residencia		

4. Certificado de REPRESENTANTE (en DSCF)

4.1. Perfil único para firma y autenticación.

Campo	Contenido	Obligatorio	Crítico
1. Basic estructure			
1.1. Version	"2"	Sí	
1.2. Serial Number	Establecido automáticamente por la CA. Número identificativo **único** del certificado.	Sí	
1.3. Signature Algorithm		Sí	
1.3.1. Identifier	1.2.840.113549.1.1.11	Sí	
1.3.2. Description	SHA-2 with RSA Signature[3]	Sí	
1.4. **Issuer Distinguished Name**		Sí	
1.4.1. Country (C)	"ES"	Sí	
1.4.2. Organization (O)	"VINTEGRIS SL"	Si	

[3] No usar el algoritmo SHA-1 por recomendación de la ETSI TS 119 312.

Campo	Contenido	Obligatorio	Crítico
1.4.3. Locality (L)	"Barcelona (see current address at https://www.vincasign.net/contact)"		
1.4.4. Organizational Unit (OU)	"EC-VINTEGRIS"		
1.4.5. Serial Number	"B62913926"	Sí	
1.4.6. Common Name (CN)	"vinCAsign Global Authority"	Sí	
1.5. Validity		Sí	
1.5.1. Not Before	Fecha de inicio de la validez	Si	
1.5.2. Not After	Fecha de expiración	Si	
1.6. Subject		Sí	
1.6.1. Country (C)	"ES"	Sí	
1.6.2. Organization (O)	Organización a la que pertenece el representante.	Si	
1.6.3. OrganizationIdentifier	NIF de la persona jurídica representada, en formato ETSI EN 319412-1 (Ejemplo: "VATES-Q0000000J)	Si	
1.6.4. organizationalUnitName (OU)	Departamento de la Organización a la que pertenece el firmante representante u otra	Sí	

Campo	Contenido	Obligatorio	Crítico
	información sobre la Organización.		
1.6.5. organizationalUnitName (OU)	Unidad de la Organización a la que pertenece el firmante representante u otra información sobre la Organización.		
1.6.6. Surname	Apellido/s de la persona física representante (como consta en el DNI/NIE)	Sí	
1.6.7. Given Name	Nombre de la persona física representante (como consta en el DNI/NIE)	Sí	
1.6.8. Title	Representante legal, …		
1.6.9. Serial Number[4]	NIF del titular (NIF es el número y letra que aparece en el DNI o NIE según corresponda "123456789Z") o codificación acorde a ETSI EN 319 412-1 "IDCES-123456789Z")	Sí	
1.6.10. Common Name (CN) [5]	00000000T Juan Casas (R: Q0000000J)	Sí	

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

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

Campo	Contenido	Obligatorio	Crítico
1.6.11. Description (OID 2.5.4.13)[6]	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		
1.6.12. emailAddress (EA)	Correo electrónico del representante	Sí	
1.7. Subject Public Key Info	2048-Bit Public key encoded in accordance with RFC3279	Sí	
2. Extensions			
2.1. Authority Key Identifier	Presente	Sí	No
2.1.1. Key Identifier			
2.2. Subject Key Identifier	Presente	Sí	NO

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

Campo		Contenido	Obligatorio	Crítico
2.3.	Key Usage		Sí	Sí
2.3.1.	Digital Signature	Seleccionado. "1"	Sí	
2.3.2.	contentCommitment	Seleccionado. "1"	Sí	
2.3.3.	Key Encipherment	No seleccionado. "0"	Sí	
2.3.4.	Data Encipherment	No seleccionado. "0"	Sí	
2.3.5.	Key Agreement	No seleccionado. "0"		
2.3.6.	Key Certificate Signature	No seleccionado. "0"		
2.3.7.	CRL Signature	No seleccionado. "0"		
2.4.	Certificate Policies		Sí	NO
2.4.1.	Policy Identifier	1.3.6.1.4.1.**47155.1.2.1**	Sí	
2.4.2.	Policy Identifier[7]	0.4.0.194112.1.2	Sí	

[7] QCP-n, política para los certificados EU cualificados emitidos a personas físicas ("QCP-n-qscd" para los emitidos en tarjeta -con DSCF-).

Campo	Contenido	Obligatorio	Crítico
2.4.3. Policy Identifier[8]	2.16.724.1.3.5.8	Sí	
2.4.4. Policy Qualifier ID		Sí	
2.4.4.1. CPS Pointer	https://policy.vincasign.net	Sí	
2.4.4.2. User Notice	"Certificado cualificado de representante emitido en DSCF. Ver https://policy.vincasign.net"	Sí	
2.5. Subject Alternative Names		Sí	NO
2.5.1. rfc822Name	Correo electrónico de la persona física representante		
2.6. Issuer Alternative Name			NO
2.7. Extended Key Usages		Sí	NO

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

Campo	Contenido	Obligatorio	Crítico
2.7.1. emailProtection	Presente	Sí	
2.7.2. clientAuth	Presente	Sí	
2.8. cRLDistributionPoint			NO
2.8.1. distributionPoint	http://crl1.vincasign.net/casub.crl	Sí	
2.8.2. distributionPoint	http://crl2.vincasign.net/casub.crl	Sí	
2.9. Authority Info Acces		Sí	NO
2.9.1. Access Method	Id-ad-ocsp	Sí	
2.9.1.1. Acces Location	http://ocsp1.vincasign.net	Sí	
2.9.1.2. Acces Location	http://ocsp2.vincasign.net		
2.9.2. caIssuersAccessMethod	id-ad-caIssuers	Sí	
2.9.2.1. Acces Location	http://www.vincasign.net/publickeys/casub.crt	Sí	
2.10. NetscapeCertType	"SSL client", "S/MIME"		
2.11. Qualified Certificate Statements		Sí	No
2.11.1. esi4-qcStatement-1	Presente	Sí	
2.11.2. esi4-qcStatement-2		No	

Campo		Contenido	Obligatorio	Crítico
2.11.3.	esi4-qcStatement-3	"15"	Sí	
2.11.4.	esi4-qcStatement-4	Presente	Sí	
2.11.5.	esi4-qcStatement-5	https://www.vincasign.net/policy/PDS-en-REP-hard/	Sí	
2.11.6.	esi4-qcStatement-6	Qct-esign	Sí	
2.12.				
2.12.1.				
2.12.2.				
2.12.3.				
2.12.4.				
2.12.5.				
2.12.6.				
2.12.7.				

5. Certificado de REPRESENTANTE (en software)

5.1. Perfil único para firma, autenticación y cifrado.

Campo	Contenido	Obligatorio	Crítico
1. Basic estructure			
1.1. Version	"2"	Sí	
1.2. Serial Number	Establecido automáticamente por la CA. Número identificativo **único** del certificado.	Sí	
1.3. Signature Algorithm		Sí	
1.3.1. Identifier	1.2.840.113549.1.1.11	Sí	
1.3.2. Description	SHA-2 with RSA Signature[9]	Sí	
1.4. **Issuer Distinguished Name**		Sí	
1.4.1. Country (C)	"ES"	Sí	
1.4.2. Organization (O)	"VINTEGRIS SL"	Si	

[9] No usar el algoritmo SHA-1 por recomendación de la ETSI TS 119 312.

Campo	Contenido	Obligatorio	Crítico
1.4.3. Locality (L)	"Barcelona (see current address at https://www.vincasign.net/contact)"		
1.4.4. Organizational Unit (OU)	"EC-VINTEGRIS"		
1.4.5. Serial Number	"B62913926"	Sí	
1.4.6. Common Name (CN)	"vinCAsign Global Authority"	Sí	
1.5. Validity		Sí	
1.5.1. Not Before	Fecha de inicio de la validez	Si	
1.5.2. Not After	Fecha de expiración	Si	
1.6. Subject		Sí	
1.6.1. Country (C)	"ES"	Sí	
1.6.2. Organization (O)	Organización a la que pertenece el suscriptor.	Si	
1.6.3. OrganizationIdentifier	NIF de la persona jurídica representada, en formato ETSI EN 319412-1 (Ejemplo: "VATES-Q0000000J)	Sí	
1.6.4. organizationalUnitName (OU)	Departamento de la Organización a la que pertenece el firmante representante u otra información sobre la Organización.	Sí	

Campo	Contenido	Obligatorio	Crítico
1.6.5. organizationalUnitName (OU)	Unidad de la Organización a la que pertenece el firmante representante u otra información sobre la Organización.		
1.6.6. Surname	Apellido/s de la persona física representante (como consta en el DNI/NIE)	Sí	
1.6.7. Given Name	Nombre de la persona física representante (como consta en el DNI/NIE)	Sí	
1.6.8. Title	Representante legal, …		
1.6.9. Serial Number[10]	NIF del titular (NIF es el número y letra que aparece en el DNI o NIE según corresponda "123456789Z") o codificación acorde a ETSI EN 319 412-1 "IDCES-123456789Z")	Sí	
1.6.10. Common Name (CN) [11]	00000000T Juan Casas (R: Q0000000J)	Sí	

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

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

Campo	Contenido	Obligatorio	Crítico
1.6.11. Description (OID 2.5.4.13)[12]	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		
1.6.12. emailAddress (EA)	Correo electrónico del representante	Sí	
1.7. Subject Public Key Info	2048-Bit Public key encoded in accordance with RFC3279	Sí	
2. Extensions			
2.1. Authority Key Identifier	Presente	Sí	No
2.1.1. Key Identifier			
2.2. Subject Key Identifier	Presente	Sí	NO

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

Campo		Contenido	Obligatorio	Crítico
2.3.	Key Usage		Sí	Sí
2.3.1.	Digital Signature	Seleccionado. "1"	Sí	
2.3.2.	contentCommitment	Seleccionado. "1"	Sí	
2.3.3.	Key Encipherment	No seleccionado. "0"	Sí	
2.3.4.	Data Encipherment	No seleccionado. "0"	Sí	
2.3.5.	Key Agreement	No seleccionado. "0"		
2.3.6.	Key Certificate Signature	No seleccionado. "0"		
2.3.7.	CRL Signature	No seleccionado. "0"		
2.4.	Certificate Policies		Sí	NO
2.4.1.	Policy Identifier	1.3.6.1.4.1.**47155.1.2.2**	Sí	
2.4.2.	Policy Identifier[13]	0.4.0.194112.1.0	Sí	

[13] QCP-n, política para los certificados EU cualificados emitidos a personas físicas ("QCP-n" para los emitidos en software -sin DSCF-).

Campo	Contenido	Obligatorio	Crítico
2.4.3. Policy Identifier[14]	2.16.724.1.3.5.8	Sí	
2.4.4. Policy Qualifier ID		Sí	
2.4.4.1. CPS Pointer	https://policy.vincasign.net	Sí	
2.4.4.2. User Notice	"Certificado cualificado de representante emitido en software. Ver https://policy.vincasign.net"	Sí	
2.5. Subject Alternative Names		Sí	NO
2.5.1. rfc822Name	Correo electrónico de la persona física representante		
2.6. Issuer Alternative Name			NO
2.7. Extended Key Usages		Sí	NO

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

Campo	Contenido	Obligatorio	Crítico
2.7.1. emailProtection	Presente	Sí	
2.7.2. clientAuth	Presente	Sí	
2.8. cRLDistributionPoint			NO
2.8.1. distributionPoint	http://crl1.vincasign.net/casub.crl	Sí	
2.8.2. distributionPoint	http://crl2.vincasign.net/casub.crl	Sí	
2.9. Authority Info Acces		Sí	NO
2.9.1. Access Method	Id-ad-ocsp	Sí	
2.9.1.1. Acces Location	http://ocsp1.vincasign.net	Sí	
2.9.1.2. Acces Location	http://ocsp2.vincasign.net		
2.9.2. calssuersAccessMethod	id-ad-calssuers	Sí	
2.9.2.1. Acces Location	http://www.vincasign.net/publickeys/casub.crt	Sí	
2.10. NetscapeCertType	"SSL client", "S/MIME"		
2.11. Qualified Certificate Statements		Sí	No
2.11.1. esi4-qcStatement-1	Presente	Sí	
2.11.2. esi4-qcStatement-2		No	

Campo		Contenido	Obligatorio	Crítico
2.11.3.	esi4-qcStatement-3	"15"	Sí	
2.11.4.	esi4-qcStatement-5	https://www.vincasign.net/policy/PDS-en-REP-soft/	Sí	
2.11.5.	esi4-qcStatement-6	Qct-esign	Sí	
2.12.				
2.12.1.				
2.12.2.				
2.12.3.				
2.12.4.				
2.12.5.				
2.12.6.				
2.12.7.				

6. Certificado de persona física EMPLEADO PÚBLICO (Nivel Alto)

6.1. Perfil único para firma y autenticación.

Campo	Contenido	Obligatorio	Crítico
1. Basic estructure			
1.1. Version	"2"	Sí	
1.2. Serial Number	Establecido automáticamente por la CA. Número identificativo **único** del certificado.	Sí	
1.3. Signature Algorithm		Sí	
1.3.1. Identifier	1.2.840.113549.1.1.11	Sí	
1.3.2. Description	SHA-2 with RSA Signature[15]	Sí	
1.4. **Issuer Distinguished Name**		Sí	
1.4.1. Country (C)	"ES"	Sí	
1.4.2. Organization (O)	"VINTEGRIS SL"	Si	

[15] No usar el algoritmo SHA-1 por recomendación de la ETSI TS 119 312.

Campo	Contenido	Obligatorio	Crítico
1.4.3. Locality (L)	"Barcelona (see current address at https://www.vincasign.net/contact)"		
1.4.4. Organizational Unit (OU)	"EC-VINTEGRIS"		
1.4.5. Serial Number	"B62913926"	Sí	
1.4.6. Common Name (CN)	"vinCAsign Global Authority"	Sí	
1.5. Validity		Sí	
1.5.1. Not Before	Fecha de inicio de la validez	Si	
1.5.2. Not After	Fecha de expiración	Si	
1.6. Subject		Sí	
1.6.1. Country (C)	"ES"	Sí	
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.	Si	
1.6.3. organizationalUnitName (OU)	"Certificado electrónico de persona física empleado público nivel Alto, emitido por vinCAsign"	Sí	

Campo	Contenido	Obligatorio	Crítico
1.6.4. organizationalUnitName (OU)			
1.6.5. organizationalUnitName (OU)			
1.6.6. Surname	Primer y segundo apellido, de acuerdo con documento de identidad (DNI/Pasaporte)	Sí	
1.6.7. Given Name	Nombre de pila, de acuerdo con documento de identidad (DNI/Pasaporte)	Sí	
1.6.8. Title			
1.6.9. Serial Number	DNI/NIE del empleado	Sí	
1.6.10. Common Name (CN)	Nombre Apellido1 Apellido2 – DNI 00000000G	Sí	
1.7. Subject Public Key Info	2048-Bit Public key encoded in accordance with RFC3279	Sí	
2. Extensions			
2.1. Authority Key Identifier	Presente	Sí	No
2.1.1. Key Identifier			
2.2. Subject Key Identifier	Presente	Sí	NO
2.3. Key Usage		Sí	Sí

Campo	Contenido	Obligatorio	Crítico
2.3.1. Digital Signature	Seleccionado. "1"	Sí	
2.3.2. contentCommitment	Seleccionado. "1"	Sí	
2.3.3. Key Encipherment	No seleccionado. "0"		
2.3.4. Data Encipherment	No seleccionado. "0"		
2.3.5. Key Agreement	No seleccionado. "0"		
2.3.6. Key Certificate Signature	No seleccionado. "0"		
2.3.7. CRL Signature	No seleccionado. "0"		
2.4. Certificate Policies		Sí	NO
2.4.1. Policy Identifier	1.3.6.1.4.1.**47155.1.4.1**	Sí	
2.4.2. Policy Qualifier ID		Sí	
2.4.2.1. CPS Pointer	https://policy.vincasign.net	Sí	
2.4.2.2. User Notice	"Certificado reconocido de empleado público – nivel alto, para firma y autenticación. Ver https://policy.vincasign.net"	Sí	
2.5. Subject Alternative Names		Sí	NO

Campo	Contenido	Obligatorio	Crítico
2.5.1. rfc822Name	Correo electrónico de la persona física		
2.5.2. Directory Name	Identidad administrativa	Sí	
2.5.2.1. Tipo de certificado OID: 2.16.724.1.3.5.3.1.1	"certificado electrónico de empleado público"	Sí	
2.5.2.2. Nombre de la entidad suscriptora OID: 2.16.724.1.3.5.3.1.2	Entidad propietaria del certificado	Sí	
2.5.2.3. NIF de la entidad suscriptora OID: 2.16.724.1.3.5.3.1.3	Número de identificación fiscal de la entidad propietaria del certificado	Sí	
2.5.2.4. DNI/NIE del esponsable OID: 2.16.724.1.3.5.3.1.4	DNI o NIE del responsable	Sí	
2.5.2.5. Número de identificación personal OID: 2.16.724.1.3.5.3.1.5	NRP o NIP del responsable del suscriptor del certificado		
2.5.2.6. Nombre de pila OID: 2.16.724.1.3.5.3.1.6	Nombre de pila del responsable del certificado	Sí	

Campo	Contenido	Obligatorio	Crítico
2.5.2.7. Primer apellido OID: 2.16.724.1.3.5.3.1.7	Primer apellido del responsable del certificado	Sí	
2.5.2.8. Segundo apellido OID: 2.16.724.1.3.5.3.1.8	Segundo apellido del responsable del certificado	Sí	
2.5.2.9. Correo electrónico OID: 2.16.724.1.3.5.3.1.9	Correo electrónico del responsable del certificado		
2.5.2.10. Unidad organizativa OID: 2.16.724.1.3.5.3.1.10	Unidad, dentro de la Administración, en la que está incluido el suscriptor del certificado		
2.5.2.11. Puesto o cargo OID: 2.16.724.1.3.5.3.1.11	Puesto desempeñado por el suscriptor del certificado dentro de la Administración		
2.6. Issuer Alternative Name			NO
2.6.1. rfc822Name	info@vincasign.net		
2.7. Extended Key Usages		Sí	NO
2.7.1. emailProtection	Presente	Sí	
2.7.2. clientAuth	Presente	Sí	

Campo	Contenido	Obligatorio	Crítico
2.8. cRLDistributionPoint			NO
2.8.1. distributionPoint	http://crl1.vincasign.net/casub.crl	Sí	
2.8.2. distributionPoint	http://crl2.vincasign.net/casub.crl	Sí	
2.9. Authority Info Acces		Sí	NO
2.9.1. Access Method	Id-ad-ocsp	Sí	
2.9.1.1. Acces Location	http://ocsp1.vincasign.net	Sí	
2.9.1.2. Acces Location	http://ocsp2.vincasign.net		
2.9.2. caIssuersAccessMethod	id-ad-caIssuers	Sí	
2.9.2.1. Acces Location	http://www.vincasign.net/publickeys/casub.crt	Sí	
2.10. NetscapeCertType	"SSL client", "S/MIME"		
2.11. Qualified Certificate Statements		Sí	No
2.11.1. esi4-qcStatement-1	Indicación de certificado reconocido	Sí	
2.11.2. esi4-qcStatement-3	"15"	Sí	
2.11.3. esi4-qcStatement-4	Presente	Sí	

7. Certificado de persona física EMPLEADO PÚBLICO (Nivel Medio)

7.1. Perfil único para firma y autenticación.

Campo	Contenido	Obligatorio	Crítico
1. Basic estructure			
1.1. Version	"2"	Sí	
1.2. Serial Number	Establecido automáticamente por la CA. Número identificativo **único** del certificado.	Sí	
1.3. Signature Algorithm		Sí	
1.3.1. Identifier	1.2.840.113549.1.1.11	Sí	
1.3.2. Description	SHA-2 with RSA Signature[16]	Sí	
1.4. **Issuer Distinguished Name**		Sí	
1.4.1. Country (C)	"ES"	Sí	
1.4.2. Organization (O)	"VINTEGRIS SL"	Si	

[16] No usar el algoritmo SHA-1 por recomendación de la ETSI TS 119 312.

Campo	Contenido	Obligatorio	Crítico
1.4.3. Locality (L)	"Barcelona (see current address at https://www.vincasign.net/contact)"		
1.4.4. Organizational Unit (OU)	"EC-VINTEGRIS"		
1.4.5. Serial Number	"B62913926"	Sí	
1.4.6. Common Name (CN)	"vinCAsign Global Authority"	Sí	
1.5. Validity		Sí	
1.5.1. Not Before	Fecha de inicio de la validez	Si	
1.5.2. Not After	Fecha de expiración	Si	
1.6. Subject		Sí	
1.6.1. Country (C)	"ES"	Sí	
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.	Si	
1.6.3. organizationalUnitName (OU)	"Certificado electrónico de persona física empleado público nivel medio, emitido por vinCAsign"	Sí	

Campo	Contenido	Obligatorio	Crítico
1.6.4. organizationalUnitName (OU)			
1.6.5. organizationalUnitName (OU)			
1.6.6. Surname	Primer y segundo apellido, de acuerdo con documento de identidad (DNI/Pasaporte)	Sí	
1.6.7. Given Name	Nombre de pila, de acuerdo con documento de identidad (DNI/Pasaporte)	Sí	
1.6.8. Title			
1.6.9. Serial Number	DNI/NIE del empleado	Sí	
1.6.10. Common Name (CN)	Nombre Apellido1 Apellido2 – DNI 00000000G	Sí	
1.7. Subject Public Key Info	2048-Bit Public key encoded in accordance with RFC3279	Sí	
2. Extensions			
2.1. Authority Key Identifier	Presente	Sí	No
2.1.1. Key Identifier			
2.2. Subject Key Identifier	Presente	Sí	NO
2.3. Key Usage		Sí	Sí

Campo	Contenido	Obligatorio	Crítico
2.3.1. Digital Signature	Seleccionado. "1"	Sí	
2.3.2. contentCommitment	Seleccionado. "1"	Sí	
2.3.3. Key Encipherment	No seleccionado. "0"		
2.3.4. Data Encipherment	No seleccionado. "0"		
2.3.5. Key Agreement	No seleccionado. "0"		
2.3.6. Key Certificate Signature	No seleccionado. "0"		
2.3.7. CRL Signature	No seleccionado. "0"		
2.4. Certificate Policies		Sí	NO
2.4.1. Policy Identifier	1.3.6.1.4.1.**47155.1.4.2**	Sí	
2.4.2. Policy Qualifier ID		Sí	
2.4.2.1. CPS Pointer	https://policy.vincasign.net	Sí	
2.4.2.2. User Notice	"Certificado reconocido de empleado público – nivel medio, para firma y autenticación. Ver https://policy.vincasign.net"	Sí	
2.5. Subject Alternative Names		Sí	NO

Campo	Contenido	Obligatorio	Crítico
2.5.1. rfc822Name	Correo electrónico de la persona física		
2.5.2. Directory Name	Identidad administrativa	Sí	
2.5.2.1. Tipo de certificado OID: 2.16.724.1.3.5.3.2.1	"certificado electrónico de empleado público"	Sí	
2.5.2.2. Nombre de la entidad suscriptora OID: 2.16.724.1.3.5.3.2.2	Entidad propietaria del certificado	Sí	
2.5.2.3. NIF de la entidad suscriptora OID: 2.16.724.1.3.5.3.2.3	Número de identificación fiscal de la entidad propietaria del certificado	Sí	
2.5.2.4. DNI/NIE del esponsable OID: 2.16.724.1.3.5.3.2.4	DNI o NIE del responsable	Sí	
2.5.2.5. Número de identificación personal OID: 2.16.724.1.3.5.3.2.5	NRP o NIP del responsable del suscriptor del certificado		
2.5.2.6. Nombre de pila OID: 2.16.724.1.3.5.3.2.6	Nombre de pila del responsable del certificado	Sí	

Campo	Contenido	Obligatorio	Crítico
2.5.2.7. Primer apellido OID: 2.16.724.1.3.5.3.2.7	Primer apellido del responsable del certificado	Sí	
2.5.2.8. Segundo apellido OID: 2.16.724.1.3.5.3.2.8	Segundo apellido del responsable del certificado	Sí	
2.5.2.9. Correo electrónico OID: 2.16.724.1.3.5.3.2.9	Correo electrónico del responsable del certificado		
2.5.2.10. Unidad organizativa OID: 2.16.724.1.3.5.3.2.10	Unidad, dentro de la Administración, en la que está incluido el suscriptor del certificado		
2.5.2.11. Puesto o cargo OID: 2.16.724.1.3.5.3.2.11	Puesto desempeñado por el suscriptor del certificado dentro de la Administración		
2.6. Issuer Alternative Name			NO
2.6.1. rfc822Name	info@vincasign.net		
2.7. Extended Key Usages		Sí	NO
2.7.1. emailProtection	Presente	Sí	
2.7.2. clientAuth	Presente	Sí	

Campo	Contenido	Obligatorio	Crítico
2.8. cRLDistributionPoint			NO
2.8.1. distributionPoint	http://crl1.vincasign.net/casub.crl	Sí	
2.8.2. distributionPoint	http://crl2.vincasign.net/casub.crl	Sí	
2.9. Authority Info Acces		Sí	NO
2.9.1. Access Method	Id-ad-ocsp	Sí	
2.9.1.1. Acces Location	http://ocsp1.vincasign.net	Sí	
2.9.1.2. Acces Location	http://ocsp2.vincasign.net		
2.9.2. caIssuersAccessMethod	id-ad-caIssuers	Sí	
2.9.2.1. Acces Location	http://www.vincasign.net/publickeys/casub.crt	Sí	
2.10. NetscapeCertType	"SSL client", "S/MIME"		
2.11. Qualified Certificate Statements		Sí	No
2.11.1. esi4-qcStatement-1	Indicación de certificado reconocido	Sí	
2.11.2. esi4-qcStatement-3	"15"	Sí	

8. Certificado de SELLO ELECTRÓNICO (Nivel Alto)

8.1. Perfil único para firma y autenticación.

Campo	Contenido	Obligatorio	Crítico
1. Basic estructure			
1.1. Version	"2"	Sí	
1.2. Serial Number	Establecido automáticamente por la CA. Número identificativo **único** del certificado.	Sí	
1.3. Signature Algorithm		Sí	
1.3.1. Identifier	1.2.840.113549.1.1.11	Sí	
1.3.2. Description	SHA-2 with RSA Signature[17]	Sí	
1.4. **Issuer Distinguished Name**		Sí	
1.4.1. Country (C)	"ES"	Sí	
1.4.2. Organization (O)	"VINTEGRIS SL"	Si	

[17] No usar el algoritmo SHA-1 por recomendación de la ETSI TS 119 312.

Campo	Contenido	Obligatorio	Crítico
1.4.3. Locality (L)	"Barcelona (see current address at https://www.vincasign.net/contact)"		
1.4.4. Organizational Unit (OU)	"EC-VINTEGRIS"		
1.4.5. Serial Number	"B62913926"	Sí	
1.4.6. Common Name (CN)	"vinCAsign Global Authority"	Sí	
1.5. Validity		Sí	
1.5.1. Not Before	Fecha de inicio de la validez	Si	
1.5.2. Not After	Fecha de expiración	Si	
1.6. Subject		Sí	
1.6.1. Country (C)	"ES"	Sí	
1.6.2. Organization (O)	Denominación (nombre "oficial" de la organización) del suscriptor de servicios de certificación (custodio del certificado).	Si	
1.6.3. organizationalUnitName (OU)	Sello electrónico	Sí	
1.6.4. Surname	Primer y segundo apellido, de acuerdo con documento de identidad (DNI/Pasaporte)		

Campo	Contenido	Obligatorio	Crítico
1.6.5. Given Name	Nombre de pila, de acuerdo con documento de identidad (DNI/Pasaporte)		
1.6.6. Serial Number	NIF de la entidad.	Sí	
1.6.7. Common Name (CN)	Nombre descriptivo del sistema automático. Asegurando que dicho nombre tenga sentido y no de lugar a ambigüedades.		
1.7. Subject Public Key Info	2048-Bit Public key encoded in accordance with RFC3279	Sí	
2. Extensions			
2.1. Authority Key Identifier	Presente	Sí	No
2.1.1. Key Identifier			
2.2. Subject Key Identifier	Presente	Sí	NO
2.3. Key Usage		Sí	Sí
2.3.1. Digital Signature	Seleccionado. “1”	Sí	
2.3.2. contentCommitment	Seleccionado. “1”	Sí	
2.3.3. Key Encipherment	No seleccionado. “0”		

Campo	Contenido	Obligatorio	Crítico
2.3.4. Data Encipherment	No seleccionado. "0"		
2.3.5. Key Agreement	No seleccionado. "0"		
2.3.6. Key Certificate Signature	No seleccionado. "0"		
2.3.7. CRL Signature	No seleccionado. "0"		
2.4. Certificate Policies		Sí	NO
2.4.1. Policy Identifier	1.3.6.1.4.1.**47155.1.5.1**	Sí	
2.4.2. Policy Qualifier ID		Sí	
2.4.2.1. CPS Pointer	https://policy.vincasign.net	Sí	
2.4.2.2. User Notice	"Certificado reconocido de sello electrónico de Administración, órgano o entidad de derecho público, nivel alto. Ver https://policy.vincasign.net"	Sí	
2.5. Subject Alternative Names		Sí	NO
2.5.1. rfc822Name	Correo electrónico de la persona física		
2.5.2. Directory Name	Identidad administrativa	Sí	

Campo	Contenido	Obligatorio	Crítico
2.5.2.1. Tipo de certificado OID: 2.16.724.1.3.5.2.1.1	"sello electrónico"	Sí	
2.5.2.2. Nombre de la entidad suscriptora OID: 2.16.724.1.3.5.2.1.2	Entidad propietaria del certificado	Sí	
2.5.2.3. NIF de la entidad suscriptora OID: 2.16.724.1.3.5.2.1.3	Número de identificación fiscal de la entidad propietaria del certificado	Sí	
2.5.2.4. DNI/NIE del esponsable OID: 2.16.724.1.3.5.2.1.4	DNI o NIE del responsable del sello		
2.5.2.5. Denominación de sistema o componente OID: 2.16.724.1.3.5.2.1.5	Breve descripción de la componente que posee el certificado de sello		
2.5.2.6. Nombre de pila OID: 2.16.724.1.3.5.2.1.6	Nombre de pila del responsable del certificado de sello		
2.5.2.7. Primer apellido OID: 2.16.724.1.3.5.2.1.7	Primer apellido del responsable del certificado de sello		

Campo	Contenido	Obligatorio	Crítico
2.5.2.8. Segundo apellido OID: 2.16.724.1.3.5.2.1.8	Segundo apellido del responsable del certificado de sello		
2.5.2.9. Correo electrónico OID: 2.16.724.1.3.5.2.1.9	Correo electrónico del responsable del certificado de sello		
2.6. Issuer Alternative Name			NO
2.6.1. rfc822Name	info@vincasign.net		
2.7. Extended Key Usages		Sí	NO
2.7.1. emailProtection	Presente	Sí	
2.7.2. clientAuth	Presente	Sí	
2.8. cRLDistributionPoint			NO
2.8.1. distributionPoint	http://crl1.vincasign.net/casub.crl	Sí	
2.8.2. distributionPoint	http://crl2.vincasign.net/casub.crl	Sí	
2.9. Authority Info Acces		Sí	NO
2.9.1. Access Method	Id-ad-ocsp	Sí	
2.9.1.1. Acces Location	http://ocsp1.vincasign.net	Sí	

Campo	Contenido	Obligatorio	Crítico
2.9.1.2. Acces Location	http://ocsp2.vincasign.net		
2.9.2. calssuersAccessMethod	id-ad-calssuers	Sí	
2.9.2.1. Acces Location	http://www.vincasign.net/publickeys/casub.crt	Sí	
2.10. Qualified Certificate Statements		Sí	No
2.10.1. esi4-qcStatement-1	Indicación de certificado reconocido	Sí	
2.10.2. esi4-qcStatement-3	"15"	Sí	
2.10.3. esi4-qcStatement-4	Presente	Sí	

9. Certificado de SELLO ELECTRÓNICO (Nivel Medio)

9.1. Perfil único para firma y autenticación.

Campo	Contenido	Obligatorio	Crítico
1. Basic estructure			
1.1. Version	"2"	Sí	
1.2. Serial Number	Establecido automáticamente por la CA. Número identificativo **único** del certificado.	Sí	
1.3. Signature Algorithm		Sí	
1.3.1. Identifier	1.2.840.113549.1.1.11	Sí	
1.3.2. Description	SHA-2 with RSA Signature[18]	Sí	
1.4. **Issuer Distinguished Name**		Sí	
1.4.1. Country (C)	"ES"	Sí	
1.4.2. Organization (O)	"VINTEGRIS SL"	Si	

[18] No usar el algoritmo SHA-1 por recomendación de la ETSI TS 119 312.

Campo	Contenido	Obligatorio	Crítico
1.4.3. Locality (L)	"Barcelona (see current address at https://www.vincasign.net/contact)"		
1.4.4. Organizational Unit (OU)	"EC-VINTEGRIS"		
1.4.5. Serial Number	"B62913926"	Sí	
1.4.6. Common Name (CN)	"vinCAsign Global Authority"	Sí	
1.5. Validity		Sí	
1.5.1. Not Before	Fecha de inicio de la validez	Si	
1.5.2. Not After	Fecha de expiración	Si	
1.6. Subject		Sí	
1.6.1. Country (C)	"ES"	Sí	
1.6.2. Organization (O)	Denominación (nombre "oficial" de la organización) del suscriptor de servicios de certificación (custodio del certificado).	Si	
1.6.3. organizationalUnitName (OU)	Sello electrónico	Sí	
1.6.4. Surname	Primer y segundo apellido, de acuerdo con documento de identidad (DNI/Pasaporte)		

Campo	Contenido	Obligatorio	Crítico
1.6.5. Given Name	Nombre de pila, de acuerdo con documento de identidad (DNI/Pasaporte)		
1.6.6. Serial Number	NIF de la entidad.	Sí	
1.6.7. Common Name (CN)	Nombre descriptivo del sistema automático. Asegurando que dicho nombre tenga sentido y no de lugar a ambigüedades.		
1.7. Subject Public Key Info	2048-Bit Public key encoded in accordance with RFC3279	Sí	
2. Extensions			
2.1. Authority Key Identifier	Presente	Sí	No
2.1.1. Key Identifier			
2.2. Subject Key Identifier	Presente	Sí	NO
2.3. Key Usage		Sí	Sí
2.3.1. Digital Signature	Seleccionado. “1”	Sí	
2.3.2. contentCommitment	Seleccionado. “1”	Sí	
2.3.3. Key Encipherment	No seleccionado. “0”		

Campo	Contenido	Obligatorio	Crítico
2.3.4. Data Encipherment	No seleccionado. "0"		
2.3.5. Key Agreement	No seleccionado. "0"		
2.3.6. Key Certificate Signature	No seleccionado. "0"		
2.3.7. CRL Signature	No seleccionado. "0"		
2.4. Certificate Policies		Sí	NO
2.4.1. Policy Identifier	1.3.6.1.4.1.**47155.1.5.2**	Sí	
2.4.2. Policy Qualifier ID		Sí	
2.4.2.1. CPS Pointer	https://policy.vincasign.net	Sí	
2.4.2.2. User Notice	"Certificado reconocido de sello electrónico de Administración, órgano o entidad de derecho público, nivel medio. Ver https://policy.vincasign.net"	Sí	
2.5. Subject Alternative Names		Sí	NO
2.5.1. rfc822Name	Correo electrónico de la persona física		
2.5.2. Directory Name	Identidad administrativa	Sí	

Campo	Contenido	Obligatorio	Crítico
2.5.2.1. Tipo de certificado OID: 2.16.724.1.3.5.2.2.1	"sello electrónico"	Sí	
2.5.2.2. Nombre de la entidad suscriptora OID: 2.16.724.1.3.5.2.2.2	Entidad propietaria del certificado	Sí	
2.5.2.3. NIF de la entidad suscriptora OID: 2.16.724.1.3.5.2.2.3	Número de identificación fiscal de la entidad propietaria del certificado	Sí	
2.5.2.4. DNI/NIE del esponsable OID: 2.16.724.1.3.5.2.2.4	DNI o NIE del responsable del sello		
2.5.2.5. Denominación de sistema o componente OID: 2.16.724.1.3.5.2.2.5	Breve descripción de la componente que posee el certificado de sello		
2.5.2.6. Nombre de pila OID: 2.16.724.1.3.5.2.2.6	Nombre de pila del responsable del certificado de sello		
2.5.2.7. Primer apellido OID: 2.16.724.1.3.5.2.2.7	Primer apellido del responsable del certificado de sello		

Campo	Contenido	Obligatorio	Crítico
2.5.2.8. Segundo apellido OID: 2.16.724.1.3.5.2.2.8	Segundo apellido del responsable del certificado de sello		
2.5.2.9. Correo electrónico OID: 2.16.724.1.3.5.2.2.9	Correo electrónico del responsable del certificado de sello		
2.6. Issuer Alternative Name			NO
2.6.1. rfc822Name	info@vincasign.net		
2.7. Extended Key Usages		Sí	NO
2.7.1. emailProtection	Presente	Sí	
2.7.2. clientAuth	Presente	Sí	
2.8. cRLDistributionPoint			NO
2.8.1. distributionPoint	http://crl1.vincasign.net/casub.crl	Sí	
2.8.2. distributionPoint	http://crl2.vincasign.net/casub.crl	Sí	
2.9. Authority Info Acces		Sí	NO
2.9.1. Access Method	Id-ad-ocsp	Sí	
2.9.1.1. Acces Location	http://ocsp1.vincasign.net	Sí	

Campo	Contenido	Obligatorio	Crítico
2.9.1.2. Acces Location	http://ocsp2.vincasign.net		
2.9.2. calssuersAccessMethod	id-ad-calssuers	Sí	
2.9.2.1. Acces Location	http://www.vincasign.net/publickeys/casub.crt	Sí	
2.10. Qualified Certificate Statements		Sí	No
2.10.1. esi4-qcStatement-1	Indicación de certificado reconocido	Sí	
2.10.2. esi4-qcStatement-3	"15"	Sí	