	PERFILES DE CERTIFICADOS CUALIFICADOS BANKFLIP	Política	OID pol ETSI	OID pol BANKFLIP
	De PERSONA FÍSICA			
1.1	Certificado cualificado de Persona Física ciudadano en Software	QCP-n	0.4.0.194112.1.0	1.3.6.1.4.1.60078.1.1.1
1.2	Certificado cualificado de Persona Física ciudadano en HSM centralizado	QCP-n	0.4.0.194112.1.0	1.3.6.1.4.1.60078.1.1.2
1.3	Certificado cualificado de Persona Física ciudadano en QSCD centralizado	QCP-n-qscd	0.4.0.194112.1.2	1.3.6.1.4.1.60078.1.1.3
	De PERSONA FISICA REPRESENTANTE			
2.1	de persona física representante de Persona Jurídica ante las administraciones en Software	QCP-n	0.4.0.194112.1.0	1.3.6.1.4.1.60078.1.2.1
2.2	de persona física Representante de Persona Jurídica ante las administraciones en HSM centralizado	QCP-n	0.4.0.194112.1.0	1.3.6.1.4.1.60078.1.2.2
2.3	de persona física Representante de Persona Jurídica ante las administraciones en QSCD centralizado	QCP-n-qscd	0.4.0.194112.1.2	1.3.6.1.4.1.60078.1.2.3
3.1	de persona física Representante de Entidad sin Personalidad Jurídica ante las administraciones en Software	QCP-n	0.4.0.194112.1.0	1.3.6.1.4.1.60078.1.3.1
	de persona física Representante de Entidad sin Personalidad Jurídica ante las administraciones en HSM centralizado			
3.2		QCP-n	0.4.0.194112.1.2	1.3.6.1.4.1.60078.1.3.2
3.3	de persona física Representante de Entidad sin Personalidad Jurídica ante las administraciones en QSCD centralizado	QCP-n-qscd	0.4.0.194112.1.2	1.3.6.1.4.1.60078.1.3.3

Nivel 0	**OID de VID**	**1.3.6.1.4.1.XXX**

Nivel 1	**OID**	**1.3.6.1.4.1.XXX.X**
	Perfiles Cualificados (QCP)	1.3.6.1.4.1.XXX.1
	Servicio de sellado de tiempo	1.3.6.1.4.1.XXX.2.1

	OID según el sujeto	**1.3.6.1.4.1.XXX.2.X**
	Certificados cualificados de Persona física	
	Ciudadano	1.3.6.1.4.1.XXX.1.1
	Representante con PJ	1.3.6.1.4.1.XXX.1.2
	Representante sin PJ	1.3.6.1.4.1.XXX.1.3
Nivel 2	**Certificados cualificados de Persona Jurídica**	
	Sello de empresa	1.3.6.1.4.1.XXX.1.4
	Certificado de TSU	1.3.6.1.4.1.XXX.2.2

OID según soporte	**1.3.6.1.4.1.XXX.1.X.X**
Certificado en HSM centralizado	1.3.6.1.4.1.XXX.2.X.1
Certificado en QSCD centralizado	1.3.6.1.4.1.XXX.2.X.2

Campo *De Persona Física*	en Software Autenticación y Firma	Oblig.	Crít.	Longitud máxima	Codificación	Observaciones OID 1.3.6.1.4.1.60078.1.1.1	Inicio
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)	BEYOND THE SCOPE S.L	Sí		64 caracteres	UTF8String	OID 2.5.4.10	
1.4.3. Locality Name (L)	“Barcelona”	Sí		128 caracteres	UTF8String	OID 2.5.4.7	
1.4.4. Organization Identifier	“VATES-B04948766”	Sí		Ilimitado	UTF8String	OID 2.5.4.97	
1.4.5. Common Name (CN)	Permisso CA Subordinada 01	Sí		64 caracteres	UTF8String	OID 2.5.4.3	
1.4.6. Organizational Unit (OU)	TSP – Permisso	Sí			UTF8String		
1.5. Validity		Sí					
1.5.1. Not Before	Fecha de inicio de validez	Sí			UTCTime	YYMMDDHHMMSSZ	
1.5.2. Not After	Fecha de expiración	Sí			UTCTime	YYMMDDHHMMSSZ	
1.6. Subject		Sí					
1.6.1. Country Name	País de residencia o nacionalidad del firmante	Sí		2 caracteres	PrintableString	OID 2.5.4.6	
1.6.2. Surname	Apellidos del firmante (como consta en el documento oficial)	Sí		40 caracteres	UTF8String	OID 2.5.4.4	
1.6.3. Given Name	Nombre del firmante (como consta en el documento oficial)	Sí		16 caracteres	UTF8String	OID 2.5.4.42	
1.6.4. Serial Number	Número de documento oficial codificado acorde a ETSI EN 319 412-1 (“IDCES-12345678Z”)	Sí		64 caracteres	PrintableString	OID 2.5.4.5	
1.6.5. Common Name	NOMBRE Y APELLIDOS DEL FIRMANTE	Sí		64 caracteres	UTF8String	OID 2.5.4.3	
1.7. Subject Public Key Info		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	
2.2. 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					
2.3.2. Content commintment	Seleccionado “1”	Sí					
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	1.3.6.1.4.1.60078.1.1.1	Sí			OID	Identificador de la política de BANKFLIP	
2.4.1.2. Policy Qualifiers		Sí					
2.4.1.1.1 CPS URI	https://qtsp.permisso.io/cps/	Sí			IA5String	URL de la DPC de BANKFLIP	
2.4.1.1.2. User Notice/Explicit text	“Certificado cualificado de Persona Física en software.“	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	Identificador de la política de certificado cualificado de persona física	
2.5. Subject Alternative Names		No	No			OID 2.5.29.17 (Marcado como NO crítico según EN 319412-2)	
2.5.1. rfc822Name	Correo electrónico de la persona física	No			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)	No			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.uanataca.com/public/pki/crl/PermissoCA1.crl	Sí			IA5String	uniformResourceIdentifier **(NO HTTPS)**	
2.7.2. distributionPoint	http://crl2.uanataca.com/public/pki/crl/PermissoCA1.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	
2.8.1.1.1 Acces Location	http://ocsp1.uanataca.com/public/pki/ocsp/	Sí			IA5String	URL de acceso al OCSP **(NO HTTPS)** uniformResourceIdentifier	
2.8.1.1.2. Acces Location	http://ocsp2.uanataca.com/public/pki/ocsp/	No			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	
2.8.2.1.1 Acces Location	https://qtsp.permisso.io/pki/subordinate1.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		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		Sí				OID 0.4.0.1862.1.5 (Sí HTTPS) URL de acceso al texto divulgativo	
2.9.4.1 PdsLocation							
2.9.4.1.1 url	https://qtsp.permisso.io/cps/	Sí			IA5String		
2.9.4.1.2 language	“EN”	Sí			PrintableString	(SIZE(2))} --ISO 639-1 language code	
2.9.5. QcType	id-etsi-qct-esign	No			SEQUENCE(2 elem) OBJECT IDENTIFIER0.4.0.1862.1.6 OCTET STRING(1 elem) SEQUENCE(1 elem) OBJECT IDENTIFIER0.4.0.1862.1.6.1	OID 0.4.0.1862.1.6.1 Certificado de firma electrónica 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		

Inicio

De PF Ciudadano	en HSM Centralizado Autenticación y Firma	Oblig.	Crít.	Longitud máxima	Codificación	Observaciones OID 1.3.6.1.4.1.60078.1.1.2	
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		
1.3.2. 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)	BEYOND THE SCOPE S.L	Sí		64 caracteres	UTF8String	OID 2.5.4.10	
1.4.3. Locality Name (L)	Barcelona	Sí		128 caracteres	UTF8String	OID 2.5.4.7	
1.4.4. Organization Identifier	VATES-B04948766	Sí		Ilimitado	UTF8String	OID 2.5.4.97	
1.4.5. Common Name (CN)	Permisso CA Subordinada 01	Sí		64 caracteres	UTF8String	OID 2.5.4.3	
1.4.6. Organizational Unit (OU)	TSP – Permisso	Sí			UTF8String		
1.5. Validity		Sí					
1.5.1. Not Before	Fecha de inicio de validez	Sí			UTCTime	YYMMDDHHMMSSZ	
1.5.2. Not After	Fecha de expiración	Sí			UTCTime	YYMMDDHHMMSSZ	
1.6. Subject		Sí					
1.6.1. Country Name	País de residencia o nacionalidad del firmante	Sí		2 caracteres	PrintableString	OID 2.5.4.6	Aparece PA
1.6.2. Surname	Apellidos del firmante (como consta en el documento oficial)	Sí		40 caracteres	UTF8String	OID 2.5.4.4	
1.6.3. Given Name	Nombre del firmante (como consta en el documento oficial)	Sí		16 caracteres	UTF8String	OID 2.5.4.42	
1.6.4. Serial Number	Número de documento oficial codificado acorde a ETSI EN 319 412-1 (“IDCES-12345678Z”)	Sí		64 caracteres	PrintableString	OID 2.5.4.5	Aparece PA
1.6.5. Common Name	NOMBRE Y APELLIDOS DEL FIRMANTE	Sí		64 caracteres	UTF8String	OID 2.5.4.3	
1.7. Subject Public Key Info		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	
2.2. 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					
2.3.2. Content commintment	Seleccionado “1”	Sí					
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	1.3.6.1.4.1.60078.1.1.2	Sí			OID	Identificador de la política de BANKFLIP	
2.4.1.2. Policy Qualifiers		Sí					
2.4.1.1.1 CPS URI	https://qtsp.permisso.io/cps/	Sí			IA5String	URL de la DPC de BANKFLIP	
2.4.1.1.2. User Notice/Explicit text	Certificado cualificado de Persona Física en HSM Centralizado	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	Identificador de la política de certificado cualificado de persona física	
2.5. Subject Alternative Names		No	No			OID 2.5.29.17 (Marcado como NO crítico según EN 319412-2)	
2.5.1. rfc822Name	Correo electrónico de la persona física	No			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)	No			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.uanataca.com/public/pki/crl/PermissoCA1.crl	Sí			IA5String	uniformResourceIdentifier **(NO HTTPS)**	
2.7.2. distributionPoint	http://crl2.uanataca.com/public/pki/crl/PermissoCA1.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	
2.8.1.1.1 Acces Location	http://ocsp1.uanataca.com/public/pki/ocsp/	Sí			IA5String	URL de acceso al OCSP **(NO HTTPS)** uniformResourceIdentifier	
2.8.1.1.2. Acces Location	http://ocsp2.uanataca.com/public/pki/ocsp/	No			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	
2.8.2.1.1 Acces Location	https://qtsp.permisso.io/pki/subordinate1.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		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		Sí				OID 0.4.0.1862.1.5 (SÍ HTTPS) URL de acceso al texto divulgativo	
2.9.4.1 PdsLocation							
2.9.4.1.1 url	https://qtsp.permisso.io/cps/	Sí			IA5String		
2.9.4.1.2 language	“EN”	Sí			PrintableString	(SIZE(2))} --ISO 639-1 language code	
2.9.5. QcType	id-etsi-qct-esign	Sí			SEQUENCE(2 elem) OBJECT IDENTIFIER0.4.0.1862.1.6 OCTET STRING(1 elem) SEQUENCE(1 elem) OBJECT IDENTIFIER0.4.0.1862.1.6.1	OID 0.4.0.1862.1.6.1 Certificado de firma electrónica 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		

Inicio

Campo *De PF Ciudadano*	en QSCD centralizado Autenticación y Firma	Oblig.	Crít.	Longitud máxima	Codificación	Observaciones OID 1.3.6.1.4.1.60078.1.1.3
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)	BEYOND THE SCOPE S.L	Sí		64 caracteres	UTF8String	OID 2.5.4.10
1.4.3. Locality Name (L)	Barcelona	Sí		128 caracteres	UTF8String	OID 2.5.4.7
1.4.4. Organization Identifier	VATES-B04948766”	Sí		Ilimitado	UTF8String	OID 2.5.4.97
1.4.5. Common Name (CN)	Permisso CA Subordinada 01	Sí		64 caracteres	UTF8String	OID 2.5.4.3
1.4.6. Organizational Unit (OU)	TSP – Permisso	Sí			UTF8String	
1.5. Validity		Sí				
1.5.1. Not Before	Fecha de inicio de validez	Sí			UTCTime	YYMMDDHHMMSSZ
1.5.2. Not After	Fecha de expiración	Sí			UTCTime	YYMMDDHHMMSSZ
1.6. Subject		Sí				
1.6.1. Country Name	País de residencia o nacionalidad del firmante	Sí		2 caracteres	PrintableString	OID 2.5.4.6
1.6.2. Surname	Apellidos del firmante (como consta en el documento oficial)	Sí		40 caracteres	UTF8String	OID 2.5.4.4
1.6.3. Given Name	Nombre del firmante (como consta en el documento oficial)	Sí		16 caracteres	UTF8String	OID 2.5.4.42
1.6.4. Serial Number	Número de documento oficial codificado acorde a ETSI EN 319 412-1 (“IDCES-12345678Z”)	Sí		64 caracteres	PrintableString	OID 2.5.4.5
1.6.5. Common Name	NOMBRE Y APELLIDOS DEL FIRMANTE	Sí		64 caracteres	UTF8String	OID 2.5.4.3
1.7. Subject Public Key Info		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
2.2. 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				
2.3.2. Content commintment	Seleccionado “1”	Sí				
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	1.3.6.1.4.1.60078.1.1.3	Sí			OID	Identificador de la política de BANKFLIP
2.4.1.2. Policy Qualifiers		Sí				
2.4.1.1.1 CPS URI	https://qtsp.permisso.io/cps/	Sí			IA5String	URL de la DPC de BANKFLIP
2.4.1.1.2. User Notice/Explicit text	Certificado cualificado de Persona Física en QSCD Centralizado	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	Identificador de la política de certificado cualificado de persona física
2.5. Subject Alternative Names		No	No			OID 2.5.29.17 (Marcado como NO crítico según EN 319412-2)
2.5.1. rfc822Name	Correo electrónico de la persona física	No			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)	No			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.uanataca.com/public/pki/crl/PermissoCA1.crl	Sí			IA5String	uniformResourceIdentifier **(NO HTTPS)**
2.7.2. distributionPoint	http://crl2.uanataca.com/public/pki/crl/PermissoCA1.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
2.8.1.1.1 Acces Location	http://ocsp1.uanataca.com/public/pki/ocsp/	Sí			IA5String	URL de acceso al OCSP **(NO HTTPS)** uniformResourceIdentifier
2.8.1.1.2. Acces Location	http://ocsp2.uanataca.com/public/pki/ocsp/	No			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
2.8.2.1.1 Acces Location	https://qtsp.permisso.io/pki/subordinate1.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		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		Sí				OID 0.4.0.1862.1.4 Dispositivo cualificado de creación de firma
2.9.4. QcPDS		Sí				OID 0.4.0.1862.1.5 (SÍ HTTPS) URL de acceso al texto divulgativo
2.9.4.1 PdsLocation						
2.9.4.1.1 url	https://qtsp.permisso.io/cps/	Sí			IA5String	
2.9.4.1.2 language	“EN”	Sí			PrintableString	(SIZE(2))} --ISO 639-1 language code
2.9.5. QcType	id-etsi-qct-esign	Sí			SEQUENCE(2 elem) OBJECT IDENTIFIER0.4.0.1862.1.6 OCTET STRING(1 elem) SEQUENCE(1 elem) OBJECT IDENTIFIER0.4.0.1862.1.6.1	OID 0.4.0.1862.1.6.1 Certificado de firma electrónica 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	

Inicio

Campo *De PF Representante PJ*	en Software Autenticación y Firma	Oblig.	Crít.	Longitud máxima	Codificación	Observaciones OID 1.3.6.1.4.1.60078.1.2.1
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)	BEYOND THE SCOPE S.L	Sí		64 caracteres	UTF8String	OID 2.5.4.10
1.4.3. Locality Name (L)	Barcelona	Sí		128 caracteres	UTF8String	OID 2.5.4.7
1.4.4. Organization Identifier	VATES-B04948766	Sí		Ilimitado	UTF8String	OID 2.5.4.97
1.4.5. Common Name (CN)	Permisso CA Subordinada 01	Sí		64 caracteres	UTF8String	OID 2.5.4.3
1.4.6. Organizational Unit (OU)	TSP – Permisso	Sí			UTF8String	
1.5. Validity		Sí				
1.5.1. Not Before	Fecha de inicio de validez	Sí			UTCTime	YYMMDDHHMMSSZ
1.5.2. Not After	Fecha de expiración	Sí			UTCTime	YYMMDDHHMMSSZ
1.6. Subject		Sí				
1.6.1. Country Name	"ES"	Sí		2 caracteres	PrintableString	OID 2.5.4.6
1.6.2. Organization Name	Organización de la que el firmante es representante	No		64 caracteres	UTF8String	OID 2.5.4.10
1.6.3. Organizational Unit Name	Departamento al que pertenece el representante	No		64 caracteres	UTF8String	OID 2.5.4.11
1.6.4. Organization Identifier	Número oficial de identificación de la persona jurídica representada, en formato ETSI EN 319412-1 (Ejemplo: “VATES-Q0000000J)	Sí		Ilimitado	UTF8String	OID 2.5.4.97
1.6.5. Title	Representante legal	No		64 caracteres	UTF8String	OID 2.5.4.12
1.6.6. Surname	Apellidos del representante (como consta en el documento oficial)	Sí		40 caracteres	UTF8String	OID 2.5.4.4
1.6.7. Given Name	Nombre del representante (como consta en el documento oficial)	Sí		16 caracteres	UTF8String	OID 2.5.4.42
1.6.8. Serial Number	Número de documento oficial codificado acorde a ETSI EN 319 412-1 (“IDCES-12345678Z”)	Sí		64 caracteres	PrintableString	OID 2.5.4.5
1.6.9. Common Name	00000000T NOMBRE APELLIDOS (R: Q0000000J)	Sí		64 caracteres	UTF8String	OID 2.5.4.3
1.6.10. Description	Una de las tres opciones: • 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		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
2.2. 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				
2.3.2. Content commintment	Seleccionado “1”	Sí				
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	1.3.6.1.4.1.60078.1.2.1	Sí			OID	Identificador de la política de BANKFLIP
2.4.1.2. Policy Qualifiers		Sí				
2.4.1.1.1 CPS URI	https://qtsp.permisso.io/cps/	Sí			IA5String	URL de la DPC de BANKFLIP
2.4.1.1.2. User Notice/Explicit text	"Certificado cualificado de persona física Representante de Persona Jurídica ante las administraciones en software.“	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	Identificador de la política de certificado cualificado de persona física
2.4.2. Policy Information		Sí				
2.4.2.1. Policy Identifier	2.16.724.1.3.5.8	Sí			OID	Identificador de la política española de represantante ante AAPP, necesario para constar como tipo 11 en Afirma
2.5. Subject Alternative Names		No	No			OID 2.5.29.17 (Marcado como NO crítico según EN 319412-2)
2.5.1. rfc822Name	Correo electrónico del representante	No			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)	No			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.uanataca.com/public/pki/crl/PermissoCA1.crl	Sí			IA5String	uniformResourceIdentifier **(NO HTTPS)**
2.7.2. distributionPoint	http://crl2.uanataca.com/public/pki/crl/PermissoCA1.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
2.8.1.1.1 Acces Location	http://ocsp1.uanataca.com/public/pki/ocsp/	Sí			IA5String	URL de acceso al OCSP **(NO HTTPS)** uniformResourceIdentifier
2.8.1.1.2. Acces Location	http://ocsp2.uanataca.com/public/pki/ocsp/	No			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
2.8.2.1.1 Acces Location	https://qtsp.permisso.io/pki/subordinate1.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		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		Sí				OID 0.4.0.1862.1.5 (SI HTTPS) URL de acceso al texto divulgativo
2.9.4.1 PdsLocation						
2.9.4.1.1 url	https://qtsp.permisso.io/cps/	Sí			IA5String	
2.9.4.1.2 language	“EN”	Sí			PrintableString	(SIZE(2))} --ISO 639-1 language code
2.9.5. QcType	id-etsi-qct-esign	No			SEQUENCE(2 elem) OBJECT IDENTIFIER0.4.0.1862.1.6 OCTET STRING(1 elem) SEQUENCE(1 elem) OBJECT IDENTIFIER0.4.0.1862.1.6.1	OID 0.4.0.1862.1.6.1 Certificado de firma electrónica 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	

Inicio

Campo *De PF Representante PJ*	en HSM centralizado Autenticación y Firma	Oblig.	Crít.	Longitud máxima	Codificación	Observaciones OID 1.3.6.1.4.1.60078.1.2.2
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)	BEYOND THE SCOPE S.L	Sí		64 caracteres	UTF8String	OID 2.5.4.10
1.4.3. Locality Name (L)	Barcelona	Sí		128 caracteres	UTF8String	OID 2.5.4.7
1.4.4. Organization Identifier	VATES-B04948766	Sí		Ilimitado	UTF8String	OID 2.5.4.97
1.4.5. Common Name (CN)	Permisso CA Subordinada 01	Sí		64 caracteres	UTF8String	OID 2.5.4.3
1.4.6. Organizational Unit (OU)	TSP – Permisso	Sí			UTF8String	
1.5. Validity		Sí				
1.5.1. Not Before	Fecha de inicio de validez	Sí			UTCTime	YYMMDDHHMMSSZ
1.5.2. Not After	Fecha de expiración	Sí			UTCTime	YYMMDDHHMMSSZ
1.6. Subject		Sí				
1.6.1. Country Name	"ES"	Sí		2 caracteres	PrintableString	OID 2.5.4.6
1.6.2. Organization Name	Organización de la que el firmante es representante	Sí		64 caracteres	UTF8String	OID 2.5.4.10
1.6.3. Organizational Unit Name	Departamento al que pertenece representante	No		64 caracteres	UTF8String	OID 2.5.4.11
1.6.4. Organization Identifier	Número oficial de identificación de la persona jurídica representada, en formato ETSI EN 319412-1 (Ejemplo: “VATES-Q0000000J)	Sí		Ilimitado	UTF8String	OID 2.5.4.97
1.6.5. Title	Nombre del título o puesto del Representante	Sí		64 caracteres	UTF8String	OID 2.5.4.12
1.6.6. Surname	Apellidos del representante (como consta en el documento oficial)	Sí		40 caracteres	UTF8String	OID 2.5.4.4
1.6.7. Given Name	Nombre del representante (como consta en el documento oficial)	Sí		16 caracteres	UTF8String	OID 2.5.4.42
1.6.8. Serial Number	Número de documento oficial codificado acorde a ETSI EN 319 412-1 (“IDCES-12345678Z”)	Sí		64 caracteres	PrintableString	OID 2.5.4.5
1.6.9. Common Name	00000000T NOMBRE APELLIDOS (R: Q0000000J)	Sí		64 caracteres	UTF8String	OID 2.5.4.3
1.6.10. Description	Una de las tres opciones: • 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		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
2.2. 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				
2.3.3. Key Encipherment	Seleccionado “1”	Sí				
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	1.3.6.1.4.1.60078.1.2.2	Sí			OID	Identificador de la política de BANKFLIP
2.4.1.2. Policy Qualifiers		Sí				
2.4.1.1.1 CPS URI	https://qtsp.permisso.io/cps/	Sí			IA5String	URL de la DPC de BANKFLIP
2.4.1.1.2. User Notice/Explicit text	Certificado cualificado de persona física representante de persona jurídica ante las administraciones en HSM Centralizado	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	Identificador de la política de certificado cualificado de persona física
2.4.2. Policy Information		Sí				
2.4.2.1. Policy Identifier	2.16.724.1.3.5.8	Sí			OID	Identificador de la política española de represantante ante AAPP, necesario para constar como tipo 11 en Afirma
2.5. Subject Alternative Names		No	No			OID 2.5.29.17 (Marcado como NO crítico según EN 319412-2)
2.5.1. rfc822Name	Correo electrónico del representante	No			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)	No			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.uanataca.com/public/pki/crl/PermissoCA1.crl	Sí			IA5String	uniformResourceIdentifier **(NO HTTPS)**
2.7.2. distributionPoint	http://crl2.uanataca.com/public/pki/crl/PermissoCA1.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
2.8.1.1.1 Acces Location	http://ocsp1.uanataca.com/public/pki/ocsp/	Sí			IA5String	URL de acceso al OCSP **(NO HTTPS)** uniformResourceIdentifier
2.8.1.1.2. Acces Location	http://ocsp2.uanataca.com/public/pki/ocsp/	No			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
2.8.2.1.1 Acces Location	https://qtsp.permisso.io/pki/subordinate1.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		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		Sí				OID 0.4.0.1862.1.5 (SÍ HTTPS) URL de acceso al texto divulgativo
2.9.4.1 PdsLocation						
2.9.4.1.1 url	https://qtsp.permisso.io/cps/	Sí			IA5String	
2.9.4.1.2 language	“EN”	Sí			PrintableString	(SIZE(2))} --ISO 639-1 language code
2.9.5. QcType	id-etsi-qct-esign	Sí			SEQUENCE(2 elem) OBJECT IDENTIFIER0.4.0.1862.1.6 OCTET STRING(1 elem) SEQUENCE(1 elem) OBJECT IDENTIFIER0.4.0.1862.1.6.1	OID 0.4.0.1862.1.6.1 Certificado de firma electrónica 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	

Inicio

Campo *De PF Representante PJ*	en QSCD centralizado Autenticación y Firma	Oblig.	Crít.	Longitud máxima	Codificación	Observaciones OID 1.3.6.1.4.1.60078.1.2.3
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)	BEYOND THE SCOPE S.L	Sí		64 caracteres	UTF8String	OID 2.5.4.10
1.4.3. Locality Name (L)	Barcelona	Sí		128 caracteres	UTF8String	OID 2.5.4.7
1.4.4. Organization Identifier	VATES-B04948766	Sí		Ilimitado	UTF8String	OID 2.5.4.97
1.4.5. Common Name (CN)	Permisso CA Subordinada 01	Sí		64 caracteres	UTF8String	OID 2.5.4.3
1.4.6. Organizational Unit (OU)	TSP – Permisso	Sí			UTF8String	
1.5. Validity		Sí				
1.5.1. Not Before	Fecha de inicio de validez	Sí			UTCTime	YYMMDDHHMMSSZ
1.5.2. Not After	Fecha de expiración	Sí			UTCTime	YYMMDDHHMMSSZ
1.6. Subject		Sí				
1.6.1. Country Name	"ES"	Sí		2 caracteres	PrintableString	OID 2.5.4.6
1.6.2. Organization Name	Organización de la que el firmante es representante	Sí		64 caracteres	UTF8String	OID 2.5.4.10
1.6.3. Organizational Unit Name	Departamento al que pertenece representante	No		64 caracteres	UTF8String	OID 2.5.4.11
1.6.4. Organization Identifier	Número oficial de identificación de la persona jurídica representada, en formato ETSI EN 319412-1 (Ejemplo: "VATES-Q0000000J)	Sí		Ilimitado	UTF8String	OID 2.5.4.97
1.6.5. Title	Nombre del título o puesto del Representante	Sí		64 caracteres	UTF8String	OID 2.5.4.12
1.6.6. Surname	Apellidos del representante (como consta en el documento oficial)	Sí		40 caracteres	UTF8String	OID 2.5.4.4
1.6.7. Given Name	Nombre del representante (como consta en el documento oficial)	Sí		16 caracteres	UTF8String	OID 2.5.4.42
1.6.8. Serial Number	Número de documento oficial codificado acorde a ETSI EN 319 412-1 ("IDCES-12345678Z")	Sí		64 caracteres	PrintableString	OID 2.5.4.5
1.6.9. Common Name	00000000T NOMBRE APELLIDOS (R: Q0000000J)	Sí		64 caracteres	UTF8String	OID 2.5.4.3
1.6.10. Description	Una de las tres opciones: • 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		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
2.2. 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				
2.3.2. Content commintment	Seleccionado "1"	Sí				
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	1.3.6.1.4.1.60078.1.2.3	Sí			OID	Identificador de la política de BANKFLIP
2.4.1.2. Policy Qualifiers		Sí				
2.4.1.1.1 CPS URI	https://qtsp.permisso.io/cps/	Sí			IA5String	URL de la DPC de BANKFLIP
2.4.1.1.2. User Notice/Explicit text	Certificado cualificado de persona física representante de persona jurídica ante las administraciones en QSCD Centralizado	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	Identificador de la política de certificado cualificado de persona física
2.4.2. Policy Information		Sí				
2.4.2.1. Policy Identifier	2.16.724.1.3.5.8	Sí			OID	Identificador de la política española de represantante ante AAPP, necesario para constar como tipo 11 en Afirma
2.5. Subject Alternative Names		No	No			OID 2.5.29.17 (Marcado como NO crítico según EN 319412-2)
2.5.1. rfc822Name	Correo electrónico del representante	No			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)	No			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.uanataca.com/public/pki/crl/PermissoCA1.crl	Sí			IA5String	uniformResourceIdentifier **(NO HTTPS)**
2.7.2. distributionPoint	http://crl2.uanataca.com/public/pki/crl/PermissoCA1.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
2.8.1.1.1 Acces Location	http://ocsp1.uanataca.com/public/pki/ocsp/	Sí			IA5String	URL de acceso al OCSP **(NO HTTPS)** uniformResourceIdentifier
2.8.1.1.2. Acces Location	http://ocsp2.uanataca.com/public/pki/ocsp/	No			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
2.8.2.1.1 Acces Location	https://qtsp.permisso.io/pki/subordinate1.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		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		Sí				OID 0.4.0.1862.1.4 Dispositivo cualificado de creación de firma
2.9.4. QcPDS		Sí				OID 0.4.0.1862.1.5 (SI HTTPS) URL de acceso al texto divulgativo
2.9.4.1 PdsLocation						
2.9.4.1.1 url	https://qtsp.permisso.io/cps/	Sí			IA5String	
2.9.4.1.2 language	"EN"	Sí			PrintableString	(SIZE(2))} --ISO 639-1 language code
2.9.5. QcType	id-etsi-qct-esign	Sí			SEQUENCE(2 elem) OBJECT IDENTIFIER0.4.0.1862.1.6 OCTET STRING(1 elem) SEQUENCE(1 elem) OBJECT IDENTIFIER0.4.0.1862.1.6.1	OID 0.4.0.1862.1.6.1 Certificado de firma electrónica 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	

Campo *De PF Representante ESPJ*	en Software Autenticación y Firma	Oblig.	Crit.	Longitud máxima	Codificación	Observaciones OID 1.3.6.1.4.1.60078.1.3.1	Inicio
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)	BEYOND THE SCOPE S.L	Sí		64 caracteres	UTF8String	OID 2.5.4.10	
1.4.3. Locality Name (L)	Barcelona	Sí		128 caracteres	UTF8String	OID 2.5.4.7	
1.4.4. Organization Identifier	VATES-B04948766	Sí		Ilimitado	UTF8String	OID 2.5.4.97	
1.4.5. Common Name (CN)	Permisso CA Subordinada 01	Sí		64 caracteres	UTF8String	OID 2.5.4.3	
1.4.6. Organizational Unit (OU)	TSP – Permisso	Sí			UTF8String		
1.5. Validity		Sí					
1.5.1. Not Before	Fecha de inicio de validez	Sí			UTCTime	YYMMDDHHMMSSZ	
1.5.2. Not After	Fecha de expiración	Sí			UTCTime	YYMMDDHHMMSSZ	
1.6. Subject		Sí					
1.6.1. Country Name	"ES"	Sí		2 caracteres	PrintableString	OID 2.5.4.6	
1.6.2. Organization Name	Organización de la que el firmante es representante	No		64 caracteres	UTF8String	OID 2.5.4.10	
1.6.3. Organizational Unit Name	Departamento al que pertenece el representante	No		64 caracteres	UTF8String	OID 2.5.4.11	
1.6.4. Organization Identifier	Número oficial de identificación de la persona jurídica representada, en formato ETSI EN 319412-1 (Ejemplo: "VATES-Q0000000J)	Sí		Ilimitado	UTF8String	OID 2.5.4.97	
1.6.5. Title	Representante legal	No		64 caracteres	UTF8String	OID 2.5.4.12	
1.6.6. Surname	Apellidos del representante (como consta en el documento oficial)	Sí		40 caracteres	UTF8String	OID 2.5.4.4	
1.6.7. Given Name	Nombre del representante (como consta en el documento oficial)	Sí		16 caracteres	UTF8String	OID 2.5.4.42	
1.6.8. Serial Number	Número de documento oficial codificado acorde a ETSI EN 319 412-1 ("IDCES-12345678Z")	Sí		64 caracteres	PrintableString	OID 2.5.4.5	
1.6.9. Common Name	00000000T NOMBRE APELLIDOS (R: Q0000000J)	Sí		64 caracteres	UTF8String	OID 2.5.4.3	
1.6.10. Description	Una de las tres opciones: • 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		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	
2.2. 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					
2.3.2. Content commintment	Seleccionado "1"	Sí					
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		Si					
2.4.1.1. Policy Identifier	1.3.6.1.4.1.60078.1.3.1	Sí			OID	Identificador de la política de BANKFLIP	
2.4.1.2. Policy Qualifiers		Si					
2.4.1.1.1 CPS URI	https://qtsp.permisso.io/cps/	Sí			IA5String	URL de la DPC de BANKFLIP	
2.4.1.1.2. User Notice/Explicit text	"Certificado cualificado de persona física Representante de Entidad sin Personalidad Jurídica ante las administraciones en software."	Sí		200 caracteres	UTF8String y NFC	Texto indicativo	
2.4.2. Policy Information		Si					
2.4.2.1. Policy Identifier	0.4.0.194112.1.0	Sí			OID	Identificador de la política de certificado cualificado de persona física	
2.4.2. Policy Information		Si					
2.4.2.1. Policy Identifier	2.16.724.1.3.5.9	Sí			OID	Identificador de la política española de representante de Entidad Sin Personalidad Jurídica ante AAPP, necesario para constar como tipo 12 en Afirma	
2.5. Subject Alternative Names		No	No			OID 2.5.29.17 (Marcado como NO crítico según EN 319412-2)	
2.5.1. rfc822Name	Correo electrónico del representante	No			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)	No			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.uanataca.com/public/pki/crl/PermissoCA1.crl	Sí			IA5String	uniformResourceIdentifier **(NO HTTPS)**	
2.7.2. distributionPoint	http://crl2.uanataca.com/public/pki/crl/PermissoCA1.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	
2.8.1.1.1 Acces Location	http://ocsp1.uanataca.com/public/pki/ocsp/	Sí			IA5String	URL de acceso al OCSP **(NO HTTPS)** uniformResourceIdentifier	
2.8.1.1.2. Acces Location	http://ocsp2.uanataca.com/public/pki/ocsp/	No			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	
2.8.2.1.1 Acces Location	https://qtsp.permisso.io/pki/subordinate1.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		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		Sí				OID 0.4.0.1862.1.5 (SI HTTPS) URL de acceso al texto divulgativo	
2.9.4.1 PdsLocation							
2.9.4.1.1 url	https://qtsp.permisso.io/cps/	Sí			IA5String		
2.9.4.1.2 language	"EN"	Sí			PrintableString	(SIZE(2))} --ISO 639-1 language code	
2.9.5. QcType	id-etsi-qct-esign	No			SEQUENCE(2 elem) OBJECT IDENTIFIER0.4.0.1862.1.6 OCTET STRING(1 elem) SEQUENCE(1 elem) OBJECT IDENTIFIER0.4.0.1862.1.6.1	OID 0.4.0.1862.1.6.1 Certificado de firma electrónica 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		

Inicio

Campo *De PF Representante ESPJ*	en HSM centralizado Autenticación y Firma	Oblig.	Crít.	Longitud máxima	Codificación	Observaciones OID 1.3.6.1.4.1.60078.1.3.2
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)	BEYOND THE SCOPE S.L	Sí		64 caracteres	UTF8String	OID 2.5.4.10
1.4.3. Locality Name (L)	Barcelona	Sí		128 caracteres	UTF8String	OID 2.5.4.7
1.4.4. Organization Identifier	VATES-B04948766	Sí		Ilimitado	UTF8String	OID 2.5.4.97
1.4.5. Common Name (CN)	Permisso CA Subordinada 01	Sí		64 caracteres	UTF8String	OID 2.5.4.3
1.4.6. Organizational Unit (OU)	TSP – Permisso	Sí			UTF8String	
1.5. Validity		Sí				
1.5.1. Not Before	Fecha de inicio de validez	Sí			UTCTime	YYMMDDHHMMSSZ
1.5.2. Not After	Fecha de expiración	Sí			UTCTime	YYMMDDHHMMSSZ
1.6. Subject		Sí				
1.6.1. Country Name	"ES"	Sí		2 caracteres	PrintableString	OID 2.5.4.6
1.6.2. Organization Name	Organización de la que el firmante es representante	Sí		64 caracteres	UTF8String	OID 2.5.4.10
1.6.3. Organizational Unit Name	Departamento al que pertenece representante	No		64 caracteres	UTF8String	OID 2.5.4.11
1.6.4. Organization Identifier	Número oficial de identificación de la persona jurídica representada, en formato ETSI EN 319412-1 (Ejemplo: "VATES-Q0000000J)	Sí		Ilimitado	UTF8String	OID 2.5.4.97
1.6.5. Title	Nombre del título o puesto del Representante	Sí		64 caracteres	UTF8String	OID 2.5.4.12
1.6.6. Surname	Apellidos del representante (como consta en el documento oficial)	Sí		40 caracteres	UTF8String	OID 2.5.4.4
1.6.7. Given Name	Nombre del representante (como consta en el documento oficial)	Sí		16 caracteres	UTF8String	OID 2.5.4.42
1.6.8. Serial Number	Número de documento oficial codificado acorde a ETSI EN 319 412-1 ("IDCES-12345678Z")	Sí		64 caracteres	PrintableString	OID 2.5.4.5
1.6.9. Common Name	00000000T NOMBRE APELLIDOS (R: Q0000000J)	Sí		64 caracteres	UTF8String	OID 2.5.4.3
1.6.10. Description	Una de las tres opciones: • 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		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
2.2. 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				
2.3.2. Content commintment	Seleccionado "1"	Sí				
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	1.3.6.1.4.1.60078.1.3.2	Sí			OID	Identificador de la política de BANKFLIP
2.4.1.2. Policy Qualifiers		Sí				
2.4.1.1.1 CPS URI	https://qtsp.permisso.io/cps/	Sí			IA5String	URL de la DPC de BANKFLIP
2.4.1.1.2. User Notice/Explicit text	Certificado cualificado de persona física representante de entidad sin personalidad jurídica ante las administraciones en HSM centralizado	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	Identificador de la política de certificado cualificado de persona física
2.4.2. Policy Information		Sí				
2.4.2.1. Policy Identifier	2.16.724.1.3.5.9	Sí			OID	Identificador de la política española de represantante de Entidad Sin Personalidad Jurídica ante AAPP, necesario para constar como tipo 12 en Afirma
2.5. Subject Alternative Names		No	No			OID 2.5.29.17 (Marcado como NO crítico según EN 319412-2)
2.5.1. rfc822Name	Correo electrónico del representante	No			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)	No			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.uanataca.com/public/pki/crl/PermissoCA1.crl	Sí			IA5String	uniformResourceIdentifier **(NO HTTPS)**
2.7.2. distributionPoint	http://crl2.uanataca.com/public/pki/crl/PermissoCA1.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
2.8.1.1.1 Acces Location	http://ocsp1.uanataca.com/public/pki/ocsp/	Sí			IA5String	URL de acceso al OCSP **(NO HTTPS)** uniformResourceIdentifier
2.8.1.1.2. Acces Location	http://ocsp2.uanataca.com/public/pki/ocsp/	No			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
2.8.2.1.1 Acces Location	https://qtsp.permisso.io/pki/subordinate1.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		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		Sí				OID 0.4.0.1862.1.5 (SI HTTPS) URL de acceso al texto divulgativo
2.9.4.1 PdsLocation						
2.9.4.1.1 url	https://qtsp.permisso.io/cps/	Sí			IA5String	
2.9.4.1.2 language	"EN"	Sí			PrintableString	(SIZE(2))} --ISO 639-1 language code
2.9.5. QcType	id-etsi-qct-esign	Sí			SEQUENCE(2 elem) OBJECT IDENTIFIER0.4.0.1862.1.6 OCTET STRING(1 elem) SEQUENCE(1 elem) OBJECT IDENTIFIER0.4.0.1862.1.6.1	OID 0.4.0.1862.1.6.1 Certificado de firma electrónica 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	

Inicio

Campo *De PF Representante ESPJ*	en QSCD centralizado Autenticación y Firma	Oblig.	Crít.	Longitud máxima	Codificación	Observaciones OID 1.3.6.1.4.1.60078.1.3.3
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)	BEYOND THE SCOPE S.L	Sí		64 caracteres	UTF8String	OID 2.5.4.10
1.4.3. Locality Name (L)	Barcelona	Sí		128 caracteres	UTF8String	OID 2.5.4.7
1.4.4. Organization Identifier	VATES-B04948766	Sí		Ilimitado	UTF8String	OID 2.5.4.97
1.4.5. Common Name (CN)	Permisso CA Subordinada 01	Sí		64 caracteres	UTF8String	OID 2.5.4.3
1.4.6. Organizational Unit (OU)	TSP – Permisso	Sí			UTF8String	
1.5. Validity		Sí				
1.5.1. Not Before	Fecha de inicio de validez	Sí			UTCTime	YYMMDDHHMMSSZ
1.5.2. Not After	Fecha de expiración	Sí			UTCTime	YYMMDDHHMMSSZ
1.6. Subject		Sí				
1.6.1. Country Name	"ES"	Sí		2 caracteres	PrintableString	OID 2.5.4.6
1.6.2. Organization Name	Organización de la que el firmante es representante	Sí		64 caracteres	UTF8String	OID 2.5.4.10
1.6.3. Organizational Unit Name	Departamento al que pertenece representante	No		64 caracteres	UTF8String	OID 2.5.4.11
1.6.4. Organization Identifier	Número oficial de identificación de la persona jurídica representada, en formato ETSI EN 319412-1 (Ejemplo: “VATES-Q0000000J)	Sí		Ilimitado	UTF8String	OID 2.5.4.97
1.6.5. Title	Nombre del título o puesto del Representante	Sí		64 caracteres	UTF8String	OID 2.5.4.12
1.6.6. Surname	Apellidos del representante (como consta en el documento oficial)	Sí		40 caracteres	UTF8String	OID 2.5.4.4
1.6.7. Given Name	Nombre del representante (como consta en el documento oficial)	Sí		16 caracteres	UTF8String	OID 2.5.4.42
1.6.8. Serial Number	Número de documento oficial codificado acorde a ETSI EN 319 412-1 (“IDCES-12345678Z”)	Sí		64 caracteres	PrintableString	OID 2.5.4.5
1.6.9. Common Name	00000000T NOMBRE APELLIDOS (R: Q0000000J)	Sí		64 caracteres	UTF8String	OID 2.5.4.3
1.6.10. Description	Una de las tres opciones: • 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		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
2.2. 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				
2.3.2. Content commintment	Seleccionado “1”	Sí				
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	1.3.6.1.4.1.60078.1.3.3	Sí			OID	Identificador de la política de BANKFLIP
2.4.1.2. Policy Qualifiers		Sí				
2.4.1.1.1 CPS URI	https://qtsp.permisso.io/cps/	Sí			IA5String	URL de la DPC de BANKFLIP
2.4.1.1.2. User Notice/Explicit text	Certificado cualificado de persona física representante de entidad sin personalidad jurídica ante las administraciones en QSCD centralizado	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	Identificador de la política de certificado cualificado de persona física
2.4.2. Policy Information		Sí				
2.4.2.1. Policy Identifier	2.16.724.1.3.5.9	Sí			OID	Identificador de la política española de representante de Entidad Sin Personalidad Jurídica ante AAPP, necesario para constar como tipo 12 en Afirma
2.5. Subject Alternative Names		No	No			OID 2.5.29.17 (Marcado como NO crítico según EN 319412-2)
2.5.1. rfc822Name	Correo electrónico del representante	No			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)	No			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.uanataca.com/public/pki/crl/PermissoCA1.crl	Sí			IA5String	uniformResourceIdentifier **(NO HTTPS)**
2.7.2. distributionPoint	http://crl2.uanataca.com/public/pki/crl/PermissoCA1.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
2.8.1.1.1 Acces Location	http://ocsp1.uanataca.com/public/pki/ocsp/	Sí			IA5String	URL de acceso al OCSP **(NO HTTPS)** uniformResourceIdentifier
2.8.1.1.2. Acces Location	http://ocsp2.uanataca.com/public/pki/ocsp/	No			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
2.8.2.1.1 Acces Location	https://qtsp.permisso.io/pki/subordinate1.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		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		Sí				OID 0.4.0.1862.1.4 Dispositivo cualificado de creación de firma
2.9.4. QcPDS		Sí				OID 0.4.0.1862.1.5 (SÍ HTTPS) URL de acceso al texto divulgativo
2.9.4.1 PdsLocation						
2.9.4.1.1 url	https://qtsp.permisso.io/cps/	Sí			IA5String	
2.9.4.1.2 language	“EN”	Sí			PrintableString	(SIZE(2))} --ISO 639-1 language code
2.9.5. QcType	id-etsi-qct-esign	Sí			SEQUENCE(2 elem) OBJECT IDENTIFIER0.4.0.1862.1.6 OCTET STRING(1 elem) SEQUENCE(1 elem) OBJECT IDENTIFIER0.4.0.1862.1.6.1	OID 0.4.0.1862.1.6.1 Certificado de firma electrónica 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	