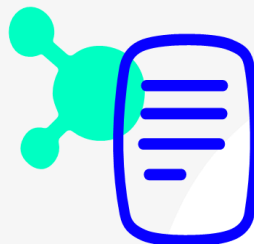


## Perfiles de certificados



## INFORMACIÓN GENERAL

<b>Distribución</b>	<b>Pública (web)</b>
<b>Fecha</b>	<b>17/05/2023</b>
<b>Descripción</b>	<b>Perfiles de certificados para su publicación en la web</b>

## CONTROL DE VERSIONES

VERSIÓN	PARTES CAMBIADAS	DESCRIPCIÓN CAMBIO	AUTOR	FECHA
1.24	Todo	Versión para publicación web	AC	17/05/2023

# Índice

1	PERFILES .....	4
1.1	Persona Física Cualificado Cloud HSM .....	4
1.2	Persona Física Vinculada .....	10
1.3	Sello electrónico Cloud HSM .....	16
1.4	Sello electrónico.....	22
1.5	Sello electrónico PSD2.....	28
1.6	SSL-EV PSD2.....	35
1.7	Sello electrónico de TSU.....	40
1.8	PF representante de PJ.....	46

## 1 PERFILES

	Gestión CENTRALIZADA (Identificación y Firma)	Oblig.	Crít.
1.1 Persona Física Cualificado Cloud HSM			
<b>1. Basic structure</b>			
1.1. Version	3	Sí	
1.2. Serial Number	Establecido automáticamente por la CA. Número identificativo único del certificado.	Sí	
1.3. Signature Algorithm		Sí	
1.3.1. Algorithm	SHA-256 with RSA Signature	Sí	
1.3.2. Parameters	No aplicable	No	
1.4. Issuer		Sí	
1.4.1. Country Name (C)	"ES"	Sí	
1.4.2. Organization Name (O)	"Logalty Servicios de Tercero de Confianza SL"	Sí	
1.4.3. Locality Name (L)	"Alcobendas"	Sí	
1.4.4. Organization Identifier	"VATES-B84492891"	Sí	
1.4.5. Common Name (CN)	"Logalty Qualified CA G2"	Sí	
1.4.6. stateOrProvinceName	"Madrid"	Sí	

1.4.7. <i>organizationalUnitName</i> (OU)	"Logalty Trust Services"	Sí	
<b>1.5. Validity</b>		Sí	
1.5.1. Not Before	Fecha de inicio de validez	Sí	
1.5.2. Not After	Fecha de expiración (3 years)	Sí	
<b>1.6. Subject</b>		Sí	
1.6.1. <i>Country Name</i>	País de residencia o nacionalidad del firmante.	Sí	
1.6.6. <i>Surname</i>	Apellidos del firmante (como consta en el documento oficial)	Sí	
1.6.7. <i>Given Name</i>	Nombre del firmante (como consta en el documento oficial)	Sí	
1.6.8. <i>Serial Number</i>	Número de documento oficial codificado acorde a ETSI EN 319 412-1 ("IDCES-123456789Z")	Sí	
1.6.9. <i>Common Name</i>	Nombre y apellidos firmante - NIF 00000000T	Sí	
<b>1.7. Subject Public Key Info</b>		Sí	
1.7.1. <i>AlgorithmIdentifier</i>			
1.7.1.1. <i>Algorithm</i>	RSA encryption	Sí	
1.7.1.2. <i>Parameters</i>	No aplicable	No	
1.7.2. <i>SubjectPublicKey</i>	Clave pública del firmante	Sí	
<b>2. Extensions</b>			

<b>2.1. Authority Key Identifier</b>	Identificador de la clave del emisor	Sí	No
<i>2.1.1. KeyIdentifier</i>		Sí	
<b>2.2. Subject Key Identifier</b>	Identificador de la clave del firmante	Sí	No
<i>2.2.1. KeyIdentifier</i>		Sí	
<b>2.3. Key Usage</b>		Sí	Sí
<i>2.3.1. Digital Signature</i>	Seleccionado "1"	Sí	
<i>2.3.2. Content commintment</i>	Seleccionado "1"	Sí	
<i>2.3.3. Key Encipherment</i>	No seleccionado. "0"		
<i>2.3.4. Data Encipherment</i>	No seleccionado. "0"		
<i>2.3.5. Key Agreement</i>	No seleccionado. "0"		
<i>2.3.6. Key Certificate Signature</i>	No seleccionado. "0"		
<i>2.3.7. CRL Signature</i>	No seleccionado. "0"		
<i>2.3.8. Encipher Only</i>	No seleccionado. "0"		
<i>2.3.9. Decipher Only</i>	No seleccionado. "0"		
<b>2.4. Certificate Policies</b>		Si	No
<i>2.4.1. Policy Information</i>		Sí	

2.4.1.1. Policy Identifier	1.3.6.1.4.1.30210.1.1.1	Sí	
2.4.1.2. Policy Qualifiers		Sí	
2.4.1.1.1 CPS URI	<a href="https://www.logalty.com/certificateauthority/">https://www.logalty.com/certificateauthority/</a>		
2.4.1.1.2. User Notice/Explicit text	“Certificado cualificado de firma electrónica cualificada de persona física con gestión de datos de creación de firma electrónica en nombre del firmante”	Sí	
2.4.2. Policy Information		Sí	
2.4.2.1. Policy Identifier	0.4.0.194112.1.2	Sí	
<b>2.5. Subject Alternative Names</b>		No	No
2.5.1. rfc822Name	Correo electrónico del firmante	No	
<b>2.6. Extended Key Usage</b>		Sí	No
2.6.1. clientAuth	Presente (1.3.6.1.5.5.7.3.2)	Sí	
2.6.2. Email protection	Presente (1.3.6.1.5.5.7.3.4)	No	
<b>2.7. cRLDistributionPoint</b>		No	No
2.7.1. distributionPoint	<a href="http://crl1.logalty.es/qualifiedLogaltySubCA02.crl">http://crl1.logalty.es/qualifiedLogaltySubCA02.crl</a>	Sí	

2.7.2. <i>distributionPoint</i>	<a href="http://crl2.logalty.es/qualifiedLogaltySubCA02.crl">http://crl2.logalty.es/qualifiedLogaltySubCA02.crl</a>	Sí	
<b>2.8. Authority Info Acces</b>		Sí	No
2.8.1. <i>Access Description</i>		Sí	
2.8.1.1. <i>Acces Method</i>	<i>id-ad-ocsp</i>	Sí	
2.8.1.2. <i>Acces Location</i>	<a href="http://ocspl.logalty.es">http://ocspl.logalty.es</a>	Sí	
2.8.2. <i>Access Description</i>		Sí	
2.8.2.1. <i>Acces Method</i>	<i>id-ad-caIssuers</i>	Sí	
2.8.2.1. <i>Acces Location</i>	<a href="http://crt.logalty.es/certificateauthority/LogaltyQualifiedCAG2.crt">http://crt.logalty.es/certificateauthority/LogaltyQualifiedCAG2.crt</a>	Sí	
<b>2.9. Qualified Certificate Statements</b>		Sí	No
2.9.1. <i>qCCompliance</i>		Sí	
2.9.2. <i>QcEuRetentionPeriod</i>	"15"	Sí	
2.9.3. <i>QcSSCD</i>		Sí	
2.9.4. <i>QcPDS</i>		Sí	



2.9.4.1 PdsLocation			
2.9.4.1.1 url	<a href="https://www.logalty.es/certificateauthority/en/LGT_PDS_receptor.v1r0.pdf">https://www.logalty.es/certificateauthority/en/LGT_PDS_receptor.v1r0.pdf</a>	Sí	
2.9.4.1.2 language	"EN"	Sí	
2.9.4.2 PdsLocation			
2.9.4.2.1 url	<a href="https://www.logalty.es/certificateauthority/es/LGT_PDS_receptor.v1r0.pdf">https://www.logalty.es/certificateauthority/es/LGT_PDS_receptor.v1r0.pdf</a>	Sí	
2.9.4.2.2 language	"ES"	Sí	
2.9.5. QcType	Qct-esign	Sí	
2.9.6. qcStatement-2			
2.9.6.1. SemanticsInformation			
2.9.6.1.1. semanticsIdNatural	0.4.0.194121.1.1		
<b>2.10. Basic Constraints</b>		Sí	Sí
2.10.1. cA	FALS	Sí	

	En SOFTWARE (Identificación y Firma)	Oblig.	Crít.
1.2 Persona Física Vinculada			
<b>1. Basic estructura</b>			
1.1. Version	3	Sí	
1.2. Serial Number	Establecido automáticamente por la CA. Número identificativo único del certificado.	Sí	
1.3. Signature Algorithm		Sí	
1.3.1. Algorithm	SHA-256 with RSA Signature	Sí	
1.3.2. Parameters	No aplicable	No	
1.4. Issuer		Sí	
1.4.1. Country Name (C)	"ES"	Sí	
1.4.2. Organization Name (O)	"Logalty Servicios de Tercero de Confianza SL"	Sí	
1.4.3. Locality Name (L)	"Alcobendas"	Sí	
1.4.4. Organization Identifier	"VATES-B84492891"	Sí	
1.4.5. Common Name (CN)	"Logalty Qualified CA G2"	Sí	
1.4.6. stateOrProvinceName	"Madrid"	Sí	

1.4.7. <i>organizationalUnitName (OU)</i>	"Logalty Trust Services"	Sí	
<b>1.5. Validity</b>		Sí	
1.5.1. <i>Not Before</i>	Fecha de inicio de validez	Sí	
1.5.2. <i>Not After</i>	Fecha de expiración (3 years)	Sí	
<b>1.6. Subject</b>		Sí	
1.6.1. <i>Country Name</i>	País de residencia o nacionalidad del firmante.	Sí	
1.6.2. <i>Organization Name</i>	Organización a la que pertenece el firmante.	Sí	
1.6.4. <i>Organization Identifier</i>	Número oficial de identificación de la persona jurídica a la que está vinculado el firmante, en formato ETSI EN 319412-1 (Ejemplo: "VATES-Q0000000J")	Sí	
1.6.5. <i>Title</i>	Cargo del firmante en la organización	No	
1.6.6. <i>Surname</i>	Apellidos del firmante (como consta en el documento oficial)	Sí	
1.6.7. <i>Given Name</i>	Nombre del firmante (como consta en el documento oficial)	Sí	
1.6.8. <i>Serial Number</i>	Número de documento oficial del firmante codificado acorde a ETSI EN 319 412-1 ("IDCES-123456789Z")	Sí	
1.6.9. <i>Common Name</i>	Nombre y apellidos firmante - NIF 00000000T	Sí	
<b>1.7. Subject Public Key Info</b>		Sí	

1.7.1. AlgorithmIdentifier			
1.7.1.1. Algorithm	RSA encryption	Sí	
1.7.1.2. Parameters	No aplicable	No	
1.7.2. SubjectPublicKey	Clave pública del firmante	Sí	
<b>2. Extensions</b>			
<b>2.1. Authority Key Identifier</b>	Identificador de la clave del emisor	Sí	No
2.1.1. KeyIdentifier		Sí	
<b>2.2. Subject Key Identifier</b>	Identificador de la clave del firmante	Sí	No
2.2.1. KeyIdentifier		Sí	
<b>2.3. Key Usage</b>		Sí	Sí
2.3.1. Digital Signature	Seleccionado "1"	Sí	
2.3.2. Content commitment	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"		

2.3.8. Encipher Only	No seleccionado. "0"		
2.3.9. Decipher Only	No seleccionado. "0"		
<b>2.4. Certificate Policies</b>		<b>Si</b>	<b>No</b>
2.4.1. Policy Information		Sí	
2.4.1.1. Policy Identifier	1.3.6.1.4.1.30210.1.2.3	Sí	
2.4.1.2. Policy Qualifiers		Sí	
2.4.1.1.1 CPS URI	<a href="https://www.logalty.com/certificateauthority/">https://www.logalty.com/certificateauthority/</a>		
2.4.1.1.2. User Notice/Explicit text	"Certificado cualificado de firma electrónica avanzada de persona física vinculada a persona jurídica"	Sí	
2.4.2. Policy Information		Sí	
2.4.2.1. Policy Identifier	0.4.0.194112.1.0	Sí	
<b>2.6. Extended Key Usage</b>		<b>Sí</b>	<b>No</b>
2.6.1. clientAuth	Presente (1.3.6.1.5.5.7.3.2)	Sí	
2.6.2. Email protection	Presente (1.3.6.1.5.5.7.3.4)	No	
<b>2.7. cRLDistributionPoint</b>		<b>No</b>	<b>No</b>
2.7.1. distributionPoint	<a href="http://crl1.logalty.es/qualifiedLogaltySubCA02.crl">http://crl1.logalty.es/qualifiedLogaltySubCA02.crl</a>	Sí	

2.7.2. <i>distributionPoint</i>	<a href="http://crl2.logalty.es/qualifiedLogaltySubCA02.crl">http://crl2.logalty.es/qualifiedLogaltySubCA02.crl</a>	<i>Sí</i>	
<b>2.8. Authority Info Acces</b>		<b>Sí</b>	<b>No</b>
2.8.1. <i>Access Description</i>		<b>Sí</b>	
2.8.1.1. <i>Acces Method</i>	<i>id-ad-ocsp</i>	<i>Sí</i>	
2.8.1.2. <i>Acces Location</i>	<a href="http://ocsp1.logalty.es">http://ocsp1.logalty.es</a>	<i>Sí</i>	
2.8.2. <i>Access Description</i>		<b>Sí</b>	
2.8.2.1. <i>Acces Method</i>	<i>id-ad-caIssuers</i>	<i>Sí</i>	
2.8.2.1. <i>Acces Location</i>	<a href="http://crt.logalty.es/certificateauthority/LogaltyQualifiedCAG2.crt">http://crt.logalty.es/certificateauthority/LogaltyQualifiedCAG2.crt</a>	<i>Sí</i>	
<b>2.9. Qualified Certificate Statements</b>		<b>Sí</b>	<b>No</b>
2.9.1. <i>qCCompliance</i>		<b>Sí</b>	
2.9.2. <i>QcEuRetentionPeriod</i>	"15"	<b>Sí</b>	
2.9.4.1 <i>PdsLocation</i>			
2.9.4.1.1 <i>url</i>	<a href="https://www.logalty.es/certificateauthority/en/LGT_PDS_emisor.v1r0.pdf">https://www.logalty.es/certificateauthority/en/LGT_PDS_emisor.v1r0.pdf</a>	<i>Sí</i>	

2.9.4.1.2 language	"EN"	Sí	
2.9.4.2 PdsLocation			
2.9.4.2.1 url	<a href="https://www.logalty.es/certificateauthority/es/LGT_PDS_emisor.v1r0.pdf">https://www.logalty.es/certificateauthority/es/LGT_PDS_emisor.v1r0.pdf</a>	Sí	
2.9.4.2.2 language	"ES"	Sí	
2.9.5. QcType	Qct-esign	Sí	
2.9.6. qcStatement-2			
2.9.6.1. SemanticsInformation			
2.9.6.1.1. semanticsIdNatural	0.4.0.194121.1.1		
<b>2.10. Basic Constraints</b>		Sí	Sí
2.10.1. cA	FALS	Sí	

	Gestión CENTRALIZADA (Identificación y Firma)	Oblig.	Crít.
1.3 Sello electrónico Cloud HSM			
<b>1. Basic estructura</b>			
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. Algorithm	SHA-256 with RSA Signature	Sí	
1.3.2. Parameters	No aplicable	No	
1.4. Issuer		Sí	
1.4.1. Country Name (C)	"ES"	Sí	
1.4.2. Organization Name (O)	"Logalty Servicios de Tercero de Confianza SL"	Sí	
1.4.3. Locality Name (L)	"Alcobendas"	Sí	
1.4.4. Organization Identifier	"VATES-B84492891"	Sí	
1.4.5. Common Name (CN)	"Logalty Qualified CA G2"	Sí	
1.4.6. stateOrProvinceName	"Madrid"	Sí	



1.4.7. <i>organizationalUnitName (OU)</i>	"Logalty Trust Services"	Sí	
<b>1.5. Validity</b>		Sí	
1.5.1. Not Before	Fecha de inicio de validez	Sí	
1.5.2. Not After	Fecha de expiración (3 years)	Sí	
<b>1.6. Subject</b>		Sí	
1.6.1. <i>Country Name</i>	País de residencia o nacionalidad de la organización	Sí	
1.6.2. <i>Organization Name</i>	Denominación oficial de la Organización titular del certificado	Sí	
1.6.4. <i>Organization Identifier</i>	Número oficial de identificación de la persona jurídica titular del certificado, en formato ETSI EN 319412-1 (Ejemplo: "VATES-Q0000000J")	Sí	
1.6.8. <i>Serial Number</i>	NIF de la empresa titular	Sí	
1.6.9. <i>Locality Name (L)</i>	Localidad de la organización	Sí	
1.6.10. <i>Common Name</i>	Nombre de la plataforma donde reside el sello	Sí	
<b>1.7. Subject Public Key Info</b>		Sí	
1.7.1. <i>AlgorithmIdentifier</i>			
1.7.1.1. <i>Algorithm</i>	RSA encryption	Sí	
1.7.1.2. <i>Parameters</i>	No aplicable	No	

1.7.2. SubjectPublicKey	Clave pública del firmante	Sí	
<b>2. Extensions</b>			
<b>2.1. Authority Key Identifier</b>	Identificador de la clave del emisor	Sí	No
2.1.1. KeyIdentifier		Sí	
<b>2.2. Subject Key Identifier</b>	Identificador de la clave del firmante	Sí	No
2.2.1. KeyIdentifier		Sí	
<b>2.3. Key Usage</b>		Sí	Sí
2.3.1. Digital Signature	Seleccionado "1"	Sí	
2.3.2. Content commitment	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"		
<b>2.4. Certificate Policies</b>		Si	No

2.4.1. Policy Information		Sí	
2.4.1.1. Policy Identifier	1.3.6.1.4.1.30210.1.3.1	Sí	
2.4.1.2. Policy Qualifiers		Sí	
2.4.1.1.1 CPS URI	<a href="https://www.logalty.com/certificateauthority/">https://www.logalty.com/certificateauthority/</a>		
2.4.1.1.2. User Notice/Explicit text	"Certificado cualificado de sello electrónico cualificado de persona jurídica con gestión de datos de creación de sello electrónico en nombre del creador de sellos"	Sí	
2.4.2. Policy Information		Sí	
2.4.2.1. Policy Identifier	0.4.0.194112.1.3	Sí	
<b>2.6. Extended Key Usage</b>		Sí	No
2.6.1. clientAuth	Presente (1.3.6.1.5.5.7.3.2)	Sí	
2.6.2. Email protection	Presente (1.3.6.1.5.5.7.3.4)	No	
<b>2.7. cRLDistributionPoint</b>		No	No
2.7.1. distributionPoint	<a href="http://crl1.logalty.es/qualifiedLogaltySubCA02.crl">http://crl1.logalty.es/qualifiedLogaltySubCA02.crl</a>	Sí	
2.7.2. distributionPoint	<a href="http://crl2.logalty.es/qualifiedLogaltySubCA02.crl">http://crl2.logalty.es/qualifiedLogaltySubCA02.crl</a>	Sí	

2.8. Authority Info Acces		Sí	No
2.8.1. Access Description		Sí	
2.8.1.1. Acces Method	<i>id-ad-ocsp</i>	Sí	
2.8.1.2. Acces Location	<a href="http://ocsp1.logalty.es">http://ocsp1.logalty.es</a>	Sí	
2.8.2. Access Description		Sí	
2.8.2.1. Acces Method	<i>id-ad-caIssuers</i>	Sí	
2.8.2.1. Acces Location	<a href="http://crt.logalty.es/certificateauthority/LogaltyQualifiedCAG2.crt">http://crt.logalty.es/certificateauthority/LogaltyQualifiedCAG2.crt</a>	Sí	
2.9. Qualified Certificate Statements		Sí	No
2.9.1. qCCompliance		Sí	
2.9.2. QcEuRetentionPeriod	"15"	Sí	
2.9.3. QcSSCD		Sí	
2.9.4. QcPDS		Sí	
2.9.4.1 PdsLocation			

2.9.4.1.1 url	<a href="https://www.logalty.es/certificateauthority/en/LGT_PDS_emisor.v1r0.pdf">https://www.logalty.es/certificateauthority/en/LGT_PDS_emisor.v1r0.pdf</a>	Sí	
2.9.4.1.2 language	"EN"	Sí	
2.9.4.2 PdsLocation			
2.9.4.2.1 url	<a href="https://www.logalty.es/certificateauthority/es/LGT_PDS_emisor.v1r0.pdf">https://www.logalty.es/certificateauthority/es/LGT_PDS_emisor.v1r0.pdf</a>	Sí	
2.9.4.2.2 language	"ES"	Sí	
2.9.5. QcType	Qct-eseal	Sí	
2.9.6. qcStatement-2			
2.9.6.1. SemanticsInformation			
2.9.6.1.2. semanticsIdLegal	0.4.0.194121.1.2		
<b>2.10. Basic Constraints</b>		Sí	Sí
2.10.1. cA	FALS	Sí	

	En SOFTWARE (Identificación y Firma)	Oblig.	Crít.
1.4 Sello electrónico			
<b>1. Basic estructura</b>			
1.1. Version	3	Sí	
1.2. Serial Number	Establecido automáticamente por la CA. Número identificativo único del certificado.	Sí	
1.3. Signature Algorithm		Sí	
1.3.1. Algorithm	SHA-256 with RSA Signature	Sí	
1.3.2. Parameters	No aplicable	No	
1.4. Issuer		Sí	
1.4.1. Country Name (C)	"ES"	Sí	
1.4.2. Organization Name (O)	"Logalty Servicios de Tercero de Confianza SL"	Sí	
1.4.3. Locality Name (L)	"Alcobendas"	Sí	
1.4.4. Organization Identifier	"VATES-B84492891"	Sí	
1.4.5. Common Name (CN)	"Logalty Qualified CA G2"	Sí	
1.4.6. stateOrProvinceName	"Madrid"	Sí	

1.4.7. <i>organizationalUnitName (OU)</i>	"Logalty Trust Services"	Sí	
<b>1.5. Validity</b>		Sí	
1.5.1. Not Before	Fecha de inicio de validez	Sí	
1.5.2. Not After	Fecha de expiración (3 years)	Sí	
<b>1.6. Subject</b>		Sí	
1.6.1. <i>Country Name</i>	País de residencia o nacionalidad de la organización	Sí	
1.6.2. <i>Organization Name</i>	Denominación oficial de la Organización titular del certificado	Sí	
1.6.4. <i>Organization Identifier</i>	Número oficial de identificación de la persona jurídica titular del certificado, en formato ETSI EN 319412-1 (Ejemplo: "VATES-Q0000000J")	Sí	
1.6.8. <i>Serial Number</i>	NIF de la empresa	Sí	
1.6.9. <i>Locality Name (L)</i>	<i>Localidad de la organización</i>	Sí	
1.6.10. <i>Common Name</i>	Nombre de la plataforma donde reside el sello	Sí	
<b>1.7. Subject Public Key Info</b>		Sí	
1.7.1. <i>AlgorithmIdentifier</i>			
1.7.1.1. <i>Algorithm</i>	RSA encryption	Sí	
1.7.1.2. <i>Parameters</i>	No aplicable	No	

1.7.2. SubjectPublicKey	Clave pública del firmante	Sí	
<b>2. Extensions</b>			
<b>2.1. Authority Key Identifier</b>	Identificador de la clave del emisor	Sí	No
2.1.1. KeyIdentifier		Sí	
<b>2.2. Subject Key Identifier</b>	Identificador de la clave del firmante	Sí	No
2.2.1. KeyIdentifier		Sí	
<b>2.3. Key Usage</b>		Sí	Sí
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"		
<b>2.4. Certificate Policies</b>		Si	No



2.4.1. Policy Information		Sí	
2.4.1.1. Policy Identifier	1.3.6.1.4.1.30210.1.3.3	Sí	
2.4.1.2. Policy Qualifiers		Sí	
2.4.1.1.1 CPS URI	<a href="https://www.logalty.com/certificateauthority/">https://www.logalty.com/certificateauthority/</a>		
2.4.1.1.2. User Notice/Explicit text	"Certificado cualificado de sello electrónico avanzado de persona jurídica"	Sí	
2.4.2. Policy Information		Sí	
2.4.2.1. Policy Identifier	0.4.0.194112.1.1	Sí	
<b>2.6. Extended Key Usage</b>		Sí	No
2.6.1. clientAuth	Presente (1.3.6.1.5.5.7.3.2)	Sí	
2.6.2. Email protection	Presente (1.3.6.1.5.5.7.3.4)	No	
<b>2.7. cRLDistributionPoint</b>		No	No
2.7.1. distributionPoint	<a href="http://crl1.logalty.es/qualifiedLogaltySubCA02.crl">http://crl1.logalty.es/qualifiedLogaltySubCA02.crl</a>	Sí	
2.7.2. distributionPoint	<a href="http://crl2.logalty.es/qualifiedLogaltySubCA02.crl">http://crl2.logalty.es/qualifiedLogaltySubCA02.crl</a>	Sí	
<b>2.8. Authority Info Acces</b>		Sí	No
2.8.1. Access Description		Sí	

2.8.1.1. Acces Method	<i>id-ad-ocsp</i>	<i>Sí</i>	
2.8.1.2. Acces Location	<a href="http://ocsp1.logalty.es">http://ocsp1.logalty.es</a>	<i>Sí</i>	
2.8.2. Access Description		<b>Sí</b>	
2.8.2.1. Acces Method	<i>id-ad-caIssuers</i>	<i>Sí</i>	
2.8.2.1. Acces Location	<a href="http://crt.logalty.es/certificateauthority/LogaltyQualifiedCAG2.crt">http://crt.logalty.es/certificateauthority/LogaltyQualifiedCAG2.crt</a>	<i>Sí</i>	
<b>2.9. Qualified Certificate Statements</b>		<b>Sí</b>	<b>No</b>
2.9.1. qCCompliance		<b>Sí</b>	
2.9.2. QcEuRetentionPeriod	"15"	<b>Sí</b>	
2.9.4. QcPDS		<b>Sí</b>	
2.9.4.1 PdsLocation			
2.9.4.1.1 url	<a href="https://www.logalty.es/certificateauthority/en/LGT_PDS_emisor.v1r0.pdf">https://www.logalty.es/certificateauthority/en/LGT_PDS_emisor.v1r0.pdf</a>	<i>Sí</i>	
2.9.4.1.2 language	"EN"	<i>Sí</i>	

2.9.4.2 PdsLocation			
2.9.4.2.1 url	<a href="https://www.logalty.es/certificateauthority/es/LGT_PDS_emisor.v1r0.pdf">https://www.logalty.es/certificateauthority/es/LGT_PDS_emisor.v1r0.pdf</a>	Sí	
2.9.4.2.2 language	"ES"	Sí	
2.9.5. QcType	Qct-eseal	Sí	
2.9.6. qcStatement-2			
2.9.6.1. SemanticsInformation			
2.9.6.1.2. semanticsIdLegal	0.4.0.194121.1.2		
<b>2.10. Basic Constraints</b>		Sí	Sí
2.10.1. cA	FALS	Sí	

	<b>En SOFTWARE</b>	<b>Oblig.</b>	<b>Crít.</b>
<b>1.5 Sello electrónico PSD2</b>			
<b>1. Basic structure</b>			
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. Algorithm	SHA-256 with RSA Signature	Sí	
1.3.2. Parameters	No aplicable	No	
1.4. Issuer		Sí	
1.4.1. Country Name (C)	"ES"	Sí	
1.4.2. Organization Name (O)	<i>"Logalty Servicios de Tercero de Confianza SL"</i>	Sí	
1.4.3. Locality Name (L)	<i>"Alcobendas"</i>	Sí	
1.4.4. Organization Identifier	<i>"VATES-B84492891"</i>	Sí	
1.4.5. Common Name (CN)	<i>"Logalty Qualified CA G2"</i>	Sí	
1.4.6. stateOrProvinceName	<i>"Madrid"</i>	Sí	

1.4.7. organizationalUnitName (OU)	"Logalty Trust Services"	Sí	
<b>1.5. Validity</b>		Sí	
1.5.1. Not Before	Fecha de inicio de validez	Sí	
1.5.2. Not After	Fecha de expiración (3 years)	Sí	
<b>1.6. Subject</b>		Sí	
1.6.1. Country Name	País de residencia o nacionalidad de la organización	Sí	
1.6.2. Organization Name	Denominación oficial de la Organización titular del certificado	Sí	
1.6.4. Organization Identifier	(GEN-5.2.1-2 ETSI 119495): Identificación según esta estructura "PSD" = tres caracteres El país del NCA = 2 caracteres (ES) "-" = 1 carácter El identificador de la NCA sin el código del país = entre 2 y 8 caracteres (BE) "-" = 1 carácter El PSP identifier = sin restricciones de caracteres (ejemplo: "PSDES-BE-"PSP identifier")	Sí	
1.6.8. Serial Number	(GEN-5.2.1-1 ETSI 119495): Número oficial de identificación de la persona jurídica titular del certificado, en formato ETSI EN 319412-1 (Ejemplo: "VATES-Q0000000J")	Sí	

1.6.9. Locality Name (L)	Localidad de la organización	Sí	
1.6.10. Common Name	Nombre del Payment Service Provider (PSP)	Sí	
<b>1.7. Subject Public Key Info</b>		Sí	
1.7.1. AlgorithmIdentifier			
1.7.1.1. Algorithm	RSA encryption	Sí	
1.7.1.2. Parameters	No aplicable	No	
1.7.2. SubjectPublicKey	Clave pública del firmante	Sí	
<b>2. Extensions</b>			
<b>2.1. Authority Key Identifier</b>	Identificador de la clave del emisor	Sí	No
2.1.1. KeyIdentifier		Sí	
<b>2.2. Subject Key Identifier</b>	Identificador de la clave del firmante	Sí	No
2.2.1. KeyIdentifier		Sí	
<b>2.3. Key Usage</b>		Sí	Sí
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"		
<b>2.4. Certificate Policies</b>		Si	No
2.4.1. Policy Information		Sí	
2.4.1.1. Policy Identifier	1.3.6.1.4.1.30210.1.3.33	Sí	
2.4.1.2. Policy Qualifiers		Sí	
2.4.1.1.1 CPS URI	<a href="https://www.logalty.com/certificateauthority/">https://www.logalty.com/certificateauthority/</a>		
2.4.1.1.2. User Notice/Explicit text	"Certificado cualificado de sello electrónico avanzado de persona jurídica para PSD2"	Sí	
2.4.2. Policy Information		Sí	
2.4.2.1. Policy Identifier	0.4.0.194112.1.1	Sí	
<b>2.6. Extended Key Usage</b>		Sí	No
2.6.1. clientAuth	Presente (1.3.6.1.5.5.7.3.2)	Sí	

2.6.2. Email protection	Presente (1.3.6.1.5.5.7.3.4)	No	
<b>2.7. cRLDistributionPoint</b>		No	No
2.7.1. distributionPoint	<a href="http://crl1.logalty.es/qualifiedLogaltySubCA02.crl">http://crl1.logalty.es/qualifiedLogaltySubCA02.crl</a>	Sí	
2.7.2. distributionPoint	<a href="http://crl2.logalty.es/qualifiedLogaltySubCA02.crl">http://crl2.logalty.es/qualifiedLogaltySubCA02.crl</a>	Sí	
<b>2.8. Authority Info Acces</b>		Sí	No
2.8.1. Access Description		Sí	
2.8.1.1. Acces Method	<i>id-ad-ocsp</i>	Sí	
2.8.1.2. Acces Location	<a href="http://ocsp1.logalty.es">http://ocsp1.logalty.es</a>	Sí	
2.8.2. Access Description		Sí	
2.8.2.1. Acces Method	<i>id-ad-caIssuers</i>	Sí	
2.8.2.1. Acces Location	<a href="http://crt.logalty.es/certificateauthority/LogaltyQualifiedCAG2.crt">http://crt.logalty.es/certificateauthority/LogaltyQualifiedCAG2.crt</a>	Sí	
<b>2.9. Qualified Certificate Statements</b>		Sí	No
2.9.1. qCCompliance		Sí	



2.9.2. QcEuRetentionPeriod	"15"	Sí	
2.9.4. QcPDS		Sí	
2.9.4.1 PdsLocation			
2.9.4.1.1 url	<a href="https://www.logalty.com/certificateauthority/pds/en/LGT_PDS_PSD2_v1r4.pdf">https://www.logalty.com/certificateauthority/pds/en/LGT_PDS_PSD2_v1r4.pdf</a>	<i>Sí</i>	
2.9.4.1.2 language	"EN"	<i>Sí</i>	
2.9.4.2 PdsLocation			
2.9.4.2.1 url	<a href="https://www.logalty.com/certificateauthority/pds/es/LGT_PDS_PSD2_v1r4.pdf">https://www.logalty.com/certificateauthority/pds/es/LGT_PDS_PSD2_v1r4.pdf</a>	<i>Sí</i>	
2.9.4.2.2 language	"ES"	<i>Sí</i>	
2.9.5. QcType	Qct-eseal	Sí	
2.9.6. qcStatement-2			
2.9.6.1. SemanticsInformation			

2.9.6.1.2. semanticsIdLegal	0.4.0.194121.1.2		
2.9.7. psd2-qcStatement	One or more of the specified roles:		
2.9.7.1. rolesOfPSP			
2.9.7.1. RoleOfPspOid / roleOfPspName	PSP_AS (0.4.0.19495.1.1) PSP_PI (0.4.0.19495.1.2) PSP_AI (0.4.0.19495.1.3) PSP_IC (0.4.0.19495.1.4)		
2.9.7.2. NCAName	Name of NCA (Bank of Spain)		
2.9.7.2. NCAId	ID of CA (ES-BE)		
<b>2.10. Basic Constraints</b>		Sí	Sí
2.10.1. cA	FALS	Sí	

		Oblig.	Crít.
<b>1.6 SSL-EV PSD2</b>			
<b>1. Basic estructura</b>			
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. Algorithm	SHA-256 with RSA Signature	Sí	
1.3.2. Parameters	No aplicable	No	
1.4. Issuer		Sí	
1.4.1. Country Name (C)	"ES"	Sí	
1.4.2. Organization Name (O)	"Logalty Servicios de Tercero de Confianza SL"	Sí	
1.4.3. Locality Name (L)	"Alcobendas"	Sí	
1.4.4. Organization Identifier	"VATES-B84492891"	Sí	
1.4.5. Common Name (CN)	"Logalty Qualified CA G2"	Sí	
1.4.6. stateOrProvinceName	"Madrid"	Sí	
1.4.7. organizationalUnitName (OU)	"Logalty Trust Services"	Sí	
1.5. Validity		Sí	
1.5.1. Not Before	Fecha de inicio de validez	Sí	
1.5.2. Not After	Fecha de expiración	Sí	
1.6. Subject		Sí	
1.6.1. Country Name	País de residencia o nacionalidad de la organización	Sí	
1.6.2. Locality	"Alcobendas"	Sí	
1.6.3. Organization Name	Organización titular del certificado	Sí	

1.6.5. <i>Organization Identifier</i>	<p align="center"><b>(GEN-5.2.1-2 ETSI 119495):</b>  Identificación según esta otra estructura  "PSD" = tres caracteres  El país del NCA = 2 caracteres (ES)  "-" = 1 carácter  El identificador de la NCA sin el código del país = entre 2 y 8 caracteres (BE)  "-" = 1 carácter  El PSP identifier = sin restricciones de caracteres  (ejemplo: "PSDES-BE-"PSP identifier")</p>	Sí	
1.6.6. <i>Serial Number</i>	<p align="center"><b>(GEN-5.2.1-1 ETSI 119495):</b>  Número oficial de identificación de la persona jurídica titular del certificado, en formato ETSI EN 319412-1  (Ejemplo: "VATES-Q0000000J")</p>	Sí	
1.6.7. <i>businessCategory</i>	Una de estas 4 categorías: "Private Organization", "Government Entity", "Business Entity", or "Non-Commercial Entity"	Sí	
1.6.8. <i>jurisdictionCountryName</i>	"ES"	Sí	
1.6.9. <i>Common Name</i>	Dominio donde residirá el certificado propiedad del PSP identificado en el campo "O" del "subject"	Sí	
<b>1.7. Subject Public Key Info</b>		Sí	
1.7.1. <i>AlgorithmIdentifier</i>			
1.7.1.1. <i>Algorithm</i>	RSA encryption	Sí	
1.7.1.2. <i>Parameters</i>	No aplicable	No	
1.7.2. <i>SubjectPublicKey</i>	Clave pública del firmante	Sí	
<b>2. Extensions</b>			
<b>2.1. Authority Key Identifier</b>	Identificador de la clave del emisor	Sí	No
2.1.1. <i>KeyIdentifier</i>		Sí	

<b>2.2. Subject Key Identifier</b>	Identificador de la clave del firmante	Sí	No
2.2.1. KeyIdentifier		Sí	
<b>2.3. Key Usage</b>		Sí	Sí
2.3.1. Digital Signature	Seleccionado "1"	Sí	
2.3.2. Content commitment	No seleccionado. "0"		
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"		
<b>2.4. Certificate Policies</b>		Si	No
2.4.1. Policy Information		Sí	
2.4.1.1. Policy Identifier	1.3.6.1.4.1.30210.1.4.23	Sí	
2.4.1.2. Policy Qualifiers		Sí	
2.4.1.1.1 CPS URI	<a href="https://www.logalty.com/certificateauthority/">https://www.logalty.com/certificateauthority/</a>		
2.4.1.1.2. User Notice/Explicit text	"Certificado cualificado de autenticación web - EV para PSD2"	Sí	
2.4.2. Policy Information		Sí	
2.4.2.1. Policy Identifier	0.4.0.194112.1.4	Sí	
2.4.3. Policy Information		Sí	
2.4.3.1. Policy Identifier	0.4.0.2042.1.4	Sí	
2.4.4. Policy Information		Sí	
2.4.4.1. Policy Identifier	2.23.140.1.1	Sí	
<b>2.5. Subject Alternative Names</b>		Sí	No
2.5.1. dNSName	Nombre DNS principal	Sí	

2.5.2. dNSName	Nombre DNS adicional	No	
<b>2.6. Extended Key Usage</b>		Sí	No
2.6.1. serverAuth	Presente (1.3.6.1.5.5.7.3.1)	Sí	
2.6.2. clientAuth	Presente (1.3.6.1.5.5.7.3.2)	Sí	
<b>2.7. cRLDistributionPoint</b>		No	No
2.7.1. distributionPoint	<a href="http://crl1.logalty.es/qualifiedLogaltySubCA02.crl">http://crl1.logalty.es/qualifiedLogaltySubCA02.crl</a>	Sí	
2.7.2. distributionPoint	<a href="http://crl2.logalty.es/qualifiedLogaltySubCA02.crl">http://crl2.logalty.es/qualifiedLogaltySubCA02.crl</a>	Sí	
<b>2.8. Authority Info Acces</b>		Sí	No
2.8.1. Access Description		Sí	
2.8.1.1. Acces Method	<i>id-ad-ocsp</i>	Sí	
2.8.1.2. Acces Location	<a href="http://ocsp1.logalty.es">http://ocsp1.logalty.es</a>	Sí	
2.8.2. Access Description		Sí	
2.8.2.1. Acces Method	<i>id-ad-caissuers</i>	Sí	
2.8.2.1. Acces Location	<a href="http://crt.logalty.es/certificateauthority/LogaltyQualifiedCAG2.crt">http://crt.logalty.es/certificateauthority/LogaltyQualifiedCAG2.crt</a>	Sí	
<b>2.9. Qualified Certificate Statements</b>		Sí	No
2.9.1. qCCompliance		Sí	
2.9.2. QcEuRetentionPeriod	"15"	Sí	
2.9.4. QcPDS		Sí	
2.9.4.1 PdsLocation			
2.9.4.1.1 url	<a href="https://www.logalty.com/certificateauthority/pds/en/LGT_PDS_corporativo_v1r5.pdf">https://www.logalty.com/certificateauthority/pds/en/LGT_PDS_corporativo_v1r5.pdf</a>	Sí	
2.9.4.1.2 language	"EN"	Sí	
2.9.4.2 PdsLocation			
2.9.4.2.1 url	<a href="https://www.logalty.com/certificateauthority/pds/es/LGT_PDS_corporativo_v1r5.pdf">https://www.logalty.com/certificateauthority/pds/es/LGT_PDS_corporativo_v1r5.pdf</a>	Sí	
2.9.4.2.2 language	"ES"	Sí	
2.9.5. QcType	QcType-web	Sí	
2.9.6. qcStatement-2			

2.9.6.1. SemanticsInformation			
2.9.6.1.2. semanticsIdLegal	0.4.0.194121.1.2		
2.9.7. psd2-qcStatement	One or more of the specified roles:		
2.9.7.1. rolesOfPSP			
2.9.7.1. RoleOfPspOid / roleOfPspName	PSP_AS (0.4.0.19495.1.1) PSP_PI (0.4.0.19495.1.2) PSP_AI (0.4.0.19495.1.3) PSP_IC (0.4.0.19495.1.4)		
2.9.7.2. NCAName	Name of NCA (Bank of Spain)		
2.9.7.2. NCAId	ID of CA (ES-BE)		
<b>2.10. Basic Constraints</b>		Sí	Sí
2.10.1. cA	FALS	Sí	

	En SOFTWARE	Oblig.	Crít.
1.7 Sello electrónico de TSU			
<b>1. Basic estructura</b>			
1.1. Version	3	Sí	
1.2. Serial Number	Establecido automáticamente por la CA. Número identificativo único del certificado.	Sí	
1.3. Signature Algorithm		Sí	
1.3.1. Algorithm	SHA-256 with RSA Signature	Sí	
1.3.2. Parameters	No aplicable	No	
1.4. Issuer		Sí	
1.4.1. Country Name (C)	"ES"	Sí	
1.4.2. Organization Name (O)	"Logalty Servicios de Tercero de Confianza SL"	Sí	
1.4.3. Locality Name (L)	"Alcobendas"	Sí	
1.4.4. Organization Identifier	"VATES-B84492891"	Sí	
1.4.5. Common Name (CN)	"Logalty Qualified CA G2"	Sí	
1.4.6. stateOrProvinceName	"Madrid"	Sí	



1.4.7. organizationalUnitName (OU)	"Logalty Trust Services"	Sí	
<b>1.5. Validity</b>		Sí	
1.5.1. Not Before	Fecha de inicio de validez	Sí	
1.5.2. Not After	Fecha de expiración (5 years)	Sí	
<b>1.6. Subject</b>		Sí	
1.6.1. Country Name	País de residencia o nacionalidad de la organización	Sí	
1.6.2. Organization Name	Denominación oficial de la Organización titular del certificado	Sí	
1.6.3. Organization Identifier	Número oficial de identificación de la persona jurídica titular del certificado, en formato ETSI EN 319412-1 (Ejemplo: "VATES-Q0000000J")	Sí	
1.6.4. Serial Number	NIF de la empresa	Sí	
1.6.5. Locality Name (L)	Localidad de la organización	Sí	
1.6.6. stateOrProvinceName	"Madrid"	Sí	
1.6.7. Common Name	Nombre de la plataforma donde reside el sello	Sí	
1.6.8 Organization Unit	Descripción organización	No	
<b>1.7. Subject Public Key Info</b>		Sí	
1.7.1. AlgorithmIdentifier			

1.7.1.1. Algorithm	EC 256 bits	Sí	
1.7.1.2. Parameters	No aplicable	No	
1.7.2. SubjectPublicKey	Clave pública del firmante	Sí	
<b>2. Extensions</b>			
<b>2.1. Authority Key Identifier</b>	Identificador de la clave del emisor	Sí	No
2.1.1. KeyIdentifier		Sí	
<b>2.2. Subject Key Identifier</b>	Identificador de la clave del firmante	Sí	No
2.2.1. KeyIdentifier		Sí	
<b>2.3. Key Usage</b>		Sí	Sí
2.3.1. Digital Signature	Seleccionado "1"	Sí	
2.3.2. Content commitment	No seleccionado. "0"		
2.3.3. Key Encipherment	No seleccionado. "0"		
2.3.4. Data Encipherment	No seleccionado. "0"		
2.3.5. Key Agreement	No seleccionado. "0"		
2.3.6. Key Certificate Signature	No seleccionado. "0"		
2.3.7. CRL Signature	No seleccionado. "0"		
2.3.8. Encipher Only	No seleccionado. "0"		

2.3.9. Decipher Only	No seleccionado. "0"		
<b>2.4. Certificate Policies</b>		Si	No
2.4.1. Policy Information		Sí	
2.4.1.1. Policy Identifier	1.3.6.1.4.1.30210.1.5.1	Sí	
2.4.1.2. Policy Qualifiers		Sí	
2.4.1.1.1 CPS URI	<a href="https://www.logalty.com/certificateauthority/">https://www.logalty.com/certificateauthority/</a>		
2.4.1.1.2. User Notice/Explicit text	Certificado cualificado de sello electrónico de persona jurídica para la expedición de sellos cualificados de tiempo electrónico	Sí	
2.4.2. Policy Information		Sí	
2.4.2.1. Policy Identifier	0.4.0.194112.1.1	Sí	
<b>2.6. Extended Key Usage</b>		Sí	Sí
2.6.1. TimeStamping	Presente (1.3.6.1.5.5.7.3.8)	Sí	
<b>2.7. cRLDistributionPoint</b>		No	No
2.7.1. distributionPoint	<a href="http://cr1.logalty.es/qualifiedLogaltySubCA02.crl">http://cr1.logalty.es/qualifiedLogaltySubCA02.crl</a>	Sí	
2.7.2. distributionPoint	<a href="http://cr2.logalty.es/qualifiedLogaltySubCA02.crl">http://cr2.logalty.es/qualifiedLogaltySubCA02.crl</a>	Sí	
<b>2.8. Authority Info Acces</b>		Sí	No

2.8.1. Access Description		Sí	
2.8.1.1. Acces Method	<i>id-ad-ocsp</i>	Sí	
2.8.1.2. Acces Location	<a href="http://ocsp1.logalty.es">http://ocsp1.logalty.es</a>	Sí	
2.8.2. Access Description		Sí	
2.8.2.1. Acces Method	<i>id-ad-caIssuers</i>	Sí	
2.8.2.1. Acces Location	<a href="http://crt.logalty.es/certificateauthority/LogaltyQualifiedCAG2.crt">http://crt.logalty.es/certificateauthority/LogaltyQualifiedCAG2.crt</a>	Sí	
<b>2.9. Qualified Certificate Statements</b>		Sí	No
2.9.1. qCCompliance		Sí	
2.9.2. QcEuRetentionPeriod	"15"	Sí	
2.9.4. QcPDS		Sí	
2.9.4.1 PdsLocation			
2.9.4.1.1 url	<a href="https://www.logalty.com/certificateauthority/pds/en/LGT_PDS_TSA_v1r4.pdf">https://www.logalty.com/certificateauthority/pds/en/LGT_PDS_TSA_v1r4.pdf</a>	Sí	

2.9.4.1.2 language	"EN"	Sí	
2.9.4.2 PdsLocation			
2.9.4.2.1 url	<a href="https://www.logalty.com/certificateauthority/pds/es/LGT_PDS_TSA_v1r4.pdf">https://www.logalty.com/certificateauthority/pds/es/LGT_PDS_TSA_v1r4.pdf</a>	Sí	
2.9.4.2.2 language	"ES"	Sí	
2.9.5. QcType	Qct-eseal	Sí	
<b>2.10. Basic Constraints</b>		Sí	Sí
2.10.1. cA	FALS	Sí	

	Gestión CENTRALIZADA (Identificación y Firma)	Oblig.	Crít.
1.8 PF representante de PJ			
<b>1. Basic estructura</b>			
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. Algorithm	SHA-256 with RSA Signature	Sí	
1.3.2. Parameters	No aplicable	No	
1.4. Issuer		Sí	
1.4.1. Country Name (C)	"ES"	Sí	
1.4.2. Organization Name (O)	"Logalty Servicios de Tercero de Confianza SL"	Sí	
1.4.3. Locality Name (L)	"Alcobendas"	Sí	
1.4.4. Organization Identifier	"VATES-B84492891"	Sí	
1.4.5. Common Name (CN)	"Logalty Qualified CA G2"	Sí	
1.4.6. stateOrProvinceName	"Madrid"	Sí	

1.4.7. organizationalUnitName (OU)	"Logalty Trust Services"	Sí	
<b>1.5. Validity</b>		Sí	
1.5.1. Not Before	Fecha de inicio de validez	Sí	
1.5.2. Not After	Fecha de expiración (3 years)	Sí	
<b>1.6. Subject</b>		Sí	
1.6.1. Country Name	País de residencia o nacionalidad del firmante.	Sí	
1.6.2. Organization Name	Organización a la que pertenece el firmante.	Sí	
1.6.4. Organization Identifier	NIF de la persona jurídica a la que está representando legalmente el firmante, en formato ETSI EN 319412-1 (Ejemplo: "VATES-Q0000000J)	Sí	
1.6.5. Title	Representante legal	No	
1.6.6. Surname	Apellidos del firmante (como consta en el documento oficial)	Sí	
1.6.7. Given Name	Nombre del firmante (como consta en el documento oficial)	Sí	

1.6.8. <i>Serial Number</i>	Número de documento oficial del firmante codificado acorde a ETSI EN 319 412-1 ("IDCES-123456789Z")	Sí	
1.6.9. <i>Common Name</i>	00000000T Nombre y Apellidos (R: Q0000000J)	Sí	
1.6.10. <i>Description</i>	<ul style="list-style-type: none"> <li>• Reg: XXX /Hoja: XXX /Tomo:XXX /Sección:XXX /Libro:XXX /Folio:XXX /Fecha: dd-mm-aaaa /Inscripción: XXX</li> <li>• Notario: Nombre Apellido1 Apellido2 /Núm Protocolo: XXX /Fecha Otorgamiento: dd-mm-aaaa</li> <li>• En Boletines Oficiales: Boletín: XXX/ /Fecha: dd-mm-aaaa /Numero resolución: XXX</li> </ul>	Sí	
<b>1.7. Subject Public Key Info</b>		Sí	
1.7.1. AlgorithmIdentifier			
1.7.1.1. Algorithm	RSA encryption	Sí	
1.7.1.2. Parameters	No aplicable	No	



1.7.2. SubjectPublicKey	Clave pública del firmante	Sí	
<b>2. Extensions</b>			
<b>2.1. Authority Key Identifier</b>	Identificador de la clave del emisor	Sí	No
2.1.1. KeyIdentifier		Sí	
<b>2.2. Subject Key Identifier</b>	Identificador de la clave del firmante	Sí	No
2.2.1. KeyIdentifier		Sí	
<b>2.3. Key Usage</b>		Sí	Sí
2.3.1. Digital Signature	Seleccionado "1"	Sí	
2.3.2. Content commitment	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"		
2.3.8. Encipher Only	No seleccionado. "0"		

2.3.9. Decipher Only	No seleccionado. "0"		
<b>2.4. Certificate Policies</b>		Sí	No
2.4.1. Policy Information		Sí	
2.4.1.1. Policy Identifier	1.3.6.1.4.1.30210.1.6.3	Sí	
2.4.1.2. Policy Qualifiers		Sí	
2.4.1.1.1 CPS URI	<a href="https://www.logalty.com/certificateauthority/">https://www.logalty.com/certificateauthority/</a>		
2.4.1.1.2. User Notice/Explicit text	Certificado cualificado de firma electrónica avanzada de persona física representante de persona jurídica ante las AAPP.	Sí	
2.4.2. Policy Information		Sí	
2.4.2.1. Policy Identifier	0.4.0.194112.1.0	Sí	
2.4.3. Policy Information		Sí	

2.4.3.1. Policy Identifier	2.16.724.1.3.5.8	Sí	
<b>2.5. Subject Alternative Names</b>		No	No
2.5.1. rfc822Name	Correo electrónico del firmante	No	
<b>2.6. Extended Key Usage</b>		Sí	No
2.6.1. clientAuth	Presente (1.3.6.1.5.5.7.3.2)	Sí	
2.6.2. Email protection	Presente (1.3.6.1.5.5.7.3.4)	No	
<b>2.7. cRLDistributionPoint</b>		No	No
2.7.1. distributionPoint	<a href="http://cr1.logalty.es/qualifiedLogaltySubCA02.crl">http://cr1.logalty.es/qualifiedLogaltySubCA02.crl</a>	Sí	
2.7.2. distributionPoint	<a href="http://cr2.logalty.es/qualifiedLogaltySubCA02.crl">http://cr2.logalty.es/qualifiedLogaltySubCA02.crl</a>	Sí	
<b>2.8. Authority Info Acces</b>		Sí	No
2.8.1. Access Description		Sí	

2.8.1.1. Acces Method	<i>id-ad-ocsp</i>	<i>Sí</i>	
2.8.1.2. Acces Location	<a href="http://ocsp1.logalty.es">http://ocsp1.logalty.es</a>	<i>Sí</i>	
2.8.2. Access Description		<b>Sí</b>	
2.8.2.1. Acces Method	<i>id-ad-caIssuers</i>	<i>Sí</i>	
2.8.2.1. Acces Location	<a href="http://crt.logalty.es/certificateauthority/LogaltyQualifiedCAG2.crt">http://crt.logalty.es/certificateauthority/LogaltyQualifiedCAG2.crt</a>	<i>Si</i>	
<b>2.9. Qualified Certificate Statements</b>		<b>Sí</b>	<b>No</b>
2.9.1. qCCompliance		<b>Sí</b>	
2.9.2. QcEuRetentionPeriod	"15"	<b>Sí</b>	
2.9.4. QcPDS		<b>Sí</b>	
2.9.4.1 PdsLocation			
2.9.4.1.1 url	<a href="https://www.logalty.com/certificateauthority/pds/en/LGT_PDS_individual_v1r4.pdf">https://www.logalty.com/certificateauthority/pds/en/LGT_PDS_individual_v1r4.pdf</a>	<i>Sí</i>	
2.9.4.1.2 language	"EN"	<i>Sí</i>	

2.9.4.2 PdsLocation			
2.9.4.2.1 url	<a href="https://www.logalty.com/certificateauthority/pds/es/LGT_PDS_individual_v1r4.pdf">https://www.logalty.com/certificateauthority/pds/es/LGT_PDS_individual_v1r4.pdf</a>	Sí	
2.9.4.2.2 language	"ES"	Sí	
2.9.5. QcType	Qct-esign	Sí	
2.9.6. qcStatement-2			
2.9.6.1. SemanticsInformation			
2.9.6.1.1. semanticsIdNatural	0.4.0.194121.1.1		
<b>2.10. Basic Constraints</b>		Sí	Sí
2.10.1. cA	FALS	Sí	