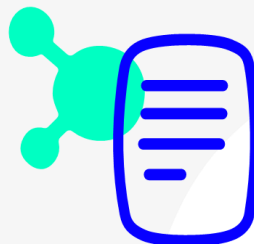


Perfiles de certificados

2024



INFORMACIÓN GENERAL

Distribución	Pública (web)
Fecha	17/10/2024
Descripción	Perfiles de certificados para su publicación en la web

CONTROL DE VERSIONES

VERSIÓN	PARTES CAMBIADAS	DESCRIPCIÓN CAMBIO	AUTOR	FECHA
1.24	Todo	Versión para publicación web	AC	17/05/2023
2	Todo	Se eliminan todos los perfiles excepto el sello de TSU.	AC	17/10/2024

INDICE

1	PERFILES	3
1.1	Sello electrónico de TSU	3

1 PERFILES

	En SOFTWARE	Oblig.	Crít.
1.1 Sello electrónico de TSU			
1. Basic structure			
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. <i>stateOrProvinceName</i>	"Madrid"	Sí	
1.4.7. <i>organizationalUnitName (OU)</i>	"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 (5 years)	Sí	
1.6. Subject		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	
1.6.3. <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	
1.6.4. <i>Serial Number</i>	NIF de la empresa	Sí	
1.6.5. <i>Locality Name (L)</i>	Localidad de la organización	Sí	
1.6.6. <i>stateOrProvinceName</i>	"Madrid"	Sí	
1.6.7. <i>Common Name</i>	Nombre de la plataforma donde reside el sello	Sí	
1.6.8 <i>Organization Unit</i>	Descripción organización	No	
1.7. Subject Public Key Info		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	
2. Extensions			
2.1. Authority Key Identifier	Identificador de la clave del emisor	Sí	No
2.1.1. KeyIdentifier		Sí	
2.2. Subject Key Identifier	Identificador de la clave del firmante	Sí	No
2.2.1. KeyIdentifier		Sí	
2.3. Key Usage		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"		
2.4. Certificate Policies		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	https://www.logalty.com/certificateauthority/ Certificado cualificado de sello electrónico de persona jurídica para la expedición de sellos cualificados de tiempo electrónico		
2.4.1.1.2. User Notice/Explicit text		Sí	
2.4.2. Policy Information		Sí	
2.4.2.1. Policy Identifier	0.4.0.194112.1.1	Sí	
2.6. Extended Key Usage		Sí	Sí
2.6.1. TimeStamping	Presente (1.3.6.1.5.5.7.3.8)	Sí	
2.7. cRLDistributionPoint		No	No
2.7.1. distributionPoint	http://crl1.logalty.es/qualifiedLogaltySubCA02.crl	Sí	
2.7.2. distributionPoint	http://crl2.logalty.es/qualifiedLogaltySubCA02.crl	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	http://ocsp1.logalty.es	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	http://crt.logalty.es/certificateauthority/LogaltyQualifiedCAG2.crt	Sí	
2.9. Qualified Certificate Statements		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	https://www.logalty.com/certificateauthority/pds/en/LGT_PDS_TSA_v1r4.pdf	Sí	

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