Perfil de certificado

Sello electrónico de Administración Pública

1. NIVEL ALTO

CAMPO	DESCRIPCIÓN	VALORES
1. X.509V1		
1.1. Versión	V3	2
1.2. Serial Number	Nº identificativo único	*Automático*
1.3. Signature Algorithm	Tipo de algoritmo. OID 2.16.840.1.101.3.4.2	SHA256RSA
1.4. Issuer Distinguished Name		
1.4.1. Country (C)	ES	ES
1.4.2. Organization (O)	Denominación oficial del prestador	TESORERIA GENERAL DE LA SEGURIDAD SOCIAL
1.4.3 Organizational Unit (OU)	Unidad Organizativa responsable de la emisión	GERENCIA DE INFORMATICA DE LA SEGURIDAD SOCIAL
1.4.4. Locality (L)	Localización	MADRID
1.4.5. Organizational Unit (OU)	Unidad organizativa dentro del prestador de servicios, responsable de la emisión del certificado.	GISS01
1.4.6. Serial Number	Número único de identificación de la entidad de certificación	Q2827003A
1.4.8. Common Name (CN)	Nombre común del certificado de la CA subordinada	SUBCA GISS01
1.5. Validity		
1.5.1. Not Before	Fecha inicio validez YYMMDDHHMMSSZ	YYMMDDHHMMSSZ
1.5.2. Not After	Fecha fin validez YYMMDDHHMMSSZ	YYMMDDHHMMSSZ
1.6. Subject		
1.5.1. Country (C)	ES	ES
1.5.2. Organization (O)	Denominación del suscriptor	"Nombre oficial de la Entidad" Ej: SECRETARIA DE ESTADO DE LA SEGURIDAD SOCIAL
1.5.4. Organizational Unit (OU)	Unidad organizativa dentro del prestador de servicios, responsable de la emisión del certificado.	ACTUACION AUTOMATIZADA
1.5.5. Organizational Unit (OU)	Tipo certificado= "sello electrónico"	SELLO ELECTRONICO
1.5.3 Organizational Unit (OU)	Identificación del suscriptor según DIR3	"Número DIR3 de la Entidad" Ej: SE = E04926001
1.5.6. Descripción	Descripción uso certificado	NIVEL ALTO
1.5.7. Serial Number	Número único de identificación de la entidad	"CIF de la Entidad" Ej: SE = S2819001E
1.5.9. Common Name (CN)	Denominación del certificado	"Nombre del sello electrónico" Ej: "SELLO ELECTRONICO DE LA SEGURIDAD SOCIAL"
1.7. Subject Public Key Info	Clave pública del certificado	(RSA 2048 bits)
2. X.509v3 Extensions		
2.1. Authority Key Identifier		
2.1.1. Key Identifier	Identificador de clave pública del emisor. Path de identificación	*Automático*

2.1.2. AuthorityCertIssuer	Nombre de la CA a la que corresponde esa clave	*Automático*
2.1.3. AuthorityCertSerialNumber	Número de serie del certificado de la CA	*Automático*
2.2. Subject Key Identifier	Identificador de la clave pública del suscriptor	*Automático*
2.3. Key Usage		
2.3.1. Digital Signature		"1"
2.3.2. Content Commitment		"1"
2.3.3. Key Encipherment		"1"
2.3.4. Data Encipherment		"0"
2.3.5. Key Agreement		"0"
2.3.6. Key CertificateSignature		"0"
2.3.7. CRL Signature		"0"
2.4 Extended Key Usage		
2.4.1. Email Protection		"1"
2.4.2. Client Authentication		"1"
2.5. Qualified Certificate Statements		
2.5.1. QcCompliance	Indicación de certificado cualificado	OID 0.4.0.1862.1.1
2.5.2. QcEuRetentionPeriod	Período de conservación: 15 años	OID 0.4.0.1862.1.3 =15
2.5.3. QcSSCD	Uso de dispositivo seguro de firma	OID 0.4.0.1862.1.4
2.5.4. QcType-eseal	Certificado de Sello	OID 0.4.0.1862.1.6.2
2.5.5. QcPDS	Lugar donde se encuentra la PDS	OID 0.4.0.1862.1.5 http://www.seg-social.es/ACGISS https://sede.seg-social.gob.es/descarga/ACGISS_PDSSeal.pdf
2.6. Certificate Policies		
2.6.1. Policy Identifier	Certificado de sello de nivel alto según política AGE	2.16.724.1.3.5.6.1
2.6.2. Policy Identifier	QCP-l-qscd	0.4.0.194112.1.3
2.6.3. Policy Identifier	OID asociado a la PC de ACGISS	2.16.724.1.4.2.2.1.1.2
2.6.4. Policy Qualifier ID		
2.6.4.1 CPS Pointer	URL de la Política de certificación	http://www.seg-social.es/ACGISS
2.6.4.2 User Notice	URL Condiciones de Uso	Certificado cualificado de sello electrónico, nivel alto. Consulte las condiciones de uso en http://www.seg-social.es/ACGISS Nuevo CIF de la GISS desde jun 2017: Q2802407C
2.7. Subject Alternative Name		
2.7.2. Directory Name	Identidad Administrativa	
2.7.2.1. Tipo de certificado	Indica la naturaleza del certificado	2.16.724.1.3.5.6.1.1 = SELLO ELECTRONICO DE NIVEL ALTO
2.7.2.2. Nombre de la entidad suscriptora	Entidad suscriptora del certificado	2.16.724.1.3.5.6.1.2 = "Nombre de la Entidad suscriptora" Ej: SECRETARIA DE ESTADO DE LA SEGURIDAD SOCIAL
2.7.2.3. NIF entidad suscriptora	CIF de le Entidad suscriptora	2.16.724.1.3.5.6.1.3 = "CIF Entidad" Ej: SE = S2819001E
2.8. Issuer Alternative Name	Nombre alternativo de la persona de contacto de la entidad emisora	
2.8.1. rfc822Name	Correo electrónico de contacto	acgiss.soporte.giss@seg-social.es
2.9. cRLDistributionPoint		

2.9.1. distributionPoint	Punto de distribución nº1	http://crl.seg-social.gob.es/ac_sub.crl
2.10. Authority Info Access		
2.10.1. Access Method	ID de On-line Certificate Status Protocol	Id-ad-ocsp
2.10.2. Access Location	dirección web del OCSP	http://ocsp.seg-social.gob.es/
2.10.3. Access Method	ID de localización del certificado de CA emisora del certificado	Id-ad-caIssuers
2.10.4. Access Location	URL acceso a certificado SUBCA	http://www.seg-social.es/ACGISS/Certs/SUBCA_GISS01
2.11. Basic Constraints		
2.11.2. Path Length Constraints	Puede especificarse un número máximo de niveles.	Ninguno

2. NIVEL MEDIO

CAMPO	DESCRIPCIÓN	VALORES
1. X.509V1		
1.1. Versión	V3	2
1.2. Serial Number	Nº identificativo único	*Automático*
1.3. Signature Algorithm	Tipo de algoritmo. OID 2.16.840.1.101.3.4.2	SHA256RSA
1.4. Issuer Distinguished Name		
1.4.1. Country (C)	ES	ES
1.4.2. Organization (O)	Denominación oficial del prestador	TESORERIA GENERAL DE LA SEGURIDAD SOCIAL
1.4.3 Organizational Unit (OU)	Unidad Organizativa responsable de la emisión	GERENCIA DE INFORMATICA DE LA SEGURIDAD SOCIAL
1.4.4. Locality (L)	Localización	MADRID
1.4.5. Organizational Unit (OU)	Unidad organizativa dentro del prestador de servicios, responsable de la emisión del certificado.	GISS01
1.4.6. Serial Number	Número único de identificación de la entidad de certificación	Q2827003A
1.4.8. Common Name (CN)	Nombre común del certificado de la CA subordinada	SUBCA GISS01
1.5. Validity		
1.5.1. Not Before	Fecha inicio validez YYMMDDHHMMSSZ	YYMMDDHHMMSSZ
1.5.2. Not After	Fecha fin validez YYMMDDHHMMSSZ	YYMMDDHHMMSSZ
1.6. Subject		
1.5.1. Country (C)	ES	ES
1.5.2. Organization (O)	Denominación del suscriptor	"Nombre oficial de la Entidad" Ej: SECRETARIA DE ESTADO DE LA SEGURIDAD SOCIAL
1.5.4. Organizational Unit (OU)	Unidad organizativa dentro del prestador de servicios, responsable de la emisión del certificado.	ACTUACION AUTOMATIZADA
1.5.5. Organizational Unit (OU)	Tipo certificado= "sello electrónico"	SELLO ELECTRONICO
1.5.3 Organizational Unit (OU)	Identificación del suscriptor según DIR3	"Número DIR3 de la Entidad" Ej: SE = E04926001
1.5.6. Descripción	Descripción uso certificado	NIVEL MEDIO
1.5.7. Serial Number	Número único de identificación de la entidad	"CIF de la Entidad" Ej: SE = S2819001E

1.5.9. Common Name (CN)	Denominación del certificado	"Nombre del sello electrónico" Ej: "SELLO ELECTRONICO DE LA SEGURIDAD SOCIAL"
1.7. Subject Public Key Info	Clave pública del certificado	(RSA 2048 bits)
2. X.509v3 Extensions		
2.1. Authority Key Identifier		
2.1.1. Key Identifier	Identificador de clave pública del emisor. Path de identificación	*Automático*
2.1.2. AuthorityCertIssuer	Nombre de la CA a la que corresponde esa clave	*Automático*
2.1.3. AuthorityCertSerialNumber	Número de serie del certificado de la CA	*Automático*
2.2. Subject Key Identifier	Identificador de la clave pública del suscriptor	*Automático*
2.3. Key Usage		
2.3.1. Digital Signature		"1"
2.3.2. Content Commitment		"1"
2.3.3. Key Encipherment		"1"
2.3.4. Data Encipherment		"0"
2.3.5. Key Agreement		"0"
2.3.6. Key CertificateSignature		"0"
2.3.7. CRL Signature		"0"
2.4 Extended Key Usage		
2.4.1. Email Protection		"1"
2.4.2. Client Authentication		"1"
2.5. Qualified Certificate Statements		
2.5.1. QcCompliance	Indicación de certificado cualificado	OID 0.4.0.1862.1.1
2.5.2. QcEuRetentionPeriod	Período de conservación: 15 años	OID 0.4.0.1862.1.3 =15
2.5.3. QcType-eseal	Certificado de Sello	OID 0.4.0.1862.1.6.2
2.5.4. QcPDS	Lugar donde se encuentra la declaración PDS	OID 0.4.0.1862.1.5 http://www.seg-social.es/ACGISS https://sede.seg-social.gob.es/descarga/ACGISS_PDSSeal.pdf
2.6. Certificate Policies		
2.6.1. Policy Identifier	Certificado de sello de nivel medio según política AGE	2.16.724.1.3.5.6.2
2.6.2. Policy Identifier	QCP-l	0.4.0.194112.1.1
2.6.3. Policy Identifier	OID asociado a la PC de ACGISS	2.16.724.1.4.2.2.1.1.1
2.6.4. Policy Qualifier ID		
2.6.4.1 CPS Pointer	URL de la Política de certificación	http://www.seg-social.es/ACGISS
2.6.4.2 User Notice	URL Condiciones de Uso	Certificado cualificado de sello electrónico, nivel medio/sustancial. Consulte las condiciones de uso en http://www.seg-social.es/ACGISS Nuevo CIF de la GISS desde jun 2017: Q2802407C
2.7. Subject Alternative Name		
2.7.2. Directory Name	Identidad Administrativa	
2.7.2.1. Tipo de certificado	Indica la naturaleza del certificado	2.16.724.1.3.5.6.2.1 = SELLO ELECTRONICO DE NIVEL MEDIO

2.7.2.2. Nombre de la entidad suscriptora	Entidad suscriptora del certificado	2.16.724.1.3.5.6.2.2 = "Nombre de la Entidad suscriptoras" Ej: SECRETARIA DE ESTADO DE LA SEGURIDAD SOCIAL
2.7.2.3. NIF entidad suscriptora	CIF de le Entidad suscriptora	2.16.724.1.3.5.6.2.3 = "CIF Entidad" Ej: SE = S2819001E
2.8. Issuer Alternative Name	Nombre alternativo de la persona de contacto de la entidad emisora	
2.8.1. rfc822Name	Correo electrónico de contacto	acgiss.soporte.giss@seg-social.es
2.9. cRLDistributionPoint		
2.9.1. distributionPoint	Punto de distribución nº1	http://crl.seg-social.gob.es/ac_sub.crl
2.10. Authority Info Access		
2.10.1. Access Method	ID de On-line Certificate Status Protocol	Id-ad-ocsp
2.10.2. Access Location	dirección web del OCSP	http://ocsp.seg-social.gob.es/
2.10.3. Access Method	ID de localización del certificado de CA emisora del certificado	Id-ad-caIssuers
2.10.4. Access Location	URL acceso a certificado SUBCA	http://www.seg-social.es/ACGISS/Certs/SUBCA_GISS01
2.11. Basic Constraints		
2.11.2. Path Length Constraints	Puede especificarse un número máximo de niveles.	Ninguno