Perfil de certificado

Empleado público

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.	GISS01
1.4.6. Serial Number	Número único de identificación de la entidad de certificación	Q2827003A
1.4.7. 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		
1.6.1. Country (C)	ES	ES
1.6.2. Organization (O)	Denominación "oficial" de Administración suscriptora del certificado.	SECRETARIA DE ESTADO DE LA SEGURIDAD SOCIAL
1.6.3. Organizational Unit (OU)	Tipo de certificado	CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO
1.6.4. Organizational Unit (OU)	Subdivisión interna según categoría del certificado	PERSONALES
1.6.5. Organizational Unit (OU)	Subdivisión interna a efectos de gestión	Dos dígitos asignados automáticamente
1.6.6. Serial Number	NIF/NIE del titular	IDCES-"NIF/NIE"
1.6.7. Surname	Primer y segundo apellido y DNI	"PRIMER APELLIDO" (espacio) "SEGUNDO APELLIDO" (espacio-guión-espacio) "NIF/NIE"
1.6.8. Given Name	Nombre de pila	"NOMBRE"
1.6.9. Common Name (CN)	Nombre del titular	"NOMBRE" (espacio) "PRIMER APELLIDO" (espacio) "SEGUNDO APELLIDO" (espacio) (espacio-guión-espacio) "NIF/NIE"
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. KeyIdentifier	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*
2.5. 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	OID 0.4.0.1862.1.3 =15
2.5.3. QcType-esign	Certificado de firma	OID 0.4.0.1862.1.6.1
2.5.4. QcPDS	Lugar donde se encuentra la declaración PDS en inglés	OID 0.4.0.1862.1.5 https://sede.seg-social.gob.es/ACGISS/en/PDSempleado
2.6. Certificate Policies		
2.6.1. Policy Identifier	OID que indica certificado de empleado público nivel medio según política AGE	2.16.724.1.3.5.7.2
2.6.2. Policy Identifier	QCP-n	0.4.0.194112.1.0
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 empleado público, nivel medio. Consulte las condiciones de uso en http://www.seg-social.es/ACGISS
2.7. Subject Alternative Name		
2.7.2. Directory Name	Identidad Administrativa	
2.7.2.1. Tipo de certificado	Indica la naturaleza del certificado	2.16.724.1.3.5.7.2.1 = CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO (de nivel medio)
2.7.2.2. Nombre de la entidad suscriptora	Nombre de la Entidad suscriptora de la que depende el empleado	2.16.724.1.3.5.7.2.2 = SECRETARIA DE ESTADO DE LA SEGURIDAD SOCIAL
2.7.2.3. CIF entidad suscriptora	CIF de la Entidad suscriptora	2.16.724.1.3.5.7.2.3 = S2819001E
2.7.2.4. DNI/NIE del responsable	NIF/NIE del empleado	2.16.724.1.3.5.7.2.4 = "NIF/NIE"
2.7.2.6. Nombre de pila	Nombre del empleado	2.16.724.1.3.5.7.2.6 = "NOMBRE"
2.7.2.7. Primer apellido	Primer apellido del empleado	2.16.724.1.3.5.7.2.7 = "PRIMER APELLIDO"
2.7.2.8. Segundo apellido	Segundo apellido del empleado	2.16.724.1.3.5.7.2.8 = "SEGUNDO APELLIDO"
2.8. Issuer Alternative Name	Nombre alternativo 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

3. X.509v3 Extensions (FIRMA Y AUTENTICACIÓN)		
2.3. Key Usage		
2.3.1. Digital Signature		"1"
2.3.2. Content Commitment		"1"

2.3.3. Key Encipherment		"0"
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"
2.6. Certificate Policies		
2.6.3. Policy Identifier	OID asociado al certificado de firma y autenticación	2.16.724.1.4.2.2.1.2.11

4. X.509v3 Extensions (CIFRADO)		
2.3. Key Usage		
2.3.1. Digital Signature		"0"
2.3.2. Content Commitment		"0"
2.3.3. Key Encipherment		"1"
2.3.4. Data Encipherment		"1"
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		"0"
2.6. Certificate Policies		
2.6.3. Policy Identifier	OID asociado al certificado de cifra	2.16.724.1.4.2.2.1.2.12