



Real Casa de la Moneda
Fábrica Nacional
de Moneda y Timbre

DIRECCIÓN DE SISTEMAS DE INFORMACIÓN
DEPARTAMENTO CERES

DEFINICIÓN DE PERFILES AC REPRESENTACIÓN

v 8.0

Referencia:

Documento clasificado como: *Público*

Contenido

Introducción	3
1. Perfiles de certificado.....	3
1.1. Perfil certificado AC Representación.....	3
1.2. Perfil certificado de representante para administradores únicos y solidarios	5
1.3. Perfil certificado de representante de persona jurídica	8
1.4. Perfil certificado de representante de entidad sin personalidad jurídica.....	11
Anexo. Propuesta DTIC de los perfiles de certificados de representante de abril 2016.....	14

Introducción

En el presente documento se describe tanto el perfil del certificado de la CA encargada de la emisión de certificados de representante de persona jurídica, así como los perfiles de los certificados emitidos por dicha CA.

1. Perfiles de certificado

1.1. Perfil certificado AC Representación

Campo		Contenido	Obligatorio
1.	Version	2	Sí
2.	Serial Number	Número identificativo único del certificado.	Sí
3.	Signature Algorithm	Sha256withRsaEncryption	Sí
4.	Issuer Distinguish Name	Entidad emisora del certificado (CA Raíz)	Sí
	4.1. Country	C=ES	Sí
	4.2. Organization	Denominación (nombre "oficial" de la organización) del <i>Prestador de Servicios de Confianza</i> (emisor del certificado). O=FNMT-RCM	Sí
	4.3. Organizational Unit	OU=AC RAIZ FNMT-RCM	Sí
5.	Validity	Hasta 31/12/2029	Sí
6.	Subject		Sí
	6.1. Country	C=ES	Sí
	6.2. Organization	Denominación (nombre "oficial" de la organización) del <i>Prestador de Servicios de Confianza</i> (emisor del certificado). O=FNMT-RCM.	Sí
	6.3. Organizational Unit	OU=CERES	Sí
	6.4. CommonName	CN=AC Representación	Sí
7.	Authority Key Identifier	Identificador de la clave pública de la entidad raíz. Medio para identificar la clave pública correspondiente a la clave privada utilizada por la CA para firmar el certificado de esta CA Subordinada	Sí
8.	Subject Public Key Info	Clave pública de la CA Subordinada de Representación codificada según el estándar PKCS#1 de RSA.	Sí
9.	Subject Key Identifier	Identificador de la clave pública de la CA Subordinada. Medio para identificar certificados que contienen una clave pública particular y facilita la construcción de rutas de certificación.	Sí
10.	Key Usage	Uso permitido de las claves certificadas.	Sí
	10.1. Digital Signature	0	Sí
	10.2. Content Commitment	0	Sí

Campo		Contenido	Obligatorio
	10.3. Key Encipherment	0	Sí
	10.4. Data Encipherment	0	Sí
	10.5. Key Agreement	0	Sí
	10.6. Key Certificate Signature	1	Sí
	10.7. CRL Signature	1	Sí
11. Certificate Policies		Política de certificación	Sí
	11.1. Policy Identifier	2.5.29.32.0 (anyPolicy)	Sí
	11.2. Policy Qualifier Id		Sí
	11.2.1 CPS Pointer	http://www.cert.fnmt.es/dpcs/	Sí
	11.2.2 User Notice	Sujeto a las condiciones de uso expuestas en la Declaración de Prácticas de Certificación de la FNMT-RCM (C/ Jorge Juan, 106-28009-Madrid-España)	Sí
12. CRL Distribution Point			Sí
	12.1. Distribution Point 1	Punto de distribución 1 de la CRL (ARL) ldap://ldapfnmt.cert.fnmt.es/CN=CRL,OU=AC%20RAIZ%20FNMT-RCM,O=FNMT-RCM,C=ES?authorityRevocationList;binary?base?objectclass=cRLDistributionPoint	Sí
	12.2. Distribution Point 2	Punto de distribución 2 de la CRL (ARL) http://www.cert.fnmt.es/crls/ARLFNMTRCM.crl	Sí
13. Authority Info Access			Sí
	13.1. Access Method 1	Identificador de método de acceso a la información de revocación: 1.3.6.1.5.5.7.48.1 (ocsp)	Sí
	13.2. Access Location 1	http://ocspfnmtmca.cert.fnmt.es/ocspfnmtmca/OcspResponder	Sí
	13.3. Access Method 2	Identificador de método de acceso a la información de certificados adicionales necesarios para la validación: 1.3.6.1.5.5.7.48.2 (ca cert)	Sí
	13.4. Access Location 2	http://www.cert.fnmt.es/certs/ACRAIFNMTRCM.crt	Sí
14. Basic Constraints			Sí
	14.1. cA	Valor TRUE (CA)	Sí
	14.2. pathLenConstraint	0	Sí

1.2. Perfil certificado de representante para administradores únicos y solidarios

Campo		Contenido	Obligatorio
1.	Version	2	Sí
2.	Serial Number	Número identificativo único del certificado.	Sí
3.	Signature Algorithm	Sha256withRsaEncryption	Sí
4.	Issuer Distinguish Name	Entidad emisora del certificado (CA Subordinada)	Sí
	4.1. Country	C=ES	Sí
	4.2. Organization	Denominación (nombre "oficial" de la organización) del <i>Prestador de Servicios de Confianza</i> (emisor del certificado). O=FNMT-RCM	Sí
	4.3. Organizational Unit	OU=CERES	Sí
	4.4. CommonName	CN=AC Representación	Sí
5.	Validity	2 años	Sí
6.	Subject	Identificación/descripción del <i>Representante</i> y de la <i>Entidad representada</i>	Sí
	6.1. Country	C=ES	Sí
	6.2. Organization	Razón social de la <i>Entidad Representada</i>	Sí
	6.3. OrganizationIdentifier	NIF de la <i>Entidad Representada</i>	Sí
	6.4. CommonName	NIF, nombre y primer apellido del <i>Representante</i> y NIF de la <i>Entidad representada</i> .	Sí
	6.5. Surname	Apellidos del <i>Representante</i>	Sí
	6.6. GivenName	Nombre de pila del <i>Representante</i>	Sí
	6.7. SerialNumber	NIF del <i>Representante</i>	Sí
	6.8. Description	Codificación del documento público que acredita las facultades del firmante o los datos registrales.	Sí
7.	Authority Key Identifier	Identificador de la clave pública del PSC. Medio para identificar la clave pública correspondiente a la clave privada utilizada por la CA para firmar un certificado.	Sí
8.	Subject Public Key Info	Clave pública del <i>Firmante</i> , codificada de acuerdo con el algoritmo criptográfico. En este caso RSA Encryption.	Sí
9.	Subject Key Identifier	Identificador de la clave pública del <i>Firmante</i> . Medio para identificar certificados que contienen una clave pública particular y facilita la construcción de rutas de certificación.	Sí
10.	Key Usage	Uso permitido de las claves certificadas.	Sí
	10.1. Digital Signature	1	Sí
	10.2. Content Commitment	1	Sí
	10.3. Key Encipherment	1	Sí

Campo			Contenido	Obligatorio
	10.4. Data Encipherment		0	Sí
	10.5. Key Agreement		0	Sí
	10.6. Key Certificate Signature		0	Sí
	10.7. CRL Signature		0	Sí
11. Extended Key Usage			Uso mejorado o extendido de las claves	Sí
	11.1. Email Protection		1.3.6.1.5.5.7.3.4	Sí
	11.2. Client Authentication		1.3.6.1.5.5.7.3.2	Sí
12. Qualified Certificate Statements			Extensiones cualificadas.	
	12.1. QcCompliance		Certificado es cualificado.	Sí
	12.2. QcType		Qct-esign	Sí
	12.3. QcPDS		{ https://www.cert.fnmt.es/pds/PDS_es.pdf , es}, { https://www.cert.fnmt.es/pds/PDS_en.pdf , en}	Sí
	12.4. QcEuRetentionPeriod		15 años	Sí
13. Certificate Policies			Política de certificación	Sí
	13.1. Policy Identifier		1.3.6.1.4.1.5734.3.11.1	Sí
	13.1.1. Policy Qualifier Id			
		13.1.1.1. CPS Pointer	http://www.cert.fnmt.es/dpcs/	Sí
		13.1.1.2. User Notice	Certificado electrónico de representante de persona jurídica en sus relaciones con las AAPP o en la contratación de bienes o servicios que sean propios o concernientes a su giro o tráfico ordinario	Sí
	13.2. Policy Identifier		0.4.0.194112.1.0	
	13.3. Policy Identifier		2.16.724.1.3.5.8	Sí
14. Subject Alternative Names			Identificación/descripción del <i>Representante</i> y de la <i>Entidad representada</i>	Sí
	14.1. rfc822 Name		Correo electrónico del <i>Representante</i>	Sí
	14.2. Directory Name			
		14.2.1. Nombre	Nombre de pila del <i>Representante</i> Id Campo/Valor: 1.3.6.1.4.1.5734.1.1 =Nombre de pila	Sí
		14.2.2. Apellido1	Primer apellido del <i>Representante</i> Id Campo/Valor: 1.3.6.1.4.1.5734.1.2 =Apellido 1	Sí
		14.2.3. Apellido2	Segundo apellido del <i>Representante</i> Id Campo/Valor: 1.3.6.1.4.1.5734.1.3 =Apellido 2	Opcional
		14.2.4. NIF	NIF del <i>Representante</i> Id Campo/Valor: 1.3.6.1.4.1.5734.1.4=NIF	Sí
		14.2.5. Razón Social	Razón social de la <i>Entidad Representada</i> 1.3.6.1.4.1.5734.1.6=Razón social	Sí
		14.2.6. NIF de la entidad	NIF de la <i>Entidad Representada</i> 1.3.6.1.4.1.5734.1.7=NIF	Sí

Campo		Contenido	Obligatorio
	14.2.7. Cargo / Poder	Cargo o poder del <i>Representante</i> dentro de la entidad 1.3.6.1.4.1.5734.1.20 =Cargo	Sí
15. CRL Distribution Point			Sí
	15.1. Distribution Point 1	Punto de distribución 1 de la CRL ldap://ldaprep.cert.fnmt.es/CN=CRL<xxx>, OU=AC%20Representacion, OU=CERES,O=FNMT- RCM,C=ES?certificateRevocationList;binary?base?objectclass= cRLDistributionPoint	Sí
	15.2. Distribution Point 2	Punto de distribución 2 de la CRL http://www.cert.fnmt.es/crlsrep/CRLnnn.crl	Sí
16. Authority Info Access			Sí
	16.1. Access Method 1	Identificador de método de acceso a la información de revocación: 1.3.6.1.5.5.7.48.1 (ocsp)	Sí
	16.2. Acces Location 1	http://ocsprep.cert.fnmt.es/ocsprep/OcspResponder	Sí
	16.3. Access Method 2	Identificador de método de acceso a la información de certificados adicionales necesarios para la validación: 1.3.6.1.5.5.7.48.2 (ca cert)	Sí
	16.4. Acces Location 2	http://www.cert.fnmt.es/certs/ACREP.crt	Sí
17. Basic Constraints		Esta extensión sirve para identificar si el sujeto de certificación es una CA así como el máximo nivel de "profundidad" permitido para las cadenas de certificación".	Sí
	17.1. cA	Valor FALSE (entidad final)	Sí

1.3. Perfil certificado de representante de persona jurídica

Campo		Contenido	Obligatorio
1.	Version	2	Sí
2.	Serial Number	Número identificativo único del certificado.	Sí
3.	Signature Algorithm	Sha256withRsaEncryption	Sí
4.	Issuer Distinguish Name	Entidad emisora del certificado (CA Subordinada)	Sí
	4.1. Country	C=ES	Sí
	4.2. Organization	Denominación (nombre "oficial" de la organización) del Prestador de Servicios de Confianza (emisor del certificado). O=FNMT-RCM	Sí
	4.3. Organizational Unit	OU=CERES	Sí
	4.4. CommonName	CN=AC Representación	Sí
5.	Validity	2 años	Sí
6.	Subject	Identificación/descripción del Representante y de la Entidad representada	Sí
	6.1. Country	C=ES	Sí
	6.2. Organization	Razón social de la Entidad Representada	Sí
	6.3. OrganizationIdentifier	NIF de la Entidad Representada	Sí
	6.4. CommonName	NIF, nombre y primer apellido del Representante y NIF de la Entidad representada.	Sí
	6.5. Surname	Apellidos del Representante	Sí
	6.6. GivenName	Nombre de pila del Representante	Sí
	6.7. SerialNumber	NIF del Representante	Sí
	6.8. Description	Identificador de los documentos públicos que acreditan las facultades del Representante 2.5.4.13=Id de documentos públicos	Sí
7.	Authority Key Identifier	Identificador de la clave pública del PSC. Medio para identificar la clave pública correspondiente a la clave privada utilizada por la CA para firmar un certificado.	Sí
8.	Subject Public Key Info	Clave pública del Firmante, codificada de acuerdo con el algoritmo criptográfico. En este caso RSA Encryption.	Sí
9.	Subject Key Identifier	Identificador de la clave pública del Firmante. Medio para identificar certificados que contienen una clave pública particular y facilita la construcción de rutas de certificación.	Sí
10.	Key Usage	Uso permitido de las claves certificadas.	Sí
	10.1. Digital Signature	1	Sí
	10.2. Content Commitment	1	Sí
	10.3. Key Encipherment	1	Sí
	10.4. Data Encipherment	0	Sí

Campo			Contenido	Obligatorio
	10.5. Key Agreement		0	Sí
	10.6. Key Certificate Signature		0	Sí
	10.7. CRL Signature		0	Sí
11. Extended Key Usage			Uso mejorado o extendido de las claves	Sí
	11.1. Email Protection		1.3.6.1.5.5.7.3.4	Sí
	11.2. Client Authentication		1.3.6.1.5.5.7.3.2	Sí
	11.3.			
12. Qualified Certificate Statements			Extensiones cualificadas.	
	12.1. QcCompliance		Certificado es cualificado.	Sí
	12.2. QcType		Qct-esign	Sí
	12.3. QcPDS		{ https://www.cert.fnmt.es/pds/PDS_es.pdf , es}, { https://www.cert.fnmt.es/pds/PDS_en.pdf , en}	Sí
	12.4. QcEuRetentionPeriod		15 años	Sí
13. Certificate Policies			Política de certificación	Sí
	13.1. Policy Identifier		1.3.6.1.4.1.5734.3.11.2	Sí
	13.1.1. Policy Qualifier Id			
		13.1.2. CPS Pointer	http://www.cert.fnmt.es/dpcs/	Sí
		13.1.3. User Notice	Certificado electrónico de representante de persona jurídica en sus relaciones con las AAPP, Entidades y Organismos Públicos vinculados o dependientes de las mismas	Sí
	13.2. Policy Identifier		0.4.0.194112.1.0	Sí
	13.3. Policy Identifier		2.16.724.1.3.5.8	Sí
14. Subject Alternative Names			Identificación/descripción del <i>Representante</i> y de la <i>Entidad</i>	Sí
	14.1. rfc822 Name		Correo electrónico del <i>Representante</i>	Sí
	14.2. Directory Name			
		14.2.1. Nombre	Nombre de pila del <i>Representante</i> Id Campo/Valor: 1.3.6.1.4.1.5734.1.1 =Nombre de pila	Sí
		14.2.2. Apellido1	Primer apellido del <i>Representante</i> Id Campo/Valor: 1.3.6.1.4.1.5734.1.2 =Apellido 1	Sí
		14.2.3. Apellido2	Segundo apellido del <i>Representante</i> Id Campo/Valor: 1.3.6.1.4.1.5734.1.3 =Apellido 2	Opcional
		14.2.4. NIF	NIF del <i>Representante</i> Id Campo/Valor: 1.3.6.1.4.1.5734.1.4=NIF	Sí
		14.2.5. Razón Social	Razón social de la <i>Entidad Representada</i> 1.3.6.1.4.1.5734.1.6=Razón social	Sí
		14.2.6. NIF de la entidad	NIF de la <i>Entidad Representada</i> 1.3.6.1.4.1.5734.1.7=NIF	Sí
15. CRL Distribution Point				Sí

Campo		Contenido	Obligatorio
	15.1. Distribution Point 1	Punto de distribución 1 de la CRL ldap://ldaprep.cert.fnmt.es/CN=CRL<xxx>, OU=AC%20Representacion, OU=CERES,O=FNMT- RCM,C=ES?certificateRevocationList;binary?base?objectclass=cR LDistributionPoint	Sí
	15.2. Distribution Point 2	Punto de distribución 2 de la CRL (ARL) http://www.cert.fnmt.es/crlsrep/CRLnnn.crl	Sí
16. Authority Info Access			Sí
	16.1. Access Method 1	Identificador de método de acceso a la información de revocación: 1.3.6.1.5.5.7.48.1 (ocsp)	Sí
	16.2. Acces Location 1	http://ocsprep.cert.fnmt.es/ocsprep/OcspResponder	Sí
	16.3. Access Method 2	Identificador de método de acceso a la información de certificados adicionales necesarios para la validación: 1.3.6.1.5.5.7.48.2 (ca cert)	Sí
	16.4. Acces Location 2	http://www.cert.fnmt.es/certs/ACREP.crt	Sí
17. Basic Constraints		Esta extensión sirve para identificar si el sujeto de certificación es una CA así como el máximo nivel de "profundidad" permitido para las cadenas de certificación".	Sí
	17.1. cA	Valor FALSE (entidad final)	Sí

1.4. Perfil certificado de representante de entidad sin personalidad jurídica

Campo		Contenido	Obligatorio
1.	Version	2	Sí
2.	Serial Number	Número identificativo único del certificado.	Sí
3.	Signature Algorithm	Sha256withRsaEncryption	Sí
4.	Issuer Distinguish Name	Entidad emisora del certificado (CA Subordinada)	Sí
	4.1. Country	C=ES	Sí
	4.2. Organization	Denominación (nombre "oficial" de la organización) del <i>Prestador de Servicios de Confianza</i> (emisor del certificado). O=FNMT-RCM	Sí
	4.3. Organization Unit	OU=CERES	Sí
	4.4. CommonName	CN=AC Representación	Sí
5.	Validity	2 años	Sí
6.	Subject	Identificación/descripción del <i>Representante</i> y de la <i>Entidad representada</i>	Sí
	6.1. Country	C=ES	Sí
	6.2. Organization	Razón social de la <i>Entidad Representada</i>	Sí
	6.3. OrganizationIdentifier	NIF de la <i>Entidad Representada</i>	Sí
	6.4. CommonName	NIF, nombre y primer apellido del <i>Representante</i> y NIF de la <i>Entidad representada</i>	Sí
	6.5. Surname	Apellidos del <i>Representante</i>	Sí
	6.6. GivenName	Nombre de pila del <i>Representante</i>	Sí
	6.7. SerialNumber	NIF del <i>Representante</i>	Sí
	6.8. Description	Identificador de los documentos públicos que acreditan las facultades del <i>Representante</i> 2.5.4.13=Id de documentos públicos	Sí
7.	Authority Key Identifier	Identificador de la clave pública del PSC. Medio para identificar la clave pública correspondiente a la clave privada utilizada por la CA para firmar un certificado.	Sí
8.	Subject Public Key Info	Clave pública del <i>Firmante</i> , codificada de acuerdo con el algoritmo criptográfico. En este caso RSA Encryption.	Sí
9.	Subject Key Identifier	Identificador de la clave pública del <i>Firmante</i> . Medio para identificar certificados que contienen una clave pública particular y facilita la construcción de rutas de certificación.	Sí
10.	Key Usage	Uso permitido de las claves certificadas.	Sí
	10.1. Digital Signature	1	Sí
	10.2. Content Commitment	1	Sí
	10.3. Key Encipherment	1	Sí

	10.4. Data Encipherment		0	Sí
	10.5. Key Agreement		0	Sí
	10.6. Key Certificate Signature		0	Sí
	10.7. CRL Signature		0	Sí
11. Extended Key Usage			Uso mejorado o extendido de las claves	Sí
	11.1. Email Protection		1.3.6.1.5.5.7.3.4	Sí
	11.2. Client Authentication		1.3.6.1.5.5.7.3.2	Sí
12. Qualified Certificate Statements			Extensiones cualificadas.	
	12.1. QcCompliance		Certificado es cualificado.	Sí
	12.2. QcType		Qct-esign	Sí
	12.3. QcPDS		{ https://www.cert.fnmt.es/pds/PDS_es.pdf , es}, { https://www.cert.fnmt.es/pds/PDS_en.pdf , en}	Sí
	12.4. QcEuRetentionPeriod		15 años	Sí
13. Certificate Policies			Política de certificación	Sí
	13.1. Policy Identifier		1.3.6.1.4.1.5734.3.11.3	Sí
	13.1.1. Policy Qualifier Id			
		13.1.2. CPS Pointer	http://www.cert.fnmt.es/dpcs/	Sí
		13.1.3. User Notice	Certificado electrónico de representante de entidad sin personalidad jurídica para el ámbito tributario y cualquier otro previsto por la legislación vigente	Sí
	13.2. Policy Identifier		0.4.0.194112.1.0	
	13.3. Policy Identifier		2.16.724.1.3.5.9	Sí
14. Subject Alternative Names			Identificación/descripción del <i>Representante</i> y de la <i>Entidad</i>	Sí
	14.1. rfc822 Name		Correo electrónico del <i>Representante</i>	Sí
	14.2. Directory Name			
		14.2.1. Nombre	Nombre de pila del <i>Representante</i> Id Campo/Valor: 1.3.6.1.4.1.5734.1.1 =Nombre de pila	Sí
		14.2.2. Apellido1	Primer apellido del <i>Representante</i> Id Campo/Valor: 1.3.6.1.4.1.5734.1.2 =Apellido 1	Sí
		14.2.3. Apellido2	Segundo apellido del <i>Representante</i> Id Campo/Valor: 1.3.6.1.4.1.5734.1.3 =Apellido 2	Opcional
		14.2.4. NIF	NIF del <i>Representante</i> Id Campo/Valor: 1.3.6.1.4.1.5734.1.4=NIF	Sí
		14.2.5. Razón Social	Nombre de la <i>Entidad sin personalidad jurídica</i> representada 1.3.6.1.4.1.5734.1.6=Razón social	Sí
		14.2.6. NIF de la entidad	NIF de la <i>Entidad sin personalidad jurídica</i> 1.3.6.1.4.1.5734.1.7=NIF	Sí
		14.2.7. Tipo de ESPJ	Tipo de <i>Entidad sin personalidad jurídica</i> 1.3.6.1.4.1.5734.1.22=Tipo de entidad.	Sí
15. CRL Distribution Point				Sí

	15.1. Distribution Point 1	Punto de distribución 1 de la CRL ldap://ldaprep.cert.fnmt.es/CN=CRL<xxx>, OU=AC%20Representacion, OU=CERES, O=FNMT- RCM, C=ES?certificateRevocationList;binary?base?objectclass=cR LDistributionPoint	Si
	15.2. Distribution Point 2	Punto de distribución 2 de la CRL (ARL) http://www.cert.fnmt.es/crlsrep/CRLnnn.crl	Si
16. Authority Info Access			Si
	16.1. Access Method 1	Identificador de método de acceso a la información de revocación: 1.3.6.1.5.5.7.48.1 (ocsp)	Si
	16.2. Acces Location 1	http://ocsprep.cert.fnmt.es/ocsprep/OcspResponder	Si
	16.3. Access Method 2	Identificador de método de acceso a la información de certificados adicionales necesarios para la validación: 1.3.6.1.5.5.7.48.2 (ca cert)	Si
	16.4. Acces Location 2	http://www.cert.fnmt.es/certs/ACREP.crt	Si
17. Basic Constraints		Esta extensión sirve para identificar si el sujeto de certificación es una CA así como el máximo nivel de "profundidad" permitido para las cadenas de certificación".	Si
	17.1. cA	Valor FALSE (entidad final)	Si

Anexo. Propuesta DTIC de los perfiles de certificados de representante de abril 2016

- *Codificación del atributo Common Name*

Se propone una codificación del campo Common Name que permite al usuario identificar el certificado como uno de representación, distinguiéndolo de uno de Persona Física básico, a través del literal 'R: '. Así mismo se permite identificar la Persona Jurídica representada para facilitar la selección de certificado en caso de una Persona Física que represente a varias Personas Jurídicas.

El campo tiene un tamaño máximo de 64 caracteres según la RFC 5280.

Campo	Contenido	Ejemplo	tamaño *
NIF	número DNI/NIE	12345678Z	10
Nombre	Tal y como figura en el DNI/NIE	Pedro Antonio	
Apellido 1	Tal y como figura en el DNI/NIE	López	
Literal	(R:)		4
NIF de la empresa	NIF de la empresa, tal como figura en los registros oficiales.	B0085974Z	9
Literal	)		2
Literal	AUTENTIC, FIRMA o CIFRADO		8

*(contando espacio en blanco posterior)