Real Casa de la Moneda
Fábrica Nacional
de Moneda y Timbre

DIRECCIÓN DE SISTEMAS DE INFORMACIÓN
DEPARTAMENTO CERES

DOCUMENTO DE PERFILES DE LA CA DE COMPONENTES

	NOMBRE	FECHA
Elaborado por:	Área Técnica	03/05/2012
Revisado por:		
Aprobado por:		

HISTÓRICO DEL DOCUMENTO			
Versión	**Fecha**	**Descripción**	**Autores**
1.0	03/05/2012	Creación del documento	Jl6078, Ec6165
1.1	12/07/2012	KeyUsage marcada como crítica	Jl6078
1.2	05/03/2013	División de perfiles en PF y PJ Añadidas políticas para cada perfil Añadido RDN LocalityName en Subject Eliminación de los datos del responsable en PJ Modificaciones en extensión KeyUsage	Jl6078, Ec6165
1.3	06/03/2013	Eliminado LocalityName de perfiles PF	Jl6078,Ec6165
1.4	27/06/2013	Eliminada extensión QcStatement de certificado de componente genérico (sello electrónico) Renombrados los tipos de certificado	Jl6078,Ec6165

		Sustitución de rol *titular* por rol *suscriptor*	
1.5	26/07/2013	Renombrado tipo de certificado *Sello electrónico* como *Sello de entidad*	Ec6165
1.6	30/07/2013	Eliminado *Policy Qualifier Id User Notice* de la extensión *CertificatePolicies*. No es necesario ya que se trata de certificados NO reconocidos	Ec6165
1.7	20/11/2013	Eliminado algoritmo sha1 del perfil del certificado de la CA y cambiado algoritmo sha1 por sha256 en los certificados de componente: a partir del 1 de enero de 2016 Microsoft no permitirá el algoritmo sha1 en certificados SSL y de firma de código.	Ec6165
1.8	22/06/2016	Eliminados certificados cuyo suscriptor es una persona física (adaptación eIDAS). Eliminados usos combinados de EKU no permitidos en certificados (requs. Microsoft) Eliminado uso anyExtendedKeyUsage en todos los certificados (requs. Microsoft)	
1.9	07/10/2016	Modificados perfiles para cumplimiento del Reglamento (UE) 910/2014, relativo a eIDAS: - Cambio en la semántica de la identificación de entidades. - Adaptación de la extensión QcStatements. - Adaptación de la extensión CertificatePolicies y cambio de los OIDs específicos de la FNMT. En el certificado de sello se activa el bit ContentCommitment. Se modifica la duración de los certificados SSL para que sea de 1 o 2 años y así cumplir el requisito EV de no superar 27 meses.	Área Técnica
1.10	01/12/2016	Se eliminan las extensiones cualificadas (Qualified Certificate Statements y Policy Identifier QCP-w) del certificado wildcard. Ver acta del proyecto de Adaptaciones eIDAS	Área Técnica

		del 30/11/2016	
1.10.1	03/01/2017	Debido a un cambio en el alcance de la auditoría ETSI N series, los certificados web (SSL, SAN y wildcard) no serán cualificados. Por ello, en el caso de estos certificados se seguirá una política de certificación OV. Esto implica: - En la extensión *Qualified Certificate Statements*, se elimina el campo *QcCompliance.* - En la extensión *Certificate Policies*: o Se elimina del campo *User notice* la palabra cualificado. o Se cambia el identificador de política QCP-w por el identificador OVCP definido en la ETSI 319 411-1. En el caso de los certificados wildcard, se vuelve a añadir la extensión *Qualified Certificate Statements*, sin el campo *QcCompliance.* Y se añade el identificador de política OVCP.	Área Técnica

Referencia:

Documento clasificado como: *Sólo para uso interno*

Contenido

1. OBJETO

El objeto de este documento es la definición de los perfiles relativos a la nueva infraestructura de certificados de Componentes.

Se incluye el perfil del certificado de la CA Subordinada y el de Componentes.

2. PERFILES

2.1. CA SUBORDINADA COMPONENTES

Campo		Contenido	Obligatoriedad	Criticidad	Especificaciones
1. Version		2	Sí		Integer:=2 ([RFC5280] describe la versión del certificado. El valor 2 equivale a decir que el certificados es versión 3 (X509v3)
2. Serial Number		Número identificativo único del certificado.	Sí		Integer. SerialNumber = ej: 111222. Establecido automáticamente por la Entidad de Certificación. [RFC5280]. Será un "integer" positivo, no mayor 20 octetos (1- 2^{159}).
3. Signature Algorithm		Sha256withRsaEncryption	Sí		Identificando el tipo de algoritmo OID: 1.2.840.113549.1.1.11
4. Issuer Distinguish Name		Entidad emisora del certificado (CA Raíz)	Sí		
	4.1. Country	C=ES	Sí		Se codificará de acuerdo a "ISO 3166-1-alpha-2 code elements". PrintableString, tamaño 2 (rfc5280)
	4.2. Organization	Denominación (nombre "oficial" de la organización) del prestador de servicios de certificación (emisor del certificado). O=FNMT-RCM	Sí		UTF8 String, tamaño máximo 128 (rfc5280)
	4.3. Organization Unit	OU=AC RAIZ FNMT-RCM	Sí		UTF8 String, tamaño máximo 128 (rfc5280)
5. Validity		15 años	Sí		
6. Subject		Entidad emisora del certificado (CA Subordinada)	Sí		
	6.1. Country	C=ES	Sí		Se codificará de acuerdo a "ISO 3166-1-alpha-2 code elements". PrintableString, tamaño 2 (rfc5280)

	6.2. Organization	Denominación (nombre "oficial" de la organización) del prestador de servicios de certificación (emisor del certificado). O=FNMT-RCM.	Sí		UTF8 String, tamaño máximo 128 (rfc5280)
	6.3. Organization Unit	OU=AC Componentes Informáticos	Sí		UTF8 String, tamaño máximo 128 (rfc5280)
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		RFC 5280: hash SHA-1 de 20 bytes calculado sobre el valor BIT STRING del campo subjectPublicKey del emisor del certificado (excluyendo etiqueta, longitud y número de bits no usados). Coincide con el campo Subject Key Identifier de la CA raíz.
8. Subject Public Key Info		Clave pública de la CA de Componentes, codificada según el estándar PKCS#1 de RSA. La longitud de la clave será 2048 bits.	Sí		Campo que contiene la clave pública del certificado.
9. Subject Key Identifier		Identificador de la clave pública de la CA de Componentes.	Sí		RFC 5280: hash SHA-1 de 20 bytes calculado sobre el valor BIT STRING del campo subjectPublicKey del sujeto (excluyendo etiqueta, longitud y número de bits no usados).
10. Key Usage		Uso permitido de las claves del certificado.	Sí	Sí	Normalizado en norma X509
	10.1. Digital Signature	0	Sí		Permite realizar la operación de firma electrónica.
	10.2. Content Commitment	0	Sí		Se refiere a la cualidad de un tipo de certificado que indica al software en el que se usa que debe permitir que el usuario conozca lo que firma.
	10.3. Key Encipherment	0	Sí		Se utiliza para gestión y transporte de claves para establecimiento de sesiones seguras
	10.4. Data Encipherment	0	Sí		Se utiliza para cifrar datos que no sean claves criptográficas.
	10.5. Key Agreement	0	Sí		Para uso en el proceso de acuerdo de claves
	10.6. Key Certificate Signature	1	Sí		Si se activa el bit, permite que el certificado sea utilizado para firmar otros certificados. Este uso se utiliza en los certificados de autoridades de certificación.
	10.7. CRL Signature	1	Sí		Si se activa el bit, permite la firma de listas de revocación de certificados. Este uso se utiliza en los certificados de autoridades de certificación.
11. Certificate Policies		Política de certificación	Sí	No	

	11.1. Policy Identifier		2.5.29.32.0 (anyPolicy)	Sí		Atendiendo a la rfc5280: " *PolicyInformation SHOULD only contain an OID.* *In a CA certificate,these policy information terms limit the set of policies for certification paths which include this certificate. When a CA does not wish to limit the set of policies for certification paths which include this certificate, it MAY assert the special policy anyPolicy, with a value of { 2 5 29 32 0 }*"
	11.2. Policy Qualifier Id					
		11.2.1 CPS Pointer	http://www.cert.fnmt.es/dpcs/	Sí		IA5String String. URL de la declaración de prácticas de certificación.
		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		UTF8 String. Longitud máxima 200 caracteres.
12. CRL Distribution Point				Sí	No	
	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		Ruta donde reside la CRL (punto de distribución 1).
	12.2. Distribution Point 2		Punto de distribución 2 de la CRL (ARL) http://www.cert.fnmt.es/crls/ARLFNMTRCM.crl	Sí		Ruta del servicio LDAP donde reside la CRL (punto de distribución 2).
13. Basic Constraints					Sí	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.
	13.1. Subject Type		CA			Tipo de sujeto: Autoridad de Certificación.
	13.2. Path Length		0			Un pathLenConstraint de cero indica que esta CA no puede emitir certificados para otras CAs subordinadas, únicamente puede emitir certificados para entidades finales.
14. Authority Info Access				Sí		
	14.1. Access Method 1		Identificador de método de acceso a la información de revocación: 1.3.6.1.5.5.7.48.1 (ocsp)			OCSP (1.3.6.1.5.5.7.48.1)
	14.2. Acces Location 1		http://ocspfnmtrcmca.cert.fnmt.es/ocspfnmtrcmca/OcspResponder			URL del servicio de OCSP

	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)			Certificado de la CA emisora: De la rfc 5280: *"the id-ad-caIssuers OID is used when the additional information lists certificates that were issued to the CA that issued the certificate containing this extension. The referenced CA issuers description is intended to aid certificate users in the selection of a certification path that terminates at a point trusted by the certificate user."*
	Access Location 2	http://www.cert.fnmt.es/certs/ACRAIZFNMTRCM.crt			Ruta para descarga de certificados adicionales para la validación de la cadena de certificación. En este caso la ruta del certificado de la CA raíz de la FNMT-RCM.

2.2. COMPONENTES

2.2.1. Certificado de sello de entidad

Campo		Contenido	Obligatoriedad	Criticidad	Especificaciones
1. Version		2	Sí		Integer:=2 ([RFC5280] describe la versión del certificado. El valor 2 equivale a decir que el certificados es versión 3 (X509v3)
2. Serial Number		Número identificativo único del certificado.	Sí		Integer. SerialNumber = ej: 111222. Establecido automáticamente por la Entidad de Certificación. [RFC5280]. Será un "integer" positivo, no mayor de 20 octetos (1- 2^{159}). El número de serie se asignará de forma aleatoria.
3. Signature Algorithm		Sha256withRsaEncryption	Sí		Identificando el tipo de algoritmo OID: 1.2.840.113549.1.1.11
4. Issuer Distinguish Name		Entidad emisora del certificado (CA Subordinada)	Sí		
	4.1. Country	C=ES	Sí		Se codificará de acuerdo a "ISO 3166-1-alpha-2 code elements". PrintableString, tamaño 2 (rfc5280)
	4.2. Organization	Denominación (nombre "oficial" de la organización) del prestador de servicios de certificación (emisor del certificado). O=FNMT-RCM.	Sí		UTF8 String, tamaño máximo 128 (rfc5280)
	4.3. Organization Unit	Unidad organizativa dentro del prestador de servicios, responsable de la emisión del certificado.	Sí		UTF8 String, tamaño máximo 128 (rfc5280).

Campo		Contenido	Obligatoriedad	Criticidad	Especificaciones
		OU=CERES			
	4.4. Serial Number	Número único de identificación de la entidad, aplicable de acuerdo con el país. En España, NIF de la entidad suscriptora. serialNumber=Q2826004J	Sí		PrintableString, tamaño 64 (X520). En nuestro caso, el tamaño es 9
	4.5. Common Name	cn= AC Componentes Informáticos	Sí		UTF8 String (rfc5280)
5. Validity		Variable	Sí		La duración será variable (1, 2 ó 3 años) y se definirá a la hora de solicitar el certificado. El aprobador del mismo, deberá verificar si el valor es correcto.
6. Subject		Identificación/descripción del suscriptor del certificado y del componente	Sí		
	6.1. Country	C=ES	Sí		Se codificará de acuerdo a "ISO 3166-1-alpha-2 code elements". PrintableString, tamaño 2 (rfc5280)
	6.2. LocalityName	Nombre de la localidad del suscriptor	Sí		UTF8String (rfc5280). Por ejemplo: L=Madrid
	6.3. Organization	Denominación del suscriptor	Sí		UTF8String (rfc5280). Por ejemplo: O=Ministerio de Economía
	6.4. Organizational Unit	Departamento o área del suscriptor para el que se emite el certificado.	No		UTF8String (rfc5280). Por ejemplo: OU=Departamento de Informática
	6.5. Serial Number	NIF del suscriptor	Sí		PrintableString (rfc5280). Por ejemplo: SN= Q0000000J
	6.6. Organization Identifier	Identificador de la organización distinto del nombre Según la norma técnica ETSI EN 319 412-1 (VATES + NIF de la entidad)	Sí		Por ejemplo: organizationidentifier=VATES-Q0000000J
	6.7. Common Name	Denominación del componente	Sí		UTF8String (rfc5280). Por ejemplo: CN=Servicio de Registro
7. Authority Key Identifier		Identificador de la clave pública de la CA de Componentes. Medio para identificar la clave pública correspondiente a la clave privada utilizada por la CA para firmar el certificado de componente.	Sí	No	RFC 5280: hash SHA-1 de 20 bytes calculado sobre el valor BIT STRING del campo subjectPublicKey del emisor del certificado (excluyendo etiqueta, longitud y número de bits no usados). Coincide con el campo Subject Key Identifier de la CA emisora.
8. Subject Public Key Info		Clave pública del componente, codificada según el estándar PKCS#1 de RSA.	Sí	No	Campo que contiene la clave pública del certificado.

Campo		Contenido	Obligatoriedad	Criticidad	Especificaciones
		La longitud de la clave será 2048 bits.			
9. Subject Key Identifier		Identificador de la clave pública del componente.	Sí	No	RFC 5280: hash SHA-1 de 20 bytes calculado sobre el valor BIT STRING del campo subjectPublicKey del sujeto (excluyendo etiqueta, longitud y número de bits no usados).
10. Key Usage		Uso permitido de las claves certificadas.		Sí	Normalizado en norma X509
	10.1. Digital Signature	1	Sí		Permite realizar la operación de firma electrónica
	10.2. Content Commitment	1	Sí		Se refiere a la cualidad de un tipo de certificado que indica al software en el que se usa que debe permitir que el usuario conozca lo que firma.
	10.3. Key Encipherment	1	Sí		Se utiliza para gestión y transporte de claves para establecimiento de sesiones seguras
	10.4. Data Encipherment	0	Sí		Se utiliza para cifrar datos que no sean claves criptográficas.
	10.5. Key Agreement	0	Sí		Para uso en el proceso de acuerdo de claves
	10.6. Key Certificate Signature	0	Sí		Se permite usa para firmar certificados. Se utiliza en los certificados de autoridades de certificación.
	10.7. CRL Signature	0	Sí		Se permite para firmar listas de revocación de certificados.
11. Extended Key Usage		Uso mejorado o extendido de las claves	Sí	No	Esta extensión indica que uno o más propósitos para los cuales el certificado de clave pública se puede utilizar, además de o en lugar de los usos básicos que se indican en la extensión KeyUsage.
	11.1. Email Protection	1.3.6.1.5.5.7.3.4	No		Protección de correo electrónico.
	11.2. Client Authentication	1.3.6.1.5.5.7.3.2	No		Autenticación de cliente
12. Qualified Certificate Statements		Extensiones cualificadas.	Sí	No	ETSI TS 101 862 define la inclusión de ciertas declaraciones para certificados cualificados
	12.1. QcCompliance (0.4.0.1862.1.1)	Certificado cualificado	Sí		Indicación de certificado cualificado
	12.2. QcEuRetentionPeriod (0.4.0.1862.1.3)	15 años	Sí		Número de años a partir de la caducidad del certificado que se dispone de los datos de registro y otro información relevante. En este caso la Ley obliga: “Conservar registrada por cualquier medio seguro toda la información y documentación relativa a un certificado reconocido y las declaraciones de prácticas de certificación vigentes en cada momento, al menos durante 15 años contados desde el momento de su expedición, de manera que puedan verificarse las firmas efectuadas con el mismo

Campo			Contenido	Obligatoriedad	Criticidad	Especificaciones
	12.3. QcType (0.4.0.1862.1.6)		Id-etsi-qct-eseal (0.4.0.1862.1.6.2)	Sí		Indica que el certiticado es de sello . Certificate for electronic seals as defined in Regulation (EU) No 910/2014
	12.4. QcPDS(0.4.0.1862.1.5)		{https://www.cert.fnmt.es/pds/PDS_COMP_es.pdf, es},{https://www.cert.fnmt.es/pds/PDS_COMP_en.pdf, en}	Sí		Lugar donde se encuentra la declaración PDS
13. Certificate Policies			Política de certificación	Sí	No	
	13.1. Policy Identifier		1.3.6.1.4.1.5734.3.9.19	Sí		Identificador de la política
	13.1.1 Policy Qualifier Id			Sí		
		13.1.1.1 CPS Pointer	http://www.cert.fnmt.es/dpcs/	Sí		IA5String String. URL de las condiciones de uso.
		13.1.1.2 User Notice	Certificado cualificado de sello electrónico según reglamento europeo eIDAS. Sujeto a las condiciones de uso expuestas en la DPC de la FNMT-RCM (C/Jorge Juan 106-28009-Madrid-España)	Sí		UTF8 String. Longitud máxima 200 caracteres.
	13.2. Policy Identifier		QCP-l (0.4.0.194112.1.1)	Sí		Certificado cualificado de sello, acorde al Reglamento UE 910/2014 Itu-t(0) Identified-organizatio(4) etsi(0) qualifed-certificate-policies(194112) policy-identifiers(1) qcp-legal(1)
14. Subject Alternative Names				Sí	No	
	14.1. Denominación del componente		Id Campo / Valor: 1.3.6.1.4.1.5734.1.8 = < Denominación del componente>	Sí		
15. CRL Distribution Point			Informa acerca de cómo se obtiene la información de la CRL asociada al certificado.	Sí	No	
	15.1. Distribution Point 1		Punto de publicación de la CRL1. ldap://ldapcomp.cert.fnmt.es/CN=CRL<xxx*>, OU=AC%20Componentes%20Informaticos, O=FNMT-RCM,C=ES?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint *xxx: número entero identificador de la CRL (CRL particionadas)	Sí		Ruta del servicio LDAP donde reside la CRL (punto de distribución 1).
	15.2. Distribution Point 2		Punto de publicación de la CRL2. http://www.cert.fnmt.es/crlscomp/CRLnnn.crl	Sí		Ruta donde reside la CRL (punto de distribución 2).
16. Authority Info				Sí	No	

Campo		Contenido	Obligatoriedad	Criticidad	Especificaciones
Access					
	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://ocspcomp.cert.fnmt.es/ocsp/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		Entidad emisora de los certificados (CA Subordinada) De la rfc 5280: *"the id-ad-caIssuers OID is used when the additional information lists certificates that were issued to the CA that issued the certificate containing this extension. The referenced CA issuers description is intended to aid certificate users in the selection of a certification path that terminates at a point trusted by the certificate user."*
	16.4. Access Location 2	http://www.cert.fnmt.es/certs/ACCOMP.crt	Sí		Ruta para descarga de certificados adicionales para la validación de la cadena de certificación. En este caso la ruta del certificado de la CA subordinada de la raíz de la FNMT-RCM.
17. Basic Contraints		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	Sí	De la rf5280: *"This extension MAY appear as a critical or non-critical extension in end entity certificates.*
	17.1. Subject Type	Valor FALSE (entidad final)			Con este certificado no se pueden emitir otros certificados.

2.2.2. Certificado de componente de firma de código

Campo	Contenido	Obligatoriedad	Criticidad	Especificaciones
1. Version	2	Sí		Integer:=2 ([RFC5280] describe la versión del certificado. El valor 2 equivale a decir que el certificados es versión 3 (X509v3)
2. Serial Number	Número identificativo único del certificado.	Sí		Integer. SerialNumber = ej: 111222. Establecido automáticamente por la Entidad de Certificación. [RFC5280]. Será un "integer" positivo, no mayor de 20 octetos (1- 2^{159}). El número de serie se asignará de forma aleatoria.
3. Signature Algorithm	Sha256withRsaEncryption	Sí		Identificando el tipo de algoritmo OID: 1.2.840.113549.1.1.11

Campo		Contenido	Obligatoriedad	Criticidad	Especificaciones
4. Issuer Distinguish Name		Entidad emisora del certificado (CA Subordinada)	Sí		
	4.1. Country	C=ES	Sí		Se codificará de acuerdo a "ISO 3166-1-alpha-2 code elements". PrintableString, tamaño 2 (rfc5280)
	4.2. Organization	Denominación (nombre "oficial" de la organización) del prestador de servicios de certificación (emisor del certificado). O=FNMT-RCM.	Sí		UTF8 String, tamaño máximo 128 (rfc5280)
	4.3. Organization Unit	OU=AC Componentes Informáticos	Sí		UTF8 String, tamaño máximo 128 (rfc5280).
5. Validity		Variable	Sí		La duración será variable (1, 2 ó 3 años) y se definirá a la hora de solicitar el certificado. El aprobador del mismo, deberá verificar si el valor es correcto.
6. Subject		Identificación/descripción del suscriptor del certificado y del componente	Sí		
	6.1. Country	C=ES	Sí		Se codificará de acuerdo a "ISO 3166-1-alpha-2 code elements". PrintableString, tamaño 2 (rfc5280)
	6.2. LocalityName	Nombre de la localidad del suscriptor	Sí		UTF8String (rfc5280). Por ejemplo: L=Madrid
	6.3. Organization	Denominación del suscriptor	Sí		UTF8String (rfc5280). Por ejemplo: O=Ministerio de Economía
	6.4. Organizational Unit	Departamento o área del suscriptor para el que se emite el certificado.	No		UTF8String (rfc5280). Por ejemplo: OU=Departamento de Informática
	6.5. Serial Number	NIF del suscriptor	Sí		PrintableString (rfc5280). Por ejemplo: SN= Q0000000J
	6.6. Common Name	Denominación del componente	Sí		UTF8String (rfc5280). Por ejemplo: CN= FIRMA APPLETS
7. Authority Key Identifier		Identificador de la clave pública de la CA de Componentes. Medio para identificar la clave pública correspondiente a la clave privada utilizada por la CA para firmar el certificado de componente.	Sí	No	RFC 5280: hash SHA-1 de 20 bytes calculado sobre el valor BIT STRING del campo subjectPublicKey del emisor del certificado (excluyendo etiqueta, longitud y número de bits no usados). Coincide con el campo Subject Key Identifier de la CA emisora.
8. Subject Public Key Info		Clave pública del componente, codificada según el estándar PKCS#1 de RSA.	Sí	No	Campo que contiene la clave pública del certificado.

Campo			Contenido	Obligatoriedad	Criticidad	Especificaciones
			La longitud de la clave será 2048 bits.			
9. Subject Key Identifier			Identificador de la clave pública del componente.	Sí	No	RFC 5280: hash SHA-1 de 20 bytes calculado sobre el valor BIT STRING del campo subjectPublicKey del sujeto (excluyendo etiqueta, longitud y número de bits no usados).
10. Key Usage			Uso permitido de las claves certificadas.	Sí	Sí	Normalizado en norma X509
	10.1. Digital Signature		1			Permite realizar la operación de firma electrónica
	10.2. Content Commitment		0			Se refiere a la cualidad de un tipo de certificado que indica al software en el que se usa que debe permitir que el usuario conozca lo que firma.
	10.3. Key Encipherment		0			Se utiliza para gestión y transporte de claves para establecimiento de sesiones seguras
	10.4. Data Encipherment		0			Se utiliza para cifrar datos que no sean claves criptográficas.
	10.5. Key Agreement		0			Para uso en el proceso de acuerdo de claves
	10.6. Key Certificate Signature		0			Se permite usa para firmar certificados. Se utiliza en los certificados de autoridades de certificación.
	10.7. CRL Signature		0			Se permite para firmar listas de revocación de certificados.
11. Extended Key Usage			Uso mejorado o extendido de las claves	Sí	No	Esta extensión indica que uno o más propósitos para los cuales el certificado de clave pública se puede utilizar, además de o en lugar de los usos básicos que se indican en la extensión KeyUsage.
	11.1. Code Signing		1.3.6.1.5.5.7.3.3	Sí		Firma de código ejecutable descargable.
12. Certificate Policies			Política de certificación	Sí	No	
	12.1. Policy Identifier		1.3.6.1.4.1.5734.3.9.4	Sí		Identificador de la política
	12.2. Policy Qualifier Id			Sí		
		12.2.1 CPS Pointer	http://www.cert.fnmt.es/dpcs/	Sí		IA5String String. URL de las condiciones de uso.
13. Subject Alternative Names					No	
	13.1. Denominación del componente		Id Campo / Valor: 1.3.6.1.4.1.5734.1.8 = < Denominación del componente>	Sí		

Campo		Contenido	Obligatoriedad	Criticidad	Especificaciones
14. CRL Distribution Point		Informa acerca de cómo se obtiene la información de la CRL asociada al certificado.	Sí	No	
	14.1. Distribution Point 1	Punto de publicación de la CRL1. ldap://ldapcomp.cert.fnmt.es/CN=CRL<xxx*>, OU=AC%20Componentes%20Informaticos, O=FNMT-RCM,C=ES?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint *xxx: número entero identificador de la CRL (CRL particionadas)	Sí		Ruta del servicio LDAP donde reside la CRL (punto de distribución 1).
	14.2. Distribution Point 2	Punto de publicación de la CRL2. http://www.cert.fnmt.es/crlscomp/CRLnnn.crl	Sí		Ruta donde reside la CRL (punto de distribución 2).
15. Authority Info Access			Sí	No	
	15.1. Access Method 1	Identificador de método de acceso a la información de revocación: 1.3.6.1.5.5.7.48.1 (ocsp)	Sí		
	15.2. Acces Location 1	http://ocspcomp.cert.fnmt.es/ocsp/OcspResponder	Sí		
	15.3. 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		Entidad emisora de los certificados (CA Subordinada) De la rfc 5280: *"the id-ad-caIssuers OID is used when the additional information lists certificates that were issued to the CA that issued the certificate containing this extension. The referenced CA issuers description is intended to aid certificate users in the selection of a certification path that terminates at a point trusted by the certificate user."*
	15.4. Access Location 2	http://www.cert.fnmt.es/certs/ACCOMP.crt	Sí		Ruta para descarga de certificados adicionales para la validación de la cadena de certificación. En este caso la ruta del certificado de la CA subordinada de la raíz de la FNMT-RCM.
16. Basic Contraints		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	Sí	De la rf5280: "*This extension MAY appear as a critical or non-critical extension in end entity certificates.*
	16.1. Subject Type	Valor FALSE (entidad final)			Con este certificado no se pueden emitir otros certificados.

2.2.3. Certificado SSL estándar

Campo		Contenido	Obligatoriedad	Criticidad	Especificaciones
1. Version		2	Sí		Integer:=2 ([RFC5280] describe la versión del certificado. El valor 2 equivale a decir que el certificados es versión 3 (X509v3)
2. Serial Number		Número identificativo único del certificado.	Sí		Integer. SerialNumber = ej: 111222. Establecido automáticamente por la Entidad de Certificación. [RFC5280]. Será un "integer" positivo, no mayor de 20 octetos (1- 2^{159}). El número de serie se asignará de forma aleatoria.
3. Signature Algorithm		Sha256withRsaEncryption	Sí		Identificando el tipo de algoritmo OID: 1.2.840.113549.1.1.11
4. Issuer Distinguish Name		Entidad emisora del certificado (CA Subordinada)	Sí		
	4.1. Country	C=ES	Sí		Se codificará de acuerdo a "ISO 3166-1-alpha-2 code elements". PrintableString, tamaño 2 (rfc5280)
	4.2. Organization	Denominación (nombre "oficial" de la organización) del prestador de servicios de certificación (emisor del certificado). O=FNMT-RCM.	Sí		UTF8 String, tamaño máximo 128 (rfc5280)
	4.3. Organization Unit	OU=AC Componentes Informáticos	Sí		UTF8 String, tamaño máximo 128 (rfc5280).
5. Validity		Variable	Sí		La duración será variable (1 ó 2 años) y se definirá a la hora de solicitar el certificado. El aprobador del mismo, deberá verificar si el valor es correcto.
6. Subject		Identificación/descripción del suscriptor del certificado y del componente	Sí		
	6.1. Country	C=ES	Sí		Se codificará de acuerdo a "ISO 3166-1-alpha-2 code elements". PrintableString, tamaño 2 (rfc5280)
	6.2. LocalityName	Nombre de la localidad del suscriptor	Sí		UTF8String (rfc5280). Por ejemplo: L=Madrid
	6.3. Organization	Denominación del suscriptor	Sí		UTF8String (rfc5280). Por ejemplo: O=Ministerio de Economía
	6.4. Organizational Unit	Departamento o área del suscriptor para el que se emite el certificado.	No		UTF8String (rfc5280). Por ejemplo: OU=Departamento de Informática
	6.5. Serial Number	NIF del suscriptor	Sí		PrintableString (rfc5280). Por

Campo		Contenido	Obligatoriedad	Criticidad	Especificaciones
					ejemplo: SN= Q0000000J
	6.6. OrganizationIdentifier	Identificador de la Organización Según la norma ETSI EN 319 412-1(VATES+NIF de la entidad)	Sí		Por ejemplo: organizationidentifier=VATES-Q0000000J
	6.7. Common Name	Dominio para el que se expide el certificado	Sí		UTF8String (rfc5280). CN=www.fnmt.es
7. Authority Key Identifier		Identificador de la clave pública de la CA de Componentes. Medio para identificar la clave pública correspondiente a la clave privada utilizada por la CA para firmar el certificado de componente.	Sí	No	RFC 5280: hash SHA-1 de 20 bytes calculado sobre el valor BIT STRING del campo subjectPublicKey del emisor del certificado (excluyendo etiqueta, longitud y número de bits no usados). Coincide con el campo Subject Key Identifier de la CA emisora.
8. Subject Public Key Info		Clave pública del componente, codificada según el estándar PKCS#1 de RSA. La longitud de la clave será 2048 bits.	Sí	No	Campo que contiene la clave pública del certificado.
9. Subject Key Identifier		Identificador de la clave pública del componente.	Sí	No	RFC 5280: hash SHA-1 de 20 bytes calculado sobre el valor BIT STRING del campo subjectPublicKey del sujeto (excluyendo etiqueta, longitud y número de bits no usados).
10. Key Usage		Uso permitido de las claves certificadas.	Sí	Sí	Normalizado en norma X509
	10.1. Digital Signature	1			Permite realizar la operación de firma electrónica
	10.2. Content Commitment	0			Se refiere a la cualidad de un tipo de certificado que indica al software en el que se usa que debe permitir que el usuario conozca lo que firma.
	10.3. Key Encipherment	1			Se utiliza para gestión y transporte de claves para establecimiento de sesiones seguras
	10.4. Data Encipherment	0			Se utiliza para cifrar datos que no sean claves criptográficas.
	10.5. Key Agreement	0			Para uso en el proceso de acuerdo de claves
	10.6. Key Certificate Signature	0			Se permite usa para firmar certificados. Se utiliza en los certificados de autoridades de certificación.
	10.7. CRL Signature	0			Se permite para firmar listas de revocación de certificados.
11. Extended Key Usage		Uso mejorado o extendido de las claves	Sí	No	Esta extensión indica que uno o más propósitos para los cuales el certificado de clave pública se puede utilizar, además de o en lugar de los usos básicos que se indican en la

Campo			Contenido	Obligatoriedad	Criticidad	Especificaciones
						extensión KeyUsage.
	11.1. Server Authentication		1.3.6.1.5.5.7.3.1	Sí		Autenticación de servidor
12. Qualified Certificate Statements			Extensiones cualificadas.	Sí	No	ETSI TS 101 862 define la inclusión de ciertas declaraciones para certificados cualificados
	QcEuRetentionPeriod (0.4.0.1862.1.3)		15 años	Sí		Número de años a partir de la caducidad del certificado que se dispone de los datos de registro y otro información relevante. En este caso la Ley obliga: "Conservar registrada por cualquier medio seguro toda la información y documentación relativa a un certificado reconocido y las declaraciones de prácticas de certificación vigentes en cada momento, al menos durante 15 años contados desde el momento de su expedición, de manera que puedan verificarse las firmas efectuadas con el mismo.".
	QcType (0.4.0.1862.1.6)		qct-web (0.4.0.1862.1.6.3)			Certificado de autenticación web
	QcPDS (0.4.0.1862.1.5)		{https://www.cert.fnmt.es/pds/PDS_COMP_es.pdf, es},{https://www.cert.fnmt.es/pds/PDS_COMP_en.pdf, en}	Sí		Lugar donde se encuentra la declaración PDS, así como el idioma del documento.
13. Certificate Policies			Política de certificación	Sí	No	
	13.1. Policy Identifier		1.3.6.1.4.1.5734.3.9.16	Sí		Identificador de la política asociado a la DPC o PC
	13.1.1 Policy Qualifier Id			Sí		
		13.1.1.1 CPS Pointer	http://www.cert.fnmt.es/dpcs/	Sí		IA5String String. URL de las condiciones de uso.
		13.1.1.2 User Notice	"Certificado SSL estándar según reglamento europeo eIDAS. Sujeto a las condiciones de uso expuestas en la DPC de la FNMT-RCM (C/Jorge Juan 106-28009-Madrid-España)"	Sí		UTF8 String. Longitud máxima 200 caracteres.
	13.2. Policy Identifier		OVCP (0.4.0.2042.1.7)	Sí		Política de certificación OV para certificados de sitio web acorde al Reglamento UE 910/2014 itu-t(0) identified-organization(4) etsi(0) other-certificate-policies(2042) policy-identifiers(1) ovcp (7)
14. Subject Alternative Names				Sí	No	
	14.1. DNSName		Id Campo / Valor: NombreDNS = Dominio	Sí		Dominio para el que se emite el certificado
15. CRL Distribution Point			Informa acerca de cómo se obtiene la información de la CRL asociada al certificado.	Sí	No	

Campo		Contenido	Obligatoriedad	Criticidad	Especificaciones
	15.1. Distribution Point 1	Punto de publicación de la CRL1. ldap://ldapcomp.cert.fnmt.es/CN=CRL<xxx*>, OU=AC%20Componentes%20Informaticos, O=FNMT-RCM,C=ES?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint *xxx: número entero identificador de la CRL (CRL particionadas)	Sí		Ruta del servicio LDAP donde reside la CRL (punto de distribución 1).
	15.2. Distribution Point 2	Punto de publicación de la CRL2. http://www.cert.fnmt.es/crlscomp/CRLnnn.crl	Sí		Ruta donde reside la CRL (punto de distribución 2).
16. Authority Info Access			Sí	No	
	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://ocspcomp.cert.fnmt.es/ocsp/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		Entidad emisora de los certificados (CA Subordinada) De la rfc 5280: *"the id-ad-caIssuers OID is used when the additional information lists certificates that were issued to the CA that issued the certificate containing this extension. The referenced CA issuers description is intended to aid certificate users in the selection of a certification path that terminates at a point trusted by the certificate user."*
	16.4. Access Location 2	http://www.cert.fnmt.es/certs/ACCOMP.crt	Sí		Ruta para descarga de certificados adicionales para la validación de la cadena de certificación. En este caso la ruta del certificado de la CA subordinada de la raíz de la FNMT-RCM.
17. Basic Contraints		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	Sí	De la rf5280: "*This extension MAY appear as a critical or non-critical extension in end entity certificates.*
	17.1. Subject Type	Valor FALSE (entidad final)			Con este certificado no se pueden emitir otros certificados.

2.2.4. Certificado SSL wildcard

Campo		Contenido	Obligatoriedad	Criticidad	Especificaciones
1. Version		2	Sí		Integer:=2 ([RFC5280] describe la versión del certificado. El valor 2 equivale a decir que el certificados es versión 3 (X509v3)
2. Serial Number		Número identificativo único del certificado.	Sí		Integer. SerialNumber = ej: 111222. Establecido automáticamente por la Entidad de Certificación. [RFC5280]. Será un "integer" positivo, no mayor de 20 octetos (1- 2^{159}). El número de serie se asignará de forma aleatoria.
3. Signature Algorithm		Sha256withRsaEncryption	Sí		Identificando el tipo de algoritmo OID: 1.2.840.113549.1.1.11
4. Issuer Distinguish Name		Entidad emisora del certificado (CA Subordinada)	Sí		
	4.1. Country	C=ES	Sí		Se codificará de acuerdo a "ISO 3166-1-alpha-2 code elements". PrintableString, tamaño 2 (rfc5280)
	4.2. Organization	Denominación (nombre "oficial" de la organización) del prestador de servicios de certificación (emisor del certificado). O=FNMT-RCM.	Sí		UTF8 String, tamaño máximo 128 (rfc5280)
	4.3. Organization Unit	OU=AC Componentes Informáticos	Sí		UTF8 String, tamaño máximo 128 (rfc5280).
5. Validity		Variable	Sí		La duración será variable (1 ó 2 años) y se definirá a la hora de solicitar el certificado. El aprobador del mismo, deberá verificar si el valor es correcto.
6. Subject		Identificación/descripción del suscriptor del certificado y del componente	Sí		
	6.1. Country	C=ES	Sí		Se codificará de acuerdo a "ISO 3166-1-alpha-2 code elements". PrintableString, tamaño 2 (rfc5280)
	6.2. LocalityName	Nombre de la localidad del suscriptor	Sí		UTF8String (rfc5280). Por ejemplo: L=Madrid
	6.3. Organization	Denominación del suscriptor	Sí		UTF8String (rfc5280). Por ejemplo: O=Ministerio de Economía
	6.4. Organizational Unit	Departamento o área del suscriptor para el que se emite el certificado.	No		UTF8String (rfc5280). Por ejemplo: OU=Departamento de Informática
	6.5. Serial Number	NIF del suscriptor	Sí		PrintableString (rfc5280). Por ejemplo:

Campo		Contenido	Obligatoriedad	Criticidad	Especificaciones
					SN= Q0000000J
	6.6. OrganizationIdentifier	Identificador de la Organización Según la norma ETSI EN 319 412-1(VATES+NIF de la entidad)	Sí		Por ejemplo: organizationidentifier=VATES-Q0000000J
	6.7. Common Name	Dominio wildcard para el que se expide el certificado.	Sí		UTF8String (rfc5280). Por ejemplo: CN=*.cert.fnmt.es
7. Authority Key Identifier		Identificador de la clave pública de la CA de Componentes. Medio para identificar la clave pública correspondiente a la clave privada utilizada por la CA para firmar el certificado de componente.	Sí	No	RFC 5280: hash SHA-1 de 20 bytes calculado sobre el valor BIT STRING del campo subjectPublicKey del emisor del certificado (excluyendo etiqueta, longitud y número de bits no usados). Coincide con el campo Subject Key Identifier de la CA emisora.
8. Subject Public Key Info		Clave pública del componente, codificada según el estándar PKCS#1 de RSA. La longitud de la clave será 2048 bits.	Sí	No	Campo que contiene la clave pública del certificado.
9. Subject Key Identifier		Identificador de la clave pública del componente.	Sí	No	RFC 5280: hash SHA-1 de 20 bytes calculado sobre el valor BIT STRING del campo subjectPublicKey del sujeto (excluyendo etiqueta, longitud y número de bits no usados).
10. Key Usage		Uso permitido de las claves certificadas.	Sí	Sí	Normalizado en norma X509
	10.1. Digital Signature	1			Permite realizar la operación de firma electrónica
	10.2. Content Commitment	0			Se refiere a la cualidad de un tipo de certificado que indica al software en el que se usa que debe permitir que el usuario conozca lo que firma.
	10.3. Key Encipherment	1			Se utiliza para gestión y transporte de claves para establecimiento de sesiones seguras
	10.4. Data Encipherment	0			Se utiliza para cifrar datos que no sean claves criptográficas.
	10.5. Key Agreement	0			Para uso en el proceso de acuerdo de claves
	10.6. Key Certificate Signature	0			Se permite usa para firmar certificados. Se utiliza en los certificados de autoridades de certificación.
	10.7. CRL Signature	0			Se permite para firmar listas de revocación de certificados.
11. Extended Key Usage		Uso mejorado o extendido de las claves	Sí	No	Esta extensión indica que uno o más propósitos para los cuales el certificado de clave pública se puede utilizar, además de o en lugar de los usos básicos que se indican en la extensión KeyUsage.

Campo			Contenido	Obligatoriedad	Criticidad	Especificaciones
	11.1. Server Authentication		1.3.6.1.5.5.7.3.1	Sí		Autenticación de servidor
12. Qualified Certificate Statements			Extensiones cualificadas.	Sí	No	ETSI TS 101 862 define la inclusión de ciertas declaraciones para certificados cualificados
	12.1. QcEuRetentionPeriod (0.4.0.1862.1.3)		15 años	Sí		Número de años a partir de la caducidad del certificado que se dispone de los datos de registro y otro información relevante. En este caso la Ley obliga: "Conservar registrada por cualquier medio seguro toda la información y documentación relativa a un certificado reconocido y las declaraciones de prácticas de certificación vigentes en cada momento, al menos durante 15 años contados desde el momento de su expedición, de manera que puedan verificarse las firmas efectuadas con el mismo.".
	12.2. QcType (0.4.0.1862.1.6)		qct-web (0.4.0.1862.1.6.3)			Certificado de autenticación web
	12.3. QcPDS (0.4.0.1862.1.5)		{https://www.cert.fnmt.es/pds/PDS_COMP_es.pdf, es},{https://www.cert.fnmt.es/pds/PDS_COMP_en.pdf, en}	Sí		Lugar donde se encuentra la declaración PDS, así como el idioma del documento.
13. Certificate Policies			Política de certificación	Sí	No	
	13.1. Policy Identifier		1.3.6.1.4.1.5734.3.9.17	Sí		Identificador de la política asociado a la DPC o PC
	13.1.1 Policy Qualifier Id			Sí		
		13.1.1.1 CPS Pointer	http://www.cert.fnmt.es/dpcs/	Sí		IA5String String. URL de las condiciones de uso.
		13.1.1.2 User Notice	"Certificado SSL wildcard según reglamento europeo eIDAS. Sujeto a las condiciones de uso expuestas en la DPC de la FNMT-RCM (C/Jorge Juan 106-28009-Madrid-España)"	Sí		UTF8 String. Longitud máxima 200 caracteres.
	13.2. Policy Identifier		OVCP (0.4.0.2042.1.7)	Sí		Política de certificación OV para certificados de sitio web acorde al Reglamento UE 910/2014 itu-t(0) identified-organization(4) etsi(0) other-certificate-policies(2042) policy-identifiers(1) ovcp (7)
14. Subject Alternative Names				Sí	No	
	14.1. DNSName		Id Campo / Valor: NombreDNS = Dominio wildcard	Sí		Dominio para el que se emite el certificado
15. CRL Distribution Point			Informa acerca de cómo se obtiene la información de la CRL asociada al certificado.	Sí	No	
	15.1. Distribution Point 1		Punto de publicación de la CRL1.	Sí		Ruta del servicio LDAP donde reside

Campo		Contenido	Obligatoriedad	Criticidad	Especificaciones
		ldap://ldapcomp.cert.fnmt.es/CN=CRL<xxx*>, OU=AC%20Componentes%20Informaticos, O=FNMT-RCM,C=ES?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint *xxx: número entero identificador de la CRL (CRL particionadas)			la CRL (punto de distribución 1).
	15.2. Distribution Point 2	Punto de publicación de la CRL2. http://www.cert.fnmt.es/crlscomp/CRLnnn.crl	Sí		Ruta donde reside la CRL (punto de distribución 2).
16. Authority Info Access			Sí	No	
	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://ocspcomp.cert.fnmt.es/ocsp/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		Entidad emisora de los certificados (CA Subordinada) De la rfc 5280: *"the id-ad-caIssuers OID is used when the additional information lists certificates that were issued to the CA that issued the certificate containing this extension. The referenced CA issuers description is intended to aid certificate users in the selection of a certification path that terminates at a point trusted by the certificate user."*
	16.4. Access Location 2	http://www.cert.fnmt.es/certs/ACCOMP.crt	Sí		Ruta para descarga de certificados adicionales para la validación de la cadena de certificación. En este caso la ruta del certificado de la CA subordinada de la raíz de la FNMT-RCM.
17. Basic Contraints		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	Sí	De la rf5280: *"This extension MAY appear as a critical or non-critical extension in end entity certificates.*
	17.1. Subject Type	Valor FALSE (entidad final)			Con este certificado no se pueden emitir otros certificados.

2.2.5. Certificado SSL multidominio (SAN / UCC)

Campo		Contenido	Obligatoriedad	Criticidad	Especificaciones
1. Version		2	Sí		Integer:=2 ([RFC5280] describe la versión del certificado. El valor 2 equivale a decir que el certificados es versión 3 (X509v3)
2. Serial Number		Número identificativo único del certificado.	Sí		Integer. SerialNumber = ej: 111222. Establecido automáticamente por la Entidad de Certificación. [RFC5280]. Será un "integer" positivo, no mayor de 20 octetos (1- 2^{159}). El número de serie se asignará de forma aleatoria.
3. Signature Algorithm		Sha256withRsaEncryption	Sí		Identificando el tipo de algoritmo OID: 1.2.840.113549.1.1.11
4. Issuer Distinguish Name		Entidad emisora del certificado (CA Subordinada)	Sí		
	4.1. Country	C=ES	Sí		Se codificará de acuerdo a "ISO 3166-1-alpha-2 code elements". PrintableString, tamaño 2 (rfc5280)
	4.2. Organization	Denominación (nombre "oficial" de la organización) del prestador de servicios de certificación (emisor del certificado). O=FNMT-RCM.	Sí		UTF8 String, tamaño máximo 128 (rfc5280)
	4.3. Organization Unit	OU=AC Componentes Informáticos	Sí		UTF8 String, tamaño máximo 128 (rfc5280).
5. Validity		Variable	Sí		La duración será variable (1 ó 2 años) y se definirá a la hora de solicitar el certificado. El aprobador del mismo, deberá verificar si el valor es correcto.
6. Subject		Identificación/descripción del suscriptor del certificado y del componente	Sí		
	6.1. Country	C=ES	Sí		Se codificará de acuerdo a "ISO 3166-1-alpha-2 code elements". PrintableString, tamaño 2 (rfc5280)
	6.2. LocalityName	Nombre de la localidad del suscriptor	Sí		UTF8String (rfc5280). Por ejemplo: L=Madrid
	6.3. Organization	Denominación del suscriptor	Sí		UTF8String (rfc5280). Por ejemplo: O=Ministerio de Economía
	6.4. Organizational Unit	Departamento o área del suscriptor para el que se emite el certificado.	No		UTF8String (rfc5280). Por ejemplo: OU=Departamento de Informática
	6.5. Serial Number	NIF del suscriptor	Sí		PrintableString (rfc5280). Por ejemplo:

Campo		Contenido	Obligatoriedad	Criticidad	Especificaciones
					SN= Q0000000J
	6.6. OrganizationIdentifier	Identificador de la Organización Según la norma ETSI EN 319 412-1(VATES+NIF de la entidad)	Sí		Por ejemplo: organizationidentifier=VATES-Q0000000J
	6.7. Common Name	Dominio principal para el que se expide el certificado	Sí		UTF8String (rfc5280). CN=www.fnmt.es
7. Authority Key Identifier		Identificador de la clave pública de la CA de Componentes. Medio para identificar la clave pública correspondiente a la clave privada utilizada por la CA para firmar el certificado de componente.	Sí	No	RFC 5280: hash SHA-1 de 20 bytes calculado sobre el valor BIT STRING del campo subjectPublicKey del emisor del certificado (excluyendo etiqueta, longitud y número de bits no usados). Coincide con el campo Subject Key Identifier de la CA emisora.
8. Subject Public Key Info		Clave pública del componente, codificada según el estándar PKCS#1 de RSA. La longitud de la clave será 2048 bits.	Sí	No	Campo que contiene la clave pública del certificado.
9. Subject Key Identifier		Identificador de la clave pública del componente.	Sí	No	RFC 5280: hash SHA-1 de 20 bytes calculado sobre el valor BIT STRING del campo subjectPublicKey del sujeto (excluyendo etiqueta, longitud y número de bits no usados).
10. Key Usage		Uso permitido de las claves certificadas.	No	Sí	Normalizado en norma X509
	10.1. Digital Signature	1	Sí		Permite realizar la operación de firma electrónica
	10.2. Content Commitment	0	Sí		Se refiere a la cualidad de un tipo de certificado que indica al software en el que se usa que debe permitir que el usuario conozca lo que firma.
	10.3. Key Encipherment	1	Sí		Se utiliza para gestión y transporte de claves para establecimiento de sesiones seguras
	10.4. Data Encipherment	0	Sí		Se utiliza para cifrar datos que no sean claves criptográficas.
	10.5. Key Agreement	0	Sí		Para uso en el proceso de acuerdo de claves
	10.6. Key Certificate Signature	0	Sí		Se permite usa para firmar certificados. Se utiliza en los certificados de autoridades de certificación.
	10.7. CRL Signature	0	Sí		Se permite para firmar listas de revocación de certificados.
11. Extended Key Usage		Uso mejorado o extendido de las claves	Sí	No	Esta extensión indica que uno o más propósitos para los cuales el certificado de clave pública se puede utilizar, además de o en lugar de los usos básicos que se indican en la extensión KeyUsage.

Campo			Contenido	Obligatoriedad	Criticidad	Especificaciones
	11.1. Server Authentication		1.3.6.1.5.5.7.3.1	Sí		Autenticación de servidor
12. Qualified Certificate Statements			Extensiones cualificadas.	Sí	No	ETSI TS 101 862 define la inclusión de ciertas declaraciones para certificados cualificados
	12.1. QcEuRetentionPeriod (0.4.0.1862.1.3)		15 años	Sí		Número de años a partir de la caducidad del certificado que se dispone de los datos de registro y otro información relevante. En este caso la Ley obliga: "Conservar registrada por cualquier medio seguro toda la información y documentación relativa a un certificado reconocido y las declaraciones de prácticas de certificación vigentes en cada momento, al menos durante 15 años contados desde el momento de su expedición, de manera que puedan verificarse las firmas efectuadas con el mismo.".
	12.2. QcType (0.4.0.1862.1.6)		qct-web (0.4.0.1862.1.6.3)	Sí		Certificado de autenticación web
	12.3. QcPDS (0.4.0.1862.1.5)		{https://www.cert.fnmt.es/pds/PDS_COMP_es.pdf, es},{https://www.cert.fnmt.es/pds/PDS_COMP_en.pdf, en}	Sí		Lugar donde se encuentra la declaración PDS, así como el idioma del documento.
13. Certificate Policies			Política de certificación	Sí	No	
	13.1. Policy Identifier		1.3.6.1.4.1.5734.3.9.18	Sí		Identificador de la política asociado a la DPC o PC
	13.1.1 Policy Qualifier Id			Sí		
		13.1.1.1 CPS Pointer	http://www.cert.fnmt.es/dpcs/	Sí		IA5String String. URL de las condiciones de uso.
		13.1.1.2 UserNotice	"Certificado SSL multidominio según reglamento europeo eIDAS. Sujeto a las condiciones de uso expuestas en la DPC de la FNMT-RCM (C/Jorge Juan 106-28009-Madrid-España)"	Sí		UTF8 String. Longitud máxima 200 caracteres.
	13.2. Policy Identifier		OVCP (0.4.0.2042.1.7)	Sí		Política de certificación OV para certificados de sitio web acorde al Reglamento UE 910/2014 itu-t(0) identified-organization(4) etsi(0) other-certificate-policies(2042) policy-identifiers(1) ovcp (7)
14. Subject Alternative Names				Sí	No	
	14.1. DNSName		Id Campo / Valor: NombreDNS = Dominio	Sí		Dominio para el que se emite el certificado
	14.2. DNSName		Id Campo / Valor: NombreDNS = Dominio_2	Sí		Dominio para el que se emite el certificado

Campo		Contenido	Obligatoriedad	Criticidad	Especificaciones
	14.3. DNSName	Id Campo / Valor: NombreDNS = Dominio_*n*	No		Dominio para el que se emite el certificado n <= 12
15. CRL Distribution Point		Informa acerca de cómo se obtiene la información de la CRL asociada al certificado.	Sí	No	
	15.1. Distribution Point 1	Punto de publicación de la CRL1. ldap://ldapcomp.cert.fnmt.es/CN=CRL<xxx*>, OU=AC%20Componentes%20Informaticos, O=FNMT-RCM,C=ES?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint *xxx: número entero identificador de la CRL (CRL particionadas)	Sí		Ruta del servicio LDAP donde reside la CRL (punto de distribución 1).
	15.2. Distribution Point 2	Punto de publicación de la CRL2. http://www.cert.fnmt.es/crlscomp/CRLnnn.crl	Sí		Ruta donde reside la CRL (punto de distribución 2).
16. Authority Info Access			Sí	No	
	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://ocspcomp.cert.fnmt.es/ocsp/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		Entidad emisora de los certificados (CA Subordinada) De la rfc 5280: *"the id-ad-caIssuers OID is used when the additional information lists certificates that were issued to the CA that issued the certificate containing this extension. The referenced CA issuers description is intended to aid certificate users in the selection of a certification path that terminates at a point trusted by the certificate user."*
	16.4. Access Location 2	http://www.cert.fnmt.es/certs/ACCOMP.crt	Sí		Ruta para descarga de certificados adicionales para la validación de la cadena de certificación. En este caso la ruta del certificado de la CA subordinada de la raíz de la FNMT-RCM.
17. Basic Contraints		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	Sí	De la rf5280: "*This extension MAY appear as a critical or non-critical extension in end entity certificates.*
	17.1. Subject Type	Valor FALSE (entidad final)			Con este certificado no se pueden emitir otros certificados.