DIRECCIÓN DE SISTEMAS DE INFORMACIÓN
DEPARTAMENTO CERES

DOCUMENTO DE PERFILES DE LA AUTORIDAD DE CERTIFICACIÓN
AC COMPONENTES INFORMÁTICOS

Documento clasificado como: *Público*

Contenido

1. OBJETO

El objeto de este documento es la definición de los perfiles de los certificados emitidos por la autoridad de certificación *AC Componentes Informáticos* de la FNMT-RCM. Así mismo, se incluye la definición del perfil de la propia autoridad.

2. PERFILES

2.1. CA SUBORDINADA COMPONENTES

Campo		Contenido	Obligatoriedad
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 prestador de servicios de certificación (emisor del certificado). O=FNMT-RCM	Sí
	4.3. Organization Unit	OU=AC RAIZ FNMT-RCM	Sí
5. Validity		15 años	Sí
6. Subject		Entidad emisora del certificado (CA Subordinada)	Sí
	6.1. Country	C=ES	Sí
	6.2. Organization	Denominación (nombre "oficial" de la organización) del prestador de servicios de certificación (emisor del certificado). O=FNMT-RCM.	Sí
	6.3. Organization Unit	OU=AC Componentes Informáticos	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 de Componentes, codificada según el estándar PKCS#1 de RSA. La longitud de la clave será 2048 bits.	Sí

Campo			Contenido	Obligatoriedad
9. Subject Key Identifier			Identificador de la clave pública de la CA de Componentes.	Sí
10. Key Usage			Uso permitido de las claves del certificado.	Sí
	10.1. Digital Signature		0	Sí
	10.2. Content Commitment		0	Sí
	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			
		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. Basic Constraints				
	13.1. Subject Type		CA	
	13.2. Path Length		0	
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)	

Campo		Contenido	Obligatoriedad
	14.2. Acces Location 1	http://ocspfnmtrcmca.cert.fnmt.es/ocspfnmtrcmca/OcspResponder	
	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)	
	Access Location 2	http://www.cert.fnmt.es/certs/ACRAIZFNMTRCM.crt	

2.2. CERTIFICADOS DE COMPONENTES

2.2.1. Certificado de componente de sello de entidad

Campo		Contenido	Obligatoriedad
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 certificación (emisor del certificado). O=FNMT-RCM.	Sí
	4.3. Organization Unit	OU=AC Componentes Informáticos	Sí
5. Validity		Variable	Sí
6. Subject		Identificación/descripción del suscriptor del certificado y del componente	Sí
	6.1. Country	C=ES	Sí
	6.2. LocalityName	Nombre de la localidad del suscriptor	Sí
	6.3. Organization	Denominación del suscriptor	Sí

Campo		Contenido	Obligatoriedad
	6.4. Organizational Unit	Departamento o área del suscriptor para el que se emite el certificado.	No
	6.5. Serial Number	NIF del suscriptor	Sí
	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
	6.7. Common Name	Denominación del componente	Sí
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
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
9. Subject Key Identifier		Identificador de la clave pública del componente.	Sí
10. Key Usage		Uso permitido de las claves certificadas.	
	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	No
	11.2. Client Authentication	1.3.6.1.5.5.7.3.2	No
12. Qualified Certificate Statements		Extensiones cualificadas.	Sí
	12.1. QcCompliance (0.4.0.1862.1.1)	Certificado cualificado	Sí
	12.2. QcEuRetentionPeriod (0.4.0.1862.1.3)	15 años	Sí
	12.3. QcType (0.4.0.1862.1.6)	Id-etsi-qct-eseal (0.4.0.1862.1.6.2)	Sí

Campo			Contenido	Obligatoriedad
	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
13. Certificate Policies			Política de certificación	Sí
	13.1. Policy Identifier		1.3.6.1.4.1.5734.3.9.19	Sí
	13.1.1 Policy Qualifier Id			Sí
		13.1.1.1 CPS Pointer	http://www.cert.fnmt.es/dpcs/	Sí
		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 FNMT-RCM con NIF: Q2826004-J (C/Jorge Juan 106-28009-Madrid-España)"	Sí
	13.2. Policy Identifier		QCP-l (0.4.0.194112.1.1)	Sí
14. Subject Alternative Names				Sí
	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
	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
	15.2. Distribution Point 2		Punto de publicación de la CRL2. http://www.cert.fnmt.es/crlscomp/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://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
	16.4. Access Location 2		http://www.cert.fnmt.es/certs/ACCOMP.crt	Sí

Campo		Contenido	Obligatoriedad
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
	17.1. Subject Type	Valor FALSE (entidad final)	

2.2.2. Certificado de componente de firma de código

Campo		Contenido	Obligatoriedad
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 certificación (emisor del certificado). O=FNMT-RCM.	Sí
	4.3. Organization Unit	OU=AC Componentes Informáticos	Sí
5. Validity		Variable	Sí
6. Subject		Identificación/descripción del suscriptor del certificado y del componente	Sí
	6.1. Country	C=ES	Sí
	6.2. LocalityName	Nombre de la localidad del suscriptor	Sí
	6.3. Organization	Denominación del suscriptor	Sí
	6.4. Organizational Unit	Departamento o área del suscriptor para el que se emite el certificado.	No
	6.5. Serial Number	NIF del suscriptor	Sí
	6.6. Common Name	Denominación del componente	Sí

Campo			Contenido	Obligatoriedad
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
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
9. Subject Key Identifier			Identificador de la clave pública del componente.	Sí
10. Key Usage			Uso permitido de las claves certificadas.	Sí
	10.1. Digital Signature		1	
	10.2. Content Commitment		0	
	10.3. Key Encipherment		0	
	10.4. Data Encipherment		0	
	10.5. Key Agreement		0	
	10.6. Key Certificate Signature		0	
	10.7. CRL Signature		0	
11. Extended Key Usage			Uso mejorado o extendido de las claves	Sí
	11.1. Code Signing		1.3.6.1.5.5.7.3.3	Sí
12. Certificate Policies			Política de certificación	Sí
	12.1. Policy Identifier		1.3.6.1.4.1.5734.3.9.4	Sí
	12.2. Policy Qualifier Id			Sí
		12.2.1 CPS Pointer	http://www.cert.fnmt.es/dpcs/	Sí
13. Subject Alternative Names				
	13.1. Denominación del componente		Id Campo / Valor: 1.3.6.1.4.1.5734.1.8 = < Denominación del componente>	Sí
14. CRL Distribution Point			Informa acerca de cómo se obtiene la información de la CRL asociada al certificado.	Sí
	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
	14.2. Distribution Point 2		Punto de publicación de la CRL2.	Sí

Campo		Contenido	Obligatoriedad
		http://www.cert.fnmt.es/crlscomp/CRLnnn.crl	
15. Authority Info Access			Sí
	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
	15.4. Access Location 2	http://www.cert.fnmt.es/certs/ACCOMP.crt	Sí
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
	16.1. Subject Type	Valor FALSE (entidad final)	

2.2.3. Certificado de autenticación de sitio web estándar

Campo		Contenido	Obligatoriedad
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 certificación (emisor del certificado). O=FNMT-RCM.	Sí
	4.3. Organization Unit	OU=AC Componentes Informáticos	Sí
5. Validity		Variable	Sí
6. Subject		Identificación/descripción del suscriptor del certificado y del componente	Sí

Campo		Contenido	Obligatoriedad
	6.1. Country	C=ES	Sí
	6.2. LocalityName	Nombre de la localidad del suscriptor	Sí
	6.3. Organization	Denominación del suscriptor	Sí
	6.4. Organizational Unit	Departamento o área del suscriptor para el que se emite el certificado.	No
	6.5. Serial Number	NIF del suscriptor	Sí
	6.6. OrganizationIdentifier	Identificador de la Organización Según la norma ETSI EN 319 412-1(VATES+NIF de la entidad)	Sí
	6.7. Common Name	Dominio para el que se expide el certificado	Sí
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
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
9. Subject Key Identifier		Identificador de la clave pública del componente.	Sí
10. Key Usage		Uso permitido de las claves certificadas.	Sí
	10.1. Digital Signature	1	
	10.2. Content Commitment	0	
	10.3. Key Encipherment	1	
	10.4. Data Encipherment	0	
	10.5. Key Agreement	0	
	10.6. Key Certificate Signature	0	
	10.7. CRL Signature	0	
11. Extended Key Usage		Uso mejorado o extendido de las claves	Sí
	11.1. Server Authentication	1.3.6.1.5.5.7.3.1	Sí
12. Qualified Certificate Statements		Extensiones cualificadas.	Sí

Campo			Contenido	Obligatoriedad
	QcEuRetentionPeriod (0.4.0.1862.1.3)		15 años	Sí
	QcType (0.4.0.1862.1.6)		qct-web (0.4.0.1862.1.6.3)	
	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
13. Certificate Policies			Política de certificación	Sí
	13.1. Policy Identifier		1.3.6.1.4.1.5734.3.9.16	Sí
	13.1.1 Policy Qualifier Id			Sí
		13.1.1.1 CPS Pointer	http://www.cert.fnmt.es/dpcs/	Sí
		13.1.1.2 User Notice	"Certificado estándar de autenticación de sitio web según reglamento europeo eIDAS. Sujeto a condiciones de uso según DPC de FNMT-RCM, NIF: Q2826004-J (C/Jorge Juan 106-28009-Madrid-España)"	Sí
	13.2. Policy Identifier		OVCP (0.4.0.2042.1.7)	Sí
14. Subject Alternative Names				Sí
	14.1. DNSName		Id Campo / Valor: NombreDNS = Dominio	Sí
15. CRL Distribution Point			Informa acerca de cómo se obtiene la información de la CRL asociada al certificado.	Sí
	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
	15.2. Distribution Point 2		Punto de publicación de la CRL2. http://www.cert.fnmt.es/crlscomp/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://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
	16.4. Access Location 2		http://www.cert.fnmt.es/certs/ACCOMP.crt	Sí

Campo		Contenido	Obligatoriedad
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
	17.1. Subject Type	Valor FALSE (entidad final)	

2.2.4. Certificado de autenticación de sitio web wildcard

Campo		Contenido	Obligatoriedad
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 certificación (emisor del certificado). O=FNMT-RCM.	Sí
	4.3. Organization Unit	OU=AC Componentes Informáticos	Sí
5. Validity		Variable	Sí
6. Subject		Identificación/descripción del suscriptor del certificado y del componente	Sí
	6.1. Country	C=ES	Sí
	6.2. LocalityName	Nombre de la localidad del suscriptor	Sí
	6.3. Organization	Denominación del suscriptor	Sí
	6.4. Organizational Unit	Departamento o área del suscriptor para el que se emite el certificado.	No
	6.5. Serial Number	NIF del suscriptor	Sí
	6.6. OrganizationIdentifier	Identificador de la Organización Según la norma ETSI EN 319 412-1(VATES+NIF de la entidad)	Sí
	6.7. Common Name	Dominio wildcard para el que se expide el certificado.	Sí

Campo			Contenido	Obligatoriedad
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
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
9. Subject Key Identifier			Identificador de la clave pública del componente.	Sí
10. Key Usage			Uso permitido de las claves certificadas.	Sí
	10.1. Digital Signature		1	
	10.2. Content Commitment		0	
	10.3. Key Encipherment		1	
	10.4. Data Encipherment		0	
	10.5. Key Agreement		0	
	10.6. Key Certificate Signature		0	
	10.7. CRL Signature		0	
11. Extended Key Usage			Uso mejorado o extendido de las claves	Sí
	11.1. Server Authentication		1.3.6.1.5.5.7.3.1	Sí
12. Qualified Certificate Statements			Extensiones cualificadas.	Sí
	12.1. QcEuRetentionPeriod (0.4.0.1862.1.3)		15 años	Sí
	12.2. QcType (0.4.0.1862.1.6)		qct-web (0.4.0.1862.1.6.3)	í
	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
13. Certificate Policies			Política de certificación	Sí
	13.1. Policy Identifier		1.3.6.1.4.1.5734.3.9.17	Sí
	13.1.1 Policy Qualifier Id			Sí
		13.1.1.1 CPS Pointer	http://www.cert.fnmt.es/dpcs/	Sí

Campo			Contenido	Obligatoriedad
		13.1.1.2 User Notice	"Certificado wildcard de autenticación de sitio web según reglamento europeo eIDAS. Sujeto a condiciones de uso según DPC de FNMT-RCM, NIF: Q2826004-J (C/Jorge Juan 106-28009-Madrid-España)"	Sí
	13.2. Policy Identifier		OVCP (0.4.0.2042.1.7)	Sí
14. Subject Alternative Names				Sí
	14.1. DNSName		Id Campo / Valor: NombreDNS = Dominio wildcard	Sí
15. CRL Distribution Point			Informa acerca de cómo se obtiene la información de la CRL asociada al certificado.	Sí
	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
	15.2. Distribution Point 2		Punto de publicación de la CRL2. http://www.cert.fnmt.es/crlscomp/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://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
	16.4. Access Location 2		http://www.cert.fnmt.es/certs/ACCOMP.crt	Sí
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
	17.1. Subject Type		Valor FALSE (entidad final)	

2.2.5. Certificado de autenticación de sitio web multidominio (SAN / UCC)

Campo	Contenido	Obligatoriedad
1. Version	2	Sí

Campo		Contenido	Obligatoriedad
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 certificación (emisor del certificado). O=FNMT-RCM.	Sí
	4.3. Organization Unit	OU=AC Componentes Informáticos	Sí
5. Validity		Variable	Sí
6. Subject		Identificación/descripción del suscriptor del certificado y del componente	Sí
	6.1. Country	C=ES	Sí
	6.2. LocalityName	Nombre de la localidad del suscriptor	Sí
	6.3. Organization	Denominación del suscriptor	Sí
	6.4. Organizational Unit	Departamento o área del suscriptor para el que se emite el certificado.	No
	6.5. Serial Number	NIF del suscriptor	Sí
	6.6. OrganizationIdentifier	Identificador de la Organización Según la norma ETSI EN 319 412-1(VATES+NIF de la entidad)	Sí
	6.7. Common Name	Dominio principal para el que se expide el certificado	Sí
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
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
9. Subject Key Identifier		Identificador de la clave pública del componente.	Sí
10. Key Usage		Uso permitido de las claves certificadas.	No
	10.1. Digital Signature	1	Sí
	10.2. Content Commitment	0	Sí

Campo			Contenido	Obligatoriedad
	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. Server Authentication		1.3.6.1.5.5.7.3.1	Sí
12. Qualified Certificate Statements			Extensiones cualificadas.	Sí
	12.1. QcEuRetentionPeriod (0.4.0.1862.1.3)		15 años	Sí
	12.2. QcType (0.4.0.1862.1.6)		qct-web (0.4.0.1862.1.6.3)	Sí
	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
13. Certificate Policies			Política de certificación	Sí
	13.1. Policy Identifier		1.3.6.1.4.1.5734.3.9.18	Sí
	13.1.1 Policy Qualifier Id			Sí
		13.1.1.1 CPS Pointer	http://www.cert.fnmt.es/dpcs/	Sí
		13.1.1.2 UserNotice	"Certificado multidominio de autenticación de sitio web según reglamento europeo eIDAS. Sujeto a condiciones de uso según DPC de FNMT-RCM, NIF: Q2826004-J (C/Jorge Juan 106-28009-Madrid-España)"	Sí
	13.2. Policy Identifier		OVCP (0.4.0.2042.1.7)	Sí
14. Subject Alternative Names				Sí
	14.1. DNSName		Id Campo / Valor: NombreDNS = Dominio	Sí
	14.2. DNSName		Id Campo / Valor: NombreDNS = Dominio_*2*	Sí
	14.3. DNSName		Id Campo / Valor: NombreDNS = Dominio_*n*	No
15. CRL Distribution Point			Informa acerca de cómo se obtiene la información de la CRL asociada al certificado.	Sí

Campo		Contenido	Obligatoriedad
	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
	15.2. Distribution Point 2	Punto de publicación de la CRL2. http://www.cert.fnmt.es/crlscomp/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://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
	16.4. Access Location 2	http://www.cert.fnmt.es/certs/ACCOMP.crt	Sí
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
	17.1. Subject Type	Valor FALSE (entidad final)	