DIRECCIÓN DE SERVICIOS DIGITALES E INNOVACIÓN
DEPARTAMENTO CERES

DOCUMENTO DE PERFILES DE LA AC SERVIDORES SEGUROS

Referencia:

Documento clasificado como: *Público*

Contenido

1. OBJETO

El objeto de este documento es la definición de los perfiles relativos a la infraestructura de certificados de autenticación de sitios web OV (AC Servidores Seguros Tipo 2).

Se incluyen los perfiles de los certificados AC Raíz, AC Subordinada y de los certificados de entidad final: Certificado OV, Certificado SAN OV y Certificado Wildcard OV.

2. PERFILES

2.1. AC RAIZ FNMT-RCM SERVIDORES SEGUROS

Campo		Contenido	Ext. Critica	Especificaciones
1. Version		2		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.		Establecido automáticamente por la Entidad de Certificación. [RFC5280]. Será un "integer" positivo, no mayor 20 octetos (1-2^{159}). El número de serie se asignará de forma aleatoria.
3. Signature Algorithm		ecdsa-with-SHA384 Claves: ECC P-384 bits		OID: 1.2.840.10045.4.3.3
4. Issuer Distinguish Name		Entidad emisora del certificado (CA Raíz)		
	4.1. Country	C=ES		Se codificará de acuerdo a "ISO 3166-1-alpha-2 code elements". PrintableString, tamaño 2 (rfc5280)
	4.2 Organization	O=FNMT-RCM		UTF8 String
	4.3 Organization Unit	OU=Ceres		UTF8 String (rfc5280)
	4.4 OrganizationIddentifier	VATES- Q2826004J		UTF8 String
	4.5 CommonName	cn=AC RAIZ FNMT-RCM SERVIDORES SEGUROS		UTF8 String (rfc5280)
5. Validity		25 años		UTCTime (rfc5280)
6. Subject				
	6.1. Country	C=ES		Se codificará de acuerdo a "ISO 3166-1-alpha-2 code elements". PrintableString, tamaño 2 (rfc5280)
	6.2. Organization	O=FNMT-RCM		UTF8 String
	6.3. Organization Unit	OU=Ceres		UTF8 String (rfc5280)
	6.4. OrganizationIddentifier	VATES- Q2826004J		UTF8 String

Campo		Contenido	Ext. Critica	Especificaciones
	6.5. CommonName	cn=AC RAIZ FNMT-RCM SERVIDORES SEGUROS		UTF8 String (rfc5280)
7. Subject Public Key Info		ECC P-384 bits		Campo para transportar la clave pública y para identificar el algoritmo asociado.
8. Subject Key Identifier		Identificador de la clave pública de la CA. Medio para identificar certificados que contienen una clave pública particular y facilita la construcción de rutas de certificación.		RFC 5280: hash SHA-1 de 20 bytes calculado sobre el valor BIT STRING del campo subjectPublicKey (excluyendo etiqueta, longitud y número de bits no usados).
9. Key Usage		Uso permitido de las claves certificadas.	Sí	Normalizado en norma X509 y RFC 5280
	9.1. Digital Signature	0		Ver X509 y RFC 5280
	9.2. Content Commitment	0		Ver X509 y RFC 5280
	9.3. Key Encipherment	0		Ver X509 y RFC 5280
	9.4. Data Encipherment	0		Ver X509 y RFC 5280
	9.5. Key Agreement	0		Ver X509 y RFC 5280
	9.6. Key Certificate Signature	1		Ver X509 y RFC 5280
	9.7. CRL Signature	1		Ver X509 y RFC 5280
10. Basic Constraints			Sí	
	10.1. cA	Valor TRUE (CA)		De la rfc 5280: "The cA boolean indicates whether the certified public key may be used to verify certificate signatures."
	10.2. pathLenConstraint	Ninguna		No existe restricción de longitud de ruta a nivel de CA Raíz

2.2. AC SUBORDINADA SERVIDORES SEGUROS TIPO2 (OV)

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	SHA384withECDSA Claves: ECC P-384 bits	Sí		Identificando el tipo de algoritmo OID: 1.2.840.10045.4.3.3

Campo		Contenido	Obligatoriedad	Criticidad	Especificaciones
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	O=FNMT-RCM	Sí		UTF8 String (rfc5280)
	4.3. Organization Unit	OU=Ceres	Sí		UTF8 String (rfc5280)
	4.4. OrganizationIdentifier	VATES- Q2826004J	Sí		
	4.5. CommonName	cn=AC RAIZ FNMT-RCM SERVIDORES SEGUROS	Sí		UTF8 String (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	O=FNMT-RCM.	Sí		UTF8 String (rfc5280)
	6.3. Organizational Unit	OU=Ceres	Sí		UTF8 String (rfc5280)
	6.4. OrganizationIdentifier	VATES- Q2826004J	Sí		
	6.5. Common Name	cn=AC SERVIDORES SEGUROS TIPO2	Sí		UTF8 String (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		ECC P-384 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.

Campo		Contenido	Obligatoriedad	Criticidad	Especificaciones
	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		
12. CRL Distribution Point			Sí	No	
	12.1. Distribution Point 1	Punto de distribución 1 de la CRL http://www.cert.fnmt.es/crls/ARLSERVIDORESSEGUROS.crl	Sí		Ruta del servicio HTTP donde reside la CRL (punto de distribución).
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://ocspfnmtssr.cert.fnmt.es/ocspssr/OcspResponder			URL del servicio de OCSP

Campo		Contenido	Obligatoriedad	Criticidad	Especificaciones
	14.3. 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)			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.*"
	14.4. Access Location 2	http://www.cert.fnmt.es/certs/ACRAIZSERVIDORESSEGUROS.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.

2.3. CERTIFICADOS DE AUTENTICACIÓN DE SITIOS WEB

2.3.1. Certificado OV

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. [RFC5280]. Será un "integer" positivo, no mayor de 20 octetos (1-2^{159}). Establecido automáticamente y con un valor aleatorio por la Autoridad de Certificación.
3. Signature Algorithm		SHA384withECDSA Claves: ECC P-384 bits	Sí		Identificando el tipo de algoritmo de firma. OID: 1.2.840.10045.4.3.3
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	O=FNMT-RCM.	Sí		Denominación (nombre "oficial" de la organización) del prestador de servicios de certificación (emisor del certificado). UTF8 String tamaño máximo 64 (rfc5280)
	4.3. organizationalUnit	OU=Ceres	Sí		Unidad organizativa dentro del prestador de servicios, responsable de la emisión del certificado.

Campo		Contenido	Obligatoriedad	Criticidad	Especificaciones
					UTF8 String tamaño máximo 64 (rfc5280)
	4.4. OrganizationIdentifier	VATES- Q2826004J	Sí		
	4.5. Common Name	cn=AC SERVIDORES SEGUROS TIPO2	Sí		UTF8 String (rfc5280).
5. Validity		1 año	Sí		Validez de los certificados
6. Subject		Identificación/descripción del responsable de las claves certificadas	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. stateOrProvinceName	Nombre del estado o Provincia	Sí		UTF8String (rfc5280). Por ejemplo: ST=Madrid
	6.3. LocalityName	Nombre de la localidad del suscriptor	Sí		UTF8String (rfc5280). Por ejemplo: L=Madrid
	6.4. Organization	Denominación del suscriptor	Sí		UTF8String (rfc5280). Tamaño máximo 64. Por ejemplo: O=Ministerio de Economía
	6.5. SerialNumber	NIF del suscriptor	Sí		PrintableString (rfc5280). Tamaño 64 (X520). En nuestro caso, el tamaño es 9. Por ejemplo: serialNumber=Q0000000J
	6.6. OrganizationIdentifier	Identificador de la Organización	Sí		UTF8String Según la norma ETSI EN 319 412-1: VATES+NIF de la entidad Por ejemplo: organizationidentifier=VATES- Q0000000J
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		ECC P-384 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).

Campo		Contenido	Obligatoriedad	Criticidad	Especificaciones
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 usar 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. Server Authentication	1.3.6.1.5.5.7.3.1	Sí		Autenticación de servidor
	11.2. Client Authentication	1.3.6.1.5.5.7.3.2	Si		Autenticación de cliente
12. Qualified Certificate Statements		Extensiones cualificadas.	Sí	No	
	12.1. QcEuRetentionPeriod (0.4.0.1862.1.3)	15 años	Sí		ETSI EN 319 412-5 V2.1.1 – Apartado 4.3.3 Número de años a partir de la caducidad del certificado que se dispone de los datos de registro y otra 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. id-qcspkixQCSyntax-v2 (1.3.6.1.5.5.7.11.2)	semanticsId-Legal (0.4.0.194121.1.2)	No		ETSI EN 319 412-1 Semántica de persona jurídica

Campo			Contenido	Obligatoriedad	Criticidad	Especificaciones
	12.3. QcType (0.4.0.1862.1.6)		qct-web (0.4.0.1862.1.6.3)	Sí		ETSI EN 319 412-5 V2.1.1 – Apartado 4.2.3 Certificado de autenticación web
	12.4. QcPDS (0.4.0.1862.1.5)		{https://www.cert.fnmt.es/pds/PDS_SS2_es.pdf, es}, {https://www.cert.fnmt.es/pds/PDS_SS2_en.pdf, en}	Sí		ETSI EN 319 412-5 V2.1.1 – Apartado 4.3.4 Lugar donde se encuentra la declaración PDS, así como el idioma del documento.
13. Certificate Policies			Política de certificación	Sí	No	Atendiendo a ETSI EN 319 411-1 V1.1.1, apartado 6.3.3-g), [OVCP] The CP identifier shall be: i) as specified in clause 5.3 item f); ii) as specified in BRG [5], clause 7.1.6.1; and/or iii) an OID, allocated by the TSP, other relevant stakeholder or further standardization for a certificate policy enhancing the policy requirements defined in the present document.
	13.1. Policy Identifier		2.23.140.1.2.2 (organization-validated)	Sí		
	13.2. Policy Identifier		0.4.0.2042.1.7 (ovcp)	Sí		{joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) baseline-requirements(2) organization-validated(2)} (2.23.140.1.2.2)
	13.3. Policy Identifier		1.3.6.1.4.1.5734.3.16.2.1	Sí		
	13.3.1 Policy Qualifier Id			Sí		
		13.3.1.1 CPS Pointer	http://www.cert.fnmt.es/dpcs/	Sí		IA5String String. URL de las condiciones de uso.
14. SignedCertificateTimestampList (SCT)						
	14.1. signed certificate timestamp (OID 1.3.6.1.4.1.11129.2.4.2)		SCT (Octet String) obtenidos al publicar en un log el pre-certificado. Se obtendrá un SCT por cada log en el que se publique este certificado.	Sí		RFC 6962.
15. Subject Alternative Names				Sí	No	
	15.1. DNSName		Nombre de dominio	Sí		UTF8 String, tamaño máximo 128. Por ejemplo: DNSName = www.xxxxxx.es
16. CRL Distribution Point			Informa acerca de cómo se obtiene la información de la CRL asociada al certificado.	Sí	No	

Campo		Contenido	Obligatoriedad	Criticidad	Especificaciones
	16.1. Distribution Point	Punto de publicación de la CRL http://www.cert.fnmt.es/crlsservseguros/CRLT2.crl	Sí		Ruta donde reside la CRL (punto de distribución 2).
17. Authority Info Access			Sí	No	
	17.1. Access Method 1	Identificador de método de acceso a la información de revocación: 1.3.6.1.5.5.7.48.1 (ocsp)	Sí		
	17.2. Acces Location 1	http://ocspfnmtss2.cert.fnmt.es/ocspss2/OcspResponder	Sí		
	17.3. 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.*"
	17.4. Access Location 2	http://www.cert.fnmt.es/certs/ACSS2.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.
18. 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.*
	18.1. Subject Type	Valor FALSE (entidad final)			Con este certificado no se pueden emitir otros certificados.

2.3.2. Certificado SAN OV

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. [RFC5280]. Será un "integer" positivo, no mayor de 20 octetos ($1-2^{159}$).

Campo		Contenido	Obligatoriedad	Criticidad	Especificaciones
					Establecido automáticamente y con un valor aleatorio por la Autoridad de Certificación.
3. Signature Algorithm		SHA384withECDSA Claves: ECC P-384 bits	Sí		Identificando el tipo de algoritmo de firma. OID: 1.2.840.10045.4.3.3
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	O=FNMT-RCM.	Sí		Denominación (nombre "oficial" de la organización) del prestador de servicios de certificación (emisor del certificado). UTF8 String tamaño máximo 64 (rfc5280)
	4.3. organizationalUnit	OU=Ceres	Sí		Unidad organizativa dentro del prestador de servicios, responsable de la emisión del certificado. UTF8 String tamaño máximo 64 (rfc5280)
	4.4. OrganizationIdentifier	VATES- Q2826004J	Sí		
	4.5. Common Name	cn=AC SERVIDORES SEGUROS TIPO2	Sí		UTF8 String (rfc5280).
5. Validity		1 año	Sí		Validez de los certificados
6. Subject		Identificación/descripción del responsable de las claves certificadas	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. stateOrProvinceName	Nombre del estado o Provincia	Sí		UTF8String (rfc5280). Por ejemplo: ST=Madrid
	6.3. LocalityName	Nombre de la localidad del suscriptor	Sí		UTF8String (rfc5280). Por ejemplo: L=Madrid
	6.4. Organization	Denominación del suscriptor	Sí		UTF8String (rfc5280). Tamaño máximo 64. Por ejemplo: O=Ministerio de Economía
	6.5. SerialNumber	NIF del suscriptor	Sí		PrintableString (rfc5280). Tamaño 64 (X520). En nuestro caso, el tamaño es 9.

Campo		Contenido	Obligatoriedad	Criticidad	Especificaciones
					Por ejemplo: serialNumber=Q0000000J
	6.6. OrganizationIdentifier	Identificador de la Organización	Sí		UTF8String Según la norma ETSI EN 319 412-1: VATES+NIF de la entidad Por ejemplo: organizationidentifier=VATES- Q0000000J
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		ECC P-384 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	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 usar 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. Server Authentication	1.3.6.1.5.5.7.3.1	Sí		Autenticación de servidor
	11.2. Client Authentication	1.3.6.1.5.5.7.3.2	Si		Autenticación de cliente

Campo			Contenido	Obligatoriedad	Criticidad	Especificaciones
12. Qualified Certificate Statements			Extensiones cualificadas.	Sí	No	
	12.1. QcEuRetentionPeriod (0.4.0.1862.1.3)		15 años	Sí		ETSI EN 319 412-5 V2.1.1 – Apartado 4.3.3 Número de años a partir de la caducidad del certificado que se dispone de los datos de registro y otra 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. id-qcspkixQCSyntax-v2 (1.3.6.1.5.5.7.11.2)		semanticsId-Legal (0.4.0.194121.1.2)	No		ETSI EN 319 412-1 Semántica de persona jurídica
	12.3. QcType (0.4.0.1862.1.6)		qct-web (0.4.0.1862.1.6.3)	Sí		ETSI EN 319 412-5 V2.1.1 – Apartado 4.2.3 Certificado de autenticación web
	12.4. QcPDS (0.4.0.1862.1.5)		{https://www.cert.fnmt.es/pds/PDS_SS2_es.pdf, es},{https://www.cert.fnmt.es/pds/PDS_SS2_en.pdf, en}	Sí		ETSI EN 319 412-5 V2.1.1 – Apartado 4.3.4 Lugar donde se encuentra la declaración PDS, así como el idioma del documento.
13. Certificate Policies			Política de certificación	Sí	No	Atendiendo a ETSI EN 319 411-1 V1.1.1, apartado 6.3.3-g), [OVCP] The CP identifier shall be: i) as specified in clause 5.3 item f); ii) as specified in BRG [5], clause 7.1.6.1; and/or iii) an OID, allocated by the TSP, other relevant stakeholder or further standardization for a certificate policy enhancing the policy requirements defined in the present document.
	13.1. Policy Identifier		2.23.140.1.2.2 (organization-validated)	Sí		
	13.2. Policy Identifier		0.4.0.2042.1.7 (ovcp)	Sí		
	13.3. Policy Identifier		1.3.6.1.4.1.5734.3.16.2.3	Sí		
	13.3.1 Policy Qualifier Id			Sí		
		13.3.1.1 CPS Pointer	http://www.cert.fnmt.es/dpcs/	Sí		IA5String String. URL de las condiciones de uso.

Campo		Contenido	Obligatoriedad	Criticidad	Especificaciones
14. SignedCertificateTimestampList (SCT)					
	14.1. signed_certificate_timestamp (OID 1.3.6.1.4.1.11129.2.4.2)	SCT (Octet String) obtenidos al publicar en un log el pre-certificado. Se obtendrá un SCT por cada log en el que se publique este certificado.	Sí		RFC 6962.
15. Subject Alternative Names			Sí	No	
	15.1. DNSName	Id Campo / Valor: NombreDNS = Dominio_1	Sí		UTF8 String, tamaño máximo 128. Por ejemplo: DNSName = www.xxxxxx.es
	15.2. DNSName	Id Campo / Valor: NombreDNS = Dominio_2	Sí		UTF8 String, tamaño máximo 128. Por ejemplo: DNSName = www.xxxxxx.es
	15.3. DNSName	Id Campo / Valor: NombreDNS = Dominio_n	Sí		UTF8 String, tamaño máximo 128. Por ejemplo: DNSName = www.xxxxxx.es n<=12
16. CRL Distribution Point		Informa acerca de cómo se obtiene la información de la CRL asociada al certificado.	Sí	No	
	16.1. Distribution Point	Punto de publicación de la CRL. http://www.cert.fnmt.es/crlsservseguros/CRLT2.crl	Sí		Ruta donde reside la CRL (punto de distribución).
17. Authority Info Access			Sí	No	
	17.1. Access Method 1	Identificador de método de acceso a la información de revocación: 1.3.6.1.5.5.7.48.1 (ocsp)	Sí		
	17.2. Acces Location 1	http://ocspfnmtss2.cert.fnmt.es/ocspss2/OcspResponder	Sí		
	17.3. 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.*"
	17.4. Access Location 2	http://www.cert.fnmt.es/certs/ACSS2.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

Campo		Contenido	Obligatoriedad	Criticidad	Especificaciones
					subordinada de la raíz de la FNMT-RCM.
18. 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.*
	18.1. Subject Type	Valor FALSE (entidad final)			Con este certificado no se pueden emitir otros certificados.

2.3.3. Certificado WildCard OV

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. [RFC5280]. Será un "integer" positivo, no mayor de 20 octetos (1-2^{159}). Establecido automáticamente y con un valor aleatorio por la Autoridad de Certificación.
3. Signature Algorithm		SHA384withECDSA Claves: ECC P-384 bits	Sí		Identificando el tipo de algoritmo de firma. OID: 1.2.840.10045.4.3.3
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	O=FNMT-RCM.	Sí		Denominación (nombre "oficial" de la organización) del prestador de servicios de certificación (emisor del certificado). UTF8 String tamaño máximo 64 (rfc5280)
	4.3. organizationalUnit	OU=Ceres	Sí		Unidad organizativa dentro del prestador de servicios, responsable de la emisión del certificado. UTF8 String tamaño máximo 64 (rfc5280)
	4.4. OrganizationIdentifier	VATES- Q2826004J	Sí		
	4.5. Common Name	cn=AC SERVIDORES SEGUROS TIPO2	Sí		UTF8 String (rfc5280).

Campo		Contenido	Obligatoriedad	Criticidad	Especificaciones
5. Validity		1 año	Sí		Validez de los certificados
6. Subject		Identificación/descripción del responsable de las claves certificadas	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. stateOrProvinceName	Nombre del estado o Provincia	Sí		UTF8String (rfc5280). Por ejemplo: ST=Madrid
	6.3. LocalityName	Nombre de la localidad del suscriptor	Sí		UTF8String (rfc5280). Por ejemplo: L=Madrid
	6.4. Organization	Denominación del suscriptor	Sí		UTF8String (rfc5280). Tamaño máximo 64. Por ejemplo: O=Ministerio de Economía
	6.5. SerialNumber	NIF del suscriptor	Sí		PrintableString (rfc5280). Tamaño 64 (X520). En nuestro caso, el tamaño es 9. Por ejemplo: serialNumber=Q0000000J
	6.6. OrganizationIdentifier	Identificador de la Organización	Sí		UTF8String Según la norma ETSI EN 319 412-1: VATES+NIF de la entidad Por ejemplo: organizationidentifier=VATES- Q0000000J
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		ECC P-384 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

Campo		Contenido	Obligatoriedad	Criticidad	Especificaciones
					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 usar 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. Server Authentication	1.3.6.1.5.5.7.3.1	Sí		Autenticación de servidor
	11.2. Client Authentication	1.3.6.1.5.5.7.3.2	Si		Autenticación de cliente
12. Qualified Certificate Statements		Extensiones cualificadas.	Sí	No	
	12.1. QcEuRetentionPeriod (0.4.0.1862.1.3)	15 años	Sí		ETSI EN 319 412-5 V2.1.1 – Apartado 4.3.3 Número de años a partir de la caducidad del certificado que se dispone de los datos de registro y otra 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. id-qcspkixQCSyntax-v2 (1.3.6.1.5.5.7.11.2)	semanticsId-Legal (0.4.0.194121.1.2)	No		ETSI EN 319 412-1 Semántica de persona jurídica
	12.3. QcType (0.4.0.1862.1.6)	qct-web (0.4.0.1862.1.6.3)	Sí		ETSI EN 319 412-5 V2.1.1 – Apartado 4.2.3 Certificado de autenticación web
	12.4. QcPDS (0.4.0.1862.1.5)	{https://www.cert.fnmt.es/pds/PDS_SS2_es.pdf, es}, {https://www.cert.fnmt.es/pds/PDS_SS2_en.pdf, en}	Sí		ETSI EN 319 412-5 V2.1.1 – Apartado 4.3.4

Campo			Contenido	Obligatoriedad	Criticidad	Especificaciones
						Lugar donde se encuentra la declaración PDS, así como el idioma del documento.
13. Certificate Policies			Política de certificación	Sí	No	Atendiendo a ETSI EN 319 411-1 V1.1.1, apartado 6.3.3-g), [OVCP] The CP identifier shall be: i) as specified in clause 5.3 item f); ii) as specified in BRG [5], clause 7.1.6.1; and/or iii) an OID, allocated by the TSP, other relevant stakeholder or further standardization for a certificate policy enhancing the policy requirements defined in the present document.
	13.1. Policy Identifier		2.23.140.1.2.2 (organization-validated)	Sí		
	13.2. Policy Identifier		0.4.0.2042.1.7 (ovcp)	Sí		
	13.3. Policy Identifier		1.3.6.1.4.1.5734.3.16.2.2	Sí		
	13.3.1 Policy Qualifier Id			Sí		
		13.3.1.1 CPS Pointer	http://www.cert.fnmt.es/dpcs/	Sí		IA5String String. URL de las condiciones de uso.
14. SignedCertificateTimestampList (SCT)						
	14.1. signed certificate timestamp (OID 1.3.6.1.4.1.11129.2.4.2)		SCT (Octet String) obtenidos al publicar en un log el pre-certificado. Se obtendrá un SCT por cada log en el que se publique este certificado.	Sí		RFC 6962.
15. Subject Alternative Names				Sí	No	
	15.1. DNSName		Id Campo / Valor: NombreDNS = Dominio wildcard	Sí		UTF8 String, tamaño máximo 128. Por ejemplo: DNSName = www.xxxxxx.es
	15.2. DNSName		Nombre de dominio base	Sí		UTF8 String, tamaño máximo 128. Por ejemplo: DNSName = www.xxxxxx.es
16. CRL Distribution Point			Informa acerca de cómo se obtiene la información de la CRL asociada al certificado.	Sí	No	
	16.1. Distribution Point		Punto de publicación de la CRL. http://www.cert.fnmt.es/crlsservseguros/CRLT2.crl	Sí		Ruta donde reside la CRL (punto de distribución).
17. Authority Info Access				Sí	No	

Campo		Contenido	Obligatoriedad	Criticidad	Especificaciones
	17.1. Access Method 1	Identificador de método de acceso a la información de revocación: 1.3.6.1.5.5.7.48.1 (ocsp)	Sí		
	17.2. Acces Location 1	http://ocspfnmtss2.cert.fnmt.es/ocspss2/OcspResponder	Sí		
	17.3. 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.*"
	17.4. Access Location 2	http://www.cert.fnmt.es/certs/ACSS2.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.
18. 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.*
	18.1. Subject Type	Valor FALSE (entidad final)			Con este certificado no se pueden emitir otros certificados.