Real Casa de la Moneda
Fábrica Nacional
de Moneda y Timbre

DIRECCIÓN DE SISTEMAS DIGITALES E INNOVACIÓN
DEPARTAMENTO CERES

DEFINICIÓN PERFILES DE CERTIFICADO EMITIDOS POR AC CONSULARES G2

	NOMBRE	FECHA
Elaborado por:	FNMT-RCM	28/10/2024
Revisado por:	FNMT-RCM	28/10/2024
Aprobado por:	FNMT-RCM	15/11/2024

HISTÓRICO DEL DOCUMENTO		
Versión	**Fecha**	**Descripción**
0.1	06/09/2024	Versión Inicial
0.2	28/10/2024	Se actualiza las urls de PDS, se modifica en el Common Name y el Subject Alternative Names el formato del NICC
1.0	11/11/2024	Se elimina el uso de clave "Key Encipherment" para certificados finales, tanto RSA como ECC

Referencia:

Documento clasificado como: *Público*

1. Introducción 3
2. Perfil de certificado de AC CONSULARES G2 4
3. Perfiles de certificado de entidades finales 9
3.1. Certificados entidad final residentes en el extranjero (AC Consulares) 9

1. INTRODUCCIÓN

El presente documento describe en detalle los perfiles de los distintos tipos de certificado que emite la Autoridad de Certificación "*AC Consulares G2*".

Los tipos de certificado que emite la "*AC Consulares G2*" son:

- Certificado de entidad final de residentes en el extranjero (AC Consulares)

2. PERFIL DE CERTIFICADO DE AC CONSULARES G2

Campo	Contenido	Obligatorio	Criticidad	Descripción
1. Versión	2	Si		Integer:= 2 [RFC5280] Identifica la versión del certificado. El valor 2 equivale a decir que el certificado es versión 3 (X509v3)
2. Serial Number	Número identificativo único del certificado. Este número se asigna de forma aleatoria.	Si		Integer. SerialNumber = ej: 111222. Número de identificación del certificado establecido automáticamente por la Entidad de Certificación. [RFC5280]. Será un "integer" positivo, no mayor 20 octetos (1- 2159).
3. Signature Algorithm	ecdsa-with-SHA384	Si		String. Algoritmo utilizado para la encriptación OID: 1.2.840.10045.4.3.3
4. Issuer Distinguish Name	Autoridad de Certificación emisora del certificado	Si		Los valores del Issuer debe ser exactamente igual al Subject de la AC Raíz.
4.1. Country	C=ES	Si		PrintableString, tamaño 2 (rfc5280). Codificación del país de acuerdo con la ISO 3166. En el caso de España "ES" Se codificará de acuerdo a "ISO 3166-1-alpha-2 code elements".
4.2. Organization	Denominación del prestador de servicios de confianza que emite el certificado. (nombre "oficial" de la organización) o=FNMT-RCM.	Si		UTF8 String, tamaño máximo 64 (rfc5280)
4.3. Organization Identifier	Número único de identificación de la entidad, aplicable de acuerdo con el país. En España, NIF de la entidad suscriptora. organizationIdentifier=VATES-Q2826004J			PrintableString, tamaño 64 (X520). En nuestro caso, el tamaño es 9 caracteres Según la norma técnica ETSI EN 319 412-1 (VATES + NIF de la entidad) - 3 caracteres para indicar el tipo legal de identificador (VAT= documento de identificación fiscal) - 2 caracteres para identificar el país ISO 3166-1 [2]

Campo		Contenido	Obligatorio	Criticidad	Descripción
					- 1 carácter "-" 0x2D (ASCII), U+002D (UTF-8)
	4.4. Common Name	CA del prestador de servicios de confianza bajo la cual se generar el certificado electrónico cn= AC RAIZ FNMT-RCM G2	Si		UTF8 String, tamaño máximo 64 (rfc5280).
5. Validity		15 años	Si		String Validez del certificado electrónico
	5.1. Not before	UTCTime YYMMDDHHMMSSZ	Si		Fecha desde la que es válida el certificado
	5.2. Not after	UTCTime YYMMDDHHMMSSZ	Si		Fecha hasta la que es válida el certificado
6. Subject			Si		Identificación del titular asociado a la clave pública
	6.1. Country	C=ES	Si		PrintableString, tamaño 2 (rfc5280). Codificación del país de acuerdo con la ISO 3166. En el caso de España "ES" Se codificará de acuerdo a "ISO 3166-1-alpha-2 code elements".
	6.2. Organization	Denominación del prestador de servicios de confianza que emite el certificado. (nombre "oficial" de la organización) o=FNMT-RCM.	Si		UTF8 String, tamaño máximo 64 (rfc5280)
	6.3. Organization Identifier	Número único de identificación de la entidad, aplicable de acuerdo con el país. En España, NIF de la entidad suscriptora. organizationIdentifier=VATES-Q2826004J			PrintableString, tamaño 64 (X520). En nuestro caso, el tamaño es 9 caracteres Según la norma técnica ETSI EN 319 412-1 (VATES + NIF de la entidad) - 3 caracteres para indicar el tipo legal de identificador (VAT= documento de identificación fiscal) - 2 caracteres para identificar el país ISO 3166-1 [2] - 1 carácter "-" 0x2D (ASCII), U+002D (UTF-8)

Campo	Contenido	Obligatorio	Criticidad	Descripción
6.4. Common Name	CA del prestador de servicios de confianza bajo la cual se generar el certificado electrónico. El valor que tomará será (según CA subordinada) cn= AC CONSULARES G2	Si		UTF8 String, tamaño máximo 64 (rfc5280) -
7. Autority Key Identifier	Identificador de la clave pública de la AC RAIZ FNMT-RCM G2. Medio para identificar la clave pública correspondiente a la clave privada utilizada por la CA para firmar un certificado.	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 AC emisora.
8. Subject Public Key Info	Clave pública del Firmante, codificada de acuerdo con el algoritmo criptográfico. En este caso Secp256r1.	Sí	No	Campo para transportar la clave pública y para identificar el algoritmo con el cual se utiliza la clave. ECC P-256 bits
9. Subject Key Identifier	Identificador de la clave pública del Firmante. Es el medio para identificar certificados que contienen una clave pública particular y facilita la construcción de rutas de certificación.	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		Sí	Sí	Normalizado en norma X509 y RFC 5280.
10.1. Digital Signature	0	Sí		Uso de autenticación (0 – NO / 1 – SI)
10.2. Content Commitment	0	Sí		Firma Electrónica (0 – NO / 1 – SI)
10.3. Key Encipherment	0	Sí		Cifra de claves (0 – NO / 1 – SI)
10.4. Data Encipherment	0			Cifra de datos (0 – NO / 1 – SI)
10.5. Key Agreement	0	Sí		Negociado de claves(0 – NO / 1 – SI)
10.6. Key Certificate Signature	1	Sí		Verificar firmas de otros certificados (0 – NO / 1 – SI)
10.7. CRL Signature	1	Sí		Firma de Certification Revocation List CRL (0 – NO / 1 – SI)

Campo	Contenido	Obligatorio	Criticidad	Descripción
11. Extended Key Usage	Uso mejorado o extendido de las claves			Esta extensión indica uno o más propósitos para los cuales el certificado de clave pública se puede utilizar, en compatibilidad con los usos básicos que se indican en la extensión KeyUsage. Nota: Se trata de una AC Subordinada técnicamente restringida.
11.1. Client Authentication	1.3.6.1.5.5.7.3.2	Sí		Autenticación de cliente.
11.2. Document Signing	1.3.6.1.4.1.311.10.3.12	Sí		Firma de documentos.
11.3. Adobe Authentic Document Trust	1.2.840.113583.1.1.5	Sí		Firma de documentos PDF.
12. Certificate Policies		Sí		Políticas de certificación
12.1. Policy Identifier	2.5.29.32.0 (anyPolicy)	Sí		Identificador de la política de identificación. Política a definida por el PSC en el que se encuadre este certificado
13. CRL Distribution Point	Puntos de distribución de las listas de distribución de las listas de revocación de los certificados Electrónicos	Sí	No	
13.1. Distribution Point 1	Punto de distribución 1 de la CRL (ARL) http://www.cert.fnmt.es/crls/ARLFNMTRCMG2.crl	Sí		Ruta donde reside la CRL (punto de distribución 1).
14. Authority Info Access		Sí	No	
14.1. Access Method 1	Identificador de método de acceso a la información de revocación OSCP - 1.3.6.1.5.5.7.48.1	Sí		Acceso al servicio OCSP
14.2. Access Location 1	http://ocspcaraizg2.cert.fnmt.es/ocspcaraizG2/OcspResponder	Sí		Ruta para acceder al servicio OCSP. No es necesario firmar las peticiones OCSP

Campo	Contenido	Obligatorio	Criticidad	Descripción
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)	Sí		Emisor de la entidad emisora de certificados (CA Raíz) 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/ACRAIZFNMTG2.crt	Sí		Ruta para descarga de certificados adicionales para la validación de la cadena de certificación.
15. Basic Constrains	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". También sirve para distinguir una CA de las entidades finales	Sí	Sí	De la rf5280: " This extension MAY appear as a critical or non-critical extension in end entity certificates.
15.1. cA	Entidad Final (valor TRUE)	Sí		Boolean Indica que el certificado es de una autoridad de certificación. Con este certificado se pueden emitir otros.
15.2. pathLength	0			

3. PERFILES DE CERTIFICADO DE ENTIDADES FINALES

3.1. CERTIFICADOS ENTIDAD FINAL RESIDENTES EN EL EXTRANJERO (AC CONSULARES)

Campo	Contenido	Obligatorio	Criticidad	Descripción
1. Versión	2	Si		Integer:= 2 [RFC5280] Identifica la versión del certificado. El valor 2 equivale a decir que el certificado es versión 3 (X509v3)
2. Serial Number	Número identificativo único del certificado. Este número se asigna de forma aleatoria.	Si		Integer. SerialNumber = ej: 111222. Número de identificación del certificado establecido automáticamente por la Entidad de Certificación. [RFC5280]. Será un "integer" positivo, no mayor 20 octetos (1- 2159).
3. Signature Algorithm	ecdsa-with-SHA256	Si		String. Algoritmo utilizado para la encriptación OID: 1.2.840.10045.4.3.2
4. Issuer Distinguish Name	Autoridad de Certificación emisora del certificado	Si		
4.1. Country	C=ES	Si		PrintableString, tamaño 2 (rfc5280). Codificación del país de acuerdo con la ISO 3166. En el caso de España "ES" Se codificará de acuerdo a "ISO 3166-1-alpha-2 code elements".
4.2. Organization	Denominación del prestador de servicios de confianza que emite el certificado. (nombre "oficial" de la organización) o=FNMT-RCM.	Si		UTF8 String, tamaño máximo 64 (rfc5280)
4.3. Organization Identifier	Número único de identificación de la entidad, aplicable de acuerdo con el país. En España, NIF de la entidad suscriptora. organizationIdentifier=VATES-Q2826004J			PrintableString, tamaño 64 (X520). En nuestro caso, el tamaño es 9 caracteres Según la norma técnica ETSI EN 319 412-1 (VATES + NIF de la entidad) - 3 caracteres para indicar el tipo legal de identificador (VAT= documento de identificación fiscal)

Campo		Contenido	Obligatorio	Criticidad	Descripción
					- 2 caracteres para identificar el país ISO 3166-1 [2] - 1 carácter "-" 0x2D (ASCII), U+002D (UTF-8)
	4.4. Common Name	CA del prestador de servicios de confianza bajo la cual se generar el certificado electrónico. El valor que tomará será (según CA subordinada) cn=AC CONSULARES G2	Si		UTF8 String, tamaño máximo 64 (rfc5280)
5. Validity		4 años	Si		String Validez del certificado electrónico
	5.1. Not before	UTCTime YYMMDDHHMMSSZ	Si		Fecha desde la que es válida el certificado
	5.2. Not after	UTCTime YYMMDDHHMMSSZ	Si		Fecha hasta la que es válida el certificado
6. Subject			Si		Identificación del titular asociado a la clave pública
	6.1. Country	C=ES	Si		PrintableString, tamaño 2 (rfc5280). Codificación del país de acuerdo con la ISO 3166. En el caso de España "ES" Se codificará de acuerdo a "ISO 3166-1-alpha-2 code elements".
	6.2. SerialNumber	Número de identificación consular NICC (Número de identificación Consular Central) (PrintableString (rfc5280))	Si		Se codificará de acuerdo a ETSI EN 319 412-1. PrintableString (rfc5280). **EX:ES-00000000T** (solo se pueden usar dos caracteres en "EX" como Id de Exteriores)
	6.3. Given Name	Nombre del titular, de acuerdo con el documento de identidad.	Sí		UTF8 String (rfc5280) Tamaño máximo 50 carácter. Por ejemplo: givenName= JUAN
	6.4. Surname	Apellidos del titular, de acuerdo con el documento de identidad.	Sí		UTF8 String, tamaño máximo 50 caracteres (rfc5280). Por ejemplo: Sn= ESPAÑOL ESPAÑOL

Campo	Contenido	Obligatorio	Criticidad	Descripción
6.5. Common Name	Apellidos, Nombre y NICC del titular.	Si		UTF8 String, (rfc5280). Tamaño máximo 164 caracteres. cn= Español Español Juan – 00000000T
7. Authority Key Identifier	Identificador de la clave pública del PSC. Medio para identificar la clave pública correspondiente a la clave privada utilizada por la CA para firmar un certificado	Sí		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 AC emisora.
8. Subject Public Key Info	Clave pública del Firmante, codificada de acuerdo con el algoritmo criptográfico.	Sí	No	Campo para transportar la clave pública y para identificar el algoritmo con el cual se utiliza la clave. En RSA la longitud de la clave será 2048 bits. En ECC (Secp256r1) la longitud de la clave ECC P-256 bits
9. Subject Key Identifier	Identificador de la clave pública del Firmante. Es el medio para identificar certificados que contienen una clave pública particular y facilita la construcción de rutas de certificación.	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		Sí	Sí	Normalizado en norma X509 y RFC 5280.
10.1. Digital Signature	1	Sí		Uso de autenticación (0 – NO / 1 – SI)
10.2. Content Commitment	1	Sí		Firma Electrónica (0 – NO / 1 – SI)
10.3. Key Encipherment	0	Sí		Cifra de claves (0 – NO / 1 – SI)
10.4. Data Encipherment	0			Cifra de datos (0 – NO / 1 – SI)
10.5. Key Agreement	0	Sí		Negociado de claves(0 – NO / 1 – SI)
10.6. Key Certificate Signature	0	Sí		Verificar firmas de otros certificados (0 – NO / 1 – SI)

Campo	Contenido	Obligatorio	Criticidad	Descripción
10.7. CRL Signature	0	Sí		Firma de Certification Revocation List CRL (0 – NO / 1 – SI)
11. Extended Key Usage	Uso mejorado o extendido de las claves			Esta extensión indica uno o más propósitos para los cuales el certificado de clave pública se puede utilizar, en compatibilidad con los usos básicos que se indican en la extensión KeyUsage.
11.1. Client Authentication	1.3.6.1.5.5.7.3.2	Sí		Autenticación de cliente.
11.2. Document Signing	1.3.6.1.4.1.311.10.3.12	Sí		Firma de documentos
11.3. Adobe Authentic Document Trust	1.2.840.113583.1.1.5	Sí		Firma de documentos PDF.
12. Qualified Certificate Statements	Extensiones cualificadas		No	ETSI EN 319 411-2 y ETSI EN 319 412-5 definen la inclusión de ciertas declaraciones para certificados cualificados.
12.1. QcCompliance (0.4.0.1862.1.1)	Certificado es cualificado	Sí		Indica que el certificado es cualificado. Solo si no está explícito en las políticas indicadas en la extensión correspondiente
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 otra información relevante
12.3. QcType (0.4.0.1862.1.6)	Qct-esign (0.4.0.1862.1.6.1)	Sí		Indica que el certificado es cualificado y se ha emitido para crear firmas electrónicas.
12.4. QcPDS (0.4.0.1862.1.5)	{https://www.cert.fnmt.es/pds/PDS_Consular_es.pdf,es es},{https://www.cert.fnmt.es/pds/PDS_Consular_en.pdf, en}	Si		Indica un enlace a la PKI Disclosure Statement, así como el idioma del documento.
12.5. id-qcspkixQCSyntax-v2 (1.3.6.1.5.5.7.11.2)	semanticsId-Natural (0.4.0.194121.1.1)	Si		Indica que el campo subject sigue la semántica propuesta por la ETSI EN 319 412-1
	NameRegistrationAuthorities https://exteriores.gob.es	Sí		https://exteriores.gob.es
13. Certificate Policies		Sí		Políticas de certificación
13.1. Policy Identifier	1.3.6.1.4.1.5734.3.26.1.0	Sí		Identificador de la política de identificación Política a definida por el PSC en el que se encuadre este certificado

Campo	Contenido	Obligatorio	Criticidad	Descripción
13.2. Policy Qualifier ID		Sí		
13.2.1. CPS Pointer	http://www.cert.fnmt.es/dpcs/	Sí		IA5String String. URI a la CPS o declaración de política de certificación
13.2.2. User Notice	Certificado cualificado de firma electrónica. Sujeto a las condiciones de uso expuestas en la DPC de la FNMT-RCM con NIF: Q2826004-J	Sí		UTF8 String. Longitud máxima 200 caracteres.
13.3. Policy Identifier	0.4.0.194112.1.0	Sí		QCP-n: certificate policy for EU qualified certificates issued to natural persons.
14. Subject Alternative Names		Sí	No	Identificación/descripción del Representante y de la Entidad representada
14.1. Directory Name		Sí		
14.1.1. Nombre	Id Campo/Valor: 1.3.6.1.4.1.5734.1.1=<nombre>	Sí		UTF8 String Nombre de pila del suscriptor del certificado Id Campo/Valor: 1.3.6.1.4.1.5734.1.1=JUAN
14.1.2. Apellido 1	Id Campo/Valor: 1.3.6.1.4.1.5734.1.2=<apellido1>	Sí		UTF8 String Primer apellido del suscriptor del certificado Id Campo/Valor: 1.3.6.1.4.1.5734.1.2=ESPAÑOL
14.1.3. Apellido 2	Id Campo/Valor: 1.3.6.1.4.1.5734.1.3=<apellido2>	Sí		UTF8 String Segundo apellido del suscriptor del certificado Id Campo/Valor: 1.3.6.1.4.1.5734.1.3=ESPAÑOL
14.1.4. NICC	Id Campo/Valor: 1.3.6.1.4.1.5734.1.47=<NICC>	Sí		UTF8 String. Tamaño 9. Número de identificación Consular Central. EJEMPLO: 1.3.6.1.4.1.5734.1.47= 00000000T
15. CRL Distribution Point	Puntos de distribución de las listas de distribución de las listas de revocación de los certificados Electrónicos	Sí	No	
15.1. Distribution Point 1	Punto de publicación de la CRL1	Sí		Ruta donde reside la CRL (punto de distribución 1).

Campo	Contenido	Obligatorio	Criticidad	Descripción
	http://www.cert.fnmt.es/crlsacconsu/CRL<xxx*>.crl *xxx: número entero identificador de la CRL (CRL particionadas)			
16. Authority Info Access		Sí	No	
16.1. Access Method 1	Identificador de método de acceso a la información de revocación OSCP - 1.3.6.1.5.5.7.48.1	Sí		Acceso al servicio OCSP
16.2. Access Location 1	http://ocspconsug2.cert.fnmt.es/ocspconsuG2/OcspResponder	Sí		URL para acceder al servicio OCSP. No es necesario firmar las peticiones OCSP
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		Emisor de la entidad emisora de certificados (CA Raíz) 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/ACCONSUG2.crt	Sí		Ruta para descarga de certificados adicionales para la validación de la cadena de certificación.
17. Basic Constrains	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". También sirve para distinguir una CA de las entidades finales	Sí	Sí	De la rf5280: "This extension MAY appear as a critical or non-critical extension in end entity certificates.
17.1. cA	Entidad Final (valor FALSE)	Sí		Boolean Indica que el certificado NO es de una autoridad de certificación. Con este certificado NO se pueden emitir otros.