Real Casa de la Moneda
Fábrica Nacional
de Moneda y Timbre

DIRECCIÓN DE SERVICIOS DIGITALES E INNOVACIÓN
DEPARTAMENTO CERES

DEFINICIÓN DE PERFILES AC USUARIOS

	NOMBRE	FECHA
Elaborado por:	FNMT-RCM	04/08/2023
Revisado por:	FNMT-RCM	18/08/2023
Aprobado por:	FNMT-RCM	28/08/2023

Referencia:

Documento clasificado como: *Público*

Índice

1. Objeto 3
2. Perfil CA Subordinada Persona Física 3
3. Perfil Persona física 6

1. Objeto

En el presente documento se describen los perfiles de los certificados de la ”AC subordinada Usuarios” y de los certificados de usuario final (personas físicas).

2. Perfil CA Subordinada Persona Física

Campo		Contenido	Oblig	Crit	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}). El número de serie se asignará de forma aleatoria.
3. Signature Algorithm		Sha256withRsaEncryption	Sí		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. Organizational Unit	Denominación de la Unidad Organizativa ou = AC RAIZ FNMT-RCM	Sí		UTF8 String, tamaño máximo 128 (rfc5280)
5. Validity		15 años	Sí		
6. Subject			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. Organizational Unit	Denominación de la Unidad Organizativa	Sí		UTF8 String, tamaño máximo 128 (rfc5280)

Campo		Contenido	Oblig	Crit	Especificaciones
		ou= Ceres			
	6.4. Common Name	cn= AC FNMT Usuarios	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 AC raíz.
8. Subject Public Key Info		Clave pública de la AC Subordinada FNMT Usuarios, codificada según el estándar PKCS#1 de RSA.	Sí		Campo para transportar la clave pública y para identificar el algoritmo con el cual se utiliza la clave. La longitud de la clave será 2048
9. Subject Key Identifier		Identificador de la clave pública de la CA Subordinada. Medio para identificar certificados que contienen una clave pública particular y facilita la construcción de rutas de certificación.	Sí		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	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		Se permite usa para firmar certificados. Este uso se utiliza en los certificados de autoridades de certificación.
	10.7. CRL Signature	1	Sí		Se permite para firmar listas de revocación de certificados. Este uso se utiliza en los certificados de autoridades de certificación.
11. Certificate Policies		Política de certificación	Sí		
	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*

Campo			Contenido	Oblig	Crit	Especificaciones
						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			Sí		
		11.2.1 CPS Pointer	http://www.cert.fnmt.es/dpcs/	Sí		IA5String String. URL de las condiciones de uso.
		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		
	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	Sí	
	13.1. cA		Valor TRUE (CA)	Sí		De la rfc 5280: "The cA boolean indicates whether the certified public key may be used to verify certificate signatures."
	13.2. pathLenConstraint		0	Sí		Un pathLenConstraint de cero indica que ningún no pueden existir más certificados de CA intermedios en la ruta de certificación.
14. Authority Info Access				Sí	No	
	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)	Sí		OCSP (1.3.6.1.5.5.7.48.1)
	14.2. Access Location 1		http://ocspfnmtrcmca.cert.fnmt.es/ocspfnmtrcmca/OcspResponder	Sí		URL del servicio de OCSP
	14.3. Access Method 2		Identificador de método de acceso a la información de	Sí		Certificado de la CA emisora: De la rfc 5280: "the idad-calssuers OID is used when the additional information lists

Campo		Contenido	Oblig	Crit	Especificaciones
		certificados adicionales necesarios para la validación: 1.3.6.1.5.5.7.48.2 (ca cert)			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/ACRAIZFNMTRCM.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 raíz de la FNMTRCM.

3. Perfil Persona física

Campo		Contenido	Oblig	Crit	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}). El número de serie se asignará de forma aleatoria.
3. Signature Algorithm		sha256WithRSAEncryption	Sí		Object Identifier 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. Organizational Unit	Denominación de la Unidad Organizativa ou= Ceres	Sí		UTF8 String, tamaño máximo 128 (rfc5280)
	4.4. Common Name	cn= AC FNMT Usuarios	Sí		UTF8 String, tamaño máximo 128 (rfc5280)
5. Validity		Variable	Sí		Validez de 4 años

Campo		Contenido	Oblig	Crit	Especificaciones
6. Subject		Identificación/descripción del titular de las claves certificadas	Sí		
	6.1. Country	C=ES. (PrintableString, tamaño 2 (rfc5280))	Sí		Se codificará de acuerdo a "ISO 3166-1-alpha-2 code elements". PrintableString, tamaño 2 (rfc5280)
	6.2. SerialNumber	NIF del titular. (PrintableString (rfc5280))	Sí		Se codificará de acuerdo a ETSI EN 319 412-1. PrintableString (rfc5280). Ejemplo: serialNumber= IDCES-00000000T
	6.3. Given Name	Nombre de pila, de acuerdo con documento de identidad. (UTF8String tamaño máximo 50 caracteres)	Sí		UTF8String (rfc5280). Por ejemplo: givenName=Juan
	6.4. Surname	Apellidos de acuerdo con documento de identificación. (UTF8String tamaño máximo 50 caracteres)	Sí		UTF8String (rfc5280). Por ejemplo: sn=Español Español
	6.5. Common Name	Apellidos, Nombre y NIF del titular. (UTF8String tamaño máximo 164 caracteres)	Sí		UTF8String (rfc5280). Por ejemplo: 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 titular, codificada de acuerdo con el algoritmo criptográfico. En este caso RSA Encryption.	Sí		Campo para transportar la clave pública y para identificar el algoritmo con el cual se utiliza la clave. La longitud de la clave será 2048 bits.
9. Subject Key Identifier		Identificador de la clave pública del titular. 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		Uso permitido de las claves certificadas.	Sí	Sí	Normalizado en norma X509
	10.1. Digital Signature	1	Sí		Ver X509 y RFC 5280.
	10.2. Content Commitment	1	Sí		Ver X509 y RFC 5280.
	10.3. Key Encipherment	1	Sí		Ver X509 y RFC 5280.
	10.4. Data Encipherment	0	Sí		Ver X509 y RFC 5280.
	10.5. Key Agreement	0	Sí		Ver X509 y RFC 5280.
	10.6. Key Certificate Signature	0	Sí		Ver X509 y RFC 5280.

Campo			Contenido	Oblig	Crit	Especificaciones
	10.7. CRL Signature		0	Sí		Ver X509 y RFC 5280.
11. Extended Key Usage			Uso mejorado o extendido de las claves	Sí	No	Ver X509 y RFC 5280..
	11.1. Client Authentication		1.3.6.1.5.5.7.3.2	Sí		Ver X509 y RFC 5280.
	11.2. Document Signing		1.3.6.1.4.1.311.10.3.12	Si		
	11.3. Adobe Authentic Documents Trust		1.2.840.113583.1.1.5	Si		
12. Qualified Certificate Statements			Extensiones cualificadas.	Sí	No	ETSI EN 319 411-2 y ETSI EN 319 412-5 definen la inclusión de ciertas declaraciones para certificados cualificados.
	12.1. QcCompliance		Certificado es cualificado.	Sí		Indica que el certificado es cualificado.
	12.2. QcType		Qct-esign	Sí		Indica que el certificado es cualificado y se ha emitido para crear firmas electrónicas.
	12.3. QcPDS		{https://www.cert.fnmt.es/pds/PDSACUsuarios_es.pdf, es},{https://www.cert.fnmt.es/pds/ PDSACUsuarios_en.pdf, en}	Sí		Indica un enlace a la PKI Disclosure Statement, así como el idioma del documento.
	12.4. QcEuRetentionPeriod		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.
13. Certificate Policies			Política de certificación	Sí		
	13.1. Policy Identifier		1.3.6.1.4.1.5734.3.10.1	Sí		Identificador de la política
	13.2. Policy Qualifier Id					
		13.2.1. CPS Pointer	http://www.cert.fnmt.es/dpcs/	Sí		IA5String String. URL de las condiciones de uso.
		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 (C/Jorge Juan 106-28009-Madrid-España)	Sí		UTF8 String. Longitud máxima 200 caracteres.
	13.2.3. 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			Identificación/descripción del titular	Sí	No	
	14.1. rfc822 Name		Correo electrónico del titular	Opcional		
	14.2. Directory Name					

Campo			Contenido	Oblig	Crit	Especificaciones
		14.2.1. Nombre	Nombre de pila del titular del certificado Id Campo/Valor: 1.3.6.1.4.1.5734.1.1 =<Nombre de pila	Sí		UTF8 String. Por ejemplo: 1.3.6.1.4.1.5734.1.1=JUAN
		14.2.2. Apellido1	Primer apellido del titular del certificado Id Campo/Valor: 1.3.6.1.4.1.5734.1.2 =<Apellido 1	Sí		UTF8 String. Por ejemplo: 1.3.6.1.4.1.5734.1.2=ESPAÑOL
		14.2.3. Apellido2	Segundo apellido del titular del certificado Id Campo/Valor: 1.3.6.1.4.1.5734.1.3 =<Apellido 2	Opcional		UTF8 String. Por ejemplo: 1.3.6.1.4.1.5734.1.3 =ESPAÑOL
		14.2.4. NIF	Identificador de identidad del titular del certificado. (NIF). Id Campo/Valor: 1.3.6.1.4.1.5734.1.4=<NIF	Sí		UTF8 String, tamaño 9. Por ejemplo: 1.3.6.1.4.1.5734.1.4=99999999R
15. CRL Distribution Point				Sí	No	
	15.1. Distribution Point 1		Punto distribución de la CRL: URI: ldap://ldapusu.cert.fnmt.es/CN=CRLU<xxx*>,CN=AC%20FNMT%20Usuarios,OU=Ceres,O=FNMT-RCM,C=ES?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint	Sí		Ruta donde reside la CRL (punto de distribución 1). *xxx: número entero que identifica la CRL (CRLs particionadas)
	15.2. Distribution Point 2		Punto de distribución 2 de la CRL: URI: http://www.cert.fnmt.es/crlsacusu/CRLU<xxx*>.crl	Sí		Ruta donde reside la CRL (punto de distribución 2). *xxx: número entero que identifica la CRL (CRLs particionadas)
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		OCSP (1.3.6.1.5.5.7.48.1)
	16.2. Access Location 1		http://ocspusu.cert.fnmt.es/ocspusu/OcspResponder	Sí		URL del servicio de 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		Certificado de la CA emisora: De la rfc 5280: "the idad- 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

Campo		Contenido	Oblig	Crit	Especificaciones
					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/ACUSU.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 persona física
17. Basic Constraints		Esta extensión sirve para identificar si el sujeto de certificación es una CA así como el máximo nivel de "profundidad" permitido para las cadenas de certificación".	Sí	Sí	De la rf5280: "This extension MAY appear as a critical or non-critical extension in end entity certificates.
	17.1. cA	Valor FALSE (entidad final)	Sí		De la rfc 5280: "The cA boolean indicates whether the certified public key may be used to verify certificate signatures."