



Real Casa de la Moneda
Fábrica Nacional
de Moneda y Timbre

DIRECCIÓN DE SISTEMAS DE INFORMACIÓN
DEPARTAMENTO CERES

DEFINICIÓN DE PERFILES CAS DE USUARIOS

v 2.1

Referencia:

Documento clasificado como: *Público*

Contenido

1.	Introducción	3
2.	Perfil CA Subordinada Persona Física	3
3.	Perfil Persona física	4

1. Introducción

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	Obligatorio
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. Organizational Unit	Denominación de la Unidad Organizativa ou = AC RAIZ FNMT-RCM	Sí
5.	Validity	15 años	Sí
6.	Subject		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. Organizational Unit	Denominación de la Unidad Organizativa ou= Ceres	Sí
	6.4. Common Name	cn= AC FNMT Usuarios	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 AC Subordinada FNMT Usuarios, codificada según el estándar PKCS#1 de RSA.	Sí
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
10.	Key Usage	Uso permitido de las claves certificadas.	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			Sí
		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) <code>ldap://ldapfnmt.cert.fnmt.es/CN=CRL,OU=AC%20RAIZ%20FNMT-RCM,O=FNMT-RCM,C=ES?authorityRevocationList;binary?base?objectclass=cRLDistributionPoint</code>		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				Sí
	13.1. cA	Valor TRUE (CA)		Sí
	13.2. pathLenConstraint	0		Sí
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)		Sí
	14.2. Acces Location 1	http://ocspfnmtrcmca.cert.fnmt.es/ocspfnmtrcmca/OcspResponder		Sí
	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
	14.4. Acces Location 2	http://www.cert.fnmt.es/certs/ACRAIZFNMTRCM.crt		Sí

3. Perfil Persona física

Campo		Contenido	Oblig
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. Organizational Unit	Denominación de la Unidad Organizativa ou= Ceres	Sí
	4.4. Common Name	cn= AC FNMT Usuarios	Sí
5.	Validity	4 años	Sí
6.	Subject	Identificación/descripción del titular de las claves certificadas	Sí
	6.1. Country	C=ES	Sí

	6.2. SerialNumber	NIF del titular	Sí
	6.3. Given Name	Nombre de pila, de acuerdo con documento de identidad	Sí
	6.4. Surname	Apellidos de acuerdo con documento de identificación	Sí
	6.5. Common Name	Apellidos, Nombre y NIF del titular	Sí
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
8. Subject Public Key Info	Clave pública del titular, codificada de acuerdo con el algoritmo criptográfico. En este caso RSA Encryption.		Sí
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
10. Key Usage	Uso permitido de las claves certificadas.		Sí
	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	Opcional
	11.2. Client Authentication	1.3.6.1.5.5.7.3.2	Sí
12. Qualified Certificate Statements	Extensiones cualificadas.		Sí
	12.1. QcCompliance	Certificado es cualificado.	Sí
	12.2. QcType	Qct-esign	Sí
	12.3. QcPDS	{ https://www.cert.fnmt.es/pds/PDSACUusuarios_es.pdf , es},{ https://www.cert.fnmt.es/pds/PDSACUusuarios_en.pdf , en}	Sí
	12.4. QcEuRetentionPeriod	15 años	Sí
13. Certificate Policies	Política de certificación		Sí
	13.1. Policy Identifier	1.3.6.1.4.1.5734.3.10.1	Sí
	13.2. Policy Qualifier Id		
	13.2.1. CPS Pointer	http://www.cert.fnmt.es/dpcs/	Sí
	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

	13.2.3. Policy Identifier	0.4.0.194112.1.0	Sí
14. Subject Alternative Names		Identificación/descripción del titular	Sí
	14.1. rfc822 Name	Correo electrónico del titular	Opcional
	14.2. Directory Name		
	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
	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
	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
	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
15. CRL Distribution Point			Sí
	15.1. Distribution Point 1	Punto de distribución 1 de la CRL ldap://ldapusu.cert.fnmt.es/CN=CRL<xxx*>, CN=AC%20FNMT%20Usuarios, OU=CERES, O=FNMT-RCM, C=ES?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint	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://ocspusu.cert.fnmt.es/ocspusu/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. Acces Location 2	http://www.cert.fnmt.es/certs/ACUSU.crt	Sí
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
	17.1. cA	Valor FALSE (entidad final)	Sí