Perfil de Certificado con Seudónimo Justicia

CTEAJE

Ficha del Documento

NOMBRE DEL DOCUMENTO	Perfil de Certificado con Seudónimo Justicia
CÓDIGO DEL DOCUMENTO	
VERSIÓN	1.0
CLASIFICACIÓN [1]	

Control de Versiones del Documento

VERSIÓN	AUTOR	FECHA	DESCRIPCIÓN
1.0	CTEAJE	18/10/2016	Versión aprobada en la CP de Asturias

[1] Los niveles de clasificación son:

A: Rojo - Prioritario: Obligado cumplimiento y clasificado de carácter urgente.

B: Naranja - Necesario: Obligado cumplimiento aún no clasificado urgente.

C: Verde - Recomendación: Cumplimiento conveniente pero no obligado.

Índice

1. CONSIDERACIONES GENERALES

1.1 Objeto

El presente documento describe el perfil de certificado de seudónimo para su uso en el ámbito de la Administración de Justicia.

En lo no expresamente descrito en este documento, se recomienda utilizar como guía orientativa el documento Perfiles de Certificados 2.0[2] (versión de mayo de 2016), que en el ámbito de la Administración General del Estado se ha publicado para favorecer la interoperabilidad en el empleo de certificados, especialmente en sus usos de firma electrónica y de sello electrónico.

En el conjunto de las administraciones públicas se ha hecho necesario actualizar las pautas de codificación de los perfiles de certificados por la vigencia de varias normativas, algunas muy recientes: Real Decreto 1671/2009 (con la modificación del Real Decreto 668/2015, de 17 de julio), Ley 39/2015 de 1 de Octubre, de Procedimiento Administrativo Común de las Administraciones Públicas, Ley 40/2015 de 1 de Octubre, de Régimen Jurídico del Sector Publico (LRJ) y Reglamento (UE) 910/2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior (eIDAS).

Para que los certificados sean cualificados, deberán cumplir el Reglamento UE 910/2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior, y su normativa de desarrollo, entre la que cabe destacar, en el plano técnico la norma EN 319 412 (dividida en 5 partes).

1.2 Alcance

De acuerdo al artículo 15.1 de las Bases del Esquema judicial de interoperabilidad y seguridad, cuando los Prestadores de Servicios de certificación emitan certificados de personal al servicio de la Administración de Justicia, o para los sistemas de firma electrónica o de sello electrónico automatizados, podrán incluir en los campos de unidad organizativa, la información necesaria para identificar adecuadamente al ente u órgano titular del sello, de conformidad con el artículo 20 de la Ley 18/2011, de 5 de julio.

El marco legal de referencia en la prestación de servicios de certificación ha sido hasta muy recientemente la Ley 59/2003, de 19 de diciembre, de firma electrónica. Sin embargo, con la aprobación del Reglamento (UE) 910/2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y su entrada en vigor en aspectos esenciales el 1 de julo de 2016, se han hecho evidentes algunos aspectos que requerirán una armonización reforzada en breve plazo.

Uno de ellos es la interpretación de los requisitos que determinan que un certificado tenga la consideración de cualificado.

Según el artículo 8 de la Ley 59/2003, de 19 de diciembre, de firma electrónica (apartado 2), el período de validez de los certificados electrónicos será adecuado a las características y tecnología empleada para generar los datos de creación de firma. En el caso de los

[2] https://administracionelectronica.gob.es/ctt/politicafirma/descargas

certificados reconocidos (cualificados con la denominación del Reglamento) este período no podrá ser superior a cinco años. En cambio, el Reglamento y su normativa de desarrollo no establecen una limitación al plazo de vigencia de los certificados cualificados.

Según el artículo 11 de la Ley 59/2003, de 19 de diciembre, de firma electrónica, los certificados reconocidos (cualificados con la denominación del Reglamento) incluirán entre otros datos, la identificación del firmante, en el supuesto de personas físicas, por su nombre y apellidos y su número de documento nacional de identidad o a través de un seudónimo que conste como tal de manera inequívoca y, en el supuesto de personas jurídicas, por su denominación o razón social y su código de identificación fiscal.

En cambio, el Reglamento y su normativa de desarrollo no establecen la exigencia del uso del número de documento nacional de identidad y, de hecho, prevén diferentes códigos identificadores según el documento identificativo aportado, lo que se refleja en la norma EN 319 412-1.

No obstante, en tanto no se publique la normativa que evite discrepancias de interpretación como las indicadas, en este documento se ha optado por definir un certificado de seudónimo que utilice como código identificador un número de identificación profesional construido con la misma regla que se define en la norma EN 319 412-1, de modo que, en el futuro, sirva también para certificados cualificados de personal al servicio de la Administración de Justicia sin que estos deban ser codificados como de seudónimo.

2. CARACTERIZACIÓN DE LOS PERFILES DE CERTIFICADOS DE EMPLEADO PÚBLICO CON SEUDÓNIMO EN EL ÁMBITO DE LA ADMINISTRACIÓN DE JUSTICIA

En este apartado se describen los campos que componen los perfiles de los certificados de empleado público con seudónimo.

CERTIFICADOS Y PERFILES	NIVEL MEDIO/SUSTANCIAL	NIVEL ALTO
Empleado público con seudónimo	Perfil de firma, autenticación y cifrado independiente o agregado según las necesidades del organismo. SW y HW	Perfil independiente para firma y autenticación con uso de dispositivo cualificado de creación de firma.

Tabla 1. Certificados y perfiles

2.1 Clasificación de campos/taxonomía

Para la interpretación de los campos son de aplicación las siguientes normas técnicas: X509 v3, X.501, X.520, RFC 3739, RFC 5280, EN 319 412.

Los campos singulares acordados para identificar al certificado de empleado público con seudónimo en el ámbito de la Administración de Justicia son:

- Fijos:
  - Descripción del tipo de certificado

- Datos de identificación (seudónimo, formado por el Número de identificación de personal) de titular del certificado
- Datos de identificación personal de titular del certificado
  - Nombre de pila
  - Primer apellido
  - Segundo apellido
- Nombre de la entidad a la que está adscrito el empleado
- NIF de la entidad
- Unidad a la que está adscrito el cargo o puesto que desempeña el empleado público
- Cargo o puesto de trabajo

- Opcionales
  - Dirección de correo electrónico

3. IDENTIFICADOR DE OBJETOS

Para facilitar la interoperabilidad con los certificados emitidos en el marco de la Administración General del Estado, se adopta el concepto de Identidad Administrativa para la vertebración de Identificadores de Objeto (Object Identifier, OID), y por tanto el objeto Identidad Administrativa definido en el siguiente arco: 2.16.724.1.3.5.X.X como base para identificarlo,

- 2.16.724.1.3.5.4.1= CERTIFICADO ELECTRÓNICO DE EMPLEADO PUBLICO CON SEUDÓNIMO (Nivel Alto)
- 2.16.724.1.3.5.4.2= CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO CON SEUDÓNIMO (Nivel Medio/Sustancial))

4. CERTIFICADO DE EMPLEADO PÚBLICO CON SEUDÓNIMO

Los certificados de firma electrónica y autenticación deberán ser acordes a la normativa europea, en concreto al Anexo I del Reglamento UE 910/2014 que especifica los requisitos para los certificados cualificados de persona física y su normativa de desarrollo. Los dispositivos calificados de creación de firma deberán alinearse con el Anexo II del citado Reglamento.

El Prestador de Servicios de Certificación deberá asignar Policy Identifier con OIDs diferentes para cada tipo de certificado. Especialmente deberá asignar OID distintos para los certificados de firma, identificación y cifrado.

4.1 Criterios de composición del campo CN para un certificado de empleado público con seudónimo en el ámbito de la Administración de Justicia

- Incluir obligatoriamente en el campo TITLE el PUESTO O CARGO o literal 'SEUDÓNIMO' (en caso de la Administración de Justicia, el CUERPO).
- Incluir obligatoriamente un SÍMBOLO o CARÁCTER que separe el cargo/literal del seudónimo del titular del certificado.
- Incluir obligatoriamente el SEUDÓNIMO (en caso de la Administración de Justicia, el Número de Personal en el ámbito de la Administración de Justicia precedido de los caracteres "JU:ES-", según lo definido en la norma EN319 412-1).
- Incluir obligatoriamente un SÍMBOLO o CARÁCTER que separe el seudónimo del organismo en que presta los servicios el titular del certificado.
- Incluir obligatoriamente el NOMBRE OFICIAL DEL ORGANISMO, tal y como figura en el boletín oficial correspondiente (en caso de la Administración de Justicia podrá tener dos valores: ADMINISTRACIÓN DE JUSTICIA o CONSEJO GENERAL DEL PODER JUDICIAL).
- No se podrá incluir nombre y apellidos (en caso de la Administración de Justicia se incluye el nombre y apellidos en la sección del certificado "Subject Alternative Names" con los Oid´s: 2.16.724.1.3.5.7.2.6 para el nombre, 2.16.724.1.3.5.7.2.7 para el primer apellido y 2.16.724.1.3.5.7.2.8 segundo apellido)[3].
- No se podrá incluir el número de DNI/NIE.
- Se podrá incluir opcionalmente un literal (AUTENTICACIÓN, FIRMA o CIFRADO) que identifique la tipología del certificado. Este identificador siempre estará al final del CN y entre paréntesis. En el caso de un nivel de aseguramiento medio/sustancial, si se agrupan varios perfiles en un único certificado, no se deberá incluir esta opción.

Ejemplos:

CARRERA JUDICIAL - JU:ES-J000001279 - CONSEJO GENERAL DEL PODER JUDICIAL

C. AUXILIO JUDICIAL - JU:ES-A000000011N - ADMINISTRACIÓN DE JUSTICIA

CARRERA FISCAL - JU:ES-F000002482E - ADMINISTRACIÓN DE JUSTICIA

4.2 Campos comunes a los niveles medio y alto

CAMPO	CONTENIDO	R	OBSERVACIONES
3. X.509v1 Field			-
3.1. Version	2 (= v3)	Sí	Integer:=2([RFC5280] describe la versión del certificado al usar extensiones, es decir, para v3 su valor debe ser 2)
3.2. Serial Number	Número identificativo único del certificado.	Sí	Integer. SerialNumber = p. ej: 111222. Establecido automáticamente por la Entidad de Certificación. [RFC5280]

[3] https://administracionelectronica.gob.es/ctt/politicafirma/descargas

CAMPO	CONTENIDO	R	OBSERVACIONES
			integer positivo, no mayor 20 octetos (1-2^{159}) Se utilizará para identificar de manera unívoca el certificado
3.3. Issuer Distinguished Name		Sí	Todos los campos destinados a identificar/describir el prestador de servicios serán codificados en formato UTF8
3.3.1. Country (C)	ES	Sí	C = p. ej: ES (PrintableString) Se codificará de acuerdo a "ISO 3166-1alpha-2 code elements" Size [RFC 5280] 3
3.3.2. Organization (O)	Denominación (nombre "oficial" de la organización) del prestador de servicios de certificación (emisor del certificado).	Sí	O = p. ej: MINISTERIO DE FOMENTO (String UTF8) Size [RFC 5280] 128
3.3.3. Locality (L)	Localidad/dirección del prestador de servicios de certificación		L = p. ej: MADRID (String UTF8) Size [RFC 5280] 128 Si bien el campo está estipulado para introducir la localidad, se contempla la posibilidad de incluir la dirección completa
3.3.4. Organizational Unit (OU)	Unidad organizativa dentro del prestador de servicios, responsable de la emisión del certificado.	Sí	OU = p. ej: AUTORIDAD DE CERTIFICACIÓN CERTICA (String UTF8) Size [RFC 5280] 128 Se contempla el nombre de la entidad que ha emitido el certificado
3.3.5. Serial Number	Número único de identificación de la entidad, aplicable de acuerdo con el país. En España, NIF.	*	NIF = NIF entidad suscriptora, p. ej: S2833002 (Printable String) Size = 9
3.3.6. Organization Identifier	Identificador de la organización Según la norma técnica ETSI EN 319 412-1 (VATES + NIF de la entidad)	*	Organization Identifier p. ej: VATESS2833002.
3.3.7. Common Name (CN)	Nombre común de la organización prestadora de servicios de certificación (emisor del certificado)	Sí	CN = p. ej: CERTICA Root CA (String UTF8) Size [RFC 5280] 80
3.4. Validity	Definido por el Prestador de Servicios Electrónicos de Confianza	Sí	Los datos de validez creados antes del 2050 se codificarán utilizando UTCTime. A partir del 2050 se utilizará la codificación GeneralizedTime en la cual se utilizan dos dígitos más para especificar el año (4 en lugar de 2)
3.4.1. Not Before	Fecha de inicio de validez	Sí	Fecha de inicio de validez, formato: UTCTime YYMMDDHHMMSSZ
3.4.2. Not After	Fecha de fin de validez	Sí	Fecha fin de validez, formato: UTCTime YYMMDDHHMMSSZ
3.5. Subject	Todos los campos destinados a identificar/describir al	Sí	Según la RFC5280 esta parte se ha de rellenar con carácter obligatorio

CAMPO	CONTENIDO	R	OBSERVACIONES
	custodio/responsable del certificado serán codificados utilizando UTF8		Según la ETSI-QC se debe reflejar obligatoriamente el campo Country Ver RFC3739 / ETSI 101862
3.5.1. Country (C)	Estado cuya ley rige el nombre, que será "España" por tratarse de entidades públicas.	Sí	C = p. ej: ES (PrintableString) Se codificará de acuerdo a “ISO 3166-1alpha-2 code elements” Size [RFC 5280] 3
3.5.2. Organization (O)	Denominación (nombre “oficial”) de la Administración, organismo o entidad de derecho público suscriptora del certificado, a la que se encuentra vinculada el empleado.	Sí	O = p. ej: MINISTERIO DE INTERIOR (String UTF8) Size [RFC 5280] 128 (En el caso de la ADMINISTRACIÓN DE JUSTICIA: “ADMINISTRACIÓN DE JUSTICIA”)
3.5.3. Organizational Unit (OU)	Descripción del tipo de certificado	Sí	OU = CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO CON SEUDÓNIMO (String UTF8) Size [RFC 5280] 128
3.5.4. Organizational Unit OU)	Unidad, dentro de la Administración, en la que está incluida el suscriptor del certificado		Unidad = p. ej: DIRECCIÓN GENERAL DE LA POLICÍA (String) Size [RFC 5280] 128 (En el caso de la ADMINISTRACIÓN DE JUSTICIA: “CONSEJO GENERAL DEL PODER JUDICIAL” o “ADMINISTRACIÓN DE JUSTICIA”)
3.5.5. Organizational Unit OU)	Código DIR3 de la unidad		OU = p. ej: E04976701
3.5.6. Pseudonym	Seudónimo Obligatorio según ETSI EN 319 412-2	Sí	Ej: NIP 111111111 (En el caso de la ADMINISTRACIÓN DE JUSTICIA: LETRA (1) - CÓDIGO PERSONAL (9) + DIGITO DE CONTROL (1). Por ejemplo:“JU:ES-L123456789W”)
3.5.7. Title	Debe incluir el puesto o cargo de la persona física, que le vincula con la Administración, organismo o entidad de derecho público suscriptora del certificado.		Title = p. Ej: SUBINSPECTOR. Nombre descriptivo del puesto o cargo que ostenta el responsable del certificado (String UTF8) Size [RFC 5280] 128 (En el caso de la ADMINISTRACIÓN DE JUSTICIA: Por ejemplo: Title=“CARRERA JUDICIAL“ o Title=“CARRERA FISCAL“ o Title=“C. LETRADOS DE LA ADMINISTRACIÓN DE JUSTICIA”)
3.5.8. Common Name (CN)	Se deben introducir el seudónimo y el organismo (Ver Criterios de Composición del campo CN para un empleado público con seudónimo).	Sí	Ej: SUBINSPECTOR – NIP 11111111 – DIRECCIÓN GENERAL DE POLICÍA (FIRMA) (String UTF8)) Size [RFC 5280] 132 (En el caso de la ADMINISTRACIÓN DE JUSTICIA: Por ejemplo: “C. LETRADOS DE LA ADMINISTRACIÓN DE JUSTICIA – JU:ES-L123456789W – ADMINISTRACIÓN DE JUSTICIA”)

CAMPO	CONTENIDO	R	OBSERVACIONES
3.6. Subject Public Key Info	Clave pública de la persona, codificada de acuerdo con el algoritmo criptográfico.	Sí	Campo para transportar la clave pública y para identificar el algoritmo con el cual se utiliza la clave. (String UTF8)

Tabla 2.Campos del certificado comunes a niveles medio y alto

(*) Se deberá incluir al menos uno de los campos SerialNumber u OrganizationIdentifier

4.2.1 Extensiones del certificado

CAMPO	CONTENIDO	R	OBSERVACIONES
4. X.509v3 Extensions			
4.1. Authority Key Identifier	Presente, de acuerdo con RFC 5280.		Medio para identificar la clave pública correspondiente a la clave privada utilizada para firmar un certificado, por ejemplo en los casos en que el emisor tiene múltiples claves de firma.
4.1.1. Key Identifier	Presente, de acuerdo con RFC 5280.		Identificador de la clave pública del emisor (String UTF8)
4.1.2. AuthorityCertIss uer	Path de identificación de certificación		Nombre de la CA a la que corresponde la clave identificada en keyIdentifier (String UTF8) Size 128
4.1.3. AuthorityCertSeri alNumber	Número de serie del certificado de CA		(Integer)
4.2. Subject Key Identifier	Presente, de acuerdo con RFC 5280.	Sí	Identificador de la clave pública del suscriptor o poseedor de claves (derivada de utilizar la función de Hash sobre la clave pública del sujeto). Medio para identificar certificados que contienen una clave pública particular y facilita la construcción de rutas de certificación.
4.3. cRLDistributionPoint		Sí	Indica cómo se obtiene la información de CRL.
4.3.1. distributionPoint	Punto de distribución de la CRL, número 1	Sí	Web donde resida la CRL (punto de distribución 1 -http. (String UTF8)
4.3.2. distributionPoint	Punto de distribución de la CRL, número 2		Web donde resida la CRL (punto de distribución 2 – http/https o con servidor autenticado). (String UTF8)
4.4. Authority Info Access		Sí	
4.4.1. Access Method	Id-ad-ocsp	Sí	ID de On-line Certificate Status Protocol
4.4.2. Access Location	(dirección web)	Sí	URL de On-line Certificate Status Protocol. Especifica el emplazamiento de la información (String UTF8)
4.4.3. Access Method	Id-ad-calssuers	Sí	ID de localización del certificado de la CA

CAMPO	CONTENIDO	R	OBSERVACIONES
4.4.4. Access Location	(dirección web)	Sí	URL de localización del certificado de la CA. Especifica el emplazamiento de la información (String UTF8)
4.5. Issuer Alternative Name	Nombre alternativo de la persona de contacto de la Entidad de Certificación emisora		
4.5.1. rfc822Name	Correo electrónico de contacto de la Entidad de Certificación emisora		Correo electrónico de contacto de la entidad de certificación emisora, p. ej: soporte.certica@mfom.es (String) Size [RFC 5280] 255

Tabla 3. Extensiones del certificado

Se incluye la información del apartado "2.4. Subject Alternate Names" correspondiente al perfil de empleado público sin seudónimo de nivel alto y del apartado "2.5. Subject Alternate Names" correspondiente al perfil de empleado público sin seudónimo de nivel medio/sustancial.

En particular:

- Nombre
- Primer apellido
- Segundo apellido

En el campo destinado a informar sobre el certificado "User notice" (2.4.2.2 correspondiente al perfil de empleado público con seudónimo de nivel alto y 2.5.2.2 correspondiente al perfil de empleado público con seudónimo de nivel medio/sustancial) se incluye la siguiente mención:

> *"Certificado cualificado de empleado público con seudónimo en el ámbito de la Administración de Justicia. 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)."*

5. CUADROS RESUMEN

Dentro del concepto **VALORES** se marcan entrecomillados y en negrita aquellos valores que deberán aparecer exactamente tal y como están aquí expresados en los campos/extensiones indicados.

CONCEPTO	OBLIGATORIO/ RECOMENDABLE	VALORES
Criterios de composición del campo CN para un certificado de empleado público con seudónimo	Obligatorios	• Incluir obligatoriamente el PUESTO O CARGO o literal 'SEUDÓNIMO', • Incluir obligatoriamente un SÍMBOLO o CARÁCTER que

CONCEPTO	OBLIGATORIO/ RECOMENDABLE	VALORES
		separe el cargo/literal del seudónimo del titular del certificado • Incluir obligatoriamente el SEUDÓNIMO, • Incluir obligatoriamente un SÍMBOLO o CARÁCTER que separe el seudónimo del organismo en que presta los servicios el titular del certificado • Incluir obligatoriamente el NOMBRE OFICIAL DEL ORGANISMO, tal y como figura en el boletín oficial correspondiente. • Se podrá incluir opcionalmente un literal (AUTENTICACIÓN, FIRMA o CIFRADO) que identifique la tipología del certificado. Este identificador siempre estará al final del CN y entre paréntesis. En el caso de un nivel de aseguramiento medio/sustancial, si se agrupan varios perfiles en un único certificado, no se deberá incluir esta opción. • (En el caso de la ADMINISTRACIÓN DE JUSTICIA: LETRA (1) - CÓDIGO PERSONAL (9) + DIGITO DE CONTROL (1). Por ejemplo: “JU:ES-L123456789W”)

Tabla 4. Composición campo CN para certificado de empleado público con seudónimo

CERTIFICADO	CAMPOS OBLIGATORIOS	VALORES
CERTIFICADO ELECTRÓNICO DE EMPLEADO PÚBLICO CON SEUDÓNIMO	• Version • Serial Number • Issuer Distinguished Name (Country (C), Organization (O), Organizational Unit (OU), Common Name (CN)) • Validity (Not Before, Not After) • Subject (Country (C), Organization (O), Organizational Unit (OU), Pseudonym, Common Name (CN)) • Subject Public Key Info • Signature Algorithm	• V3 • Número de serie • Nombre de la entidad emisora • Validez definida por el Prestador de Servicios Electrónicos de Confianza • C=”**ES**”, O=Organización, OU= “**CERTIFICADO ELECTRÓNICO DE EMPLEADO PUBLICO CON SEUDÓNIMO**”, seudónimo, CN=seudónimo + organismo • Clave pública del certificado • Algoritmo de Firma

Tabla 5.Certificado de empleado público con seudónimo – Campos obligatorios

CERTIFICADO	EXTENSIONES OBLIGATORIAS	VALORES
CERTIFICADO ELECTRÓNICO DE EMPLEADO PÚBLICO CON SEUDÓNIMO	• Authority Key Identifier • Subject Key Identifier • CRLDistributionPoint (distributionPoint,) • Authority Info Access (Access Method, Access Location del OCSP y de caIssuer) • Key Usage • Extended Key Usage • Qualified Certificate Statements • Certificate Policies (Policy Identifier, Policy Qualifier ID [CPS Pointer, User Notice], EU qualified certificate policy Identifier) • Subject Alternative Names (Directory Name)	• Identificador de la clave pública de la CA • Identificados de la clave pública del subscriptor • Información de acceso a la CRL • Información de acceso a OCSP, información de acceso al certificado de la CA emisora • Key Usage o FIRMA ALTO: **"Content Commitment"** o AUTENTICACIÓN ALTO: **"Digital Signature"** o CIFRADO ALTO: **"Key Encipherment", "Data Encipherment"** • FIRMA Y AUTENTICACIÓN NIVEL MEDIO/SUSTANCIAL: **"Digital Signature", "Content Commitment", "Key Encipherment",** Extended Key Usage o AUTENTICACIÓN ALTO: **"Email Protection", "Client Authentication"** o **CIFRADO ALTO**: **"Email Protection", "Client Authentication"** o FIRMA Y AUTENTICACIÓN NIVEL MEDIO/SUSTANCIAL: **"Email Protection", "Client Authentication"** • Qualified Certificate Statements o NIVEL ALTO FIRMA: **"QcCompliance", "QcEuRetentionPeriod", "QcSSCD", QcType- esign, QcPDS** o NIVEL MEDIO/SUSTANCIAL: **"QcCompliance", "QcEuRetentionPeriod", , QcType- esign, QcPDS** • OID asignado por el PSC a la política bajo la que se emite el certificado, URL de la DPC y mensaje explícito. . EU qualified certificate policy Identifier: o NIVEL ALTO FIRMA: QCP-nqscd o NIVEL MEDIO/SUSTANCIAL:

CERTIFICADO	EXTENSIONES OBLIGATORIAS	VALORES
		QCP-n • IDENTIDAD ADMINISTRATIVA EMPLEADO PUBLICO CON SEUDÓNIMO

Tabla 6.Certificado de empleado público con seudónimo – Extensiones obligatorias

(*) Las extensiones son de obligada inclusión en estos perfiles de certificados, pero deberán estar marcadas como no críticas dentro de los certificados, a menos que los estándares las establezcan como críticas.

CERTIFICADO	CAMPOS RECOMENDABLES	VALORES
CERTIFICADO ELECTRÓNICO DE EMPLEADO PÚBLICO CON SEUDÓNIMO	• Issuer Distinguished Name (Locality, Serial Number, Organization Identifier) • Subject (Organizational Unit (OU), Organization Identifier, Title)	• L= Localidad del PSC • SN= NIF del emisor • OI= Identificador de la organización según ETSI EN 319 412-1 • OU=Unidad del Empleado, • OI= Identificador de la organización según ETSI EN 319 412-1 • Title= Puesto o cargo del empleado
	•	•

Tabla 7.Certificado de empleado público con seudónimo – Campos recomendables

CERTIFICADO	EXTENSIONES RECOMENDABLES	VALORES
CERTIFICADO ELECTRÓNICO DE EMPLEADO PÚBLICO CON SEUDÓNIMO	• Issuer Alternative Name • Subject Alternative Names	• rfc822Name=Correo electrónico de la CA emisora • rfc822Name=Correo electrónico de contacto de la unidad (genérico), User Principal Name (UPN)=nombre de inicio de sesión en Windows

Tabla 8.Certificado de empleado público con seudónimo – Extensiones recomendables

CERTIFICADO	CAMPOS "IDENTIDAD ADMINISTRATIVA" FIJOS	VALORES
CERTIFICADO ELECTRÓNICO DE EMPLEADO PÚBLICO CON SEUDÓNIMO	• Tipo de certificado • Nombre de la entidad suscriptora • NIF entidad suscriptora • seudónimo	• OID: 2.16.724.1.3.5.4.x.1 = **"CERTIFICADO ELECTRÓNICO DE EMPLEADO PUBLICO CON SEUDÓNIMO"** • OID: 2.16.724.1.3.5.4.x.2 = Entidad Suscriptora (Organización) • OID: 2.16.724.1.3.5.4.x.3 = NIF entidad suscriptora • *OID: 2.16.724.1.3.5.4.x.12 = seudónimo del empleado* *Donde x tiene valor 1 para un Nivel de Aseguramiento Alto y 2 para Medio/Sustancial*

Tabla 9.Certificado de empleado público con seudónimo – Campos identidad administrativa fijos

CERTIFICADO	CAMPOS "IDENTIDAD ADMINISTRATIVA" OPCIONALES	
CERTIFICADO ELECTRÓNICO DE EMPLEADO PÚBLICO CON SEUDÓNIMO	• Número de identificación de personal • Correo electrónico • Unidad organizativa • Puesto o cargo	• OID2.16.724.1.3.5 .4.x.5 = NRP o NIP del empleado • OID: 2.16.724.1.3.5.4.x.9 = Correo electrónico del empleado • OID: 2.16.724.1.3.5.4.x.10 = Unidad del empleado • OID: 2.16.724.1.3.5.4.x.11 = Puesto o Cargo del empleado • *Donde x tiene valor 1 para un Nivel de Aseguramiento Alto y 2 para Medio/Sustancial*

Tabla 10. Certificado de empleado público con seudónimo – Campos identidad administrativa opcionales

6. ANEXO CODIFICACIÓN DEL NÚMERO PROFESIONAL PARA EL SEUDÓNIMO

El código de identificación de seudónimo (número profesional de la Administración de Justicia) estará formado por una letra correspondiente al CARGO y CUERPO, un valor numérico de 9 caracteres y una letra de control para minimizar errores de transcripción. A este código se le anteponen las letras JU:ES- para que el código sea compatible con lo indicado en la norma EN 319-412-1 apartado “5.1.3 Natural person semantics identifier”.

6.1 Cargo y letra relativa al Cuerpo

Se asignará CARGO y una letra dependiendo del tipo de profesional atendiendo a la siguiente tabla:

TIPO PROFESIONAL	LETRA ASIGNADA
C. AUXILIO JUDICIAL	A
C. E. AYUDANTE DE LABORATORIO DEL INTCF	Y
C. E. FACULTATIVO DEL INTCF	X
CARRERA FISCAL	F
C. GESTIÓN PROCESAL Y ADMINISTRATIVA	G
CARRERA JUDICIAL	J
C. LETRADOS DE LA ADMINISTRACIÓN DE JUSTICIA	L
C. N. MÉDICOS FORENSES	I
C. E. TÉCNICO ESPECIALISTA DE LABORATORIO INTCF	E
C. TRAMITACIÓN PROCESAL Y ADMINISTRATIVA	T

Tabla 11.Codificación tipos de profesional

Nota: las abreviaturas “C.” corresponden a Cuerpo, “C. E.” a Cuerpo Especial, “C. N.” a Cuerpo Nacional y “INTCF” a Instituto Nacional de Toxicología y Ciencias Forenses.

6.2 Número de identificación

Se utilizará un secuencial asignado a cada persona, según la ordenación establecida, y rellenado de tantos ceros a la izquierda como sea necesario hasta completar una longitud de 9 caracteres.

Los secuenciales se resetearán en cada tipo de profesional comenzando desde el número 1.

6.3 Dígito de Control

Se utiliza un dígito de control al final del código para evitar posibles errores en la gestión o intercambio de los códigos. El algoritmo usado para calcular dicho dígito, que en este caso

es una letra, vendrá dado de sustituir el resto resultante de la división del código (sin la letra del profesional) por 23, según la siguiente tabla:

RESTO	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
DC	R	W	A	G	M	Y	F	P	D	X	B	N	J	Z	S	Q	V	H	L	C	K	E	T

- Ejemplo obtención DG:

  Dado el siguiente código: JU:ES-J**000001279**

  - Se divide la parte numérica del código numérico entre 23:
  - 1279 / 23 = 55 ; Resto = 14
  - Se sustituye el resto obtenido por la letra correspondiente de la tabla de arriba:

    14 → S
  - Se añade el dígito de control al código, quedando de la siguiente manera:
  - CARRERA JUDICIAL - JU:ES-J000001279**S** - CONSEJO GENERAL DEL PODER JUDICIAL

6.4 Title

Los cargos son los indicados en la tabla anterior que se reproduce a continuación:

TIPO PROFESIONAL	LETRA ASIGNADA
C. AUXILIO JUDICIAL	A
C. E. AYUDANTE DE LABORATORIO DEL INTCF	Y
C. E. FACULTATIVO DEL INTCF	X
CARRERA FISCAL	F
C. GESTIÓN PROCESAL Y ADMINISTRATIVA	G
CARRERA JUDICIAL	J
C. LETRADOS DE LA ADMINISTRACIÓN DE JUSTICIA	L
C. N. MÉDICOS FORENSES	I
C. E. TÉCNICO ESPECIALISTA DE LABORATORIO INTCF	E
C. TRAMITACIÓN PROCESAL Y ADMINISTRATIVA	T

Tabla 12.Codificación tipos de profesional

Nota: las abreviaturas “C.” corresponden a Cuerpo, “C. E.” a Cuerpo Especial, “C. N.” a Cuerpo Nacional y “INTCF” a Instituto Nacional de Toxicología y Ciencias Forenses.

6.5 Unidad Organizativa

Por defecto, se ha establecido como organismo de pertenencia la “ADMINISTRACIÓN DE JUSTICIA”, salvo en el caso de Jueces y Magistrados para los que debe figurar en su lugar “CONSEJO GENERAL DEL PODER JUDICIAL”.

6.6 CommonName

Formado por la concatenación de CARGO, CÓDIGO y ORGANIZACIÓN, separados por espacio, guión alto y espacio.

COMMON NAME = ${TITLE} + ‘ - ’ + ‘JU:ES’ + ‘-’ + ${ID} + ‘ - ’ + ‘${**ORGANIZATIONAL UNIT**}’

Ejemplos:

CARRERA JUDICIAL - JU:ES-J000002500J - CONSEJO GENERAL DEL PODER JUDICIAL