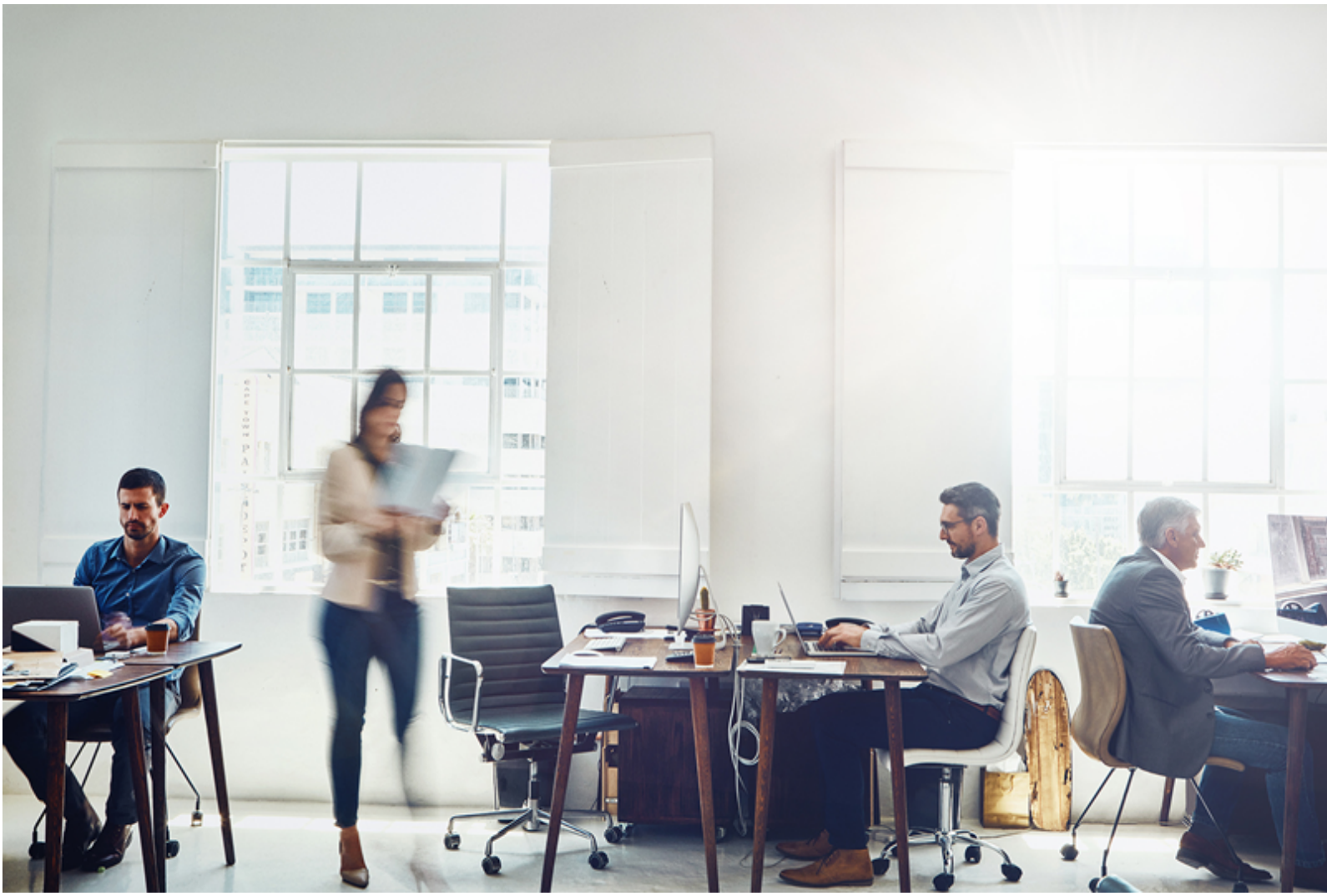
Documento Perfiles de los Certificados de Firmaprofesional

Perfiles de certificados no cualificados de la raíz cualificada de Firmaprofesional

Versión: 220314

Clasificación: Público



BARCELONA
EDIF. ESADECREAPOLIS
AV. TORRE BLANCA, 57 - LOCAL M2
08173 SANT CUGAT DEL VALLÈS
+34 934 774 245

MADRID
VELÁZQUEZ 59, 1º CTRO.-IZDA.
28001 MADRID
+34 915 762 181

WWW.FIRMAPROFESIONAL.COM

Histórico de versiones

Versión	Sección y cambios	Fecha
210628	Versión inicial adaptada conforme a la Ley 6/2020	28/06/2021
220314	• Incorporación de EKU "Adobe Authentic Documents Trust"	14/03/2022

Índice

1. Introducción **4**

2. Perfiles de la autoridad de certificación CFEA **5**

2.1. Perfil de los certificados de firma electrónica avanzada (CFEA) 6

2.1.1. Nombre Distinguido (DN) 6

2.1.2. Extensiones de los certificados 7

3. Perfiles de la autoridad de certificación OTC **8**

3.1. Perfil de los certificados de un solo uso (OTC) 8

3.1.1. Nombre Distinguido (DN) 8

3.1.2. Extensiones de los certificados 9

1. Introducción

En el presente documento se describen los perfiles de los certificados privados emitidos por Firmaprofesional como Prestador de Servicios de Certificación.

Para la elaboración de los Perfiles de los Certificados se ha tenido en cuenta las siguientes disposiciones:

- Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE (de ahora en adelante, eIDAS)
- Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.
- Política de Firma y de Certificados de la Administración General del Estado:. Anexo 2: Perfiles de certificados electrónicos.
- ETSI EN 319 412 Electronic Signatures and Infrastructures (ESI); Certificate Profiles
- "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates" publicada en https://wwww.cabforum.org/

Los perfiles de los diferentes certificados emitidos por Firmaprofesional se agrupan de la siguiente forma, en función de las Políticas a las que van asociados:

A. Certificados de Firma Electrónica Avanzada (CFEA), que se emiten bajo la Autoridad de Certificación Subordinada Privada AC Firmaprofesional - CFEA 2020

B. Certificados de un solo uso (OTC), emitidos bajo la Autoridad de Certificación Subordinada Privada AC Firmaprofesional - OTC 2020

2. Perfiles de la autoridad de certificación CFEA

El perfil del certificado de CA Subordinada Privada AC Firmaprofesional - CFEA que está vigente es el siguiente:

- CN = AC Firmaprofesional - CFEA 2020
- Hash SHA1: 63957dbde8b5fa714ad34c0dd49bc141c604833f
- Válido desde el 30 de julio de 2020 hasta el 31 de diciembre de 2030
- Tipo de Clave: RSA 2048 bits - SHA256
- Restricciones técnicas (extendedKeyUsage):
    - Autenticación del cliente (1.3.6.1.5.5.7.3.2)
    - Inicio de sesión de tarjeta inteligente (1.3.6.1.4.1.311.20.2.2)
    - Adobe Authentic Documents Trust (1.2.840.113583.1.1.5)

2.1. Perfil de los certificados de firma electrónica avanzada (CFEA)

2.1.1. Nombre Distinguido (DN)

Campo del DN	Nombre	Descripción
CN, Common Name	Nombre	*Nombre y apellidos del firmante*
serialNumber	Número de serie	*NIF, NIE o número de pasaporte del firmante*[1]. *Ej: "IDCES-123456789Z"*
GN, givenName	Nombre de pila	*Nombre de pila del firmante tal y como aparece en el documento de identidad utilizado*
SN, surName	Apellidos	*Apellidos del firmante tal y como aparecen en el documento de identidad utilizado*
T, Title (opcional)	Cargo, título o especialidad	*Cargo, título o especialidad del firmante*
O, Organization	Organización	*Nombre del suscriptor (empresa o entidad privada o pública) con la que existe una vinculación con el firmante. Se rellena automáticamente.*

[1] En caso de que el firmante no disponga de NIF o NIE, se indicará el Número de Pasaporte en el formato indicado en el apartado correspondiente de la CPS. Se seguirá la codificación acorde a ETSI EN 319 412-1

2.1.2. Extensiones de los certificados

Extensión	Crítica	Valor
X509v3 Basic Constraints	Sí	CA:FALSE
X509v3 Key Usage	Sí	Digital Signature Content Commitment Key Encipherment
X509v3 Extended Key Usage	-	TLS Web Client Authentication Adobe Authentic Documents Trust (1.2.840.113583.1.1.5)
X509v3 Subject Key Identifier	-	*<id de la clave pública del certificado, obtenido a partir del hash de la misma>*
X509v3 Authority Key Identifier	-	*<id de la clave pública del certificado de la CA, obtenido a partir del hash de la misma>*
X509v3 CRL Distribution Points	-	*<URI de la CRL>*
X509v3 Certificate Policies	-	*<OID de la política de certificación correspondiente al certificado>* 1.3.6.1.4.1.13177.100.2 *<URI de la CPS>* User Notice: "Éste es un certificado de firma electrónica no cualificado para uso en entornos privados"
X509v3 Authority Information Access	-	Access Method: Id-ad-ocsp Access Location: <URI de acceso al servicio OCSP> Access Method: Id-ad-calssuers Access Location: <URI de acceso al certificado de la CA emisora>

3. Perfiles de la autoridad de certificación OTC

El perfil del certificado de CA Subordinada Privada AC Firmaprofesional -OTC que está vigente es el siguiente:

- CN = AC Firmaprofesional - OTC 2020
- Hash SHA1: 32adc15e7b31648da5fe3d0009e2a107cfe08b91
- Válido desde el 30 de julio de 2020 hasta el 31 de diciembre de 2030
- Tipo de Clave: RSA 2048 bits - SHA256
- Restricciones técnicas (extendedKeyUsage):
    - Autenticación del cliente (1.3.6.1.5.5.7.3.2)
    - Inicio de sesión de tarjeta inteligente (1.3.6.1.4.1.311.20.2.2)
    - Adobe Authentic Documents Trust (1.2.840.113583.1.1.5)

3.1. Perfil de los certificados de un solo uso (OTC)

3.1.1. Nombre Distinguido (DN)

El DN de los certificados contendrá como mínimo los elementos que se citan con el formato siguiente:

Campo del DN	Requerido	Descripción
CN, Common Name	Si	*Nombre y apellidos del firmante*
serialNumber	Si	*NIF, NIE o número de pasaporte del firmante*
E, email	No	Mail del firmante
OU	No	*DocumentHash. En formato SHA-1 o SHA-256*
OU	No	*DeviceMac.* MAC del dispositivo de firma

3.1.2. Extensiones de los certificados

Extensión	Crítica	Valor
X509v3 Basic Constraints	Sí	CA:FALSE
X509v3 Key Usage	Sí	Content Commitment
X509v3 Extended Key Usage	-	Adobe Authentic Documents Trust (1.2.840.113583.1.1.5)
X509v3 Subject Key Identifier	-	*<id de la clave pública del certificado, obtenido a partir del hash de la misma>*
X509v3 Authority Key Identifier	-	*<id de la clave pública del certificado de la CA, obtenido a partir del hash de la misma>*
X509v3 CRL Distribution Points	-	*<URI de la CRL>*
X509v3 Certificate Policies	-	*<OID de la política de certificación correspondiente al certificado>* 1.3.6.1.4.1.13177.101.2 *<URI de la CPS>* User Notice: "Single-use certificate exclusive for handwritten signatures performed on " + <nombre_RA>
X509v3 Authority Information Access	-	Access Method: Id-ad-ocsp Access Location: <URI de acceso al servicio OCSP> Access Method: Id-ad-calssuers Access Location: <URI de acceso al certificado de la CA emisora>