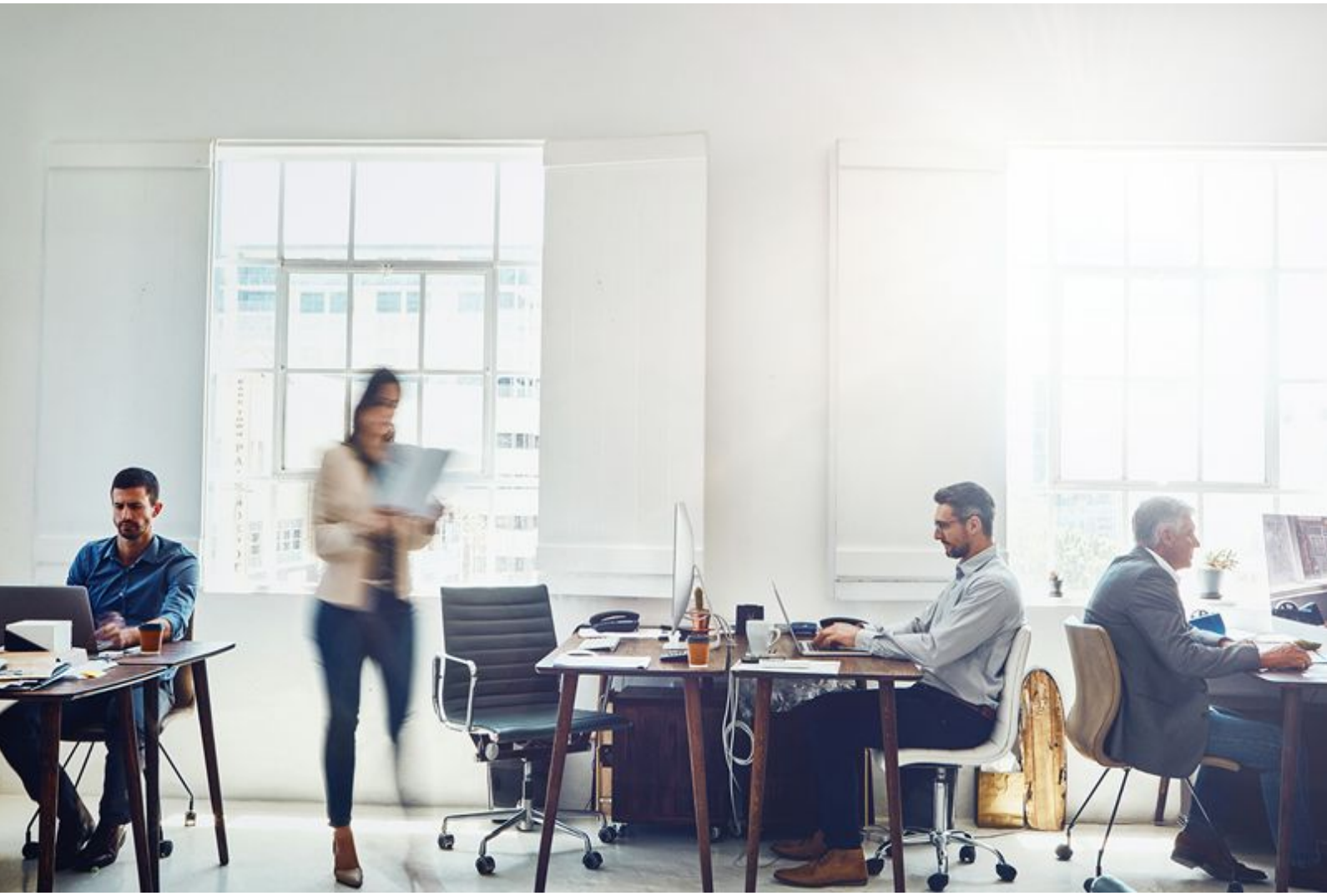
Política de Certificación

Certificados de Servicio Seguro

Versión: 210217

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 de publicación
6.0	(para consultar cambios entre versiones anteriores, por favor envíe un correo a info@firmaprofesional.com)	15/04/2014
190121	Adición de los certificados de CA. Segregación por certificados de servicio TSA, VA y CA, y diferenciación de certificados destinados a servicios cualificados Eliminación de extensiones de Perfiles de certificado para incorporarlo en documento "Perfiles de Certificados de Firmaprofesional" Inclusión de causas de revocación de certificados de CA, como requisito del CAB/Forum Actualización de la Plantilla del documento	21/01/2019
190227	Se habilita la opción de certificados de VA no cualificada sin extensión noCheck, aumentando su vigencia hasta 6 años.	27/02/2019
200806	Los certificados de QTSA pasan a ser emitidos por la CA AC Firmaprofesional - CUALIFICADOS.	06/08/2020
210217	• Adaptación a la nueva Ley 6/2020, reguladora de determinados aspectos de los servicios electrónicos de confianza.	17/02/2021

Índice

1. Introducción

1.1. Descripción General

Los Certificados de Servicio Seguro son certificados que permiten firmar evidencias digitales como Autoridad de Certificación (CA). Su emisión y utilización requerirá las máximas garantías de seguridad.

Los Certificados de Servicio Seguro se emitirán únicamente a entidades de reconocido prestigio que establezcan un acuerdo de colaboración previo con Firmaprofesional. Estas entidades deberán disponer de un dispositivo HSM certificado FIPS 140-2 Nivel 3 para la custodia de las claves privadas del certificado.

Firmaprofesional podrá emitir Certificados de Servicio Seguro Cualificados y No Cualificados según lo definido en el Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014.

Dentro de cada grupo (cualificados y no cualificados) se incluyen los distintos tipos de certificado de servicio seguro:

- Certificados de CA
- Certificados de Validación (VA)
- Certificados de Sellado de Tiempo (TSA)

En el presente documento se exponen las Condiciones Particulares referentes a estos tipos de certificados. Esta Política de Certificación está subordinada al cumplimiento de las Condiciones Generales expuestas en la Declaración de Prácticas de Certificación (CPS) de Firmaprofesional.

1.2. Identificación del Documento

Nombre:	Política de Certificación de Certificados de Servicio Seguro
Versión:	210217
Descripción:	Política de Certificación para Certificados de Servicio Seguro No Cualificados (CA, VA, TSA). y para Certificados de Servicio Seguro cualificados (QCA, QVA, QTSA).
Fecha de Emisión:	17/02/2021
OIDs	• CA: 1.3.6.1.4.1.13177.10.10.2 • VA: 1.3.6.1.4.1.13177.10.1.31.2 • TSA: 1.3.6.1.4.1.13177.10.1.4.2 • QCA: 1.3.6.1.4.1.13177.10.1.10.1 • QVA: 1.3.6.1.4.1.13177.10.1.31.1 • QTSA: 1.3.6.1.4.1.13177.10.1.4.1
Localización	http://www.firmaprofesional.com/cps

2. Entidades Participantes

2.1. Autoridades de Certificación (CA)

Los certificados de servicio seguro serán emitidos por las siguientes autoridades de certificación:

- Los de CA serán emitidos por la CA root de Firmaprofesional.
- Los de TSA los emite la CA AC Firmaprofesional - CUALIFICADOS (en versiones anteriores de este documento se emitían desde la CA AC Firmaprofesional - INFRAESTRUCTURA).
- Los de VA los emite la misma CA que emite los certificados de Entidad Final objeto de la validación

La gestión de las solicitudes y emisiones de los certificados será realizada directamente por Firmaprofesional.

Firmaprofesional establecerá:

- Qué criterios se deben cumplir para solicitar un certificado.
- Los mecanismos y procedimientos necesarios para realizar la identificación y autenticación del suscriptor, cumpliendo con lo estipulado en la CPS.

2.2. Solicitante

Estos certificados se emitirán únicamente a entidades de reconocido prestigio que establezcan un acuerdo de colaboración previo con Firmaprofesional.

2.3. Suscriptor

El suscriptor de estos certificados será la entidad que aparezca identificada en el certificado

2.4. Tercero que confía en los certificados

Los terceros que confíen en estos certificados deben tener presentes las limitaciones en su uso.

3. Características de los certificados

3.1. Periodo de validez de los certificados

Perfil	Cualificados	No Cualificados
CA	Mínimo 12 años	Mínimo 12 años
VA	1 año	• 1 año con extensión noCheck • Hasta 6 años sin extensión noCheck
TSA	Certificado: 6 años Uso de clave privada: 3 años[1]	Certificado y clave privada: 6 años

3.2. Uso particular de los certificados

3.2.1. Uso apropiado de los certificados

Estos certificados podrán usarse en los términos establecidos por la CPS, y lo establecido en la legislación vigente al respecto.

Los certificados CA y QCA podrán usarse con los siguientes propósitos:

- Garantizar la integridad de los certificados emitidos
- Identificar a la entidad firmante del certificado

Los certificados de VA y QVA podrán usarse con los siguientes propósitos:

- Garantizar la integridad de las respuestas OCSP
- Identificar a la entidad firmante

Los certificados de TSA y QTSA podrán usarse con los siguientes propósitos:

- Garantizar la integridad de los sellos de tiempo emitidos
- Identificar a la entidad firmante

[1] Firmaprofesional renovará el certificados de QTSA cada tres años.

3.2.2. Usos no autorizados de los certificados

No se permite la utilización distinta de lo establecido en esta Política y en la Declaración de Prácticas de Certificación.

Los certificados CA y QCA que no sean de Firmaprofesional no pueden emitir certificados de autenticación Web (SSL) en ninguna de sus modalidades incluidos los de Sede electrónica. Para evitarlo, estos se emitirán "Technically Constrain".

4. Procedimientos operativos

4.1. Proceso de emisión de certificados

El proceso de emisión de todas las modalidades de certificado de servicio seguro será operado manualmente por el Director Técnico de Firmaprofesional, como operador autorizado.

4.1.1. Solicitud de certificados

Estos certificados se emitirán únicamente a entidades de reconocido prestigio que establezcan un acuerdo de colaboración previo con Firmaprofesional.

El solicitante deberá contactar directamente con Firmaprofesional, proporcionando toda la documentación necesaria para verificar la identidad de la persona jurídica.

El Director Técnico de Firmaprofesional verificará el cumplimiento de los requisitos de seguridad para la infraestructura propuesta.

4.1.2. Aceptación de solicitudes

Firmaprofesional únicamente aceptará las solicitudes que cumplan con los requisitos establecidos para cada uno de los tipos de certificado.

Requisitos comunes a todos los certificados de servicio seguro:

- Documento firmado manual o digitalmente, por el Responsable Legal de la corporación por el que se autorice la emisión de estos certificados.
- En el caso que la corporación sea la propia Firmaprofesional, bastará con la aprobación del Director Técnico.

4.1.3. Tramitación de las Solicitudes

Firmaprofesional verificará la identidad y capacidad operativa de la entidad solicitante.

Si la información aportada en la solicitud es incorrecta o insuficiente, la RA denegará la petición, contactando con el solicitante para comunicarle el motivo. En caso contrario, se procederá a la firma del instrumento jurídico vinculante entre el suscriptor y/o el solicitante y Firmaprofesional.

De forma adicional a lo especificado en la CPS de Firmaprofesional para la emisión de certificados digitales:

- El procedimiento de emisión de estos certificados requerirá la supervisión directa del Departamento Técnico de Firmaprofesional.
- El proceso de emisión de estos certificados se realizará de manera manual siguiendo las máximas garantías de seguridad en el proceso.
- El acceso físico a los componentes del sistema del TSP cuya seguridad sea crítica para la prestación de sus servicios de confianza estará limitado a las personas autorizadas.

4.1.3.1. Certificados VA, QVA, TSA y CA

La generación de las claves de firma de respuestas OCSP debe llevarse a cabo en un espacio seguro, en dispositivos criptográficos hardware (HSM 140-2 Nivel 3) por personal adecuado según los roles de confianza.

La suite criptográfica escogida para cada tipo de certificados será la considerada segura en el momento de su emisión, para la duración del certificado emitido. La referencia para dicha consideración será la norma ETSI TS 119 312 en la versión vigente en el momento de emisión del certificado, o norma equivalente.

4.1.3.2. Certificados QCA / QTSA

Adicionalmente, se incluirá al menos con un control dual y testigos de Firmaprofesional, de la organización titular de la CA y del auditor externo. Además toda la actividad relativa a la generación de claves de los certificados de QCA quedará registrada en una acta notarial.

En el caso de TSA y QTSA, la clave privada generada para una TSU sólo se podrá importar a otros módulos criptográficos con fines de ofrecer Alta Disponibilidad del servicio

El Director Técnico de Firmaprofesional gestionará la obtención telemática del certificado, quedando las claves y certificado generados custodiados en el HSM.

4.2. Revocación de certificados

Debido a las especiales características de este tipo de certificados, su revocación requerirá la autorización del Director Técnico o del Director de Innovación, Cumplimiento y Tecnología de Firmaprofesional.

Este procedimiento es aplicable a todas las políticas incluidas en este documento.

En concreto, Firmaprofesional revocará un certificado de CA subordinada en un plazo de siete (7) días si ocurre algún hecho siguiente:

1. La CA subordinada solicita la revocación por escrito;
2. La CA subordinada notifica a Firmaprofesional que la solicitud original de certificado no fue autorizada y no concede retroactivamente la autorización;
3. Firmaprofesional obtiene pruebas de que la clave privada de la CA subordinada correspondiente a la clave pública en el certificado sufrió un compromiso clave o ya no cumple con los requisitos de tamaño de clave o de parámetros de clave pública y de calidad;
4. Firmaprofesional obtiene pruebas de que el certificado fue utilizado fraudulentamente;
5. Firmaprofesional es consciente de que el certificado no se emitió debidamente o la CA Subordinada no ha cumplido con esta política de certificación o con la Declaración de Prácticas de Certificación;
6. Firmaprofesional determina que alguna información que aparece en el certificado es falsa o incorrecta.
7. Firmaprofesional o la CA subordinada cesa las operaciones por cualquier razón y no ha acordado con otra CA para que proporcione el soporte de revocación para el certificado;
8. El derecho de Firmaprofesional o de la CA subordinada de emitir certificado bajo los requerimientos de esta Política ha caducado, se ha revocado o ha terminado, a menos que Firmaprofesional haya llegado a acuerdos con otra entidad para que ésta siga manteniendo el Repositorio CRL/OCSP;
9. La revocación es requerida por la Declaración de Prácticas de Certificación de Firmaprofesional.

4.3. Renovación de certificados

La renovación de todas las modalidades de certificado incluidas en esta política, implicará necesariamente realizar el proceso de generación de un nuevo certificado. Esta emisión deberá llevarse a cabo antes de la expiración del anterior, aplicándose todas las acciones necesarias para evitar la disrupción de las operaciones. El nuevo certificado se emitirá de acuerdo con los requisitos de esta política.

5. Perfil de los certificados

Al amparo de las prescripciones contenidas en la presente Política de Certificación se emiten los siguientes tipos de certificados, con sus OID asociados

TIPO DE CERTIFICADO	OID
Certificado de Autoridad de Certificación (CA)	1.3.6.1.4.1.13177.10.10.2
Certificado de Validación (VA)	1.3.6.1.4.1.13177.10.1.31.2
Certificado de Sello de Tiempo (TSA)	1.3.6.1.4.1.13177.10.1.4.2
Certificado Cualificado de Autoridad de Certificación (QCA)	1.3.6.1.4.1.13177.10.1.10.1
Certificado Cualificado de Validación (QVA)	1.3.6.1.4.1.13177.10.1.31.1
Certificado Cualificado de Sello de Tiempo (QTSA)	1.3.6.1.4.1.13177.10.1.4.1

Las extensiones utilizadas por cada tipo de certificado emitidos bajo la presente política se publican en el documento denominado "Perfiles de los certificados de Firmaprofesional" en la web de Firmaprofesional (http://www.firmaprofesional.com/cps).

firmaprofesional

Firmaprofesional, S.A.

Febrero de 2021