AUTORIDAD DE VALIDACIÓN (VA) DE FIRMAPROFESIONAL

Política de Servicio

Versión: 170405
Clasificación: Público

ATENCIÓN: El original vigente de este documento se encuentra en formato electrónico en la web de Firmaprofesional: https://www.firmaprofesional.com/cps

Histórico de versiones

Versión	Cambios	Fecha publicación
6.2	(para consultar cambios entre versiones anteriores, por favor envíe un correo a info@firmaprofesional.com)	20/05/2014
170405	Reestructuración del documento para la adaptación del servicio a los requerimientos de eiDAS	05/04/2017

Índice

1. INTRODUCCIÓN

1.1. Descripción General

Firmaprofesional es un Prestador de Servicios de Confianza que emite certificados cualificados según REGLAMENTO (UE) No 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.

Este documento tiene como objetivo describir el funcionamiento de los **Servicios de Validación de Certificados Digitales** ofrecidos por Firmaprofesional y establecer las condiciones de uso, obligaciones y responsabilidades de las distintas entidades involucradas.

Esta Política de Validación de Certificados 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 del Servicio de Validación de Certificados
Versión:	170322
Descripción:	Política del Servicio de Validación de Certificados de la Autoridad de Validación de Firmaprofesional (VA)
Fecha de Emisión:	22/03/2017
OIDs	1.3.6.1.4.1.13177.30.0.1
Localización	http://www.firmaprofesional.com/cps

2. RESUMEN

Los Servicios de Validación de certificados ofrecidos por Firmaprofesional permiten a un cliente conocer la validez de un determinado certificado digital en un momento dado.

Firmaprofesional es una Autoridad de Validación (VA o *Validation Authority*) que actúa como tercera parte de confianza validando certificados electrónicos, tanto emitidos por la propia Firmaprofesional como por otras entidades reconocidas.

Firmaprofesional ofrece diferentes servicios de validación. Algunos servicios de validación no son públicos, por lo que será necesario contratar los servicios previamente con Firmaprofesional.

Firmaprofesional no almacenará copias de las peticiones de validación a menos que se contrate previamente el servicio de custodia de peticiones OCSP.

Servicios Públicos:

- **Listas de Certificados Revocados (CRLs)**: Firmaprofesional hace público el estado de sus certificados emitiendo y publicando CRLs en servidores Web. El funcionamiento del servicio de CRLs está definido en el documento "Declaración de Prácticas de Certificación de Firmaprofesional (CPS)" en http://www.firmaprofesional.com/cps

- **Servicio OCSP público:** Firmaprofesional hace público el estado de sus certificados firmado peticiones OCSP.

Servicios Privados:

- **Servicio OCSP Privado** Servicio privado de OCSP para los certificados emitidos por Firmaprofesional. Este servicio requiere de un contrato con el cliente y ofrece garantías adicionales de disponibilidad y de soporte.

- **Servicio OCSP Privado con Custodia de Evidencias:** Este servicio es idéntico al anterior salvo que en este caso, Firmaprofesional almacena y custodia una copia de cada evidencia digital generada y la pone a disposición del cliente en caso necesario.

- **Servicio OCSP de otros prestadores:** Firmaprofesional ofrece un servicio de centralización de peticiones OCSP hacia otros prestadores de certificación, de tal manera que accediendo a un único punto de acceso, se redirigen la peticiones al servicio OCSP correspondiente de cada prestador.

3. DEFINICIONES Y ABREVIATURAS

3.1. Definiciones

- **Prestador de Servicios de Confianza (PSC)**: persona física o jurídica que presta uno o más servicios de confianza, bien como prestador cualificado o como prestador no cualificado de servicios de confianzas
- **Autoridad de Certificación (CA)**: Entidad utilizada por un PSC para emitir certificados digitales
- **Autoridad de Validación**: Entidad de confianza que proporciona información sobre la validez de los certificados digitales y de las firmas electrónicas.
- **Listas de Certificados Revocados (CRL)**: Fichero donde figura una lista de certificados revocados o suspendidos por una Autoridad de Certificación.
- **Lista de Autoridades Revocadas (ARL)**: Tipo especial de CRL emitida por una CA Raíz en la que figuran las lista de Autoridades de Certificación revocadas dentro de la Jerarquía de Certificación.
- **Protocolo OCSP:** Protocolo de comunicaciones estándar que permite realizar una consulta sobre el estado de un certificado concreto y obtener una respuesta por parte de una Autoridad de Validación
- **Módulo Criptográfico Hardware**: módulo hardware utilizado para realizar funciones criptográficas y almacenar claves en modo seguro.

3.2. Abreviaturas

ARL	*Authority Revocation List*
CA	Autoridad de Certificación
CEN	Comité Europeo de Normalización
CRL	*Certificate Revocation List*
CWA	*CEN Workshop Agreement*
FIPS	*Federal Information Processing Standards*
HSM	*Hardware Security Module*
IETF	*Internet Engineering Task Force*
OCSP	*Online Certificate Status Protocol*
PSC	Prestador de Servicios de Certificación
RFC	*Request for comment*
VA	Autoridad de Validación

4. CONCEPTOS GENERALES

4.1. Autoridad de Validación (VA)

Una Autoridad de Validación (VA) es un Prestador de Servicios de Confianza que proporciona certeza sobre la validez de los certificados digitales y sobre los documentos firmados electrónicamente en un momento dado.

4.2. Validación de Certificados Digitales

Para validar una firma electrónica o un certificado digital es necesario seguir los procedimientos descritos en el estándar RFC5280 Internet X.509 *Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*. Siguiendo este estándar validar técnicamente cualquier certificado digital, aunque para ello necesitaremos dos datos adicionales:

- Conocer el certificado de la CA que ha emitido el certificado, para verificar que ha sido emitido por una CA de confianza
- Conocer el estado actual del certificado, para verificar que no ha sido revocado

Para los certificados de autenticación de sitio web, el servicio de VA de Firmaprofesional cumple lo establecido en los *Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates* vigentes en el momento de entrada en vigor de la presente política de servicio, y transfiere la responsabilidad del cumplimimiento de los mismos para el caso de certificados emitidos por otros PSCs.

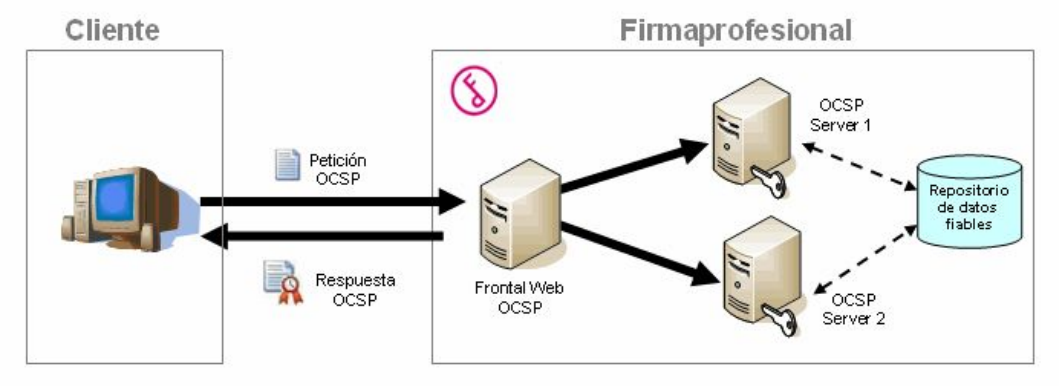
4.3. Servicio de Validación de Certificados

El Servicio de Validación de Certificados de Firmaprofesional se basa en el uso del protocolo OCSP sobre HTTP, definido en la norma RFC6960 *Online Certificate Status Protocol – OCSP*.

Los pasos a seguir para generar una petición de validación son los siguientes:

- El cliente selecciona un certificado digital para validar
- El cliente envía una petición de validación a una URL determinada de Firmaprofesional siguiendo el protocolo RFC6960 OCSP *over HTTP*, indicando el número de serie del certificado y la Autoridad de Certificación emisora del mismo
- Firmaprofesional recibe la petición, realiza un control de acceso del cliente y revisa si la petición está completa y correcta.
- Si el resultado es correcto, la VA consulta el estado actual del certificado (válido, revocado o desconocido) en su repositorio de datos fiables o reenviando la consulta a la Autoridad de Certificación emisora del mismo.

- La VA genera una respuesta con los datos fiable firmada en formato OCSP o se reenvía la respuesta obtenida de la Autoridad de Certificación emisora del mismo
- La respuesta OCSP se envía de vuelta al Cliente
- El Cliente puede validar la respuesta y, si lo cree necesario, almacenarla para futuras validaciones.
- Si se ha contratado el servicio de custodia, la VA mantendrá un registro de las respuestas generadas a disposición del cliente para su futura verificación.



4.4. Clientes

Los clientes deben adaptar sus sistemas para poder realizar peticiones de validación mediante el protocolo OCSP. Firmaprofesional no proporciona ningún software ni librerías de integración al cliente para realizar estas funciones.

Existen librerías públicas que implementan el protocolo OCSP en diversos lenguajes de programación:

- **CryptoAPI de Microsoft**: Las librerías criptográficas de Microsoft incluyen soporte protocolo OCSP por defecto en su plataforma .NET
- **BouncyCastle** (*http://www.bouncycastle.org*) y **Novosec Extensions** (*http://sourceforge.net/projects/novosec-bc-ext*) : Conjunto de librerías criptográficas que implementan el protocolo OCSP en los lenguajes Java y C#
- **OpenSSL** (http://www.openssl.org): Es una ampliación de la librería criptográfica OpenSSL que implementa el protocolo OCSP en lenguaje C.
- **IAIK:** Incluye librerías criptográficas en Java que implementan el protocolo OCSP. Estas librerías son gratuitas únicamente para propósitos no comerciales
- **Adobe Reader**: La aplicación Adobe Reader permite validar certificados incluidos en documentos PDF.

5. ENTIDADES PARTICIPANTES

5.1. Prestador de servicios de confianza (PSC)

Según la Ley de Firma Electrónica, se denomina Prestador de Servicios de Confianza (PSC) la persona física o jurídica que expide certificados electrónicos o presta otros servicios en relación con la firma electrónica.

Firmaprofesional ofrece servicios de validación de certificados, tanto de los certificados propios como de certificados emitidos por otros Prestadores de Servicios de Confianza.

5.2. Autoridad de Validación (VA)

Firmaprofesional es un Prestador de Servicios de Confianza (PSC) que actúa como Autoridad de Validación (VA). Firmaprofesional ofrecerá los servicios de validación por sí misma y por sus propios medios, sin delegarlos en ninguna otra entidad.

Firmaprofesional puede utilizar diferentes sistemas para generar respuestas de validación, proporcionando alta disponibilidad al servicio.

5.3. Cliente

Los clientes son los usuarios del servicio, los cuales envían peticiones de validación y reciben respuestas siguiendo el protocolo RFC6960.

Algunos servicios de validación de Firmaprofesional no son públicos. Para poder acceder a los servicios de validación, el Cliente deberá contratar previamente el servicio con Firmaprofesional.

6. OBLIGACIONES Y RESPONSABILIDADES

6.1. Firmaprofesional

6.1.1. Obligaciones

Firmaprofesional, actuando como Autoridad de Validación (VA) se obliga a:

- Respetar lo dispuesto en esta Política de Validación de Certificados.
- Proteger sus claves privadas de forma segura.
- Generar respuestas de validación conforme a esta Política y a los estándares de aplicación.
- Garantizar que la información de validación ofrecida se corresponde con una fuente de confianza
- Generar respuestas de validación según la información enviada por el cliente y libres de errores de entrada de datos.

- Generar respuestas de validación cuyo contenido mínimo sea el definido por la normativa vigente, cuando sea aplicable.
- Publicar esta Política de Validación de Certificados
- Informar sobre las modificaciones de la Política a clientes y terceros que confían
- Establecer los mecanismos de generación y custodia de la información relevante en las actividades descritas, protegiéndolas ante pérdida, destrucción o falsificación.
- Custodiar las respuestas generadas para los clientes que contraten el servicio de custodia

Firmaprofesional, en su actividad de prestación de servicios de certificación, responderá por el incumplimiento de lo establecido en esta Política de Validación de Certificados y, allí donde sea aplicable, por lo que dispone la Ley 59/2003, de 19 de diciembre, de firma electrónica o su normativa de desarrollo.

Sin perjuicio de lo anterior Firmaprofesional no garantizará los algoritmos y estándares criptográficos utilizados ni responderá de los daños causados por ataques externos a los mismos, siempre que hubiere aplicado la diligencia debida según el estado de la técnica en cada momento, y hubiere actuado conforme a lo dispuesto en las presentes Políticas de VA y en la legislación vigente, donde sea aplicable.

6.1.2. Responsabilidad financiera

No aplicable por no tratarse de un servicio de emisión de certificados reconocidos según lo estipulado en la Ley de 59/2003 de Firma electrónica. La VA no se hace responsable en caso de pérdidas por transacciones.

6.1.3. Exoneración de responsabilidad

Firmaprofesional no será responsable en ningún caso cuando se encuentre ante cualquiera de estas circunstancias:

- Estado de Guerra, desastres naturales, funcionamiento defectuoso de los servicios eléctricos, las redes telemáticas y/o telefónicas o de los equipos informáticos utilizados por el Cliente o por los Terceros, o cualquier otro caso de fuerza mayor.
- Por el uso indebido o fraudulento de las respuestas sobre validación.
- Por el uso indebido de la información contenida en el Certificado o en la CRL.
- Por el contenido de los mensajes o documentos firmados.
- En relación a acciones u omisiones del Cliente
- Falta de veracidad de la información suministrada para validar el certificado
- Negligencia en la conservación de sus datos de acceso al servicio de validación de certificados, en el aseguramiento de su confidencialidad y en la protección de todo acceso o revelación.

- Extralimitación en el uso del servicios de validación de certificados, según lo dispuesto en la normativa vigente y en la presente Política de VA

- Falta de comprobación de la suspensión o pérdida de vigencia del certificado electrónico de la VA publicada en el servicio de consulta sobre la vigencia de los certificados o falta de verificación de la firma electrónica.

6.1.4. Cese de la actividad de la VA

Antes del cese de su actividad la VA realizará las siguientes actuaciones:

- Informará a todos los clientes o entidades con los cuales tenga acuerdos u otro tipo de relación del cese con la anticipación mínima de 2 meses, o el periodo que establezca la legislación vigente.
- Revocará toda autorización a entidades subcontratadas para actuar en nombre de la VA en el procedimiento de respuesta de peticiones de validación.
- Informará a la administración competente, con la antelación indicada, el cese de su actividad y el destino que se vaya a dar a los sellos de tiempo emitidos hasta la fecha, especificando, en su caso, si se va a transferir la gestión y a quien.

6.2. Cliente

El Cliente estará obligado a cumplir con lo dispuesto por la normativa y además a:

- Respetar lo dispuesto en los documentos contractuales firmados con la VA.

- Verificar la respuesta obtenida de la VA

- Almacenar y conservar las respuestas de validación entregadas por la VA, si prevé que le serán necesarias en el futuro.

7. REQUERIMIENTOS OPERACIONALES

7.1. Control de Acceso

Para los servicios de validación privados, Firmaprofesional realizará un control de acceso al servicio basado en direcciones IP o en usuario y contraseña, por lo tanto el Cliente deberá informar a Firmaprofesional de las direcciones IP desde donde se realizarán las peticiones o bien, Firmaprofesional le notificará el usuario y contraseña asignado al Cliente.

Los servicios Públicos de validación no requieren control de acceso.

7.2. Obtención de Información fiable

Para poder responder de manera correcta a las peticiones de validación de certificados, la VA de Firmaprofesional debe tener acceso a fuentes de información fiables.

Para responder a peticiones de validación de certificados emitidos por CA dentro de la Jerarquía de Certificación de Firmaprofesional, la VA tendrá acceso directo al propio repositorio de la CA, por lo que la VA actuará como una fuente autorizada para decidir sobre la validez de un determinado certificado.

En el caso de que el certificado haya sido emitido por un PSC que disponga de servidor OCSP propio, la VA reenviará la petición al PSC y devolverá la respuesta al cliente sin modificarla. De este modo la respuesta provendrá directamente de una fuente autorizada.

Los Prestadores de Servicios de Certificación de confianza aceptados por Firmaprofesional son:

- Firmaprofesional — Sobre sus propios certificados
- ACA — Autoridad de Certificación de la Abogacía
- ACCV — Autoridad de Certificación de la Comunidad Valenciana
- ANCERT — Agencia Notarial de Certificación
- ANF — ANF Autoridad de Certificación
- CAMERFIRMA — Autoridad Certificación de las Cámaras de Comercio
- CATCERT — Agencia Catalana de Certificación
- DNI-e — DNI electrónico español.
- FNMT — Fábrica Nacional de Moneda y Timbre
- IZENPE — Autoridad de Certificación del gobierno vasco

Los servicios de validación de certificados de otros Prestadores no son públicos, por lo que será necesario contratar los servicios previamente con Firmaprofesional. Los servicios de validación se comercializan en forma de paquetes anuales, limitando el número máximo de peticiones de validación que un cliente puede realizar anualmente.

7.3. Tiempo de Custodia

Para el caso del **Servicio de Validación de Certificados** sin custodia no se garantiza la custodia de las respuestas enviadas. Será responsabilidad del cliente custodiarlas de manera adecuada.

Para el **Servicio de Validación por OCSP con Custodia de Evidencias,** Firmaprofesional se compromete a custodiar la información por un periodo mínimo de 15 años.

7.4. Solicitud de validaciones por OCSP

Firmaprofesional ofrece varios servicios de validación OCSP diferentes:

- **Servicio Público de Validación por OCSP**: El cliente realiza una petición de validación según el protocolo OCSP, obteniendo como respuesta una evidencia digital firmada por la VA de Firmaprofesional. Este servicio es público y accesible a través de la URL:

  http://ocsp.firmaprofesional.com

- **Servicio Privado de Validación por OCSP**: El cliente realiza una petición de validación según el protocolo OCSP, obteniendo como respuesta una evidencia digital firmada por la VA de Firmaprofesional. Este servicio es privado y accesible a través de la URL:

  http://servicios.firmaprofesional.com/ocsp

- **Servicio Privado de Validación por OCSP con Custodia de Evidencias**: Firmaprofesional almacena y custodia una copia de cada evidencia digital generada y la pone a disposición del cliente en caso necesario. Este servicio es privado y accesible a través de la URL:

  http://servicios.firmaprofesional.com/ocspdb

- **Servicio OCSP de otros prestadores:** Firmaprofesional ofrece un servicio de centralización de peticiones OCSP hacia otros prestadores de certificación, de tal manera que accediendo a un único punto de acceso, se redirigen la peticiones al servicio OCSP correspondiente de cada prestador. Este servicio es privado y accesible a través de la URL:

  http://servicios.firmaprofesional.com/ocsp

7.5. Formato de las Solicitudes

El formato de envío de las solicitudes sigue el siguiente esquema:

Content type: ***application/ocsp-request***
Method : ***POST***
Content-length: ***required***
<< Contiene la petición OCSP, codificada en DER >>

También es posible enviar **peticiones GET** según las especificaciones del estándar RFC6960, codificando los datos de la petición OCSP en formato Base64 y enviándolos en la URL:

http://ocsp.firmaprofesional.com/<peticion_ocsp_base64>
http://servicios.firmaprofesional.com/ocsp/<peticion_ocsp_base64>

Si se accede a la URL del servicio con un navegador o utilizando el método GET con formato incorrecto, el servidor mostrará una página web informando del error (y devolverá un Código 200).

Los campos opcionales según la especificación RFC6960 se tratan de la siguiente manera:

Campo	Tratamiento
CertID.hashAlgorithm	El algoritmo de hash pueden ser SHA1 o SHA256
CertID. issuerNameHash	Hash del DN del emisor (OCTET STRING)
CertID. issuerKeyHash	Hash de la clave pública del emisor (OCTET STRING)
CertID.serialNumber	Número de serie del certificado que se desea validar
nonce	Opcional. Si está presente, la respuesta contiene el mismo valor.
certReq	Su presencia y valor son ignorados.
extensions	Su presencia y valor son ignorados.

7.6. Formato de las Respuestas

Si la petición no se puede procesar, se devuelve una respuesta http indicando un código de error. Los posibles errores son:

Causa	Error	Descripción
Falta el campo content-length	411	CONTENT_LENGTH REQUIRED
Content-length demasiado grande	413	REQUEST ENTITY TOO LARGE
Content-type incorrecto	415	UNSUPORTED MEDIA TYPE
Los datos no son un ocsp request	400	BAD REQUEST
El servidor no responde	500	SERVER INTERNAL ERROR

Las respuestas se envían en el siguiente formato:

Content type: ***application/ ocsp-response***
Method: ***POST***
Content-length: ***required***
<< Contiene la respuesta OCSP en ASN.1, codificado en DER>>

Los campos opcionales según la especificación RFC6960 se tratan de la siguiente manera:

Campo	Tratamiento
ResponderID	DN del certificado OCSP firmante
nonce	Si la petición lo contiene se devuelve el mismo valor Sino se crea uno nuevo
CertID	CertID enviado en la petición
CertStatus	< good / revoked / unknow >
thisUpdate	Fecha y Hora de la firma de la respuesta
nextUpdate	+ 5 minutos
extensions	No presente
Certificados adjuntos	<Certificado OCSP>
Signature	SHA256

La respuesta “revoked” indica que el certificado está presente en la lista de certificados revocados (CRL), lo que implica que se trata de un certificado vigente y revocado, y que no se debe confiar en él.

La respuesta “good” indica que el certificado no está presente en la lista de certificados revocados. Esto no implica necesariamente que el certificado sea válido (por ejemplo, podría ser un certificado falso o estar caducado). Para validar el certificado se debe seguir el procedimiento descrito en el estándar RFC5280.

Si se pregunta por un certificado con un número de serie inexistente, el servidor OCSP podrá responder “good” o “unknown” en función de cómo esté configurado el servicio.

Para la CA “CN=AC Firmaprofesional - INFRAESTRUCTURA”, que emite los certificados de servidor web seguro, cuando se pregunte por un certificado con un número de serie inexistente, la respuesta será “unknown” (Tal como exige el estandar “*Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates”)*. Para el resto de CAs se responderá con “good”.

8. CERTIFICADOS OCSP

8.1. Generación de los certificados

Para la generación del certificado de Autoridad de Validación, se sigue la ***Política de Certificación de Servicio Seguro*** de Firmaprofesional (OID 1.3.6.1.4.1.13177.10.1.4.1), disponible en la dirección http://www.firmaprofesional.com/cps.

Las respuestas de cada CA serán firmadas por un certificado OCSP emitido por la propia CA. Los certificados OCSP utilizados tendrán una duración de 1 año, y suite criptográfica RSA 2048 bits con SHA256.

Los certificados OCSP incluyen la extensión "id-pkix-ocsp-nocheck" (1.3.6.1.5.5.7.48.1.5).

8.2. Publicación del certificado

El certificado OCSP se adjunta en la respuesta de validación según el estándar RFC6960.

Adicionalmente los certificados OCSP operativos se encuentran publicados en la web de Firmaprofesional (http://crl.firmaprofesional.com/ocsp/).

8.3. Cambio de certificado

Los certificados OCSP pueden ser cambiados en cualquier momento por otros certificados OCSP igualmente válidos según la ***Política de Certificación de Servicio Seguro*** de Firmaprofesional.

Firmaprofesional tratará de comunicar a los usuarios del servicio con la debida antelación. En todo caso, los usuarios deberían confiar en todos las respuestas de validación generadas por Firmaprofesional y firmadas con certificados OCSP válidos de dentro de la jerarquía de certificación.

9. AUTORIDADES DE CERTIFICACIÓN SOPORTADAS

9.1. CA Raíz

9.1.1. Certificado OCSP para CAROOT

Campo	Valor
Subject	C=ES, O=FIRMAPROFESIONAL, CN=OCSP ROOT
Issuer	CN=Autoridad de Certificacion Firmaprofesional CIF A62634068
S/N	53 cd 13 92 b1 50 23 ea
Validity	Not Before: Mar 16 13:05:41 2017 GMT Not After : Mar 16 13:05:41 2018 GMT
URL	http://crl.firmaprofesional.com/ocsp/ocsp-fp-root.crt

9.2. CAs Subordinadas

9.2.1. Certificado OCSP para CA INFRAESTRUCTURA

Campo	Valor
Subject	C=ES, O=FIRMAPROFESIONAL, CN=OCSP INFRAESTRUCTURA
Issuer	CN=AC Firmaprofesional - INFRAESTRUCTURA
S/N	09 8c 30 a3 d8 13 de c0
Validity	Not Before: Mar 17 12:11:07 2017 GMT Not After : Mar 17 12:11:07 2018 GMT
URL	http://crl.firmaprofesional.com/ocsp/ocsp-fp-infraestructura.crt

El servicio OCSP para la CA INFRAESTRUCTURA es capaz de identificar si un determinado certificado ha sido emitido. En caso de solicitar información sobre un certificado no emitido se responderá con un código “unknown” en lugar de “good”.

9.2.2. Certificado OCSP para CA CUALIFICADOS

Campo	Valor
Subject	C=ES, O=FIRMAPROFESIONAL, CN=OCSP CUALIFICADOS
Issuer	CN=AC Firmaprofesional - CUALIFICADOS
S/N	2baf6227a48c3f02
Validity	Not Before: Mar 17 12:14:33 2017 GMT Not After : Mar 17 12:14:33 2018 GMT
URL	http://crl.firmaprofesional.com/ocsp/ocsp-fp-cualificados.crt

9.2.3. Certificado OCSP para CA1

Campo	Valor
Subject	C=ES, O=FIRMAPROFESIONAL, CN=OCSP CA1
Issuer	CN=AC Firmaprofesional - CA1
S/N	67 29 a6 64 c5 8e a0 03
Validity	Not Before: Mar 17 12:16:41 2017 GMT Not After : Mar 17 12:16:41 2018 GMT
URL	http://crl.firmaprofesional.com/ocsp/ocsp-fp-ca1.crt

9.2.4. Certificado OCSP para CA AAPP

Campo	Valor
Subject	C=ES, O=FIRMAPROFESIONAL, CN=OCSP AAPP
Issuer	CN=AC Firmaprofesional - AAPP
S/N	2c 1d 7c a1 58 04 cb d2
Validity	Not Before: Mar 17 12:19:16 2017 GMT Not After : Mar 17 12:19:16 2018 GMT
URL	http://crl.firmaprofesional.com/ocsp/ocsp-fp-aapp.crt

9.3. CAs Subordinadas de uso Privado

9.3.1. Certificado OCSP para CA CFEA

Campo	Valor
Subject	C=ES, O=FIRMAPROFESIONAL, CN=OCSP CFEA
Issuer	CN=AC Firmaprofesional - CFEA
S/N	40 c8 c8 f1 83 fd 80 0f
Validity	Not Before: Mar 8 13:17:18 2017 GMT Not After : Mar 8 13:17:18 2018 GMT
URL	http://crl.firmaprofesional.com/ocsp/ocsp_fp_cfea.crt

9.3.2. Certificado OCSP para CA OTC

Campo	Valor
Subject	C=ES, O=FIRMAPROFESIONAL, CN=OCSP OTC
Issuer	CN=AC Firmaprofesional - OTC
S/N	13 92 21 36 a0 d8 b7 d8
Validity	Not Before: Mar 8 13:20:56 2017 GMT Not After : Mar 8 13:20:56 2018 GMT
URL	http://crl.firmaprofesional.com/ocsp/ocsp-fp-otc.crt

9.4. CAs Subordinadas pertenecientes a otros PSCs

9.4.1. Certificado OCSP para CA SIGNE

Campo	Valor
Subject	C=ES, O=FIRMAPROFESIONAL, CN=OCSP SIGNE
Issuer	CN=SIGNE Autoridad de Certificacion
S/N	61116103b1517940
Validity	Not Before: Mar 17 11:29:40 2017 GMT Not After : Mar 17 11:29:40 2018 GMT
URL	http://crl.firmaprofesional.com/ocsp/ocsp-fp-signe.crt

9.4.2. Certificado OCSP para CA SANTANDER

Campo	Valor
Subject	C=ES, O=FIRMAPROFESIONAL, CN=OCSP SANTANDER
Issuer	CN=Santander Digital Signature
S/N	61 af ca da d0 11 79 3f
Validity	Not Before: Mar 17 12:08:37 2017 GMT Not After : Mar 17 12:08:37 2018 GMT
URL	http://crl.firmaprofesional.com/ocsp/ocsp-fp-santander.crt

9.4.3. Certificado OCSP para CA SEU

Campo	Valor
Subject	C=ES, O=FIRMAPROFESIONAL, CN=OCSP SEU
Issuer	CN=SEU Autoridad de Certificacion
S/N	1f 31 67 ba 1b 20 ec 90
Validity	Not Before: Mar 17 11:44:18 2017 GMT Not After : Mar 17 11:44:18 2018 GMT
URL	http://crl.firmaprofesional.com/ocsp/ocsp-fp-seu.crt