@dministración electrónica

@firma

Declaración de Prácticas de Validación @firma

GOBIERNO DE ESPAÑA

MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS

SECRETARÍA DE ESTADO DE ADMINISTRACIONES PÚBLICAS

DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

TÍTULO: Declaración de Prácticas de Validación de @firma. (versión 9.0)

Elaboración y coordinación de contenidos:
Dirección de Tecnologías de la Información y las Comunicaciones (DTIC)

Responsable edición digital: Subdirección General de Información, Documentación y Publicaciones
1ª edición electrónica: mayo de 2016

Disponible esta publicación en el Portal de Administración Electrónica (PAe):
http://administracionelectronica.gob.es/

Edita:

© Ministerio de Hacienda y Administraciones Públicas
Secretaría General Técnica
Subdirección General de Información,
Documentación y Publicaciones
Centro de Publicaciones

Colección: administración electrónica

NIPO: 630-16-381-4

GOBIERNO DE ESPAÑA · MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS · CENTRO DE PUBLICACIONES

Plataforma @firma

Declaración de prácticas de validación de @firma

GOBIERNO DE ESPAÑA

Documento nº:	DPV_@firma
Revisión:	9.0
Fecha:	25/04/2016
Período de retención:	Permanente durante su período de vigencia + 3 años después de su anulación

CONTROL DE COMPROBACIÓN Y APROBACIÓN

Documento nº:	DPV_@firma
Revisión:	9.0
Fecha:	**25/04/2016**

REALIZADO

25/04/2016	Direccion de Proyecto

APROBADO

04/05/2016	DTIC

CONTROL DE MODIFICACIONES

Documento nº:	DPV_@firma
Revisión:	**9.0**
Fecha:	**25/04/2016**

Rev.	9.0
Fecha	25/04/2016
Autor/es	Direccion de Proyecto
Descripción	Actualizacion DPV a partir de la version 8.30

ÍNDICE

1 ACRÓNIMOS Y DEFINICIONES 7

2 REFERENCIAS 8

3 LEGISLACIÓN Y ESTÁNDARES 9
3.1 Normativa y estándares aplicados 9
3.2 Legislación de referencia 10

4 INTRODUCCIÓN 11
4.1 Objeto y alcance 11

5 DESCRIPCIÓN DE SERVICIOS 12
5.1 Servicios ofrecidos por la plataforma 12
5.1.1 Requisitos de uso de los servicios 13
5.1.2 Servicios de validación de firmas electrónicas 13
5.1.3 Servicios de upgrade de firmas electrónicas 15
5.1.4 Servicios de validación de certificados 15
5.1.4.1 Servicio de validación OCSP 15
5.1.4.2 Servicios web de validación de certificados 18
5.1.4.2.1 Información extraída de los certificados 18
5.1.4.2.2 Validación de certificados acorde a las TSL 19
5.2 Responsabilidad de uso de los servicios tecnológicos 19
5.3 Servicios administrativos 19
5.3.1 Soporte a la integración 20
5.3.2 Registro y gestión de incidencias 21
5.3.3 Gestión de cambios y corrección de errores 21
5.3.4 Administración y control de la configuración de la plataforma 21
5.3.5 Servicio de auditoría y estadísticas 22

6 USUARIOS 24
6.1 Servicios por usuarios 26
6.1.1 Soporte a la Integración 26
6.1.2 Gestión de incidencias 26
6.1.3 Gestión de cambios 27
6.1.4 Gestión de la configuración 27
6.1.5 Servicio de auditoría y estadísticas 28
6.1.6 Monitorización: Procedimientos de Alarma 28
6.2 Gestión de usuarios 29

7 POLÍTICA PROCEDIMENTAL DE LA VA 30
7.1 Administración y configuración 30
7.1.1 Administración general 30
7.1.2 Alta de una CA 31
7.1.3 Modificación de parámetros de una CA 32
7.1.4 Baja de una CA 33
7.1.5 Altas y cambios en aplicaciones 33
7.2 Acceso a los servicios de validación 33
7.3 Uso de los servicios 34
7.4 Garantía de trazabilidad y no repudio 34

8 GARANTÍA DE SEGURIDAD 35
8.1.1 Seguridad física 35
8.1.2 Seguridad lógica 35
8.1.2.1 Custodia de información transaccional 35
8.1.2.2 Custodia de claves y certificados 36
8.1.3 Seguridad operacional y de personal 36
8.1.4 Continuidad del servicio 36

9 INFORMACIÓN DE LA DECLARACIÓN DE PRÁCTICAS DE VALIDACIÓN 38
9.1 Control de versión 38
9.2 Punto de publicación 38
9.3 Responsables 38
9.4 Responsabilidades legales 38
9.4.1 Reglamentación Aplicable 39
9.4.2 Responsabilidad 39
9.4.3 Limitación de responsabilidades 39
9.4.4 Protección de datos de carácter personal 39
9.4.5 Obligaciones de la VA 41
9.4.6 Obligaciones de Usuario 41
9.4.7 Obligaciones de terceros 41

ANEXOS

A.1 ALGORITMOS Y BASES CRIPTOGRÁFICAS 44
A.1.1 FORMATOS DE FIRMA SOPORTADOS 44
A.1.2 ALGORITMOS DE HASH SOPORTADOS 47
A.1.3 ALGORITMOS DE FIRMA SOPORTADOS 48
A.2 PRESTADORES ADMITIDOS 49
A.3 INFORMACIÓN DE CONTACTO ADMINISTRATIVO 50
A.4 HERRAMIENTAS ADICIONALES DE FIRMA 51
A.5 CERTIFICADOS USADOS POR LA AUTORIDAD DE VALIDACIÓN 52
A.5.1 CERTIFICADOS PLATAFORMA DE PRODUCCION 52
A.5.2 CERTIFICADOS PLATAFORMA DE PRE- PRODUCCION 53
A.6 URL DE LOS SERVICIOS OFRECIDOS. 54

1 Acrónimos y definiciones

CAdES	CMS Advanced Electronic Signature (firma electrónica avanzada CMS)
CAID	Centro de Atención a Integradores y Desarrolladores
CEN	Comité Europeo de Estandarización
CMS	Cryptographic Message Syntax
CRL	Certificate revocation list
CWA	CEN Workshop Agreement
DPC	Declaración de prácticas de certificación
DPV	Declaración de prácticas de validación
ETSI	European Telecommunications Standards Institute
HSM	Hardware Security Module
IETF	Internet Engineering Task Force
JRE	Java Runtime Environment
MINHAP	Ministerio de Hacienda y Administraciones Públicas
PKI	Public Key Infrastructure (Infraestructura de clave pública)
Plugin	Módulo o aplicación que interactúa con otra aplicación para ampliar su funcionalidad aportándole una función o utilidad específica
SARA	Sistema de Aplicaciones y Redes para las Administraciones
SOAP	Simple Object Access Protocol
OCSP	Online Certificate Status Protocol
URI	Uniform Resource Identifier (Identificador Uniforme de Recursos)
URL	Uniform Resource Locator (Localizador Uniforme de Recursos)
VA	Validation Authority (Autoridad de validación)
WSS	Web Services Security
WYSIWYS	What You See Is What You Sign (lo que ves es lo que firmas)
XAdES	XML Advanced Electronic Signature (firma electrónica avanzada XML)
XML	eXtended Markup Language

2 Referencias

[SETSI]	Secretaria de Estado de Telecomunicaciones y Sociedad de la Información Ministerio de Industria, Energía y Turismo
[SUPPORT_SLA].	Acuerdo de Nivel de Servicio de la Plataforma de validación y firma electrónica @firma del MINHAP para Organismos Usuarios
[OASIS-WSS]	Web Services Security: SOAP Message Security 1.1 (WS-Security)
[RFC OCSP]	RFC2560
[PRU_CARGA]	Procedimiento de pruebas de carga en la Plataforma @firma y TS@
[VERSIONES]	Cambios y Novedades @firma (@Firma-CambiosYNovedades-MAN)
[Alta de aplicaciones]	Plantilla de alta de IPs y Aplicaciones en @firma
[SOAP_MAN_ENG]	Manual de Programación de Web Services de @firma 6 (Firma-Global-XMLSOAP-MAN-EN-NoFederado.pdf)
[SOAP_MAN_ESP]	Manual de Programación de Web Services de @firma 6 (Firma-Global-XMLSOAP-MAN-NoFederado.pdf)
[DSS_PROFILE]	Perfiles para la adaptación de los Web Services de @firma 6 al protocolo OASIS-DSS
[PROC-ALTA_CERT]	Procedimiento de inclusión y clasificación de certificados en @firma. (Tratamiento de certificados en firma.pdf)

3 Legislación y estándares

3.1 Normativa y estándares aplicados

ETSI EN 319 411-2	Policy requirements for certification authorities issuing qualified certificates
ETSI TS 101 861	Time stamping profile
ETSI TS 102 023	Policy requirements for time-stamping authorities
ETSI TS 101 733	Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES)
ETSI TS 103 173	Electronic Signatures and Infrastructures (ESI); CAdES Baseline Profile
ETSI TS 101 903	Electronic Signatures and Infrastructures (ESI); XML Advanced Electronic Signatures (XAdES)
ETSI TS 103 171	Electronic Signatures and Infrastructures (ESI); XAdES Baseline Profile
ETSI TS 102 778-2	Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 2: PAdES Basic - Profile based on ISO 32000-1
ETSI TS 102 778-3	Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 3: PAdES Enhanced - PAdES-BES and PAdES-EPES Profiles
ETSI TS 102 778-4	Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 4: PAdES Long Term - PAdES-LTV Profile
ETSI TS 102 778-5	Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 5: PAdES for XML Content - Profiles for XAdES signatures
PDF 32000-1:2008	Document management — Portable document format — Part 1: PDF 1.7
ETSI TS 103 172	Electronic Signatures and Infrastructures (ESI); PAdES Baseline Profile
ETSI TS 103 174	Electronic Signatures and Infrastructures (ESI); ASiC Baseline Profile

3.2 Legislación de referencia

- [eIDAS] 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.
- [Dec UE 2015/1505] Decisión de Ejecución (UE) 2015/1505 de la Comisión de 8 de septiembre de 2015 por la que se establecen las especificaciones técnicas y los formatos relacionados con las listas de confianza de conformidad con el artículo 22, apartado 5, del Reglamento (UE) no 910/2014 del Parlamento Europeo y del Consejo, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior
- [Dec UE 2015/1506] Decisión de Ejecución (UE) 2015/1506 de la Comisión de 8 de septiembre de 2015 por la que se establecen las especificaciones relativas a los formatos de las firmas electrónicas avanzadas y los sellos avanzados que deben reconocer los Organismos del sector público de conformidad con los artículos 27, apartado 5, y 37, apartado 5, del Reglamento (UE) no 910/2014 del Parlamento Europeo y del Consejo, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior
- [ENS] Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
- [ENI] Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.
- [RD 1671] Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos.
- [LPAC] Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
- [LRJ] Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
- [LOPD] Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
- [RD LOPD] Real Decreto 1720/2007, de 21 de diciembre, Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal

4 Introducción

La plataforma de Validación y firma @firma es una solución tecnológica que se centra en facilitar a las Administraciones Publicas, los servicios necesarios para implementar la identificación y firma electrónica avanzada y reconocida basada en certificados digitales de una forma eficaz y efectiva en sus aplicaciones. Se ofrecen así servicios que impulsan el uso de la certificación y firma electrónica en los sistemas de información de las diferentes Administraciones públicas.

Los servicios ofrecidos por la plataforma permiten la validación de los certificados digitales, la generación y validación de firmas electrónicas en múltiples formatos, la auditoría de las transacciones y documentos firmados, el sellado de tiempo o la compatibilidad con certificados digitales generados por múltiples prestadores de servicios de certificación. Todas estas características convierten a @firma en una solución completa de autenticación y firma electrónica.

El presente documento define los servicios proporcionados por la plataforma @firma, los usuarios y/u Organismos a los que van dirigidos y las condiciones en las que se proporcionan estos servicios.

4.1 Objeto y alcance

Los servicios de la Plataforma están disponibles para todas las entidades del sector público, según se define en el Artículo 2. *Ámbito subjetivo de aplicación* de la LPAC. Desde el Ministerio de Hacienda y Administraciones Públicas se ofrece la ayuda y el soporte necesario para que los Organismos integren estos servicios de certificación de valor añadido en los sistemas de información de Administración Electrónica que requieran identificación y firma electrónica basada en certificados digitales.

El propósito es definir un marco de uso de los servicios proporcionados la plataforma, bajo el cual se adquieren compromisos tanto por parte del usuario como por parte del proveedor del servicio.

Las entidades y personas a los que se dirige este documento son:

- La Dirección de Tecnologías de la Información y Comunicaciones (DTIC) como Órgano responsable de la Autoridad de Validación.
- Las Autoridades de Certificación o Prestadores de Servicios de Confianza.
- Los Organismos responsables de las aplicaciones usuarias de los servicios de validación.
- Los ciudadanos como usuarios finales de los servicios.

Los servicios de validación no han sido diseñados ni autorizados para ser utilizados en actividades de alto riesgo o que requieran una actividad a prueba de fallos, como las relativas al funcionamiento de instalaciones hospitalarias, nucleares, de control de tráfico aéreo o ferroviario, o cualquier otra donde un fallo pudiera conllevar la muerte, lesiones personales o daños graves al medioambiente.

5 Descripción de servicios

@firma es una plataforma de servicios horizontal que proporciona servicios de validación de certificados electrónicos y firma electrónica. Los servicios proporcionados por la plataforma @firma se dirigen a proporcionar servicios PKI a aplicaciones usuarias previamente reconocidas y configuradas tal como se desprende de los apartados siguientes.

Los servicios ofrecidos se dividen en dos grupos:

- **Servicios tecnológicos**. Proporcionan acceso a funcionalidades PKI a las aplicaciones clientes integradas. Estos servicios son invocados directamente por las distintas aplicaciones y se prestarán a través de la interfaz WS o de la interfaz OCSP.
- **Servicios administrativos**. Como parte del catálogo de servicios de la plataforma @firma se contemplan:
    - Soporte a la Integración
    - Registro de incidencias
    - Gestión de cambios y corrección de errores
    - Administración y control de la configuración de la plataforma
    - Publicación y distribución de nuevas versiones y parches
    - Registro de sugerencias y reclamaciones

  Cubriendo los distintos Acuerdos de Nivel de Servicio en función de lo dispuesto en [SUPPORT_SLA].

  Los datos de contacto para acceder a los distintos servicios se encuentran descritos en el anexo A.3 Información de contacto administrativo

Por otro lado y para complementar los servicios proporcionados por la plataforma, se proporciona un conjunto de herramientas auxiliares para facilitar la integración de los servicios proporcionados en las aplicaciones clientes. Las herramientas adicionales se encuentran detalladas en el anexo A.4 Herramientas adicionales de @firma, y a pesar de que su uso puede condicionar las acciones y condiciones descritas para los sistemas, su descripción y condición de uso queda fuera del actual documento.

5.1 Servicios ofrecidos por la plataforma

A continuación se describirán los servicios tecnológicos ofrecidos a las aplicaciones integradas. Como parte de la descripción se incorporará un apartado específico que detallará las normas comunes requeridas para el correcto uso de los servicios de la plataforma. Así mismo, y en caso de que sea necesario, se identificarán los servicios específicos. Se especificará también cuales son las condiciones mínimas necesarias para la invocación de los servicios.

5.1.1 Requisitos de uso de los servicios

Se exigirá a todas las aplicaciones pertenecientes a Organismos públicos u entidades reconocidas la aceptación de las declaraciones publicadas en este documento. Se destacan los siguientes requisitos:

- La aplicación deberá haber sido dada de alta en la plataforma. Para esto se deberá seguir el procedimiento [Alta de aplicaciones], de forma que todos los parámetros especificados sean cubiertos por la información proporcionada por el Organismo responsable de la aplicación.
- La aplicación deberá tener acceso a la red SARA y estar identificada en esta mediante una IP, la cual se deberá especificar durante el proceso de alta.
- La invocación de los servicios se realizará siguiendo los medios proporcionados por @firma, los cuales incluyen manuales, librerías y otras herramientas de apoyo.
- Se considera requisito indispensable el uso de un certificado para realizar la firma electrónica de las peticiones a @firma, que garantice la procedencia e integridad de los datos, acorde al estándar OASIS Web Service Security [OASIS-WSS]. Así mismo, @firma proporcionará una respuesta convenientemente firmada. Será responsabilidad de la aplicación cliente la firma electrónica de la petición enviada, así como la verificación y custodia si procede de la respuesta proporcionada por la plataforma.
- Se prohíbe cualquier tipo de prueba, prueba de carga o monitorización de los servicios que implique el envío de peticiones. La Autoridad de Validación es un servicio compartido por múltiples Administraciones Publicas por lo que las pruebas en producción pueden impactar negativamente en la calidad del servicio para el resto de los usuarios. Para la realización de pruebas, se dispone de un entorno de integración de la plataforma de @firma, copia del entorno de producción.
- Los responsables de las aplicaciones deberán comunicarse al servicio de soporte de la AV, a través del formulario de contacto especificado en el Anexo A3. Tanto el responsable funcional, como un responsable o contacto técnico, deberán estar actualizados en todo momento, siendo responsabilidad de dichos usuarios comunicar cualquier variación de los datos de contacto. En caso de no mantener los datos de contacto actualizados no se asegura la correcta notificación de cambios y problemas.

5.1.2 Servicios de validación de firmas electrónicas

Como Autoridad de Validación, @firma proporciona a las aplicaciones integradas la capacidad de validación de firmas electrónicas tanto ASN.1 como XML. Así mismo se proporciona capacidades para la validación de firmas electrónicas de documentos (PDF y PAdES).

La plataforma @firma proporciona el servicio de validación de firmas electrónicas a través de la interfaz DSS y la interfaz nativa tanto en inglés como español.

Servicio	Interfaz	Extensión de firma[1]	Periodo de gracia	Referencia
ValidateSignature	Nativa	No	No	[SOAP_MAN_ENG]
ValidarFirma	Nativa	No	No	[SOAP_MAN_ESP]
DSSAfirmaVerify	DSS	Sí	Sí	[DSS_PROFILE]

Tabla 1. Servicios de validación de firmas electrónicas

El servicio de validación de firmas no contemplará, por defecto, los periodos de gracia, excepto que se indique expresamente o que el periodo esté especificado por la política de firma para la validación de los certificados implicados, siempre que el formato de la firma sea EPES o se extienda a partir de éste. Esto originará que la plataforma devuelva una respuesta asíncrona, con el objetivo de que posteriormente, una vez transcurridos los periodos de gracia, se consulte el estado completo de la firma electrónica. En esta respuesta asíncrona se incorporará el identificador necesario para consultar el estado de la petición y recuperarla una vez transcurrido el periodo de gracia de los certificados.

Servicio	Interfaz	Referencia
DSSAsyncRequestStatus	DSS	[DSS_PROFILE]

Tabla 2. Servicio de consulta de estado de petición

El servicio de consulta de estado de la petición proporcionará información sobre el estado actual de una petición y, en caso de que se hayan cumplido los plazos, la respuesta de la validación completa. Esta funcionalidad puede ser obviada deliberadamente por el integrador mediante la especificación en la petición de validación.

La plataforma @firma es un servicio compartido. Con el objetivo de garantizar la igual disponibilidad para todos los usuarios, se establece un tamaño máximo de las peticiones de validación de firmas que se admiten en la plataforma. Las peticiones que superen el tamaño máximo serán descartadas. De esta manera se evita que una aplicación consuma todos los recursos disponibles y cause la degradación o indisponibilidad del servicio para el resto de usuarios. Este límite se establece igual para todas las aplicaciones y se considera suficiente para validar la mayor parte de las firmas electrónicas. Aquellos documentos que superen el límite establecido deberán firmarse con formatos explícitos que no necesiten incluir en la firma el contenido del documento. De esta forma se habilita la validación de firmas de documentos de cualquier tamaño sin afectar al resto de aplicaciones.

[1] El proceso de Extensión de Firma permite especificar un formato de destino a la petición de servicio. De esta forma la plataforma permite incluir objetos dentro de una firma válida, extendiendo su formato inicial.

Las aplicaciones podrán establecer los criterios bajo los cuales la validación de un certificado o firma se considera correcta o incorrecta. Para ello podrán especificar la política de validación de certificados que les aplica. Por defecto se asignará la política CRITICA a todas las aplicaciones, pero estas podrán solicitar a través del servicio de soporte indicado en el Anexo A.3 si desean modificar esta política. Se puede consular más información sobre las políticas de validación en el documento [DSS_PROFILE]

Los formatos de firma admitidos y lo algoritmos soportados por los distintos formatos se encuentran detallados en el anexo A.1 Algoritmos y bases criptográficas

5.1.3 Servicios de upgrade de firmas electrónicas

Además de los servicios de validación de firmas electrónicas, @firma proporciona a las aplicaciones integradas la capacidad de extender las firmas electrónicas tanto ASN.1 como XML y PDF a formatos longevos. @firma realiza la recupera las evidencias de validación necesarias para la extensión al formato longevo deseado, y construye la firma resultante. Pueden consultarse los formatos longevos soportados en el Anexo A.1.

La plataforma @firma proporciona el servicio de upgrade de firmas electrónicas únicamente a través de la interfaz DSS.

Servicio	Interfaz	Extensión de firma[2]	Periodo de gracia	Referencia
DSSAfirmaVerify	DSS	Sí	Sí	[DSS_PROFILE]

Tabla 3. Servicios de upgrade de firmas electrónicas

5.1.4 Servicios de validación de certificados

La plataforma @firma proporciona el servicio de validación de certificados multiprestador mediante dos interfaces. El comportamiento de ambas interfaces proporciona el estado de un certificado en el momento de la petición. Aunque la base tecnológica para el funcionamiento de los servicios comparte muchos puntos en común, es necesario especificar las características de cada una de las interfaces, las cuales serán definidas a continuación.

5.1.4.1 Servicio de validación OCSP

Dadas las distintas naturalezas e implementaciones de las aplicaciones clientes en el tratamiento de peticiones OCSP, el servicio OCSP proporcionado por la plataforma @firma admite distintos modos de funcionamiento, los cuales se describen a continuación y se basan en la especificación RFC2560 [RFC_OCSP] y el tratamiento del elemento RequestorName y la firma de la petición OCSP:

[2] El proceso de Extensión de Firma permite especificar un formato de destino a la petición de servicio. De esta forma la plataforma permite incluir objetos dentro de una firma válida, extendiendo su formato inicial.

- Modo anónimo. La petición OCSP no incluye el elemento RequestorName ni firma electrónica. Permite a una aplicación cliente el uso del servicio OCSP sin identificar la fuente. Este modo está deshabilitado ya que no es posible garantizar la integridad ni la procedencia de la petición.
- RequestorName conocido. La petición ha sido firmada y se ha indicado de forma correcta el identificador de la aplicación en el campo RequestorName.
- RequestorName desconocido. La petición OCSP ha sido firmada pero el elemento RequestorName no identifica ningún identificador de aplicación reconocido. Se procederá a la aceptación de la petición y su posterior validación. En el proceso de verificación del certificado firmante, se comprobará si @firma confía en dicho certificado y si está asignado a una o más aplicaciones. En caso afirmativo se procederá a evaluar el certificado contenido y a responder indicando el estado de éste. Si el certificado no es confiable o no está ligado a ninguna aplicación, se devolverá una respuesta de error.

En el siguiente diagrama se esquematiza las distintas posibilidades y su tratamiento por parte de @firma.

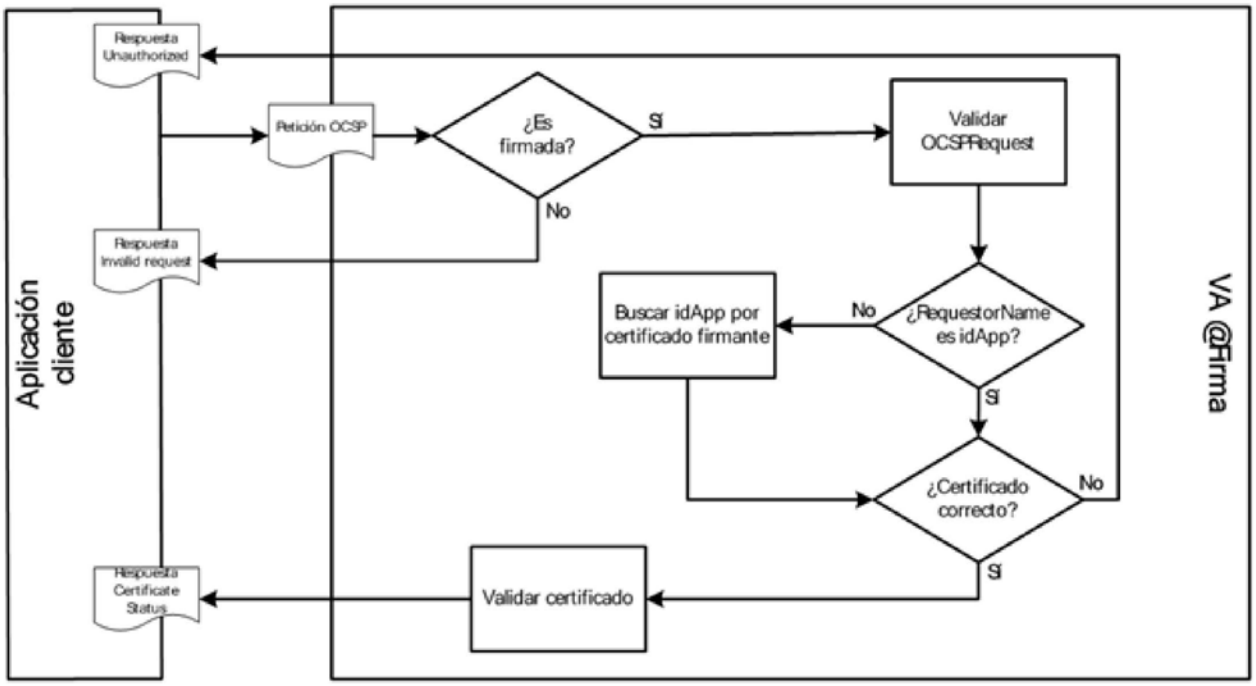

Diagrama 1. Esquema de funcionamiento de autenticación para servicio OCSP

El servicio OCSP permite la discriminación por emisor de certificado pero no por tipo de certificado, ya que la clasificación de tipos de certificados se realiza en base a atributos no incluidos en la petición OCSP. Para cubrir este aspecto, se permite especificar mediante un parámetro de configuración de la aplicación si se va a realizar una validación estricta de tipos de certificados o relajada. La validación estricta vetará cualquier emisor que incorpore

un tipo de certificado no admitido, mientras que la validación relajada (por defecto) admitirá validación de tipos de certificados inicialmente no permitidos.

Es decir, que por limitaciones del estándar OCSP, este protocolo no permite filtrar certificados por su OID. Por tanto, si distintos tipos de certificados han sido emitidos por una Autoridad de Certificación supervisada por la [SETSI] según el artículo 30.2 de la Ley de Firma Electrónica, no se pueden distinguir los certificados cualificados (Qualified Certificates), de aquellos certificados no cualificados (non Qualified certificates) o incluso de certificados no supervisados, aunque estén asociados a Declaraciones de Prácticas de Certificación distintas (con distintos identificadores-OID).

Por tanto, el servicio OCSP responder de @firma valida únicamente los certificados de Autoridades de Certificación dadas de alta en la plataforma, siguiendo el procedimiento de altas de certificados en @firma [PROC-ALTA_CERT]. Es decir, no valida certificados incluidos en las TSL especificadas en el Reglamento eIDAS [eIDAS]. Tampoco se garantiza la exclusión de certificados no cualificados o no supervisados según el Reglamento eIDAS, si estos han sido emitidos por PKI supervisadas. En caso que se quiera disponer de estas funcionalidades de @firma, sería necesario realizar las validaciones a través de los servicios WEB de @firma.

Para facilitar a las aplicaciones usuarias la gestión de la confianza en los múltiples Prestadores de Servicios de certificación incluidos en la plataforma, el OCSP responder de @firma firma todas sus respuestas con un mismo certificado, emitido por la Autoridad de Certificación del DNI para @firma. Esto implica que, acorde a la RFC6960, no se aconseja utilizar las respuestas del OCSP de @firma para construir firmas longevas fuera de la funcionalidad de @firma. Si se desea ampliar una firma con evidencias de validación de la firma para convertirla en longeva, se aconseja utilizar los servicios de upgrade de @firma (DSSafirmaVerify). Si se desea realizar el upgrade con medios propios, se aconseja realizar las validaciones a través de los servicios WEB de @firma.

A partir de lo anterior se pueden extraer los siguientes requisitos y recomendaciones de uso y configuración del servicio OCSP:

- Sólo las aplicaciones habilitadas tendrán acceso al servicio de validación de certificados por OCSP en las condiciones especificadas durante el alta de aplicación.
- Toda aplicación deberá proporcionar el certificado que firmará sus peticiones OCSP, el cual pasará a ser confiable dentro del servicio OCSP de @firma y para la aplicación indicada. El responsable de la aplicación, cómo custodio legal del certificado, deberá notificar cualquier incidencia relacionada con éste (caducidad, revocación, etc) con el fin de garantizar un correcto uso del servicio.
- Toda petición OCSP dirigida a la plataforma deberá ir convenientemente firmada con un certificado previamente indicado y asignado a la aplicación.
- A pesar de que @firma lo permite, no es recomendable emplear el mismo certificado para dar servicio a más de una aplicación. Esta casuística unida a no indicar el identificador de aplicación puede ocasionar que las condiciones de ejecución del servicio no sean estrictamente las indicadas para la aplicación objetivo.

A diferencia de los servicios web de validación de certificados, el servicio OCSP sólo proporciona información acerca del estado del certificado, no incluyendo información adicional extraída del certificado.

5.1.4.2 Servicios web de validación de certificados

Los servicios web de validación de certificados además de proporcionar información del estado de revocación del certificado, incluyen información adicional que facilita el uso de los datos contenidos en el certificado a las aplicaciones clientes, en concreto información de la identidad del suscriptor y el tipo de certificado.

El sistema de validación multiprestador permite clasificar el certificado consultado en función de distintas características especificadas previamente en configuración y acordes a lo especificado en la correspondiente DPC. Esta clasificación permite especificar métodos de validación específicos para un tipo de certificado concreto y extraer información del certificado en base a lo especificado por la DPC. Así mismo, los medios de validación serán proporcionados también por el prestador, indicando si estos son particulares para un tipo de certificado, emisores intermedios (p.e. una ACL) o universales para todos los tipos contemplados por el prestador.

En el anexo A.2 Prestadores admitidos se puede encontrar más información de los prestadores y tipos de certificados reconocidos por @firma. Desde la información incorporada por cada prestador se podrá acceder a su correspondiente DPC.

Los servicios web proporcionados que facilitan información sobre el estado de un certificado son:

Servicio	Interfaz	Proporciona información[3]	Referencia
ValidateCertificate	Nativa	No	[SOAP_MAN_ENG]
ValidarCertificado	Nativa	No	[SOAP_MAN_ESP]
GetInfoCertificate	Nativa	Sí	[SOAP_MAN_ENG]
ObtenerInfoCertificado	Nativa	Sí	[SOAP_MAN_ESP]
DSSAfirmaVerifyCertificate	DSS	Sí	[DSS_PROFILE]

Tabla 4. Servicios web de validación de certificados

5.1.4.2.1 Información extraída de los certificados

Toda la información proporcionada por la respuesta será extraída del certificado consultado, utilizando la información de parseo proporcionada por el prestador en la DPC. Dado que no existe una normativa que estipule la información que se ha de incluir en un certificado fuera de lo especificado por X509, algunos tipos de certificados pueden no proporcionar un mapeo completo de los campos, obteniéndose solamente información parcial en la respuesta.

Esta funcionalidad está disponible únicamente para los certificados dados de alta explícitamente en la plataforma, siguiendo el procedimiento de altas de certificados en

[3] Los servicios básicos de validación no realizan un parseo del certificado, por lo que no proporciona la información extraída en la respuesta.

@firma [PROC-ALTA_CERT]. Es decir, no valida certificados incluidos en las TSL especificadas en el Reglamento eIDAS [eIDAS].

5.1.4.2.2 Validación de certificados acorde a las TSL

A partir de la versión 6.2 de @firma, se incluye también la validación de certificados que no han sido explícitamente incorporados en la plataforma, si estos certificados están incluidos en las TSL publicadas por los Organismos de supervisión europeos acorde a la Decisión de Ejecución de la Comisión (EU) 2015/1505 de 8 de septiembre de 2015 por la que se establecen las especificaciones técnicas y los formatos relacionados con las listas de confianza.

En estos casos se validarán únicamente los certificados cualificados incluidos en dichas listas, y se proporcionará información básica de los mismos, como el tipo de certificado, en la medida que este sea deducible del propio certificado o de la TSL asociada, o información básica de identidad. No se proporcionará identificación detallada de identidad. Se puede consular la información que se devuelve de los certificados validados acorde a las TSL en el documento [PROC-ALTA_CERT]

La validación de los certificados incluidos en las TSL europeas esta activas por defecto para todas las aplicaciones dadas de alta en la plataforma, pero puede desactivarse a petición de la aplicación.

5.2 Responsabilidad de uso de los servicios tecnológicos

Todos los usuarios de los servicios tecnológicos ofrecidos por la Autoridad de Validación admiten estar informados de las condiciones expresadas en este documento, así como las condiciones particulares que puedan estar asociadas a servicios específicos.

El usuario Responsable de Aplicación admite la responsabilidad del buen uso de los servicios tecnológicos ofrecidos por la plataforma, debiendo identificar de forma inmediata cualquier mal uso detectado para interponer las acciones de prevención o mitigación convenientes.

En concreto será responsabilidad de la aplicación usuaria de los servicios de la Autoridad de Validación, la firma electrónica de la petición enviada, así como la verificación y custodia si procede de la respuesta proporcionada por la plataforma.

5.3 Servicios administrativos

La orientación de proveedor horizontal de servicios inherente a la Autoridad de Validación hace necesaria la provisión de servicios adicionales a los puramente tecnológicos para garantizar un catálogo de servicios completo de calidad. Estos servicios son los siguientes:

- Soporte a la Integración
- Registro y seguimiento de incidencias
- Registro de sugerencias y reclamaciones
- Gestión de cambios y corrección de errores

- Administración y control de la configuración de la plataforma
- Publicación y distribución de nuevas versiones y parches
- Servicio de auditoría y estadísticas

Se considera fundamental el cumplimiento de los tiempos especificados en el Acuerdo de Nivel de Servicio [SUPPORT_SLA] en la resolución de los distintos procedimientos, así como la operatividad de los servicios, cambios de configuración o correcciones y mantener informada a la Dirección del Proyecto sobre dicho cumplimiento.

5.3.1 Soporte a la integración

El carácter inherente a la Autoridad de Validación de proveedor horizontal de servicios, requiere que las aplicaciones clientes integren los distintos servicios incluyendo ciertas particularidades que garanticen el buen uso de dichos servicios. La Autoridad de Validación favorecerá la integración de aplicaciones y el correcto uso de los servicios proporcionados. Con este fin se proporciona documentación específica orientada a la integración de los servicios tecnológicos, herramientas adicionales para apoyar los desarrollos en aplicaciones clientes y un servicio de soporte al integrador que resuelva las dudas propias de la integración de aplicaciones.

El servicio de soporte no facilitará código fuente directamente o por referencia. No admitirá consultas sobre código fuente no facilitado en la documentación proporcionada por la AV.

Este servicio se proporcionará a través de la página web del proyecto, donde se encuentran todos los manuales, descripciones de los servicios y librerías actualizados, para los usuarios de las Administraciones Públicas registrados en el portal. También se proporciona soporte a través del formulario web referenciado en el anexo A.3 Información de contacto administrativo.

La Autoridad de Validación es un servicio compartido por múltiples Administraciones Publicas, por lo que se prohíbe la realización de cualquier tipo de prueba, prueba de carga o monitorización de los servicios, por su impacto negativo en la calidad del servicio para el resto de los usuarios.

Para la realización de pruebas de integración, se dispone de un entorno de la plataforma de @firma, réplica del entorno de producción, habilitado para la realización de pruebas. No están permitidas las pruebas de carga, ni siquiera en el entorno de pruebas, ya que al ser @firma una plataforma compartida y escalable, los resultados obtenidos no serían significativos. En la página web del proyecto, referenciada en el anexo A.3 Información de contacto administrativo, se publican los tiempos de latencia para cada uno de los servicios, así como un procedimiento de pruebas de carga en la Plataforma @firma y TS@ [PRU_CARGA]

La URL de acceso a los servicios ofrecidos por la plataforma de desarrollo es posible únicamente desde dentro de la red interadministrativa (SARA). Las URL de acceso se pueden encontrar en el Anexo A.6.

5.3.2 Registro y gestión de incidencias

Dada la criticidad de los servicios proporcionados por la Autoridad de Validación, se proporciona un servicio de registro y resolución de incidencias. Este servicio proporciona una interfaz directa con el grupo de soporte el cual, ante el reporte de un error, evaluará el alcance y la gravedad de la incidencia y procederá según establece el Acuerdo de Nivel de Servicios.

Como parte del proceso de registro y gestión de incidencias, el Centro de Atención a Integradores y Desarrolladores, proporciona un servicio de atención a sugerencias y reclamaciones ante cualquier desviación de los niveles de servicios acordados. Este servicio valorará el objeto de la sugerencia o reclamación y procederá a informar de ella al Responsable de la Autoridad de Validación, quien determinará la actuación a realizar sobre ésta.

Las incidencias se podrán comunicar a través del formulario web referenciado en el anexo A.3 Información de contacto administrativo.

Se pone a disposición de los usuarios una lista de correo a la que podrán suscribirse para estar informados de novedades y posibles actuaciones en la plataforma, problemas de disponibilidad de los prestadores incorporados o de la propia Autoridad de Validación, y de otros temas que pueden resultar de interés. La dirección de la lista a la que suscribirse se publicará en la página web del proyecto, referenciada en el anexo A3 Información de contacto administrativo.

5.3.3 Gestión de cambios y corrección de errores

Las distintas evoluciones tecnológicas incorporadas a la Autoridad de Validación, como la corrección de errores se irán incorporando a versiones sucesivas de @firma. El detalle específico de los cambios registrados en una versión se publicará en la página web del proyecto (ver Anexo A.3), en el documento [VERSIONES].

Se publicarán las distintas distribuciones así como cualquier cambio futuro que pueda repercutir en la correcta integración de las aplicaciones. Así mismo se identificarán los parches correctivos que componen una versión específica así como su posible repercusión en instalaciones o integraciones anteriores.

Aquellos cambios correspondientes a errores serán evaluados por Dirección de Proyecto y, en función de su criticidad, se dispondrá su publicación en un parche posterior. Los tiempos asignados para los distintos niveles de criticidad serán tratados directamente por Dirección de Proyecto e influirán directamente en el roadmap correctivo de la AV.

5.3.4 Administración y control de la configuración de la plataforma

El mantenimiento de la configuración de la plataforma @firma es responsabilidad de la Autoridad de Validación. Se contempla dentro de este mantenimiento las siguientes tareas:

- Alta de nuevas Aplicaciones, notificadas de acuerdo a lo especificado.

- Cambios en configuración de Aplicaciones. Cualquier cambio necesario en la configuración de una Aplicación se realizará a través de Control de la configuración.
- Alta de nuevos Prestadores de Servicios de Certificación y certificados.

Los servicios y Prestadores de Servicios de Certificación ofrecidos por la AV podrán ser modificados unilateralmente por el Responsable de la Autoridad de Validación. Los cambios se harán públicos a través de las listas de correo de novedades y de la página la página web del proyecto, referenciada en el anexo A3.

Será responsabilidad de los Organismos registrados, y de los Responsables de las Aplicaciones en última instancia, el comprobar regularmente la publicación de la documentación de la AV, para comprobar las posibles variaciones. Por su parte, la Autoridad de Validación publicará con antelación todas aquellas variaciones que puedan afectar sustancialmente desde un punto de vista legal, técnico o administrativo al Organismo y causar deterioro en el nivel de servicio de la Autoridad de Validación.

Solo se incluirían aquellos Prestadores de Servicios de Certificación que figuren como supervisados por la [SETSI] y aquellos incluidos en las Listas de confianza de los proveedores de servicios de confianza cualificados supervisados por los Estados Miembros, acorde a la Decisión de Ejecución (UE) 2015/1505.

En el caso de que uno de los Organismos registrados notifiquen la no aceptación de las modificaciones, se entenderá que desiste unilateralmente del contrato de usufructo de servicios de la AV, sin obligación de indemnizar por daños y perjuicios por estas causas y causando baja inmediata de los servicios de información que lo vinculan a la Autoridad de Validación.

Queda reservado el derecho a la modificación de los parámetros de configuración correspondientes a aplicaciones por parte de Dirección de la Autoridad de Validación siempre que se considere que la configuración entra en conflicto con los propósitos de la Autoridad de Validación. Cualquier modificación será notificada vía correo electrónico al Responsable de Aplicación, indicando los motivos que justifican el cambio de configuración.

5.3.5 Servicio de auditoría y estadísticas

Los servicios tecnológicos proporcionados por la Autoridad de Validación a las aplicaciones clientes están cubiertos por un sistema de auditoría propietario e incluido en la plataforma @firma. Este sistema almacena todos los datos correspondientes a las transacciones realizadas por la Autoridad de Validación, incluyendo toda la información que permita garantizar el origen y no repudio de las transacciones.

Los datos almacenados no incluyen las peticiones y las respuestas de servicio devueltas por la AV. Es responsabilidad de la Aplicación cliente almacenar la petición enviada a la Autoridad de Validación y la respuesta correspondiente si lo considera necesario.

Los datos almacenados incluyen:

- Los procesos realizados por la plataforma para la prestación de los servicios de cara a las aplicaciones, incluyendo respuesta de estados de certificados obtenidas de los distintos proveedores de servicios de certificación.
- Información relativa a los procesos internos del sistema, como pueden ser la verificación del estado de los PSC, chequeo de la caducidad de los certificados registrados en el sistema, etc.
- Operaciones de mantenimiento y administración llevadas a cabo a través de la herramienta de Administración.
- Las alarmas lanzadas por la plataforma para informar de alguna anomalía.

Las consultas sobre las estadísticas estarán disponibles de forma completa para Dirección y Responsable de la Autoridad de Validación. Si se solicita expresamente, mensualmente se envían a través del Centro de Atención a Integradores y Desarrolladores de @firma un informe con las estadísticas a cada organismo que hace uso de los servicios de la Autoridad de validación.

Las estadísticas de uso globales se publicarán en la página web de la Autoridad de Validación.

6 Usuarios

A continuación se definirán los distintos niveles de usuarios para posteriormente determinar tanto los servicios asociados cómo las responsabilidades a las que están sujetas tanto los distintos niveles de servicios cómo los propios usuarios.

*Se define **Usuario** de la Autoridad de Validación a cualquier Organismo, Aplicación o Persona física que directa o indirectamente acceda y/o utilice los servicios proporcionados por la plataforma @firma.*

De este modo, es usuario de la plataforma todo aquel que utiliza los servicios tecnológicos y/o administrativos proporcionados por la Autoridad de Validación. Es importante destacar que la relación existente entre estos usuarios no es excluyente, pudiendo considerarse el mismo usuario perteneciente a distintos grupos simultáneamente. Se definirán a continuación los grupos de usuarios así como sus características y rasgos distintivos.

*Se define **Organismo** a cualquier Administración Pública, órgano o entidad administrativa que en el ejercicio de sus funciones proporcione servicios de Validación de Certificados o Firmas Electrónicas mediante al menos una aplicación integrada en @firma a través de la red SARA.*

Se considerarán también Organismos aquellas entidades adheridas a convenios de distribución específicos, los cuales deberán ser tratados de forma particular e independiente, y cuyas actuaciones se incluirán dentro del ámbito del presente documento.

Se considera que el Organismo garantizará el buen uso de los servicios prestados, no pudiendo ejercer cómo proxy de servicios a terceros sin el consentimiento expreso de la Dirección de la Autoridad de Validación.

El Responsable de la Autoridad de Validación podrá restringir los niveles de acceso, así como el volumen de transacciones estimadas en función de parámetros objetivos inherentes en el sistema físico que soporta la Autoridad de Validación. En el caso de que la Autoridad de Validación no pueda garantizar los niveles de servicio en base a la previsión de volumen de peticiones del Organismo se propondrá el despliegue de una plataforma @firma en modelo federado. Es necesario aclarar que los servicios proporcionados por @firma en modelo federado no quedan sujetos a lo especificado en este documento, siendo responsabilidad del Organismo proporcionar dicha garantía y sus correspondientes Niveles de Servicio. Los servicios necesarios para el correcto funcionamiento de la plataforma federada y que recaigan en servicios proporcionados por el modelo centralizado se contemplarán como tales.

En la definición de Organismo se especifica que al menos una aplicación deberá estar integrada con @firma, definiéndose aplicación como:

*Se define **Aplicación** como la unidad mínima de configuración accesible en @firma, identificada como un usuario o usuarios directos de los servicios tecnológicos proporcionados por la plataforma (servicios web u OCSP). Toda aplicación deberá especificar los parámetros propios de configuración y securización. Así mismo, deberá especificar un interlocutor único que actuará como Responsable de Aplicación.*

La aprobación del registro de una Aplicación es responsabilidad en última instancia de la Dirección de la Autoridad de Validación.

El concepto Aplicación en @firma se define como una configuración específica a la que está asociada una prestación de servicios que se reproducirán bajo las mismas circunstancias, es decir, los parámetro de invocación de servicios serán los mismos para un mismo entorno. Aunque no se especifica obligatoriedad en la singularidad del aplicativo integrado, por motivos de seguridad y auditoría no se recomienda utilizar la misma configuración de Aplicación para distintas aplicaciones clientes.

A la hora de realizar el Alta de Aplicación se deberá especificar un Responsable de Aplicación.

*El **Responsable** de Aplicación es la persona física vinculada al Organismo propietario de la aplicación cliente, encargada de definir tanto la configuración asociada a la aplicación, como de solicitar cambios en dicha configuración e informar de cualquier cambio previsto en la integración de los servicios de la aplicación integrada. Además, se identificará al Responsable de Aplicación cómo interlocutor con el grupo de soporte y será a éste al que se informe de contingencias en el normal desarrollo de los servicios. En última instancia es el responsable de garantizar la correcta utilización de los servicios dentro de los parámetros especificados.*

El Responsable de Aplicación podrá delegar en momentos puntuales la interacción con algunos de los servicios administrativos, principalmente los asociados a soporte de aplicaciones e incidencias, a un conjunto de terceras personas.

Es responsabilidad del Organismo mantener actualizado el contacto del responsable e informar al Centro de Atención a Integradores y Desarrolladores de los cambios, a través del formulario referenciado en el anexo A3 Información de contacto administrativo.

Debido a que durante el ciclo de vida de una aplicación es posible que distintos sujetos puedan requerir el acceso a los servicios proporcionados (soporte, alta y seguimiento de incidencias, etc) esta acción se podrá realizar previa identificación por parte del Responsable de Aplicación de las personas con capacidad para acceder a dichos servicios y/o modificar la información relativa a la propia Aplicación. A todos los efectos, el Responsable de Aplicación será garante de las modificaciones y usos sobre los distintos servicios efectuados por las personas por él autorizadas.

Finalmente, es necesario identificar el usuario final de las distintas integraciones:

*El **Usuario final** es la persona física que se beneficia directamente de los servicios proporcionados por las aplicaciones integradas con @firma. La Autoridad de Validación no contempla en ningún caso el servicio prestado directamente al usuario final, por lo que deberá ser contemplado específicamente por las aplicaciones clientes*.

La Autoridad de Validación @firma no clasifica un ámbito para el Usuario final, pudiendo este pertenecer al ámbito de la Administración Pública o al público general.

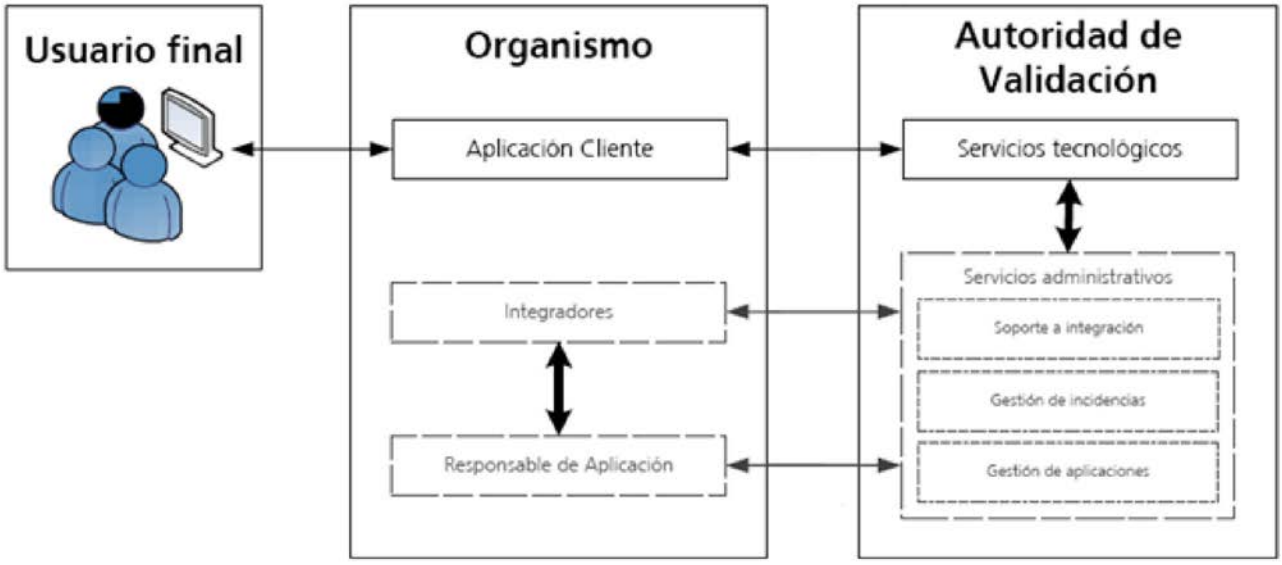

Diagrama 2. Diagrama de usuarios

6.1 Servicios por usuarios

A continuación se definen los distintos servicios identificados para cada grupo de usuarios, indicando la orientación específica del servicio.

6.1.1 Soporte a la Integración

El servicio va dirigido a etapas de desarrollo de las aplicaciones clientes. A través del Centro de Atención a Integradores y Desarrolladores se podrá acceder tanto a las herramientas y manuales puestas a disposición de los integradores, cómo consultas no contempladas en los medios proporcionados. Dado el carácter de este servicio sólo se atenderán cuestiones directamente relacionadas con la integración de servicios de @firma.

Los usuarios a los que se proporciona el servicio de Soporte a la Integración son los Responsable de las Aplicaciones y, por delegación, a los integradores implicados en el desarrollo.

6.1.2 Gestión de incidencias

Para garantizar tanto la calidad de los servicios proporcionados como su continuidad, el Centro de Atención a Integradores y Desarrolladores dispone de los medios necesarios para la gestión de incidencias de servicios de la Autoridad de Validación. El servicio está sujeto al Acuerdo de Nivel de Servicio y a las condiciones en él especificadas.

Sólo podrán acceder al servicio de gestión de incidencias los Responsables de Aplicaciones, o, por delegación, los integradores implicados en los desarrollos.

6.1.3 Gestión de cambios

La continua evolución de los servicios proporcionados, así como de los procedimientos internos utilizados en la Autoridad de Validación y los cambios originados por la correcta resolución de incidencias y errores causa una continua adaptación tanto de la plataforma @firma cómo de los servicios asociados. Para un correcto tratamiento de los cambios, se publicarán las distintas mejoras y correcciones existentes entre las distintas versiones.

Es importante destacar que previo a cualquier cambio en el entorno de producción del modelo central, se actualizará el entorno dedicado a la integración de aplicaciones, tras lo cual se notificará a todos los Organismos dicha actualización. Es responsabilidad de los correspondientes Responsables de Aplicación la verificación del correcto funcionamiento que los servicios utilizados por las Aplicaciones por la que responden. Ante la detección de cualquier problema se deberá notificar a través del servicio de gestión de incidencias.

El procedimiento de gestión de cambios incluye también la difusión de los elementos de configuración relativos a políticas de certificados a las plataformas registradas siguiendo el modelo federado. Los elementos proporcionados incluyen la estructura de certificación, tipos de certificados y mapeado de campos de un PSC determinado. Este servicio no obliga la importación de esta configuración a las plataformas del modelo federado, siendo dicha importación opcional.

6.1.4 Gestión de la configuración

Se identifican dos posibles casuísticas de configuración en base al alcance de esta:

- Denominaremos Configuración General a aquella que afecta de forma global a la Autoridad de Validación y a todas las aplicaciones en ella integrada. Cualquier cambio realizado en aspectos de configuración general deberá ser notificada a los Responsables de Aplicaciones si dicho cambio afecta al normal funcionamiento de los servicios integrados. En caso contrario los cambios acontecidos podrían no ser informados. Se considera a la Dirección de la Autoridad de Validación como responsable de estos cambios. Entran dentro de este tipo de cambios la inclusión de un nuevo PSC o tipo de certificado, cambio en certificados de firma de la plataforma, cambios o adición de mapeos de certificados, etc. Ante un cambio en la configuración que pueda afectar al funcionamiento de una aplicación, y una vez notificada tal casuística, será el Responsable de Aplicación el que deberá probar el correcto funcionamiento de la aplicación integrada en el contexto dispuesto en la notificación enviada. La AV no se responsabilizará de los fallos causados en aplicaciones integradas no notificados durante el periodo y contexto de prueba indicados en la notificación, recayendo dicha responsabilidad en el Responsable de Aplicación.
- Se denomina Configuración Particular, a aquella que afecta a una o varias aplicaciones integradas bajo un mismo Responsable de Aplicación. Entra dentro de ésta el establecimiento de la configuración de respuesta de la autoridad de validación o los prestadores y tipos de certificados particulares admitidos por la aplicación.

El proceso de configuración de la Autoridad de Validación es responsabilidad del grupo de soporte.

6.1.5 Servicio de auditoría y estadísticas

La Autoridad de Validación dispondrá de estadísticas estandarizadas y auditoría en caso de que los Responsables de Aplicación las requieran. Se podrán solicitar una vez al año a través del Centro de Atención a Integradores y Desarrolladores.

6.1.6 Monitorización: Procedimientos de Alarma

La Autoridad de Validación dispone de un sistema interno automático de aviso ante alarmas que permite el control de potenciales riesgos sobre los procesos internos y servicios de la plataforma @firma.

De esta forma, se informa al servicio de soporte en tiempo real de cualquier incidencia detectada, entre las que se pueden destacar:

- Problemas de conectividad. Admite alarmas individuales para los servicios de consulta de estado de certificados y prestadores, alarma frente a problema de conexión con base de datos y/o módulos criptográficos.
- Estados inconsistentes de certificados y prestadores. Emisión de alarma frente a prestadores caducados o revocados. Así mismo, se enviará una alarma si se detectan prestadores cercanos a su fecha de caducidad.
- Estado inconsistente del cluster de trabajo de @firma. Detecta problemas que podrían derivar en fallos del principio de alta disponibilidad. La emisión de esta alarma podría estar motivada por la caída de un servidor o la máxima conexión entre ellos.
- Problemas al recuperar claves de firma. Asociado con los procesos de firma electrónica realizados por la plataforma. Estas alarmas implican el fallo de un certificado y/o clave criptográfica.
- Estado inconsistente de la configuración del sistema. Detectará y notificará inconsistencia entre la configuración de los distintos servidores @firma, que pudiese degenerar en una pérdida parcial o total de servicio o una disminución del servicio de Alta Disponibilidad.

Todas las alarmas son completamente configurables, y permite la notificación por correo electrónico a los grupos de soporte, operadores y/o administradores de la AV.

En caso de detectarse Alarmas que pudiesen generar una pérdida de servicio general, se notificará a los Responsables de la Aplicación mediante un correo electrónico en las listas de distribución, indicando si es posible, un tiempo estimado de resolución. En caso de que la Alarma detectada afecte a una Aplicación concreta, se notificará a los Responsables de dicha Aplicación. Para ello los Responsables de la Aplicación deberán mantener actualizados tanto sus datos de contacto como los de los integradores implicados u otro personal asociado, tanto en las listas de correo como en los datos de contacto asociados a la Aplicación.

Además, se dispone de un servicio de información de estado de @firma para aplicaciones usuarias, que a partir de la información de monitorización que se obtiene de la plataforma, publica el estado de @firma en todo momento, para que las aplicaciones usuarias puedan ajustar su funcionamiento acorde al estado de @firma si lo consideran necesario.

6.2 Gestión de usuarios

La gestión integral y mantenimiento de usuarios se realizará a través del Centro de Atención a Integradores y Desarrolladores. Se contemplan los siguientes procedimientos relacionadas con la modificación de la condición de usuario:

- Alta de aplicación. Se deberá registrar tanto la Aplicación y la configuración asociada cómo el Responsable de Aplicación.
- Baja de aplicación.
- Modificar la configuración de una Aplicación.
- Cambio de Responsable de Aplicación

El Responsable de Aplicación, al solicitar un alta de aplicación deberá facilitar los datos de contacto profesionales:

- Nombre y apellidos
- Correo electrónico
- Número de teléfono
- Organismo y/o departamento

Mediante la cesión de estos datos, el Responsable de Aplicación acepta el tratamiento y almacenamiento de estos datos, cuyo único propósito es la gestión de las aplicaciones y gestión interna de la AV. La Autoridad de Validación garantiza el correcto tratamiento de dichos datos, su almacenamiento por medios seguros y la no cesión a terceros de los datos facilitados.

Cualquier modificación sobre los datos de los distintos usuarios se deberá realizar a través de los medios dispuestos por el Centro de Atención a Integradores y Desarrolladores.

7 Política procedimental de la VA

Con el fin de aclarar la política procedimental de la Autoridad de Validación, se procederá a continuación a describir el funcionamiento interno de los distintos procedimientos proporcionados por la Autoridad de Validación.

El procedimiento seguirá un ciclo de vida que contempla tres fases:

- Inicio del procedimiento. Todo procedimiento se iniciará por la aparición de un evento que se considerará cómo disparador del proceso. Se tomará como momento de inicio el instante de aparición del evento disparador. Tras este momento se procederá a tomar los requisitos y variables necesarios para una efectiva ejecución del proceso, tanto provenientes del disparador inicial del procedimiento cómo de la interacción con el usuario que activa el procedimiento.
- Actuación. Implica la ejecución del procedimiento.
- Finalización. Tras la ejecución del procedimiento se procederá a aquellas actuaciones vinculadas a la publicación de información o notificación a los distintos Usuarios.

7.1 Administración y configuración

Se considera dentro del procedimiento de Administración y Configuración de la Autoridad de Validación, aquellos procesos que implican cambios en el estado interno de la plataforma @firma que varíe en algún modo el comportamiento de la Autoridad de Validación ante la solicitud de un servicio.

Este procedimiento puede ser disparado por distintos Usuarios y admite diversas naturalezas, englobando los siguientes subprocedimientos, los cuales serán descritos posteriormente:

- Administración general
- Altas y cambios en aplicaciones
- Alta y actualizaciones de PSC

7.1.1 Administración general

Se denomina procedimiento de administración general, aquel proceso que afecta a la configuración de la plataforma @firma y causa cambios en la configuración de varios servicios o Aplicaciones. Los procedimientos de administración general son iniciados por la Dirección de la Autoridad de Validación y afectan de forma global a varias aplicaciones o servicios.

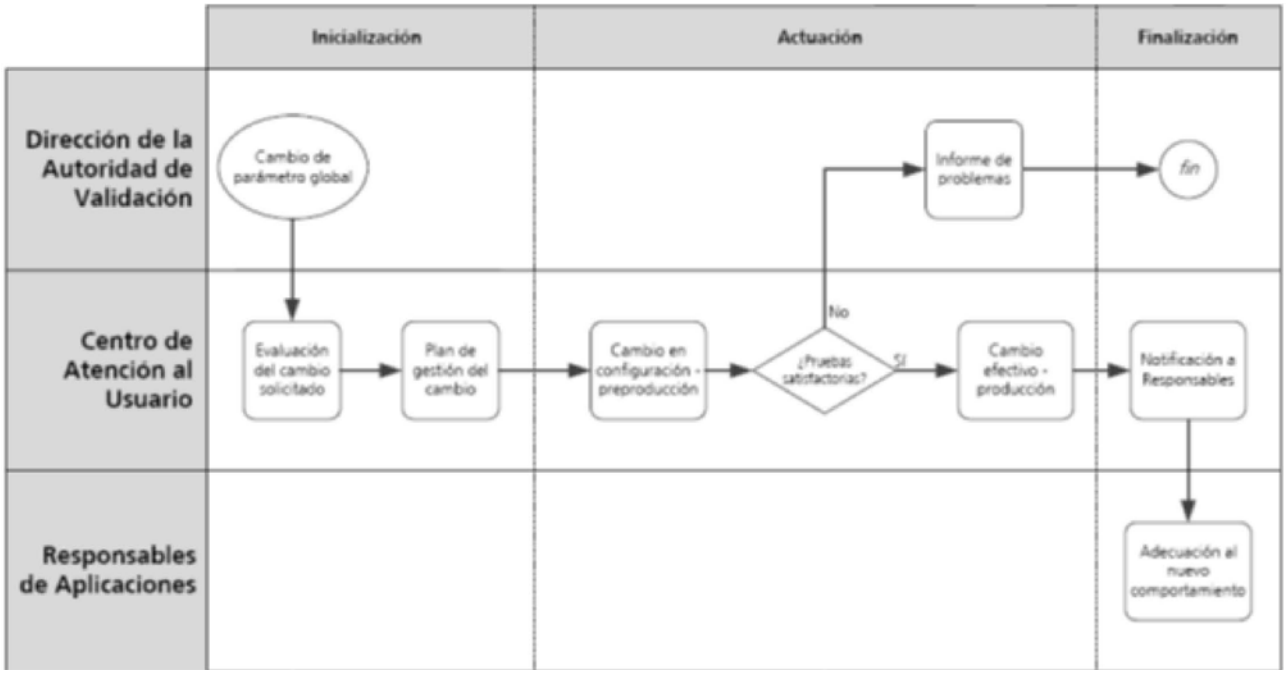

Diagrama 3. Administración General

7.1.2 Alta de una CA

El alta de una nueva Autoridad de Certificación estará siempre iniciada por la Dirección de la Autoridad de Validación. Debido a que los cambios efectuados en la plataforma para este tipo de actuaciones no implica cambios en las aplicaciones integradas, se asume que es un cambio pasivo y no se notificará explícitamente a los Usuarios, si bien se procederá a publicar tanto en la página web de @firma, cuya dirección se puede consultar en el Anexo 3, como en el actual documento (ver anexo A.2 Prestadores admitidos).

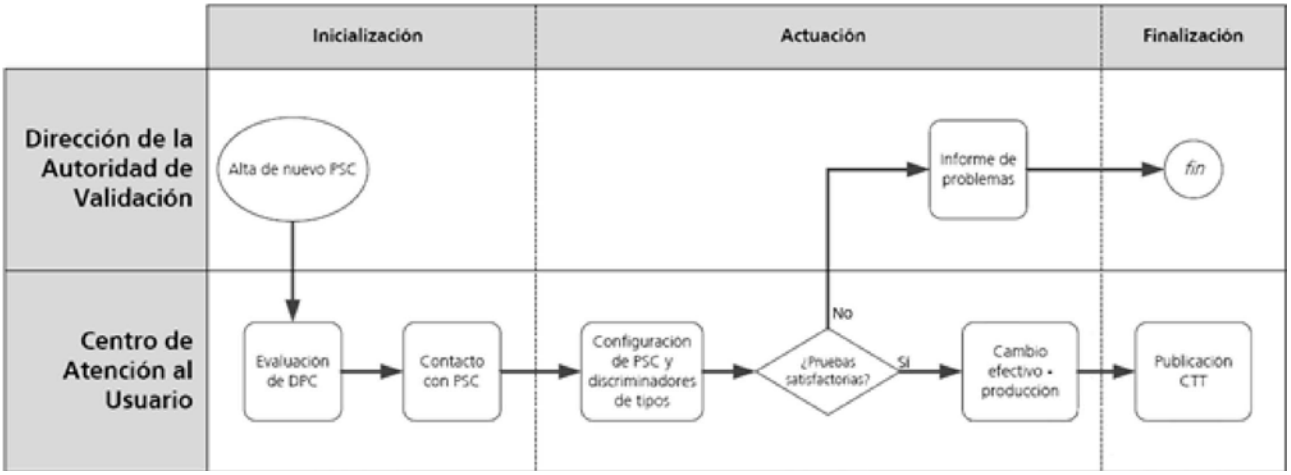

Diagrama 4. Alta de una CA

Puesto que no se incluyen CA que no estén supervisadas por sus estados miembros, los certificados cualificados emitidos por la CA ya se validaban en @firma a través de la TSL

correspondiente. Incluir la CA de forma explícita en la configuración implica la posibilidad de acceder a la información avanzada proporcionada por @firma. El alta de una CA en @firma implica la posibilidad de extraer los datos de identidad del certificado, así como otra información relevante incluida en él.

7.1.3 Modificación de parámetros de una CA

Ante cambios en los servicios y/o configuración realizados en un prestador de certificados, estos cambios deberán ser notificados a @firma previamente por los correspondientes PSC de forma que permita actualizar la configuración base de la Autoridad de Validación con el objetivo de minimizar cualquier pérdida del servicio frente a los prestadores implicados. Los cambios más comunes están relacionados con la aparición de nuevos tipos de certificados y cambios en el acceso a los servicios de validación.

Es responsabilidad del PSC informar de los futuros cambios, siendo la Autoridad de Validación la responsable de aplicar dichos cambios y comprobar su correcto funcionamiento. Si se detectase alguna incidencia en el comportamiento de la AV derivado de un cambio realizado, éste será notificado a los Usuarios, procurando minimizar la perdida de servicio y tratándolo directamente con el prestador de servicios de certificación implicado.

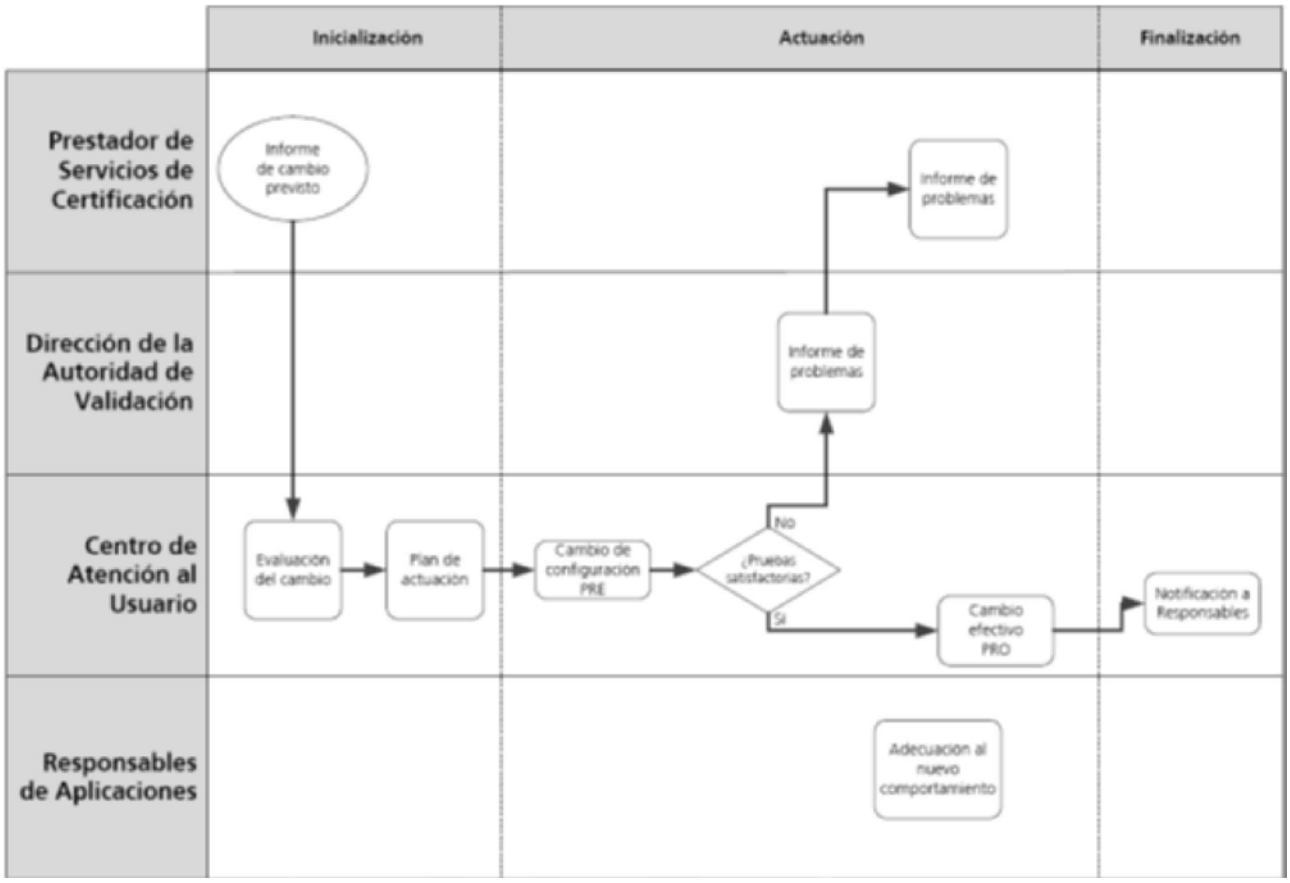

Diagrama 5. Modificación de una CA

7.1.4 Baja de una CA

Un PSC podrá solicitar la baja de una CA previamente dada de alta. Esto podrá hacerse cuando la CA pierda la condición de supervisada por la [SETSI], si el PSC determina que ya no existen certificados activos emitidos por esa CA, o cualquier otro motivo.

La baja de una CA implicará que las validaciones de certificados y firmas correspondientes a esa CA se realizarán en base a la TSL, por lo que ya no se devolverá la información de identidad incluida en el certificado ni se validaran los certificados a través del OCSP responder de @firma. No implica que dejarán de validarse en @firma.

7.1.5 Altas y cambios en aplicaciones

Un Organismo podrá solicitar el alta de una nueva aplicación o realizar modificaciones en la configuración de alguna aplicación que tenga dada de alta. El alta de nuevas aplicaciones o cambios en alguna aplicación ya dada de alta, se realizará a través de petición al Centro de Atención a Integradores y Desarrolladores (CAID), cuyo contacto puede consultarse en el Anexo A.3. Deberá enviarse el formulario de solicitud de alta (ACL) debidamente cumplimentado, tanto en el caso de altas como de modificaciones.

El cambio en una aplicación ya dada de alta, debe ser solicitado por alguno de los Responsables de la Aplicación registrados para esa aplicación concreta.

El servicio de soporte le comunicará los requisitos necesarios para el alta, entre los que puede incluirse la acreditación de la existencia de un convenio firmado (u otro instrumento jurídico de colaboración administrativa) que ampare el uso del servicio.

La aplicación deberá indicar el certificado que usará para realizar la firma electrónica de las peticiones a @firma, que garantice la procedencia e integridad de los datos. Dicho certificado no es necesario que sea un certificado cualificado, pero debe haber sido emitido por un Prestador de Servicios de Certificación supervisado por la [SETSI]. La Aplicación se responsabiliza de la custodia y buen uso de ese certificado.

La Aplicación deberá indicar un identificador de aplicación y el Código DIR3 del organismo al que pertenece. Si un organismo decide asignar el mismo identificador de aplicación para varios procedimientos/aplicaciones, deberá tener en cuenta que no podrá obtener información desagregada de dichas aplicaciones (estadísticas, errores…)

7.2 Acceso a los servicios de validación

El acceso de la Aplicación a los servicios de validación de la Autoridad de Validación @firma se hará a través de la red SARA.

Se solicitará el acceso o se comunicará cualquier incidencia relacionada con el acceso a @firma al Centro de Atención a Integradores y Desarrolladores (CAID), cuyo contacto puede consultarse en el Anexo A.3.

Las URL de conexión pueden consultarse en el Anexo A.6.

Los datos de los certificados de firma de las respuestas SOAP de la plataforma y de las respuestas OCSP pueden consultarse en el Anexo A.5.

7.3 Uso de los servicios

Las aplicaciones podrán hacer uso de los servicios de @firma para la validación de certificados y firmas de manera gratuita. Se dispone de documentación sobre los interfaces, ejemplos de integración y manuales en la página web de la solución que figura en el Anexo A.3.

Los responsables de las aplicaciones garantizan un uso racional de los servicios de @firma. Se prohíbe cualquier tipo de prueba, prueba de carga o monitorización de los servicios que implique el envío de peticiones. Para la realización de pruebas, se dispone de un entorno de integración de la plataforma de @firma, copia del entorno de producción.

En caso de detección de un uso incorrecto o incontrolado involuntario, es potestad de la Autoridad de validación deshabilitar el uso de los servicios hasta que la situación se corrija.

Para garantizar el uso compartido del servicio, se establece un límite máximo de uso de 3 millones de transacciones mensuales por Organismo. Superado este límite se considera que el uso de un medio compartido no es la situación deseable, por lo que se requerirá que el Organismo utilice la solución federada de @firma.

Un Prestador de Servicios de Certificación puede denegar el uso de sus servicios de validación a determinadas aplicaciones, si tiene una causa justificada. En caso de que un Prestador decida denegar el acceso, la plataforma @firma lo comunicará a la Aplicación afectada, así como las causas alegadas por el Prestador. En el caso de discrepancias entre la Aplicación y el Prestador en cuanto al derecho de acceso a los servicios de validación del PSC concreto, éstas deberán ser resueltas bilateralmente entre ambos, no siendo responsabilidad de la plataforma @firma la mediación entre ambos. La plataforma @firma es un intermediario en la validación y no puede ejercer de árbitro o control sobre cuestiones de derechos de acceso a los servicios de un tercero.

La denegación del uso de los servicios a una Aplicación, implicará que ésta no podrá hacer uso del servicio OCSP de @firma indicado en la sección 5.1.4.1 de este documento, ni dispondrá de los servicios de obtención de información indicados en la sección 5.1.4.2.1. La validación de las firmas y certificados del Prestador seguirá activa para aquellos certificados incluidos en la TSL española, tal como se indica en la sección 5.1.4.2.2.

7.4 Garantía de trazabilidad y no repudio

La Autoridad de Validación garantiza el no repudio de las respuestas emitidas, para lo cual realiza una custodia segura de todos los datos transaccionales para cualquier validación realizada sobre la plataforma @firma. La trazabilidad de las respuestas de validación permite asociar la petición de validación con los datos consultados a los Prestadores de Servicios de Certificación para la generación de la respuesta.

Si se desea hacer uso de esta utilidad, la Aplicación usuaria deberá almacenar la respuesta firmada de @firma, así como la petición realizada.

La Aplicación podrá solicitar acceso a las evidencias de trazabilidad y no repudio únicamente con una causa debidamente justificada, según criterio de la Autoridad de Validación. La petición deberá tramitarse a través del Centro de Atención a Integradores y Desarrolladores (CAID), cuyo contacto puede consultarse en el Anexo A.3.

8 Garantía de seguridad

La gestión de la seguridad de la Plataforma de @firma se regula mediante la Política de Seguridad de la Información aplicable a la Dirección de Tecnologías de la Información y las Comunicaciones, acorde a la legislación vigente y publicada en medios oficiales. A fecha de publicación de este documento es de aplicación la Política de Seguridad de la Información de la Secretaría de Estado de Administraciones Públicas publicada mediante orden TAP/3148/2011.

8.1.1 Seguridad física

Los sistemas físicos donde se encuentra ubicada la Autoridad de Validación están dotados de importantes medidas para garantizar la seguridad física. Todos los sistemas se encuentran en redundancia n+1 sin punto único de fallo.

Se dispone de los siguientes servicios básicos de infraestructuras en el Centro de Proceso de Datos:

- Alimentación eléctrica ininterrumpida.
- Suelo técnico.
- Sistemas de Control de Temperatura y Humedad (HVAC).
- Protección de incendios.
- Control de acceso seguro 24x7 (seguridad física)
- Doble ruta de acceso de cables.

Se aplican los procedimientos de Seguridad Física del Centro de Proceso de Datos de la DTIC, que se encuentran descritos en la normativa que regula el Sistema de Gestión de Seguridad de la DTIC acorde a la Política de Seguridad de la Información.

8.1.2 Seguridad lógica

Con el objetivo de garantizar la seguridad lógica de los datos tratados, existe un control exhaustivo de las conexiones entrantes por medio de dispositivos físicos de seguridad.

Así mismo, la plataforma @firma incorpora medios para evitar peticiones de servicio potencialmente dañinas, en base a un tipado fuerte de parámetros. Cualquier petición considerada no apta, en base a los requisitos de autenticación para la aplicación invocada o a los parámetros incorporados en la petición de servicio, será rechazada.

Se aplican los procedimientos de Seguridad Lógica del Centro de Proceso de Datos de la DTIC, que se encuentran descritos en la normativa que regula el Sistema de Gestión de Seguridad de la DTIC acorde a la Política de Seguridad de la Información.

8.1.2.1 Custodia de información transaccional

La Autoridad de Validación realiza una custodia segura de todos los datos transaccionales para cualquier operación realizada sobre la plataforma @firma. Estos datos incluyen:

- Aplicación cliente que solicita el servicio
- Servicio solicitado
- Fecha y hora de la solicitud
- Información obtenida del Prestador de Servicios de Certificación (respuesta OCSP, identificación de la CRL consultada…).

El proceso de custodia segura implica la firma electrónica y el sellado de tiempo del fichero que contiene los datos y la posterior custodia en medio físico seguro (paso a cinta), aplicando una política de retención de 15 años.

Los datos almacenados incluyen datos de carácter personal de los certificados validados.

Es de aplicación la normativa que regula el Sistema de Gestión de Seguridad de la DTIC acorde a la Política de Seguridad de la Información.

8.1.2.2 Custodia de claves y certificados

A pesar de que el servicio de firma electrónica se encuentra descontinuada y la Autoridad de Validación no admite el alta de aplicaciones en estos servicios, se mantiene el servicio para aquellas aplicaciones que ya lo estuvieran usando. En estos casos el almacenamiento de claves se realiza en un dispositivo criptográfico seguro.

La Autoridad de Validación garantiza que el acceso a estas claves está restringido a las Aplicaciones clientes a las que han sido adjudicadas por el Responsable de la Aplicación y bajo la confirmación del propietario de la clave. Así mismo, la Aplicación cliente deberá autenticar el acceso mediante el uso de firma electrónica en la petición (servicios web y servicio OCSP).

Es de aplicación la normativa que regula el Sistema de Gestión de Seguridad de la DTIC acorde a la Política de Seguridad de la Información.

8.1.3 Seguridad operacional y de personal

Es de aplicación la normativa que regula el Sistema de Gestión de Seguridad de la DTIC acorde a la Política de Seguridad de la Información.

La Autoridad de Validación somete los procedimientos de administración a un estricto control de seguridad regulado por un Plan de Seguridad de la Organización, acorde a la legislación vigente.

Dicho Plan de Seguridad puede consultarse en la Orden TAP/3148/2011, de 7 de octubre, por la que se aprueba la política de seguridad de la información en el ámbito de la administración electrónica del Ministerio de Política Territorial y Administración Pública y en el documento Política de Seguridad para el catálogo de servicios comunes de las Administraciones Públicas.

8.1.4 Continuidad del servicio

La Autoridad de Validación garantiza las condiciones de servicio expresadas en este documento en modalidad 24x7.

Cualquier pérdida de servicio no convenientemente notificada, será tratada como incidencia y pasará a contarse dentro de los protocolos y procedimientos establecidos en el Acuerdo de Nivel de Servicio de la Autoridad de Validación.

No se adquirirá responsabilidad de ningún tipo sobre las pérdidas de servicio no directamente imputables a la Autoridad de Validación, entre las cuales destacan las derivadas de red SARA o servicios de validación de terceros.

Es de aplicación la normativa que regula el Sistema de Gestión de Seguridad de la DTIC acorde a la Política de Seguridad de la Información.

9 Información de la Declaración de Prácticas de Validación

9.1 Control de versión

El documento de Declaración de Prácticas de Validación deberá mantenerse en todo momento actualizado. Para ello, el Responsable de las prácticas de validación realizará revisiones periódicas del documento, supervisando su actualización cuando se produzcan cambios organizativos o técnicos en las prácticas de validación concernientes a los proveedores de servicios de certificación y sistemas de información o cuando sea necesario para adaptarlo a las disposiciones vigentes.

El procedimiento previsto para la actualización de la Declaración de Prácticas de Validación es el siguiente:

- El Responsable de las prácticas de validación deberá recopilar y mantener actualizada la información correspondiente las prácticas de validación, como es: proveedores de servicios de certificación, cambios en las funcionalidades de la plataforma, modificaciones sobre las disposiciones vigentes, etc.
- Las Áreas Responsables de los Sistemas de Información mantendrán actualizada la documentación y procedimientos técnicos relacionados con la Declaración de Prácticas de Validación.
- El Responsable de la Declaración de Prácticas de Validación, asistido por el Responsable de las prácticas de validación revisará y aprobará las distintas versiones de la Declaración de Prácticas de Validación y, en particular, las medidas y normas de carácter organizativo y técnico.

9.2 Punto de publicación

Debido al carácter público del presente documento, éste se encuentra disponible en el Portal de Administración Electrónica (PAE) del MINHAP, en el área de descargas de la iniciativa @firma, referenciado en el anexo A.3 Información de contacto administrativo.

9.3 Responsables

El personal implicado en las prácticas de validación está identificado con la Dirección de la Autoridad de Validación, el cual asume las responsabilidades asociadas a la publicación y ejerce funciones de coordinación y control de las prácticas de validación descritas en el presente Documento de Seguridad.

El Responsable de la Declaración de Prácticas de Validación es la Dirección de Tecnologías de la Información y las Comunicaciones del MINHAP.

9.4 Responsabilidades legales

A continuación se establecen las responsabilidades que asumen las distintas partes en el uso y mantenimiento de los servicios y sus implicaciones según la normativa vigente.

9.4.1 Reglamentación Aplicable

La ejecución, interpretación, modificación o validez de la Prácticas de Validación y Revocación se regirá por lo dispuesto en la Legislación Española y en las Directivas y Reglamentos Comunitarios aplicables a este sector. Se puede encontrar referencia a la legislación aplicable en el apartado 3.2 de esta Declaración de Practicas de Validación.

9.4.2 Responsabilidad

La DTIC realizará cuantos esfuerzos sean necesarios a fin de garantizar la mayor precisión y fiabilidad posibles en las informaciones procesadas y/o transmitidas a fin de evitar errores en las mimas.

La DTIC se compromete a realizar un mantenimiento constante de los servicios de la plataforma de validación.

La DTIC pone a disposición de los usuarios la presente declaración de prácticas que podrá consultarse en el punto de publicación identificado en la página de información de la VA indicada en el Anexo A.3.

9.4.3 Limitación de responsabilidades

La DTIC no se hace responsable de la inclusión de datos incorrectos que sean consecuencia de la insuficiente o incorrecta información facilitada por el PSC.

La DTIC no se hace responsable de los errores, anomalías o averías que sean debidas a virus informáticos, fallos o problemas de la red propia o ajena o a una utilización irregular de los servicios citados en el documento, así como de la incorrecta utilización del usuario final o aplicaciones integradas.

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

- Cualquier circunstancia de exoneración definida por la política de certificación de la AC.
- Cuando el perjuicio causado fuera en el periodo de verificación de las causas de suspensión.
- Cuando el perjuicio causado fuera en el periodo de actualización de los datos contenidos en la CRL.
- Estado de Guerra, Sitio y Excepción, ante desastres naturales o cualquier otro caso de Fuerza Mayor.

9.4.4 Protección de datos de carácter personal

Desde la DTIC se cumple con la normativa vigente en protección de datos y concretamente lo dispuesto por la indicada Ley Orgánica 15/1999 de 13 de diciembre de Protección de Datos de Carácter Personal. Así como lo dispuesto en la Ley 59/2003 de Firma Electrónica.

La Autoridad de Validación de @firma es el Encargado de Tratamiento, de cuyos datos son Responsables las unidades usuarios de la Plataforma @firma. La información recopilada es la presente en los certificados que se envían a validar, y en casos puntuales de actualización

de firmas, se almacena la firma electrónica enviada, por lo que de ser una firma implícita, se almacenará también el contenido firmado, sin ser capaces de discriminar el nivel LOPD de dichos documentos. Esta información no se procesa y solo se almacena para trazabilidad de peticiones y respuestas. El nivel de seguridad de la misma es Básico.

La DTIC se responsabilizará del mantenimiento y buen funcionamiento de la aplicación y de la seguridad e integridad de los datos de carácter personal que la aplicación gestiona., mediante el cumplimiento de las siguientes directrices recogidas en su Documento de Seguridad, de acuerdo al nivel de seguridad de la Plataforma de @firma:

- Control de Acceso Lógico
- Control de Acceso Físico
- Copias de Respaldo y Recuperación
- Gestión de Incidencias
- Gestión de Equipos y Soportes
- Gestión de Entornos de Pruebas
- Gestión de Ficheros Temporales
- Régimen de Trabajo fuera de los locales
- Transmisión de Información por Medios Electrónicos
- Confidencialidad de la Información
- Regulación del Encargo de Tratamiento

El encargado del tratamiento únicamente tratará los datos conforme a las especificaciones contenidas en el presente documento y con los fines establecidos en las mismas y no los comunicará, ni siquiera para su conservación, a otras personas distintas de las autorizadas por el responsable del fichero.

La DTIC queda autorizada, en los términos establecidos en el artículo 21 del Real Decreto 1720/2007, de 21 de diciembre, a subcontratar los siguientes servicios en relación con el tratamiento del fichero:

a) Tareas de desarrollo y mantenimiento de las aplicaciones que realizan los tratamientos de datos del fichero.

b) Tareas de soporte y mantenimiento de Infraestructura técnica de los sistemas físicos y lógicos relacionados con los tratamientos de datos del fichero.

La DTIC queda autorizada a comunicar a las empresas subcontratistas aquellos datos que sean estrictamente necesarios para el cumplimiento de las subcontrataciones arriba indicadas. Las empresas subcontratistas deberán comprometerse por escrito con el encargado del tratamiento, a cumplir las obligaciones establecidas en la legislación de protección de datos en relación con los datos a los que tengan acceso con motivo de la contratación.

El tratamiento se realizará en los locales del encargado del tratamiento o en los de quien se encargue de la Infraestructura técnica de los sistemas físicos y lógicos relacionados con los tratamientos de datos del fichero.

Se considerará confidencial toda la información que no esté catalogada expresamente como pública. No se difunde información declarada como confidencial sin el consentimiento expreso por escrito de la entidad u organización que le haya otorgado el carácter de confidencialidad, a no ser que exista una imposición legal.

9.4.5 Obligaciones de la VA

La Autoridad de Validación asume las siguientes obligaciones:

- Validar las firmas y los certificados de los documentos que hayan sido firmados usando certificados emitidos por los prestadores de servicios de certificación aceptados por la misma.
- Comprobar el estado de vigencia de los certificados digitales, haciendo uso de los medios que con este fin pone cada PSC, a disposición de los usuarios y que se concretan en los sistemas basados en consulta de listas de certificados revocados (CRLs), o sistemas de comprobación en línea (OCSP) o cualesquiera otros sistemas que hayan sido aprobados.

9.4.6 Obligaciones de Usuario

El uso de los servicios de la Autoridad de Validación implica la aceptación de las Obligaciones que se describen a continuación.

Enviar a la Autoridad de Validación toda la información referente al Certificado del cual pretende comprobar la validez, así como los datos de identificación de usuario en cada solicitud de validación.

Usar las claves criptográficas de identificación de las aplicaciones usuarias frente a la Autoridad de Validación solamente para sus usos previstos, limitando con ello su uso.

Tomar las precauciones necesarias para evitar que las claves privadas sean utilizadas sin su permiso.

El usuario debe custodiar de forma diligente su clave privada y el código que le permite usarla, para evitar que se pueda suplantar su identidad y firmar peticiones en su nombre o acceder a mensajes confidenciales.

Caso de detectar cualquier indicio de que el soporte de las claves o el certificado electrónico hayan podido ser manipulados por terceras personas, o que el código haya podido ser conocido por otro, el usuario debe notificarlo a la Autoridad de Certificación que lo emitió, así como a la Autoridad de Validación, en un plazo de tiempo razonable, a fin de pedir la revocación del certificado.

Conocer y sujetarse a las garantías, límites y responsabilidades aplicables en la aceptación, uso y validación de los certificados en los que confía, y aceptar sujetarse a las mismas.

9.4.7 Obligaciones de terceros

Denominamos terceros a aquellas entidades que actúan cómo Prestadores de Servicios de Certificación y/o Autoridades de Certificación, entendiendo por tal la persona física o jurídica que expide certificados electrónicos o presta otros servicios en relación con la firma electrónica, establecidos en España en los términos recogidos en la Ley de firma electrónica.

El prestador de servicios de certificación debe cumplir las obligaciones y estar sujeto a las responsabilidades establecidas expresamente en la citada Ley 59/2003 de firma electrónica y en el 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.

En concreto se compromete a notificar a @firma con la mayor prontitud posible la existencia de cualquier problema con sus métodos de validación.

ANEXOS

A.1 Algoritmos y bases criptográficas

A pesar de que la recomendación ETSI TS 102 176-1 recomienda solamente utilizar algoritmos de hash seguros (SHA1, SHA2, Whirpool,…) como Autoridad de Validación no se obligará a las peticiones realizadas sobre firmas electrónicas y certificados que incorporen un algoritmo de hash o de firma electrónica no confiable, y se efectuará una validación en las condiciones de seguridad ofrecidas por la fortaleza estimada de dichos algoritmos.

@firma no garantiza la fortaleza de los algoritmos utilizados, aunque en caso de debilidad manifiesta de un algoritmo, se publicará dicha debilidad a los Organismos y aplicaciones afectados.

@firma proporcionará y mantendrá actualizada una suite de algoritmos para proporcionar las máximas capacidades de validación de firmas electrónicas y certificados digitales, así como de securización para los procesos internos de la propia @firma y de las respuestas proporcionadas a las aplicaciones clientes. Por este motivo, se podrá restringir el uso de algoritmos específicos en la emisión de respuestas, siendo responsabilidad de la aplicación integrada la correcta manipulación de dicha respuesta, así como su validación.

A.1.1 Formatos de firma soportados

Los formatos y formatos extendidos reconocidos se encuentran recogidos en las siguientes tablas:

CAdES	**Versión**				
	1.6.3	**1.7.3**	**1.7.4**	**1.8.1**	**1.8.3**
BES Basic Electronic Signature	✓	✓	✓	✓	✓
EPES Explicit Policy-based Electronic Signatures	✓	✓	✓	✓	✓
T Timestamp	✓	✓	✓	✓	✓
C Complete	✓	✓	✓	✓	✓
X eXtended	✓	✓	✓	✓	✓
XL Long eXtended	✓	✓	✓	✓	✓
A Archiving	✗	✓	✓	✓	✓

Tabla 5. Formatos reconocidos CAdES

CAdES BASELINE	Versión 2.2.1
B-Level Basic Level	✓
T-Level Trusted Time for Signature Existence	✓
LT-Level Long Term Level	✓
LTA-Level Long Term with Archive Time-Stamps	✓

Tabla 6. Formatos reconocidos CAdES Baseline

XAdES	Versión 1.1.1	1.2.2	1.3.2	1.4.1	1.4.2
BES Basic Electronic Signature	✓	✓	✓	✓	✓
EPES Explicit Policy-based Electronic Signatures	✓	✓	✓	✓	✓
T Timestamped	✓	✓	✓	✓	✓
C Complete	✓	✓	✓	✓	✓
X eXtended	✓	✓	✓	✓	✓
XL Long eXtended	✓	✓	✓	✓	✓
A Archiving	✓	✓	✓	✓	✓

Tabla 7. Formatos reconocidos XAdES

XAdES BASELINE	Versión 2.1.1
B-Level Basic Level	✓
T-Level Trusted Time for Signature Existence	✓
LT-Level Long Term Level	✓
LTA-Level Long Term with Archive Time-Stamps	✓

Tabla 8. Formatos reconocidos XAdES Baseline

PAdES	Versión 1.1.1	1.1.2	1.2.1
Básico Part 2 – ISO 32001	-	-	✓
BES Part 3 – Basic Electronic Signature	-	✓	-
EPES Part 3 – Explicit Policy-based Electronic Signatures	-	✓	-
LTV Part 4 – Long Term Validation	-	✓	-
XML Part 5 –Profile for XAdES	✕	-	-

Tabla 9. Formatos reconocidos PAdES

PAdES BASELINE	Versión 2.2.2
B-Level Basic Level	✓
T-Level Trusted Time for Signature Existence	✓
LT-Level Long Term Level	✓
LTA-Level Long Term with Archive Time-Stamps	✓

Tabla 10. Formatos reconocidos PAdES Baseline

ASiC BASELINE	Versión 2.2.2
ASiC-S CAdES Simple Container	✓
ASiC-S XAdES Simple Container	✓
ASiC-S Time-stamp Token Simple Container	✕
ASiC-E CAdES Extended Container	✓
ASiC-E XAdES Extended Container	✓
ASiC-E Time-stamp Token Extended Container	✕

Tabla 11. Formatos reconocidos ASiC Baseline

	Versión
XML Digital Signature	**N/A**
XMLDSig	✓
Cryptographic Message Syntax	**3.0**
CMS	✓
Open Document Format	**1.1**
ODF	✓
Open Office XML	**N/A**
OOXML	✓

Tabla 12. Otros formatos reconocidos

A.1.2 Algoritmos de hash soportados

ALGORITMO DE HASH	FORMATO DE FIRMA					
	CMS	CAdES	XMLDSIG	XAdES	PAdES	ODF/OOXML
MD2	✓	✓	✓	✓	✓	✓

MD5	✓	✓	✓	✓	✓	✓
SHA1	✓	✓	✓	✓	✓	✓
SHA256	✓	✓	✓	✓	✓	✓
SHA384	✓	✓	✓	✓	✓	✓
SHA512	✓	✓	✓	✓	✓	✓

Tabla 13. Algoritmos de hash admitidos por formato

A.1.3 Algoritmos de firma soportados

Un algoritmo de firma electrónica se compone de 2 algoritmos: uno asimétrico y uno de hash. Los algoritmos admitidos por @firma incluyen RSA o ECDSA como algoritmo asimétrico en combinación con los algoritmos de resumen anteriores.

ALGORITMO DE FIRMA	FORMATO DE FIRMA					
	CMS	CAdES	XMLDSIG	XAdES	PAdES	ODF/OOXML
MD2withRSA	✓	✓	✗	✗	✗	✗
MD5withRSA	✓	✓	✓	✓	✗	✗
SHA1withRSA	✓	✓	✓	✓	✓	✓
SHA256withRSA	✓	✓	✓	✓	✓	✓
SHA384withRSA	✓	✓	✓	✓	✓	✓
SHA512withRSA	✓	✓	✓	✓	✓	✓
SHA1withECDSA	✓	✓	✓	✓	✓	✓
SHA256withECDSA	✓	✓	✓	✓	✓	✓
SHA384withECDSA	✓	✓	✓	✓	✓	✓
SHA512withECDSA	✓	✓	✓	✓	✓	✓

Tabla 14. Algoritmos de firma admitidos por formato

A.2 Prestadores admitidos

La información de los prestadores que incluye y valida la plataforma @firma está disponible en el Portal de Administración Electrónica (ver dirección web en el Anexo 3). Para los certificados indicados, además de la validación de los certificados y firmas electrónicas realizadas con ellos, se proporciona información detallada de la identidad del sujeto poseedor del certificado, así como otra información relevante del certificado.

Además se validan todos aquellos certificados reconocidos incluidos en las TSL de los países Europeos, acorde a la Decisión de Ejecución (UE) 2015/1505 de la Comisión de 8 de septiembre de 2015 por la que se establecen las especificaciones técnicas y los formatos relacionados con las listas de confianza de conformidad con el artículo 22, apartado 5, del Reglamento (UE) no 910/2014 del Parlamento Europeo y del Consejo, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior.

A.3 Información de contacto administrativo

La información de contacto se mantiene actualizada en la página Web de la Plataforma de Validación @firma en el Portal de Administración Electrónica. A fecha de publicación de este documento, la información es la siguiente:

Centro de Atención a Integradores y Desarrolladores (CAID)	
WEB	http://administracionelectronica.gob.es/es/ctt/afirma
Contacto	https://ssweb.seap.minhap.es/ayuda/consulta/CAID
Horario	El servicio se presta de Lunes a Jueves de 08:30 a 18:30 y viernes 08:30 a 15:00, con carácter gratuito.
Dirección postal	Ministerio de Hacienda y Administraciones Públicas Dirección de Tecnologías de la Información y las Comunicaciones Att. Plataforma de validación y firma electrónica Calle María de Molina, 50, 9ª Planta 28006 – Madrid

Tabla 15. Contacto de soporte

A.4 Herramientas adicionales de Firma

Se proporcionan herramientas adicionales de firma electrónica a través de la Suite de productos de @firma. Entre estas herramientas destacan:

- Aplicaciones de firma en cliente, tanto en entornos de escritorio como en entornos móviles o firma de usuario en servidor remoto.
- Librerías de integración con @firma.
- Librerías de firma en servidor.
- Servicio de sellado de tiempo.
- Generador de copias auténticas en papel de documentos firmados electrónicamente.
- Portafirmas.

Se pueden consultar estas herramientas en la página de la Suite de @firma:

http://administracionelectronica.gob.es/PAe/SUITE@firma

A.5 Certificados usados por la Autoridad de Validación

La información sobre los certificados usados por la Autoridad de Validación se mantiene actualizada en el área de descargas de la página Web de @firma en el Portal de Administración Electrónica. A fecha de publicación de este documento, los certificados usados son los siguientes.

A.5.1 Certificados plataforma de PRODUCCION

OCSP

Algoritmo de firma	sha256RSA
Emisor	CN = AC DNIE 001 OU = DNIE O = DIRECCION GENERAL DE LA POLICIA C = ES
Subject	CN = AV DNIE MINHAP OU = MINHAP OU = DNIE O = DIRECCION GENERAL DE LA POLICIA C = ES

Tabla 16. Certificado producción OCSP

SOAP

Algoritmo de firma	sha256RSA
Emisor	C = ES O = ACCV OU = PKIACCV CN = ACCVCA-120
Subject	C = ES O = Ministerio de Hacienda y Administraciones Públicas OU = sello electrónico SERIALNUMBER = S2833002E CN = SERVICIOS DE FIRMA ELECTRONICA E IDENTIDAD DIGITAL

Tabla 17. Certificado producción SOAP

A.5.2 Certificados plataforma de PRE- PRODUCCION

Certificados de la Plataforma de Pruebas de desarrolladores, servicios estables

OCSP

Algoritmo de firma	sha256RSA
Emisor	CN = AC DNIE 001 OU = DNIE O = DIRECCION GENERAL DE LA POLICIA C = ES
Subject	CN = AV DNIE MINHAP OU = MINHAP OU = DESARROLLO OU = DNIE O = DIRECCION GENERAL DE LA POLICIA C = ES

Tabla 18. Certificado pre-producción OCSP

SOAP

Algoritmo de firma	sha256RSA
Emisor	C = ES O = ACCV OU = PKIACCV CN = ACCVCA-120
Subject	C = ES O = Ministerio de Hacienda y Administraciones Públicas OU = sello electrónico SERIALNUMBER = S2833002E CN = SERVICIOS DE FIRMA ELECTRONICA E IDENTIDAD DIGITAL - DESARROLLO

Tabla 19. Certificado pre-producción SOAP

A.6 URL de los servicios ofrecidos.

Las direcciones de acceso de los servicios ofrecidos por la Autoridad de Validación se mantiene actualizada en el área de descargas de la página Web de @firma en el Portal de Administración Electrónica. A fecha de publicación de este documento, las URL usadas son las siguientes.

URL de la plataforma de PRODUCCION	
OCSP	http://afirma.redsara.es/servidorOcsp/servidorOCSP
SOAP	http://afirma.redsara.es/afirmaws/services/
(WS modo seguro)	https://afirma.redsara.es/afirmaws/services/

Tabla 20. URL producción

URL de la plataforma de PRE-PRODUCCION (PRUEBAS DE INTEGRACION)	
OCSP	http://des-afirma.redsara.es/servidorOcsp/servidorOCSP
WS	http://des-afirma.redsara.es/afirmaws/services/
(WS modo seguro)	https://des-afirma.redsara.es/afirmaws/services/

Tabla 21. URL pre-producción