

Declaración de Prácticas de Validación

@firma v5.0

Documento nº:	@firmaV5p0_DPV_F20080708
Revisión:	8.3
Fecha:	08-07-2008
Período de retención:	Permanente durante su período de vigencia + 3 años después de su anulación

CONTROL DE COMPROBACIÓN Y APROBACIÓN

Documento nº: @firmaV5p0_DPV_F20080708
Revisión: 8.3
Fecha: 08-07-2008

REALIZADO

31-01-2008

Fernando	Roberto
Gozalo	Puerta
Díaz	Mateos
<hr/>	
Analista Firma Electrónica	Analista Firma Electrónica

COMPROBADO

31-01-2008

María Jesús
Sánchez-Roldán
Gómez
Jefe de proyecto

APROBADO

08-07-2008

Alfonso	Miguel	Laura
Berral	Álvarez	Cabezas
López	Rodríguez	Manso
<hr/>		
Director de Proyecto		

CONTROL DE MODIFICACIONES

Rev. 000
Fecha 01-10-2007
Autor/es FGD
Descripción DPV inicial

Rev. 001
Fecha 23-11-2007
Autor/es FGD, RPM
Descripción Se añaden referencias, se corrigen algunos errores y se completan puntos pendientes.

Rev. 003
Fecha 18-01-2008
Autor/es RPM
Descripción Se incluyen las observaciones y correcciones propuestas por el MAP.

Rev. 004
Fecha 31-01-2008
Autor/es RPM
Descripción Se incluyen las observaciones y correcciones propuestas por el MAP.

Rev. 005
Fecha 27-02-2008
Autor/es PJZ
Descripción Se completan los puntos 6.4 y 7.6

Rev. 8.0
Fecha 28-02-2008
Autor/es LCM
Descripción Se pasa a versión definitiva, sustituyendo la declaración de Prácticas de Certificación 7.1.

Rev. 8.1
Fecha 27-03-2008
Autor/es LCM
Descripción Se añade referencia a RD de inclusión de @firma en los ficheros de datos personales del MAP

Rev. 8.2
Fecha 26-05-2008
Autor/es Soporte @firma
Descripción Se añade nuevo certificado de Sello Electrónico (Camerfirma)

Rev. 8.3
Fecha 08-07-2008
Autor/es Soporte @firma
Descripción Modificación de los certificados de firma de respuestas del servicio OCSP responder

CONTROL DE DISTRIBUCIÓN

Documento nº: @firmaV5p0_DPV_F20080708
Revisión: 8.3
Fecha: 08-07-2008

Copias Electrónicas:

La distribución de este documento ha sido controlada a través del sistema de información.

Copias en Papel:

La vigencia de las copias impresas en papel está condicionada a la coincidencia de su estado de revisión con el que aparece en el sistema electrónico de distribución de documentos.

El control de distribución de copias en papel para su uso en proyectos u otras aplicaciones es responsabilidad de los usuarios del sistema electrónico de información.

Fecha de impresión 07/07/2008

Distribución en Papel:

Nombre o Cargo y (Organización)	Nº de Ejemplares	Referencia de la carta de transmisión_y fecha

Índice

1	Definiciones	8
2	Normas y estándares de aplicación	8
3	Introducción	9
4	Objeto y alcance.....	9
5	Servicios de la plataforma	10
5.1	Servicios ofrecidos por la Autoridad de Validación.....	11
5.2	Servicio de Validación	12
5.2.1	Validación de Certificados X.509v3 mediante http, ftp, ldap, OCSP	12
5.2.2	Obtención de información de certificados.	13
5.2.3	Validación de firma electrónica en múltiples formatos: XMLDsig, XAdES, CMS.....	13
5.2.4	Validar Firma Bloques Completo.....	13
5.2.5	Validar Firma Bloques en documento	13
5.2.6	Validación Multinivel de Certificados Reconocidos por @firma	14
5.2.7	OCSP responder	14
5.2.8	Servicio de Caché de Validación.....	14
5.3	Servicios de Firma	14
5.3.1	Servicio de Firma en servidor	14
5.3.2	Servicio de Firma y Multifirma de ficheros en cliente.....	15
5.3.3	Servicio de Custodia de Elementos de No Repudio	16
6	Usuarios	16
6.1	Organismos públicos.....	16
6.2	Usuarios Finales.....	16
6.3	Acceso a través de red SARA.....	16
6.4	Servicio de atención a usuarios	17
7	Operativa de la Autoridad de Validación.....	18
7.1	Política de Administración de la VA del MAP	18
7.1.1	Procedimientos.	18
7.1.2	Acceso a la información por “webservice” y OCSP responder.....	19
7.2	Uso de certificados y listas de revocación.....	19
7.2.1	Publicación de información.....	19
7.2.2	Descarga y actualización de información.....	20
7.3	Política de Custodia de la Información	20
7.3.1	Custodia de Certificados (HSM)	20
7.3.2	Registro de Transacciones.....	20
7.4	Operativa de seguridad	20
7.4.1	Seguridad Física	21
7.4.2	Seguridad Lógica.....	21
7.4.3	Seguridad Operacional (incluye personal)	21
7.5	Documentación de Seguridad.....	23
7.5.1	Seguridad administrativa.....	23
7.5.2	Seguridad de los sistemas de Información	25

7.5.3	Seguridad Criptológica	26
7.6	Perfiles de los certificados empleados en los servicios de validación.....	26
7.6.1	Relacionar los certificados (OCSP signing, SSL, firma, ... de la Plataforma)...	26
7.6.2	Declaración de certificados de la Plataforma	28
8	Elementos de soporte a la operación	28
8.1	Servicios de Administración.....	28
8.2	Servicios de Auditoría y Estadísticas.....	29
8.3	Servicios de Gestión.....	30
8.4	Servicios de Monitorización	31
8.5	Módulo de Gestión de Prestadores	31
8.5.1	Gestión del Árbol de Prestadores de Servicios de Certificación (PSC).....	31
8.5.2	Gestión de tipos de certificados por PSC.....	31
8.5.3	Gestión de Políticas de Confianza.....	32
8.5.4	Importación y Exportación de Elementos de Confianza entre distintas plataformas @firma.....	32
8.6	Módulo de Registro y Gestión de Eventos	32
8.6.1	Servicio de Auditoría y Estadísticas de transacciones	32
8.6.2	Servicio de Monitorización	32
8.6.3	Gestión de Autorizaciones en solicitudes de servicio.....	33
9	Proveedores de Servicios de Certificación.....	33
9.1	Proveedores Reconocidos por la Plataforma	33
9.2	Proveedores pendientes de reconocimiento por la Plataforma	34
9.3	Autoridades de Validación	35
9.4	Tipos de Certificados Reconocidos.....	35
10	Publicación de la Información de la Declaración de Prácticas de Validación.....	47
10.1	Versiones.....	47
10.2	Punto de publicación	48
10.3	Responsables.....	48
11	Responsabilidades legales	49
11.1	Reglamentación Aplicable.....	49
11.2	Responsabilidad.....	50
11.3	Limitación de responsabilidades.....	50
11.4	Protección de datos de carácter personal	51
11.5	Obligaciones de la VA del MAP	51
11.6	Obligaciones de los usuarios.....	51
11.7	Obligaciones de terceros.....	52

1 Definiciones

CEN: Comité Europeo de Estandarización

CRL: Certificate revocation list

CWA: CEN Workshop Agreement.

DNI-e: DNI electrónico.

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.

JAR: Java Archive.

JRE: Java Runtime Environment.

MAP: Ministerio de Administraciones Públicas.

PKI: Public Key Infrastructure.

Plugin (o AddOn): 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). También se usa URL.

URL: Uniform Resource Locator (Localizador Uniforme de Recursos). También se usa URI.

VA: Validation Authority.

WS-S: 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 Normas y estándares de aplicación

- CWA 14170 Security Requirements for Signature Creation Applications.
- CWA 14171 General Guidelines for electronic signature verification.
- CWA 14172-1 EESSI Conformity Assessment Guidance - Part 1: General introduction.
- CWA 14172-3 EESSI Conformity Assessment Guidance - Part 3: Trustworthy systems managing certificates for electronic signatures.

- CWA 14172-8 EESSI Conformity Assessment Guidance - Part 8: Timestamping Authority services and processes.
- ETSI TS 101 861 Time stamping profile.
- ETSI TS 102 023 Policy requirements for time-stamping authorities.
- Sistema de gestión de la calidad de la prestación del servicio, conforme ISO/IEC 9000.
- Sistema de gestión de la seguridad de la plataforma, conforme ISO/IEC 17799:2005 y a ISO-27001:2005.

3 Introducción

El presente documento consiste en la Declaración de Prácticas de Validación (DPV) de la Plataforma de Validación y firma @firma del Ministerio de Administraciones Públicas (MAP)

4 Objeto y alcance

La plataforma de Validación y firma @firma es una solución tecnológica que se centra en facilitar a las aplicaciones los complementos de seguridad necesarios para implementar la autenticación y firma electrónica avanzada basada en certificados digitales de una forma eficaz y efectiva. 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, auditoria de las transacciones y documentos firmados, sellado de tiempos 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.

De esta forma los usuarios de la plataforma se pueden beneficiar de:

- Acceder a los servicios ofrecidos por medio de mecanismos estándar como pueden ser OCSP o Webservice.
- Utilización de los servicios a través de Red SARA.
- Administración delegada para organismos.
- Se suministran reportes mensuales de actividad y transacciones de diferente naturaleza.
- Se dispone de Servicio de Soporte (Centro de Atención al Usuario) a organismos usuarios.
- Reducción de costes e inversiones: desarrollo, soporte, plataforma, etc.

- Accesibilidad a últimas versiones y evoluciones de servicios con total transparencia.

Los servicios de la Plataforma están disponibles para todo Organismo o Entidad Pública perteneciente a las diferentes Administraciones Públicas sea cual sea su ámbito: Administración General del Estado, Comunidades Autónomas, Diputaciones Provinciales o Entes Locales. Desde el Ministerio de 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 admitan autenticación y firma electrónica basada en certificados digitales.

De igual forma es competencia del MAP

- Establecer acuerdos y convenios con Prestadores de Servicios de Certificación registrados en el Ministerio de Industria, Turismo y Comercio y con la Dirección General de la Policía, para la incorporación y el reconocimiento en @firma de los certificados emitidos por dichos PSCs. En los convenios de adhesión a la plataforma se especifican las obligaciones del MAP, las del PSC y se aplica el concepto de transitividad, de forma que un solo convenio con un PSC cubre todas las aplicaciones usuarias de los Organismos usuarios de @firma, sin necesidad de que estos últimos hayan de suscribir acuerdos bilaterales con los primeros.
- Reforzar la calidad y cantidad de los servicios relacionados con la firma electrónica, a partir de impulsar el cumplimiento efectivo de la Política de Firma por parte del sector privado, y el desarrollo de la Comunicación con el programa de la Comisión Europea IDA-BGCA (Bridge Gateway CA for Public Administration) para el intercambio de listas de prestadores de confianza a nivel de la Unión Europea.
- Incluir información asociada tanto a los prestadores como a los tipos de certificados emitidos, incluyendo la necesaria para garantizar la interoperabilidad y homogeneidad de los servicios prestados por la plataforma.

5 Servicios de la plataforma

Existen dos entornos de la plataforma de @firma: uno de pre-producción para la realización de pruebas, y uno de producción, que se corresponde con el entorno real de la plataforma.

La URL de acceso a la página de bienvenida, así como las URL's de acceso a los servicios ofrecidos por la plataforma de pre-producción es:

Desde dentro de la red interadministrativa (SARA):

<https://pre-afirma.redinteradministrativa.es/afirma>

<http://pre-afirma.redinteradministrativa.es:8080/afirmaws/services/>

<http://pre-afirma.redinteradministrativa.es:443/afirmaws/services/>

La URL de acceso a la página de bienvenida, así como las URL's de acceso a los servicios ofrecidos por la plataforma de producción es:

Desde dentro de la red interadministrativa (SARA):

<https://afirma.redinteradministrativa.es/afirma>

<http://afirma.redinteradministrativa.es:8080/afirmaws/services/> (WS)

<http://afirma.redinteradministrativa.es:443/afirmaws/services/> (WS modo seguro)

5.1 Servicios ofrecidos por la Autoridad de Validación

El Ministerio de Administraciones Públicas (en adelante MAP) ha implantado un proyecto denominado "Plataforma de validación y firma electrónica". Este proyecto se centra en facilitar a las aplicaciones los complementos de seguridad necesarios para implementar la autenticación y firma electrónica avanzada basada en certificados digitales. Para ello se ofrece:

- Una aplicación centralizada que se ejecuta en los servidores del MAP y que dispone de una serie de Servicios Web que ponen a disposición de los organismos clientes una serie de funcionalidades de verificación de firma y certificados, impulsando de esta forma el uso de la certificación y firma electrónica en los sistemas de información de las diferentes Administraciones públicas que así lo requieran.

A continuación mostramos la lista de los servicios disponibles en @firma:

- Servicio de Validación
 - o Validación de Certificados X.509v3 mediante http, ftp, ldap, OCSP
 - o Obtención de información de certificados.
 - o Validación de firma electrónica en múltiples formatos: XMLDsig, XAdES, CMS...
 - o Validar Firma Bloques Completo
 - o Validar Firma Bloques en documento
 - o Validación Multinivel de Certificados Reconocidos por @firma
 - o OCSP responder
 - o Servicio de Caché de Validación
- Servicio de Firma

- Servicio de Firma en servidor
 - Firma Servidor.
 - Firma Servidor CoSign
 - Firma Servidor CounterSign
- Servicio de Firma y Multifirma de ficheros en cliente
- Servicio de Custodia de Elementos de No Repudio

La plataforma de Validación y firma @firma es una solución tecnológica que se centra en facilitar a las aplicaciones los complementos de seguridad necesarios para implementar la autenticación y firma electrónica avanzada basada en certificados digitales de una forma eficaz y efectiva.

Como complemento, se ofrece un cliente de firma electrónica, el cual proporciona una serie de funcionalidades que permiten el manejo de certificados X.509 y de las claves privadas asociadas a dichos certificados, así como las funcionalidades necesarias para la generación de distintos tipos de firma electrónica .

Asimismo incluido en el mismo cliente de firma, se encuentra un cliente de cifrado que nos permite realizar las funciones de encriptación y descifrado de datos atendiendo a diferentes algoritmos y configuraciones. Además permite la generación de sobres digitales CMS.

Con esta pieza de software que se ejecuta en la máquina cliente (applet) se consigue cerrar el círculo y ofrecer de esta forma un conjunto completo de funcionalidades de firma, cifrado y manejo de certificados.

A continuación se enumeran y describen los servicios de la Autoridad de Validación del Ministerio de Administraciones Públicas, además de ser descrito cada módulo, se descompone en las partes que contiene.

5.2 Servicio de Validación

Centraliza todos los aspectos de la validación multinivel y comprobación de validez y autenticidad de los certificados X.509 según la RFC 3280.

Este módulo también incluye un Servidor OCSP para terceros y un sistema de caché para optimizar los procesos de validación.

5.2.1 Validación de Certificados X.509v3 mediante http, ftp, ldap, OCSP

Proporciona la funcionalidad necesaria para comprobar el estado de validez de un certificado dado, pudiéndose realizar los siguientes tipos de validaciones:

- Validación Simple: resultado de la validación de la caducidad, integridad y confianza del certificado.

- Validación Estado: resultado de validación del estado del certificado. Solo será devuelto en caso de realización de una validación compleja.
- Validación Cadena: resultado de validación de la cadena de confianza del certificado. Solo será devuelto en caso de realización de una validación compleja.

Permite configurar varios niveles de validación ante un mismo PSC. De esta forma es posible que un certificado pueda ser validado por ejemplo por OSCP inicialmente, por LDAP (varios nodos) en caso de que falle el primero, y por http en el peor de los casos cuando fallen los dos métodos anteriores.

5.2.2 Obtención de información de certificados.

Permite extraer la información de un certificado mediante la aplicación del mapeo definido para su tipo. Este proceso verificará que el tipo de certificado se encuentra definido en la plataforma y que la aplicación que realiza la petición tiene acceso a dicho tipo de certificado.

Este proceso está compuesto por un analizador semántico de certificados y mapeo de campos que permite por cada tipo de certificado asociado a un PSC, establecer un "certificado tipo" donde se definen aquellos campos de interés para la plataforma. A esto se le denomina mapeado de campos.

5.2.3 Validación de firma electrónica en múltiples formatos: XMLDsig, XAdES, CMS...

Proporciona la funcionalidad de verificar la firma de un fichero dado siendo capaz de reconocer los siguientes formatos de firma: PKCS7, CMS, XMLDSignature, XAdES, XAdES-BES o XAdES-T. Todos estos formatos son admitidos para firmas 'attached' o 'detached'.

Como resultado de una verificación de firma se obtienen los datos de 'estado de la firma' (firma correcta o incorrecta), certificado/s (enumeración de el/los certificado/s con los que se firmó el fichero verificado), 'sello de tiempo' (en caso de tenerlo muestra la fecha y la hora en la que se firmó el fichero) y 'certificado de la TSA' (certificado utilizado por el servidor de sello de tiempo para generar el mismo).

5.2.4 Validar Firma Bloques Completo

Permite la verificación de una firma por bloques, reconociendo los formatos PKCS7 o CMS.

El resultado de este tipo de verificación proporciona información sobre los pasos dados para realizar la validación y el estado de la firma (correcta o incorrecta).

5.2.5 Validar Firma Bloques en documento

Proporciona la funcionalidad de validación de firmas que se generaron por @firma 4.0. Las firmas debieron haber sido generadas de modo implícito. Valida la firma del bloque así como la firma servidor contenida en el bloque de firmas y asociada al documento indicado.

Como resultado de la verificación se obtiene información sobre los pasos dados para realizar la validación y el estado de la firma (correcta o incorrecta).

5.2.6 Validación Multinivel de Certificados Reconocidos por @firma

Validación Multinivel de certificados (estructura de certificación de más de dos niveles), emitidos por cualquier PSC reconocido y configurado en la plataforma @firma a través del módulo de Gestión de PSCs.

5.2.7 OCSP responder

Servidor OCSP que permite validar certificados mediante este protocolo ante cualquier cliente que lo solicite. El servidor validará el certificado contra el PSC correspondiente mediante los protocolos http, ftp, ldap u OCSP y luego emitirá un ticket que firmará con el resultado de la validación.

5.2.8 Servicio de Caché de Validación

Caché de validación configurable en tiempo, para evitar tener que acceder al PSC ante validaciones de un mismo certificado en un corto período de tiempo.

5.3 Servicios de Firma

Centraliza todos los aspectos relativos a los diferentes tipos de firma, integración y gestión de HSM en @firma.

5.3.1 Servicio de Firma en servidor

Este servicio permite firmar y multifirmar cualquier tipo de ficheros en el servidor @firma con un certificado expedido por cualquier PSC para una entidad concreta. Una misma plataforma permite utilizar "n" certificados de servidor configurables por políticas y con la autorización de uso correspondiente para cada uno de ellos.

Las firmas electrónicas pueden ser realizadas en varios formato: PKCS#7, CMS (compatibilidad con todas sus versiones definidas por la IETF1), XMLSignature Básico y XMLSignature avanzado.

Los siguientes servicios son los ofrecidos para este tipo de firma en servidor:

5.3.1.1 Firma Servidor.

Proporciona la funcionalidad de realizar la firma de un fichero en el servidor utilizando un certificado previamente configurado en la plataforma para tal fin, siendo posible definir más de un certificado para ser usado con este tipo de firma.

El resultado que se obtiene al realizar este proceso ofrece los detalles del estado de la firma (correcta o incorrecta), un identificador único de la transacción realizada y la firma electrónica solicitada.

5.3.1.2 Firma Servidor CoSign

Ofrece la posibilidad de realizar una firma múltiple al mismo nivel de un fichero en el servidor utilizando un certificado previamente configurado en la plataforma para tal fin, siendo posible definir más de un certificado para ser usado con este tipo de firma.

Como resultado de este proceso se obtiene la información referente al estado de la firma (correcta o incorrecta), un identificador único de la transacción realizada y la firma electrónica solicitada.

5.3.1.3 Firma Servidor CounterSign

Permite la realización de una firma múltiple en cadena de un fichero dado en el servidor utilizando un certificado previamente configurado en la plataforma para tal fin, siendo posible definir más de un certificado para ser usado con este tipo de firma.

La firma múltiple en cadena es el procedimiento por el cual un firmante realiza una firma digital sobre el valor de la firma digital del firmante anterior.

El resultado que se obtiene al realizar este proceso ofrece los detalles del estado de la firma (correcta o incorrecta), un identificador único de la transacción realizada y la firma electrónica solicitada.

5.3.2 Servicio de Firma y Multifirma de ficheros en cliente

Proporciona dos tipos de servicio:

- Firma, Multifirma y Multifirma Web masiva. Este servicio permite realizar firma de formularios Web a partir de la información introducida por los usuarios, sin necesidad de realizar cambios importantes en las aplicaciones Web ya existentes. Para ello, la plataforma transforma la página Web original en "firmable" de manera transparente y proporciona los componentes necesarios para realizar el proceso de firma en el cliente. Este servicio también permite la Multifirma jerárquica, sin orden de firmantes establecido, y Multifirma de una página Web de forma masiva por un número elevado de usuarios.

- Firma, Multifirma de Ficheros en cliente. Este servicio permite firmar y multifirmar cualquier tipo de ficheros desde el entorno del cliente, proporcionando los componentes necesarios para llevarlo a cabo. Al igual que el servicio anterior permite realizar la Multifirma de manera jerárquica o sin orden de firmantes establecido.

5.3.3 Servicio de Custodia de Elementos de No Repudio

Este servicio permite configurar mediante políticas la custodia de los elementos de No Repudio generados en una transacción de firma electrónica. Este servicio admite tres posibles políticas:

- Custodia únicamente de los Elementos de No Repudio de las transacciones de firma (sin incluir el documento firmado).
- Sin Custodia de los Elementos de No Repudio de las transacciones de firma. La información de la petición de Servicio queda registrada en el servicio de Gestión de Eventos descrito con anterioridad.

6 Usuarios

A continuación se describen los colectivos relacionados con los servicios de la VA del MAP,

6.1 Organismos públicos

Los servicios de la Plataforma están disponibles para todo Organismo o Entidad Pública perteneciente a las diferentes Administraciones Públicas sea cual sea su ámbito: Administración General del Estado, Comunidades Autónomas, Diputaciones Provinciales o Entes Locales. Desde el Ministerio de 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 admitan autenticación y firma electrónica basada en certificados digitales.

6.2 Usuarios Finales

Los usuarios finales de la plataforma serán aplicaciones informáticas, dichas aplicaciones serán las que interactuarán con el usuario.

6.3 Acceso a través de red SARA

El acceso a los servicios de la Plataforma se realiza a través de S.A.R.A. -Sistema de Aplicaciones y Redes para las Administraciones-, una infraestructura tecnológica que permite y garantiza la comunicación entre las distintas administraciones además de servir de plataforma de intercambio de aplicaciones. Constituye una extranet de comunicaciones que da soporte a la interoperabilidad entre aplicaciones de diferentes organismos públicos.

Incluido dentro de la infraestructura base proporcionada por S.A.R.A., se dispone de un punto neutro de comunicaciones (PNC) que posibilita la accesibilidad a los servicios de la plataforma desde múltiples operadores de comunicaciones, dentro de un esquema de direccionamiento IP privado y con las mayores garantías de monitorización.

La red S.A.R.A. como infraestructura básica de comunicaciones y servicios telemáticos de la AGE se conecta al punto neutro mediante dos enlaces fast Ethernet (100 Mbps) en alta disponibilidad cada uno de ellos con un operador distinto.

La conexión de un nodo de la AGE con la red troncal de la IA cuenta con un enlace principal y otro de backup también con 2 operadores distintos lo que proporciona un aseguramiento en la fiabilidad y continuidad en el servicio prestado. Adicionalmente y como medida de seguridad la información transita a través de la red troncal cifrada mediante el establecimiento de túneles IPSec

S.A.R.A cuenta con un servicio de soporte 24 x 7 en el que los tiempos de respuesta y de resolución dependen de la severidad de la incidencias en base a una categorización de los servicios que por ella transitan y de los agentes que participen extremo a extremo.

6.4 Servicio de atención a usuarios

Se dispone de un equipo de soporte disponible para cooperar con los diferentes Organismos Públicos suministrando toda la información necesaria sobre el uso de los servicios así como para cooperar en las actividades de prueba e integración de los sistemas a los servicios de la Plataforma.

Los datos de contacto son:

Centro de Soporte @firma del MAP

Teléfono: 902 934 405

Horario: El servicio se presta de forma permanente (24 horas al día, 7 días a la semana) y con carácter gratuito.

Dirección de correo electrónico: soporte.afirma5@map.es

Dirección:

Ministerio de Administraciones Públicas

Dirección de Modernización Administrativa

Att. Plataforma de validación y firma DNle

María de Molina, 50, 9ª Planta.

28071 – Madrid

7 Operativa de la Autoridad de Validación

7.1 Política de Administración de la VA del MAP

Los servicios y Prestadores de Servicios de Certificación ofrecidos por la plataforma podrán ser modificados unilateralmente por el MAP. Será obligación de los organismos registrados comprobar regularmente la publicación de la documentación del MAP, para comprobar las posibles variaciones.

En el caso de que uno de los organismos registrados envíe una notificación no aceptando las modificaciones, se entenderá que desiste unilateralmente del contrato que le vincula con el MAP, sin obligación de indemnizar por daños y perjuicios por estas causas.

Todos los cambios propuestos que puedan afectar sustancialmente desde un punto de vista legal, técnico o administrativo a los organismos registrados serán notificados inmediatamente.

7.1.1 Procedimientos.

Los procedimientos son las actuaciones realizadas por soporte con la finalidad de mantener el correcto funcionamiento de la plataforma y de informar sobre el estado de la misma a la dirección del MAP.

Estos procedimientos se vienen a desglosar en categorías, con sus respectivos niveles de urgencia, impacto y tiempos de respuesta, definiendo así mismo los flujos de información.

Se clasifican en 9 grandes categorías:

- Operaciones generales
- PSC's
- Aplicaciones y usuarios
- Incidencias de la Plataforma
- Informes
- Conectividad
- Control
- Conocimiento
- Quejas y reclamaciones

El cumplimiento de los tiempos de resolución de cada uno de los procedimientos es uno de los objetivos fundamentales de Soporte, así como la operatividad de los servicios, cambios de configuración o correcciones y mantener informada a la Dirección del Proyecto sobre dicho cumplimiento.

Para ello, el Centro de Atención al Usuario debe informar a la Dirección con antelación cada vez que prevean que un procedimiento no va a ser resuelto en el tiempo asignado. De la misma manera, una vez que un procedimiento supere el tiempo máximo de resolución, se debe informar a la Dirección del Proyecto. Estas comunicaciones serán por correo electrónico y por teléfono.

7.1.2 Acceso a la información por “webservice” y OCSP responder

La plataforma permite la validación de certificados mediante “webservice” y mediante OCSP Responder. La utilidad a nivel de validación de revocación es la misma, sin embargo, el uso del “webservice” nos permite además, obtener la información relativa al certificado clasificada en el XML de respuesta del mismo.

7.2 Uso de certificados y listas de revocación

Cada PSC tiene obligación de publicar en los tiempos acordados las listas de revocación, en dichas listas se encuentran qué certificados han sido revocados y el motivo y fecha de revocación.

7.2.1 Publicación de información

Cada PSC publica la información en su página Web, a continuación se listan cada uno de ellos con su dirección Web correspondiente:

Nombre de prestador	URL de publicación de la información
DNle	http://www.dnielectronico.es/
FNMT-Ceres	http://www.cert.fnmt.es/
CATCERT	http://www.catcert.net/
CAGVA	http://www.accv.es/
IZENPE	http://www.izenpe.com/
ANF	https://www.anf.es/
Camerfirma	http://www.camerfirma.com/
ACA	https://www.redabogacia.org/
ANCERT	http://www.ancert.com/
Firma profesional	http://www.firmaprofesional.com/
Banesto	https://ca.banesto.es/
SCR	https://www.registradores.org/

DNI electrónico de Portugal (en pruebas)	http://www.cartaodocidadao.pt/
--	---

7.2.2 Descarga y actualización de información

La plataforma realiza periódicamente la descarga las CRL's de los PSCs que lo permiten, esta tarea se realiza automáticamente mediante una tarea configurable en la plataforma utilizando la opción de Gestión de Descargas de CRL's. Aunque el tiempo de vida está delimitado en la CRL la opción permite que la tarea se ejecute con una periodicidad inferior a este tiempo para tratar de mejorar la fiabilidad de las listas cacheadas. Por otro lado algún proveedor puede notificar al sistema que una CRL ha sido actualizada, si esto se produce, la plataforma descarga esa única CRL actualizando su base de datos con la información que ella contiene.

Las peticiones de OCSP se realizan en línea al PSC correspondiente a la dirección que indique el campo correspondiente en el certificado (Authority Information Access) o bien a una dirección predefinida en función del PSC.

7.3 Política de Custodia de la Información

Las aplicaciones alojan información sobre los métodos de validación, políticas de firma y custodia, información sobre el responsable y otros datos, que conforman una política de aplicación, la cual determina las reglas aplicadas a los servicios ofrecidos por la plataforma.

7.3.1 Custodia de Certificados (HSM)

Este servicio ofrece la posibilidad de custodiar todas las claves privadas de los certificados ubicados en el servidor de @firma en un módulo hardware criptográfico. De esta forma, se aporta un mayor nivel de seguridad a los certificados de organizaciones ubicados en el Servidor de @firma.

7.3.2 Registro de Transacciones

La plataforma @firma 5.0 proporciona la funcionalidad de registro y gestión de todos eventos ocurridos en la plataforma, a través del Módulo de Registro y Gestión de Eventos. Ello permite garantizar la integridad y el no repudio de toda la información generada por los distintos módulos del sistema de forma que se garantice que los datos almacenados son realmente los datos que se generaron en el sistema. Otra aplicación práctica del registro de eventos es que permite la posibilidad de generar informes y estadísticas sobre la utilización de la plataforma.

7.4 Operativa de seguridad

Los controles de acceso a la información constituyen uno de los parámetros más importantes a la hora de Administrar Seguridad. Con ellos determinamos quién puede acceder a qué datos, indicando a cada persona un tipo de acceso (perfil) específico.

Para este cometido se utilizan diferentes técnicas que se diferencian significativamente en términos de precisión, sofisticación y costos. Se utilizan por ejemplo, palabras claves, algoritmos de encriptación, listas de controles de acceso, limitaciones por ubicación de la información, horarios, etc.

Una vez determinados los controles de accesos a la Información, se hace imprescindible efectuar una eficiente administración de la Seguridad, lo que implica la implementación, seguimiento, pruebas y modificaciones sobre los "Perfiles" de los usuarios de los Sistemas.

7.4.1 Seguridad Física

Todos los sistemas se encuentran en redundancia n+1 y 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.

7.4.2 Seguridad Lógica

Además de los controles habituales del sistema operativo respecto a usuarios y listas de control de acceso, se dispone del control de acceso a los datos mediante el sistema gestor de base de datos, el cual se encarga de que sólo los usuarios con permiso puedan visualizar la información sensible.

7.4.3 Seguridad Operacional (incluye personal)

El objetivo de los controles de la seguridad ligada al personal que hará uso de la Plataforma @firma es reducir los riesgos que van asociados a errores humanos o que son fruto de un uso inapropiado de los recursos por parte de los usuarios.

Los controles de la seguridad ligada al personal están asociados a los Recursos Humanos que utilizan y tienen acceso a la Plataforma @firma, se establecen antes, durante y después de la contratación o relación laboral.

Estos controles deben ser aplicados el MAP a la hora de seleccionar el personal que trabaje para él en el ámbito de la Plataforma @firma y por los diversos Proveedores externos, cuyo personal de una manera u otra intervienen en el desarrollo, administración, mantenimiento y soporte de la Plataforma.

7.4.3.1 Condiciones de seguridad previas a la contratación de personal

Los controles establecidos son los siguientes:

- Definición de funciones y responsabilidades asociadas a cada puesto de trabajo.

- Las funciones y responsabilidades en materia de seguridad asociadas al puesto de trabajo se detallan a los candidatos durante el proceso de selección.
- Confirmación de Curriculum y/o investigación de candidatos en los procesos de selección, especialmente para puestos claves o críticos (respetando la legislación en materia de protección de datos y los derechos de los trabajadores) para tener conocimiento de la cualificación y conveniencia del personal que por motivos laborales vaya a acceder a los activos de la Plataforma @firma.

7.4.3.2 Condiciones de seguridad durante el desempeño de funciones

Los controles de seguridad dirigidos a velar por la seguridad durante el desempeño de sus funciones por parte del personal son los siguientes:

- Exigencia de firma de acuerdos o cláusulas de confidencialidad y deber de secreto en los contratos.
- Formación y entrenamiento específicos para el puesto de trabajo a ocupar y las funciones a realizar con el fin de minimizar los riesgos por falta de un adecuado conocimiento sobre los recursos y herramientas utilizados.
- Duplicidad de personal para puestos críticos.
- Asignación de privilegios de acceso a los activos y recursos de la Plataforma @firma en base a las condiciones del puesto ocupado.
- Revisión periódica de los privilegios asignados al personal en base a las funciones definidas para cada puesto.
- Registro de la actividad crítica realizada sobre los activos y recursos de la Plataforma @firma.
- Elaboración y aceptación de códigos de conducta y buenas prácticas de seguridad por parte de los empleados.
- Medidas de formación y sensibilización en materia de seguridad dirigidas a todos los empleados y colaboradores de los servicios de validación y firma electrónica del MAP para que puedan hacer un uso adecuado y acorde con la seguridad de los activos de la Plataforma @firma.
- Definición de un proceso disciplinario que permita en caso necesario aplicar las normas vigentes dentro de los procedimientos de la Administración a aquellos empleados que intencionadamente incurran en infracciones de las medidas de seguridad o tengan un comportamiento temerario o negligente en el desempeño de sus funciones.

7.4.3.3 Condiciones de seguridad al término o cambio de funciones

Se definen las condiciones de seguridad que se contemplan cuando se produce un cambio de funciones o cuando finaliza el contrato que liga a una persona a la Plataforma @firma.

Para ello se han implantado las siguientes medidas:

- Existe un procedimiento para hacer efectiva la retirada de derechos de acceso a la red, los sistemas, bases de datos y aplicaciones, a los usuarios cuando sus nuevas funciones no requieran dichos accesos o a la finalización de la relación contractual.

- Devolución de los activos por parte del Proveedor externo, si fuera el caso, a la finalización del servicio prestado al MAP o de la relación contractual concreta de un empleado de dicho Proveedor externo.

7.5 Documentación de Seguridad

Para garantizar la seguridad de la plataforma de validación del MAP e implantar las salvaguardas necesarias para la protección de los activos de este sistema se ha aplicado la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, MAGERIT versión 2, muy consolidada en proyectos de Administración electrónica, así como PILAR, su herramienta de gestión de riesgos.

Se ha colaborado con el Centro Criptográfico Nacional con el objetivo de acreditar el uso de esta plataforma para el ámbito de la Administración General del Estado y también optar a la correspondiente certificación del cumplimiento de estándares internacionales, tanto desde el punto de vista técnico como de seguridad.

Se han tenido presentes las prácticas y controles de seguridad propuestos por los Criterios de Seguridad, Normalización y Conservación de las aplicaciones utilizadas para el ejercicio de potestades del Consejo Superior de Administración Electrónica, así como las normas relevantes en la materia: UNE ISO/IEC 17799:2002 Código de buenas prácticas para la gestión de la seguridad de la información.

Por todo ello, la plataforma ha sido diseñada para garantizar la autenticidad, confidencialidad, integridad y la disponibilidad de toda la información que se intercambia tanto con las Administraciones Públicas como las Autoridades de Certificación adheridas a la plataforma.

7.5.1 Seguridad administrativa

La Seguridad Administrativa en el MAP está regulada por un Plan de Seguridad que se ajusta a la legislación vigente en materia de protección de datos personales. Este Plan establece medidas técnicas y organizativas.

La seguridad administrativa esta basada en la distribución de las responsabilidades en los siguientes roles:

- Propietario: De manera general, en términos de seguridad, el propietario de un activo es el que organizativamente tiene la responsabilidad de mantener dicho activo operativo, determinar su clasificación, su criticidad y el nivel de seguridad requerido y definir y aprobar las medidas organizativas y técnicas para su protección.
- Custodio: Es el responsable de establecer, administrar y mantener las medidas y controles de seguridad adecuados para proteger los activos de acuerdo con el nivel de protección requerido por el propietario.

- Responsable de seguridad: Es el encargado de ayudar a las figuras de Propietario y Custodio a la hora de coordinar y supervisar la implantación y cumplimiento de las medidas de seguridad y control.
- Usuario: Debe conocer el nivel de protección establecido por el Propietario de los activos que utilizan y cumplir los controles y medidas de seguridad implantados por el Custodio.

Las responsabilidades citadas se asignan a unas figuras que constituyen de esta forma el marco para crear, gestionar y mantener la infraestructura de seguridad necesaria para la protección de la Plataforma. Estas figuras son:

- El responsable propietario de la Plataforma @firma: Éste es la Dirección General de Modernización Administrativa del MAP, teniendo como responsabilidades identificar y clasificar sus activos, asignándoles el nivel de seguridad adecuado, aprobar la Política de Seguridad y velar por la implantación y correcto funcionamiento de las medidas y controles de seguridad definidos.
- Responsable/s de Sistemas de Información: Se encargan de la supervisión y coordinación de las operaciones realizadas por los diversos grupos tanto internos como externos con responsabilidad en el desarrollo, administración, mantenimiento y soporte de los Sistemas de Información.
- Responsable/s de Sistemas de Información en Proveedores externos: Se encargan de la gestión y coordinación de las operaciones realizadas por los grupos de desarrollo, administración y mantenimiento de comunicaciones, sistemas, bases de datos, aplicaciones, operación y soporte, pertenecientes a los diversos Proveedores externos.
- Desarrolladores y administradores de aplicaciones: Se encargan de las tareas relacionadas con desarrollo, gestión, mantenimiento y actualización de las aplicaciones de la Plataforma.
- Administradores y operadores de redes, sistemas y bases de datos: Se encargan de la instalación, administración, mantenimiento y actualización de los sistemas operativos, bases de datos y redes de comunicaciones.
- Grupos de soporte: Se encargan de las funciones de soporte 24x7, gestión de incidencias informáticas y de seguridad, y coordinación de las labores informativas respecto al estado de la Plataforma.
- Responsable de Seguridad: Es el encargado de ayudar a la Dirección y los Encargados de los Sistemas de Información en sus labores de definición, implantación y cumplimiento de las medidas de seguridad y control descritas en la Política de Seguridad.
- Operadores: Se trata del personal interno de la Dirección General de Modernización Administrativa, Centros Directivos, Delegaciones y Oficinas, y el personal externo (proveedores, consultores, desarrolladores, etc.) que tienen acceso a los datos de carácter personal del fichero de la Plataforma.

7.5.2 Seguridad de los sistemas de Información

El sistema informático del MAP, dispone de:

- Un procedimiento de solicitud de registro de aplicaciones en el que se registra:
 - Un nombre de aplicación al que se asigna una contraseña.
 - Responsable de la aplicación.
 - Método elegido para el uso de los servicios de la plataforma.
- Un procedimiento de gestión de incidencias en el que se incluyen las solicitudes de instalación y configuración de sistemas, en el que se registran:
 - Quien solicita la instalación o configuración
 - A que equipo se le asigna la tarea
 - Tiempo de resolución.
- Una política de control y aplicación de las mejoras de seguridad que aparecen para los sistemas existentes en la plataforma, que consiste en una revisión y aplicación de parches de seguridad mensual.
- Una política de seguridad perimetral que incluye control de antivirus y análisis de vulnerabilidades, que esta basado en una solución Hardware no intrusiva que analiza continuamente el tráfico de red y registra las alertas detectadas.
- Un procedimiento de detección y registro de intentos de accesos no autorizados. Se registra:
 - Procedencia del operador.
 - Día y hora del ataque.
 - Zonas que se han intentado acceder.
 - Manipulaciones que se han efectuado.

Todos los equipos informáticos, en especial aquellos que son utilizados para el tratamiento de datos personales, están inventariados e identificados con el nivel de acceso que tienen a los datos de carácter personal almacenados y el grado de importancia que presuponen en el marco del tratamiento de la información que aquí se gestiona.

Cualquier salida o incorporación de equipos utilizados en el tratamiento de la información, debe de ser autorizada por el Responsable del área de Informática, el cual es además, responsable del mantenimiento del inventario de equipos, su catalogo de uso y en especial, en aquellos dispositivos que almacenan información, la identificación del tipo de datos que contienen.

7.5.3 Seguridad Criptológica

La plataforma hace uso de dispositivos criptográficos de red para la custodia de las claves criptográficas que se utilizan para las operaciones de firma, no repudio e integridad de la información de las transacciones que gestiona la plataforma.

Los dispositivos criptográficos de red permiten ofrecer importantes funcionalidades como son seguridad, independencia de la aplicación y de la plataforma, flexibilidad, robustez y escalabilidad.

La parametrización de seguridad se compone de:

- Uno o más módulos HSM
- Un conjunto de tarjetas de administrador para controlar el acceso a la configuración del Mundo y a las operaciones de recuperación.
- Uno o varios conjuntos (opcional) de tarjetas de operador para controlar el acceso a las claves de aplicación (cada conjunto controla el acceso a una o varias claves de forma independiente a los demás conjuntos).
- Contraseñas e información de certificados cifrados usando la clave del Mundo y almacenados en el/los servidor/es.

7.6 Perfiles de los certificados empleados en los servicios de validación

A continuación, se relacionan los certificados utilizados en la Plataforma, así como su aplicación y uso.

7.6.1 Relacionar los certificados (OCSP signing, SSL, firma, ... de la Plataforma)

Estos son los certificados que se utilizan en la Plataforma:

PREPRODUCCIÓN

- Asunto: CN=pre-afirma.redinteradministrativa.es, OU=Servidores, O=Generalitat Valenciana, C=ES
- Emisor: CN=CAGVA,OU=PKIGVA,O=Generalitat Valenciana,C=ES
- Número de Serie: 1144077031
- Usos: procesos internos: firma de logs, firma de respuestas de la Plataforma, SSL @firma.

- Asunto: CN=AV DNIE MAP, OU=MAP, OU=PREPRODUCCION, OU=DNIE, O=DIRECCION GENERAL DE LA POLICIA,C=ES
- Emisor: CN=AC DNIE 001, OU=DNIE, O=DIRECCION GENERAL DE LA POLICIA, C=ES
- Número de Serie: 5e ff 65 a8 6c 95 f7 4b 48 60 d0 ef 31 cd 7e 76 (hexa)

- Usos: firma de respuestas del servicio OCSPResponder del MAP.
- Asunto: CN=pre-tsamap.redinteradministrativa.es, OU=PKIGVA, O=Generalitat Valenciana, C=ES
- Emisor: CN=Root CA Generalitat Valenciana, OU=PKIGVA, O=Generalitat Valenciana, C=ES
- Número de Serie: 4684e22b (hexa)
- Usos: firma de sello de tiempo.

PRODUCCIÓN

- Asunto: CN=afirma.redinteradministrativa.es, OU=Servidores, O=Generalitat Valenciana, C=ES
- Emisor: CN=CAGVA, OU=PKIGVA, O=Generalitat Valenciana, C=ES
- Número de Serie: 1144076962
- Usos: procesos internos: firma de logs, firma de respuestas de la Plataforma, SSL @firma.
- Asunto: CN=AV DNIE MAP, OU=MAP, OU=DNIE, O=DIRECCION GENERAL DE LA POLICIA, C=ES
- Emisor: CN=AC DNIE 001, OU=DNIE, O=DIRECCION GENERAL DE LA POLICIA, C=ES
- Número de Serie: 74 e0 fa 57 58 45 56 92 48 60 cf ad 96 81 bc 3c (hexa)
- Usos: firma de respuestas OCSPResponder
- Asunto: CN=TSA1 @firma, OU=PKIGVA, O=Generalitat Valenciana, C=ES
- Emisor: CN=Root CA Generalitat Valenciana, OU=PKIGVA, O=Generalitat Valenciana, C=ES
- Número de Serie: 45 8a d4 a8 (hexa)
- Usos: firma de sello de tiempo.

OTROS CERTIFICADOS COMUNES

- Asunto: CN=HAB. PAG. PER. SUBSE. DE MINISTERIO DE ADMINISTRACIONES PUBLICAS, OU=MINISTERIO ADMINISTRACIONES PUBLICAS, O=HAB. PAG. PER. SUBSE. DE MINISTERIO DE ADMINISTRACIONES PUBLICAS, L=Madrid, S=Madrid, C=ES
- Emisor: CN = Thawte Code Signing CA,O=Thawte Consulting (Pty) Ltd.,C=ZA
- Número de Serie: 11 e5 5e fd c1 28 f5 88 91 b3 af 34 30 db c8 77 (hexa)
- Usos: firma del código del cliente de firma
- Asunto: CN=DESCRIPCION CLIENTE OCSP MAP - ENTIDAD MINISTERIO DE ADMINISTRACIONES PUBLICAS - CIF S2833002E, OU=500070015 ,OU=PUBLICOS, OU=FNMT Clase 2 CA, O=FNMT, C=ES
- Emisor: OU=FNMT Clase 2 CA,O=FNMT,C=ES
- Número de Serie: 1016509177
- Usos: firma de las peticiones OCSP de la FNMT realizadas desde la Plataforma @firma

7.6.2 Declaración de certificados de la Plataforma

A continuación, se indican las URLs de las DPCs de los certificados del apartado anterior (7.1):

- Certificados de Servidor (SSL) cuyo emisor es CN=CAGVA, OU=PKIGVA, O=Generalitat Valenciana, C=ES, la URL de la DPC es:

<http://www.accv.es/pdf-politicas/PKIGVA-CP-03V1.1-c.pdf>

- Certificados de firma OCSP cuyo emisor es CN=AC DNIE 001,OU=DNIE,O=DIRECCION GENERAL DE LA POLICIA,C=ES, la URL de la DPC es:

http://www.dnielectronico.es/PDFs/politicas_de_certificacion.pdf

- Certificados de Sellado de Tiempo cuyo emisor es CN=Root CA Generalitat Valenciana,OU=PKIGVA,O=Generalitat Valenciana,C=ES, la URL de la DPC es:

<http://www.accv.es/pdf-politicas/PoliticaSelladoTiempo-V3.4.pdf>

- Certificados de Firma de Código del Cliente de firma cuyo emisor es CN=Thawte Code Signing CA,O=Thawte Consulting (Pty) Ltd.,C=ZA, la URL de la DPC es:

https://www.thawte.com/ssl-digital-certificates/free-guides-whitepapers/pdf/Thawte_CPS_3_5.pdf

- Certificados de Firma de peticiones OCSP para la FNMT cuyo emisor es OU=FNMT Clase 2 CA,O=FNMT,C=ES, la URL de la DPC es:

http://www.cert.fnmt.es/content/pages_std/docs/00034_cit_obtain_cert_0000000000%20-%20Declaracion%20de%20Practicas%20de%20Certificacion.pdf

8 Elementos de soporte a la operación

En este punto se describen los servicios internos de los que consta la plataforma @firma.

8.1 Servicios de Administración

El módulo de Administración de la plataforma de @firma v5.0 tiene como objetivo permitir la configuración de todos los elementos, susceptibles de ello, que conforman la plataforma.

Entre sus características principales se encuentran:

- Centralización de la configuración. Todos los parámetros de configuración de la plataforma @firma han sido agrupados en un único elemento de configuración, independientemente de los nodos del cluster que conforma la plataforma y de los servicios ofrecidos por la misma.
- Administración remota de la plataforma @firma y Administración delegada. La administración delegada permite que los propios organismos usuarios de la plataforma configuren sus aplicaciones y generen sus reportes de consultas y estadísticas de uso. Para mayor detalle, consulten el manual específico de Administración Delegada.
- Securización. El sistema de administración se encuentra protegido por un triple sistema de seguridad:
- Backup del fichero de configuración, dando la posibilidad de recuperar configuraciones anteriores (por seguridad, es necesario tener acceso a la plataforma por consola y ser administrador de la misma).

8.2 Servicios de Auditoría y Estadísticas

Dada la relevancia del servicio que presta la plataforma @firma, se hace necesario poseer un sistema de auditoría que permita registrar de forma permanente todas las acciones que se llevan a cabo en el sistema, lo que incluye:

- Peticiones de servicio por parte de las aplicaciones y respuestas devueltas por el sistema.
- Los procesos realizados por la plataforma para la prestación de los servicios de cara a las aplicaciones.
- Procesos internos del sistema, como pueden ser la verificación del estado de los Prestadores, 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.

El sistema de auditoría contempla además la existencia de una herramienta gráfica mediante la cual se pueda buscar, obtener y visualizar la información, además de generar estadísticas por períodos y otros parámetros diversos como por ejemplo tipos de servicios, aplicaciones, etc.

Las estadísticas de uso estarán en breve disponibles a nivel público en el portal del CTT, accediendo a la zona de usuarios del proyecto @firma. Además, mensualmente se envían a través del Centro de Atención al Usuario de @firma un informe con las estadísticas a cada organismo que hace uso de los servicios de la Autoridad de validación

8.3 Servicios de Gestión

Los servicios de gestión se encuentran centralizados en el módulo de administración de la plataforma @firma, reuniéndose en dicho modulo los siguientes servicios y competencias:

- Gestión de la configuración: Todos los parámetros de configuración de la plataforma @firma pueden ser gestionados desde un único elemento de configuración, independientemente de la arquitectura que conforma la plataforma y de los servicios ofrecidos.
- Administración delegada: Ésta permite que los propios organismos usuarios de la plataforma configuren sus aplicaciones y generen sus reportes de consultas y estadísticas de uso.
- Gestión de usuarios: Mediante éste componente es posible definir los usuarios encargados de administrar, monitorizar y auditar la plataforma.
- Gestión de aplicaciones: Este componente permite realizar gestión de aplicaciones, pudiendo configurar diversos aspectos del acceso y tratamiento de las peticiones de servicio por aplicación.
- Gestión de almacenes de servicios y contraseñas: Mediante este componente se pueden configurar los distintos almacenes de certificados registrados en la plataforma y las contraseñas que se utilizan para acceder a los mismos.
- Gestión de prestadores de servicios de certificación: Este componente permite registrar y modificar los prestadores que son aceptados por la plataforma, así como aquellos tipos de certificados que puede emitir cada uno de ellos.
- Gestión de políticas de certificación: Este componente define las diferentes políticas de certificación que podrán aplicarse a las aplicaciones registradas en la plataforma.
- Gestión de los métodos de validación: Este componente registra los distintos mecanismos de validación de certificados así como la configuración necesaria para el correcto funcionamiento de cada uno de ellos.
- Gestión de avisos de alarmas: Mediante este componente los administradores de la plataforma podrán configurar los destinatarios que deben ser informados por el lanzamiento de cada uno de los tipos de alarmas existentes en el sistema.
- Gestión de tareas: Este componente permite administrar procesos que serán ejecutados periódicamente por la plataforma en segundo plano.
- Gestión de la caché de estado de validación de certificados: A través de este componente es posible configurar ciertos parámetros que permiten que los métodos de validación de certificados optimicen el tiempo de obtención del estado de revocación de certificados.

- Planificador de descargas de CRL's: Este componente es el encargado de gestionar las tareas que van a permitir la descarga/actualización periódica de las CRL's de los prestadores reconocidos por la plataforma.
- Gestión del Servidor OCSP: Permite la configuración de los parámetros de funcionamiento del servidor OCSP que incorpora la plataforma.

8.4 Servicios de Monitorización

El servicio de monitorización permite la visualización en tiempo real de las alarmas generadas por la plataforma @firma.

Una alarma es una señal de advertencia del sistema ante un hecho no esperado, o que deba ser tenido en cuenta por los administradores. Las alarmas se identifican mediante un código determinado y pueden informar sobre aspectos diversos como:

- Falta de conectividad del servidor respecto a los Prestadores de Servicios de Certificación.
- Errores en la configuración que provoquen anomalías en el sistema.
- Avisos de caducidad próxima o revocación de los certificados de los PSC's registrados.
- Etc.

8.5 Módulo de Gestión de Prestadores

Este módulo centraliza todos los procesos de alta/modificación/baja de los Prestadores de Servicio de Certificación, en adelante PSC's, así como de sus protocolos y servidores de consultas en la plataforma @firma.

8.5.1 Gestión del Árbol de Prestadores de Servicios de Certificación (PSC)

La plataforma @firma proporciona una herramienta de Gestión intuitiva que le permite añadir cualquier PSC Reconocido y definir su estructura interna de certificación de manera automática.

8.5.2 Gestión de tipos de certificados por PSC

Por cada Prestador introducido en la plataforma @firma, la herramienta de Gestión permite definir qué tipos de certificados admite y qué estructura de campos lo componen. El

reconocimiento de los tipos de certificados admite dos posibilidades: manual y automática a partir de un certificado con clave pública emitido por el PSC.

8.5.3 Gestión de Políticas de Confianza

La plataforma permite definir varios mapeos por cada tipo de certificado y asociarlos a una política concreta de firma. Esta política es configurable y cada aplicación puede utilizar la que más crea conveniente. De esta forma un mismo certificado puede devolver distinta información a distintas aplicaciones en función de la política seleccionada por cada una de ellas.

8.5.4 Importación y Exportación de Elementos de Confianza entre distintas plataformas @firma

De cara a implantar un modelo federado de plataformas de firma, se permite exportar e importar elementos de confianza entre distintas plataformas @firma. Un ejemplo de elemento de confianza puede ser la estructura de certificación, tipos de certificados y mapeado de campos de un PSC determinado.

Atiende al modelo de servicio basado en una Federación de confianza en la que diferentes implementaciones de @firma ver 5.0 puedan intercambiar elementos de confianza.

8.6 Módulo de Registro y Gestión de Eventos

Describe el sistema de auditoria de la plataforma basado en el no repudio de los eventos generados por la misma. Incluye el motor de auditoria de la plataforma, un gestor de alarmas y una aplicación web cliente para monitorizar el servicio.

8.6.1 Servicio de Auditoría y Estadísticas de transacciones

La plataforma @firma 5.0 dispone de un sistema de Gestión de Eventos bastante potente que permite registrar y monitorizar todo el proceso de validación de un certificado y de realización de una firma digital. Además este sistema permite custodiar y firmar todos los eventos de la plataforma proporcionando la característica de no repudio.

8.6.2 Servicio de Monitorización

- Contabilidad de transacciones. Posibilidad de hacer un seguimiento concreto a las transacciones generadas en la plataforma para poder gestionarlas posteriormente.
- Reporting de actividades. La plataforma permite generar informes y estadísticas de las transacciones generadas para un mayor seguimiento y control.

- Gestión de Alarmas. La plataforma proporciona una herramienta que permite definir procesos en background para chequear y controlar una serie de indicadores definidos.

Estos procesos generan unas alarmas en caso de ser activados que permiten actuar y notificar de las mismas en situaciones críticas.

8.6.3 Gestión de Autorizaciones en solicitudes de servicio

La plataforma @firma dispone de un mecanismo de registro y autorización de las aplicaciones que pueden invocar los servicios ofrecidos. Este procedimiento consiste en lo siguiente:

- Formulario de alta de aplicación

Desde la página de bienvenida de la plataforma se puede descargar un fichero en formato EXCEL que contiene el formulario que se debe cumplimentar y enviar a SOPORTE (soporte.afirma5@map.es) para realizar la solicitud de alta de aplicación.

- Registro de la aplicación

El personal de soporte utilizando la herramienta de administración de la plataforma, registra la aplicación asignando la un identificador de aplicación único y ubicando la en una unidad organizativa.

- Alta de la dirección IP

Atendiendo a una solicitud interna de alta de IP, el grupo de administración de sistemas procede a registrar y asignar permisos de acceso para la dirección IP solicitada.

9 Proveedores de Servicios de Certificación

Los Proveedores o Prestadores de Servicios de Certificación son las personas físicas o jurídicas que expiden certificados electrónicos o prestan otros servicios en relación con la firma electrónica.

9.1 Proveedores Reconocidos por la Plataforma

Los Proveedores reconocidos por la plataforma @firma se enumeran a continuación:

- DNle

http://www.dnielectronico.es/PDFs/politicas_de_certificacion.pdf

- FNMT-Ceres
http://www.cert.fnmt.es/content/pages_std/docs/00034_cit_obtain_cert_0000000000%20-%20Declaracion%20de%20Practicas%20de%20Certificacion.pdf
- CATCERT
http://www.catcert.net/descarrega_cas/doc_legal/idCAT_dpc_cas_anterior.pdf
- CAGVA
<http://www.accv.es/pdf-politicas/ACCV-CPS-V1.7-c.pdf>
- IZENPE
http://www.izenpe.com/s15-4812/es/contenidos/informacion/administracion_vasca/es_8927/adjuntos/DPC_4.0_es.pdf
- ANF
https://www.anf.es/security/pdf/DPC_ANF_AC_v1.8.pdf
- Camerfirma
http://docs.camerfirma.com/mod_web/CPS_V.2.pdf
- ACA
https://documentacion.redabogacia.org/docushare/dsweb/Get/Document-20182/CPS_ACA_001.0.pdf
- ANCERT
http://www.ancert.com/?do=productos.getDocument&group=certificados_notariales&option=declaracion&id=121
- Firma profesional
http://www.firmaprofesional.com/cps/CPS-CPs_FP_003.0.pdf
- Banesto
<https://ca.banesto.es/documentacion.htm>
- SCR
<https://www.registradores.org/scr/SCR-CPSv.1.1.pdf>
- DNI electrónico de Portugal (en pruebas)
<http://www.cartaocidadao.pt/>

9.2 Proveedores pendientes de reconocimiento por la Plataforma

Actualmente no se encuentra ningún proveedor pendiente de reconocimiento por la plataforma.

9.3 Autoridades de Validación

La autoridad de validación es la encargada de la validación de certificados y firmas digitales realizadas por usuarios o sistemas, accediendo en caso de ser necesario a los PSC's para obtener la información de no revocación. Actualmente sólo hay una autoridad de validación (@firma) encargada de esta tarea.

9.4 Tipos de Certificados Reconocidos

- DNle

- Tipo Certificado: Autenticación de Ciudadano (SHA1)
 - Según la DPC "DNIE002-DESASIDPCyPC" versión 00.06b con fecha 07-02-2006.
 - Según el documento de Perfil de certificados "DNIE002-DESASIPerfilCert" versión 01.04b con fecha 07-02-2006.
 - Política de Certificado: 2.16.724.1.2.2.2.4
 - Tipo de clasificación: PERSONA FÍSICA.
 - Certificado reconocido por el Ministerio de Industria, Turismo y Comercio con fecha 19/12/2006.
- Tipo Certificado: Firma de Ciudadano (SHA 1)
 - Según la DPC "DNIE002-DESASIDPCyPC" versión 00.06b con fecha 07-02-2006.
 - Según el documento de Perfil de certificados "DNIE002-DESASIPerfilCert" versión 01.04b con fecha 07-02-2006.
 - Política de Certificado: 2.16.724.1.2.2.2.3
 - Tipo de clasificación: PERSONA FÍSICA.
 - Certificado reconocido por el Ministerio de Industria, Turismo y Comercio con fecha 19/12/2006.

- FNMT-Ceres

- Tipo Certificado: Persona física
 - Según la DPC con fecha 20-11-2005
 - Política de Certificado: 1.3.6.1.4.1.5734.3.5
 - Tipo de clasificación: PERSONA FÍSICA.
 - Certificado reconocido por el Ministerio de Industria, Turismo y Comercio con fecha 25/11/2004.
- Tipo Certificado: Persona Jurídica para el Ámbito Tributario
 - Según la DPC con fecha 20-11-2005
 - Política de Certificado: 1.3.6.1.4.1.5734.3.7
 - Tipo de clasificación: PERSONA JURÍDICA.
 - Certificado reconocido por el Ministerio de Industria, Turismo y Comercio con fecha 25/11/2004.

- - Tipo Certificado: Entidad sin personalidad jurídica para el Ámbito Tributario
 - Según la DPC con fecha 20-11-2005
 - Política de Certificado: 1.3.6.1.4.1.5734.3.7
 - Tipo de clasificación: PERSONA JURÍDICA.
 - Certificado reconocido por el Ministerio de Industria, Turismo y Comercio con fecha 25/11/2004.
 - Tipo Certificado: Certificado de componente
 - Según la DPC con fecha 20-11-2005
 - Política de Certificado: 1.3.6.1.4.1.5734.3.6
 - Tipo de clasificación: CERTIFICADO PARA COMPONENTES.
- CATCERT
 - Tipo Certificado: Idcat con cifrado
 - Según la DPC "ACC-PEdC-001" versión 2.0 con fecha 31-01-2005.
 - Política de Certificado: OID 1.3.6.1.4.1.15096.1.3.1.86.1
 - Tipo de clasificación: PERSONA FÍSICA.
 - Certificado reconocido por el Ministerio de Industria, Turismo y Comercio con fecha 18/01/2006.
 - Tipo Certificado: Idcat sin cifrado
 - Según la DPC "ACC-PEdC-001" versión 2.0 con fecha 31-01-2005.
 - Política de Certificado: OID 1.3.6.1.4.1.15096.1.3.1.84.1
 - Tipo de clasificación: PERSONA FÍSICA.
 - Certificado reconocido por el Ministerio de Industria, Turismo y Comercio con fecha 18/01/2006.
 - Tipo Certificado: EC-AL Certificado Personal de Identidad y Firma Reconocida (CPISR-1)
 - Según la DPC "D1111_E0650_EC-AL_N-DPC-004" versión 1.0 con fecha 20-12-2005.
 - Política de Certificado: OID 1.3.6.1.4.1.15096.1.3.1.81
 - Tipo de clasificación: PERSONA FÍSICA.
 - Tipo Certificado: EC-AL Certificado Personal de Cifrado (CPIX-1)
 - Según la DPC "D1111_E0650_EC-AL_N-DPC-004" versión 1.0 con fecha 20-12-2005.
 - Política de Certificado: OID 1.3.6.1.4.1.15096.1.3.1.41
 - Tipo de clasificación: PERSONA FÍSICA.
 - Tipo Certificado: EC-AL Certificado de Entidad de Firma Reconocida (CESR-1)
 - Según la DPC "D1111_E0650_EC-AL_N-DPC-004" versión 1.0 con fecha 20-12-2005.
 - Política de Certificado: OID 1.3.6.1.4.1.15096.1.3.1.121

- Tipo de clasificación: PERSONA JURÍDICA.
 - Tipo Certificado: EC-AL Certificado de Entidad de Cifrado (CEX-1)
 - Según la DPC "D1111_E0650_EC-AL_N-DPC-004" versión 1.0 con fecha 20-12-2005.
 - Política de Certificado: OID 1.3.6.1.4.1.15096.1.3.1.131
 - Tipo de clasificación: PERSONA JURÍDICA.
 - Tipo Certificado: EC-SAFP Certificado Personal de Identidad y Firma Reconocida (CPISR-1)
 - Según la DPC "D1111_E0650_EC-SAFP_N-DPC-004" versión 1.0 con fecha 20-12-2005.
 - Política de Certificado: OID 1.3.6.1.4.1.15096.1.3.1.81
 - Tipo de clasificación: PERSONA FÍSICA.
 - Tipo Certificado: EC-SAFP Certificado Personal de Cifrado (CPIX-1)
 - Según la DPC "D1111_E0650_EC-SAFP_N-DPC-004" versión 1.0 con fecha 20-12-2005.
 - Política de Certificado: OID 1.3.6.1.4.1.15096.1.3.1.41
 - Tipo de clasificación: PERSONA FÍSICA.
 - Tipo Certificado: EC-SAFP Certificado de Entidad de Firma Reconocida (CESR-1)
 - Según la DPC "D1111_E0650_EC-SAFP_N-DPC-004" versión 1.0 con fecha 20-12-2005.
 - Política de Certificado: OID 1.3.6.1.4.1.15096.1.3.1.121
 - Tipo de clasificación: PERSONA JURÍDICA.
 - Tipo Certificado: EC-SAFP Certificado de Entidad de Cifrado (CEX-1)
 - Según la DPC "D1111_E0650_EC-SAFP_N-DPC-004" versión 1.0 con fecha 20-12-2005.
 - Política de Certificado: OID 1.3.6.1.4.1.15096.1.3.1.131
 - Tipo de clasificación: PERSONA JURÍDICA.
 - Tipo Certificado: CATCERT GENCAT SAFP Comp CDA de Clase 1
 - Según la DPC "Estructura de Certificado CDA" versión 2.5 con fecha 5-09-2005.
 - Política de Certificado: OID 1.3.6.1.4.1.15096.1.3.1.91
 - Tipo de clasificación: CERTIFICADO PARA COMPONENTES.
- CAGVA
- Tipo Certificado: Certificado Reconocido en dispositivo seguro para el ciudadano
 - Según la DPC "ACCV-CP-06V4.0-c" con fecha 05-10-2005.
 - Política de Certificado: OID 1.3.6.1.4.1.8149.3.6.4.0
 - Tipo de clasificación: PERSONA FÍSICA.

- Certificado reconocido por el Ministerio de Industria, Turismo y Comercio con fecha 02/11/2005.
- Tipo Certificado: Certificado Reconocido en soporte software para el ciudadano
 - Según la DPC “ACCV-CP-07V3.0-c” con fecha 06-10-2005.
 - Política de Certificado: OID 1.3.6.1.4.1.8149.3.7.3.0
 - Tipo de clasificación: PERSONA FÍSICA.
 - Certificado reconocido por el Ministerio de Industria, Turismo y Comercio con fecha 02/11/2005.
- Tipo Certificado: Certificado Reconocido en soporte software para el ciudadano derogado
 - Según la DPC “PKIGVA-CP-07v1.0-c” con fecha 13-08-2003.
 - Política de Certificado: OID 1.3.6.1.4.1.8149.3.7.1.0
 - Tipo de clasificación: PERSONA FÍSICA.
 - Certificado reconocido por el Ministerio de Industria, Turismo y Comercio con fecha 02/11/2005.
- Tipo Certificado: Certificado Reconocido en soporte software para el ciudadano derogado 2
 - Según la DPC “PKIGVA-CP-07v2.0-c” con fecha 11-10-2004.
 - Política de Certificado: OID 1.3.6.1.4.1.8149.3.7.2.0
 - Tipo de clasificación: PERSONA FÍSICA.
 - Certificado reconocido por el Ministerio de Industria, Turismo y Comercio con fecha 02/11/2005.
- Tipo Certificado: Certificado de Aplicación
 - Según la DPC “PKIGVA-CP-05V2.0-c” con fecha 20-10-2004.
 - Política de Certificado: OID 1.3.6.1.4.1.8149.3.5.2.0
 - Tipo de clasificación: CERTIFICADO PARA COMPONENTES.
- Tipo Certificado: Certificado para Sellado de Tiempos
 - Según la DPC “PolíticaSelladoTiempo-V3.2.pdf” con fecha 26-01-2006.
 - Política de Certificado: OID 1.3.6.1.4.1.8149.3.20.1.0
 - Tipo de clasificación: CERTIFICADO PARA COMPONENTES.
- Tipo Certificado: Certificado para Servidores con Soporte SSL
 - Según la DPC “PKIGVA-CP-03v1.1-c” con fecha 13-08-2003.
 - Política de Certificado: OID 1.3.6.1.4.1.8149.3.2.1.4.1.0
 - Tipo de clasificación: CERTIFICADO PARA COMPONENTES.
- Tipo Certificado: Certificado Reconocido en soporte software para el ciudadano
 - Según la DPC “ACCV-CP-07V4.0-c” con fecha 13-09-2006.
 - Política de Certificado: OID 1.3.6.1.4.1.8149.3.7.4.0
 - Tipo de clasificación: PERSONA FÍSICA.

- Certificado reconocido por el Ministerio de Industria, Turismo y Comercio con fecha 02/11/2005.
 - Tipo Certificado: Certificado Reconocido de Entidad
 - Según la DPC “ACCV-CP-10V1.0-c” con fecha 0-03-2006.
 - Política de Certificado: OID 1.3.6.1.4.1.8149.3.10.1.0
 - Tipo de clasificación: PERSONA JURÍDICA.
 - Certificado reconocido por el Ministerio de Industria, Turismo y Comercio con fecha 02/11/2005.
 - Tipo Certificado: Certificado Reconocido en dispositivo seguro para el ciudadano
 - Según la DPC “ACCV-CP-06V2.0-c” con fecha 15-01-2004.
 - Política de Certificado: OID 1.3.6.1.4.1.8149.3.6.2.0
 - Tipo de clasificación: PERSONA FÍSICA.
 - Certificado reconocido por el Ministerio de Industria, Turismo y Comercio con fecha 02/11/2005.
 - Tipo Certificado: Certificado Reconocido en dispositivo seguro para el ciudadano
 - Según la DPC “ACCV-CP-06V3.0-c” con fecha 11-10-2004.
 - Política de Certificado: OID 1.3.6.1.4.1.8149.3.6.3.0
 - Tipo de clasificación: PERSONA FÍSICA.
 - Certificado reconocido por el Ministerio de Industria, Turismo y Comercio con fecha 02/11/2005.
 - Tipo Certificado: Certificado Reconocido en dispositivo seguro para el ciudadano
 - Según la DPC “ACCV-CP-06V5.0-c” con fecha 13-09-2006.
 - Política de Certificado: OID 1.3.6.1.4.1.8149.3.6.5.0
 - Tipo de clasificación: PERSONA FÍSICA.
 - Certificado reconocido por el Ministerio de Industria, Turismo y Comercio con fecha 02/11/2005.
- IZENPE
- Tipo de Certificado: Certificado de Ciudadano v2.0
 - Según la DPC “DPC_3.8_castellano_version_web.pdf” versión 3.8 con fecha 21-09-2006.
 - Política de Certificado: OID 1.3.6.1.4.1.14777.2.6
 - Tipo de clasificación: PERSONA FÍSICA.
 - Certificado reconocido por el Ministerio de Industria, Turismo y Comercio con fecha 04/03/2005.
 - Tipo de Certificado: Certificado de Entidad en tarjeta criptográfica
 - Según la DPC “DPC_3.8_castellano_version_web.pdf” versión 3.8 con fecha 21-09-2006.
 - Política de Certificado: OID 1.3.6.1.4.1.14777.2.7

- Tipo de clasificación: PERSONA JURÍDICA.
- Certificado reconocido por el Ministerio de Industria, Turismo y Comercio con fecha 04/03/2005.
- Tipo de Certificado: Certificado de Entidad en soporte Software
 - Según la DPC "DPC_3.8_castellano_version_web.pdf" versión 3.8 con fecha 21-09-2006.
 - Política de Certificado: OID 1.3.6.1.4.1.14777.2.8
 - Tipo de clasificación: PERSONA JURÍDICA.
 - Certificado reconocido por el Ministerio de Industria, Turismo y Comercio con fecha 04/03/2005.
- Tipo de Certificado: Certificado de entidad sin personalidad jurídica
 - Según la DPC "DPC_3.8_castellano_version_web.pdf" versión 3.8 con fecha 21-09-2006.
 - OID = 1.3.6.1.4.1.14777.2.9
 - Tipo de clasificación: PERSONA JURÍDICA.
 - Certificado reconocido por el Ministerio de Industria, Turismo y Comercio con fecha 04/03/2005.
- Tipo de Certificado: Certificado Personal de entidades públicas
 - Según la DPC "DPC_3.8_castellano_version_web.pdf" versión 3.8 con fecha 21-09-2006.
 - OID = 1.3.6.1.4.1.14777.4.1
 - Tipo de clasificación: PERSONA FÍSICA.
 - Certificado reconocido por el Ministerio de Industria, Turismo y Comercio con fecha 04/03/2005.
- Tipo de Certificado: Certificado Corporativo reconocido
 - Según la DPC "DPC_3.8_castellano_version_web.pdf" versión 3.8 con fecha 21-09-2006.
 - OID = 1.3.6.1.4.1.14777.4.2
 - Tipo de clasificación: PERSONA FÍSICA.
 - Certificado reconocido por el Ministerio de Industria, Turismo y Comercio con fecha 04/03/2005.
- Tipo de Certificado: Certificado Órgano administrativo
 - Según la DPC "DPC_3.8_castellano_version_web.pdf" versión 3.8 con fecha 21-09-2006.
 - OID = 1.3.6.1.4.1.14777.4.3
 - Tipo de clasificación: PERSONA JURÍDICA.
 - Certificado reconocido por el Ministerio de Industria, Turismo y Comercio con fecha 04/03/2005.
- Tipo de Certificado: Certificado de Componente no Reconocido
 - Según la DPC "DPC_3.8_castellano_version_web.pdf" versión 3.8 con fecha 21-09-2006.
 - OID = 1.3.6.1.4.1.14777.1.2.2
 - Tipo de clasificación: CERTIFICADO PARA COMPONENTES

- ANF

- Tipo de Certificado: Certificado de Clase 2 de Persona Física
 - Según la DPC “CPClase2personafisica” versión 1.3 con fecha 2-03-2005.
 - Política de Certificado: OID 1.3.6.1.4.1.18332.3.3
 - Tipo de clasificación: PERSONA FÍSICA.
 - Certificado reconocido por el Ministerio de Industria, Turismo y Comercio con fecha 25/11/2004.
- Tipo de Certificado: Certificado de Clase 2 de Persona Física Nuevo
 - Según la DPC “de Certificación de ANF AC Certificados de Clase 2 de Personas físicas” versión 1.4 con fecha 21-02-2006.
 - Política de Certificado: OID 1.3.6.1.4.1.18332.3.4
 - Tipo de clasificación: PERSONA FÍSICA.
 - Certificado reconocido por el Ministerio de Industria, Turismo y Comercio con fecha 25/11/2004.
- Tipo de Certificado: Certificado de Clase 2 de Persona Jurídica
 - Según la DPC “CPClase2entidadjuridica” versión 1.5 con fecha 15-06-2006.
 - Política de Certificado: OID 1.3.6.1.4.1.18332.2.4
 - Tipo de clasificación: PERSONA JURÍDICA.
 - Certificado reconocido por el Ministerio de Industria, Turismo y Comercio con fecha 25/11/2004.

- Camerfirma

- Tipo de Certificado: Persona Física. Soporte Software. Clave generada por PSC
 - Según la DPC “Política de Certificación de Certificado Cameral de Persona Física” versión 1.1.1 con fecha 20-10-2004.
 - Política de Certificado: OID 1.3.6.1.4.1.17326.10.9.2.1.1
 - Tipo de clasificación: PERSONA FÍSICA.
 - Certificado reconocido por el Ministerio de Industria, Turismo y Comercio con fecha 25/11/2004.
- Tipo de Certificado: Persona Física. Soporte Software. Clave generada por Usuario
 - Según la DPC “Política de Certificación de Certificado Cameral de Persona Física” versión 1.1.1 con fecha 20-10-2004.
 - Política de Certificado: OID 1.3.6.1.4.1.17326.10.9.2.1.2
 - Tipo de clasificación: PERSONA FÍSICA.
 - Certificado reconocido por el Ministerio de Industria, Turismo y Comercio con fecha 25/11/2004.

- Tipo de Certificado: Persona Física. Soporte Hardware. Clave generada por PSC
 - Según la DPC “Política de Certificación de Certificado Cameral de Persona Física” versión 1.1.1 con fecha 20-10-2004.
 - Política de Certificado: OID 1.3.6.1.4.1.17326.10.9.2.2.1
 - Tipo de clasificación: PERSONA FÍSICA.
 - Certificado reconocido por el Ministerio de Industria, Turismo y Comercio con fecha 25/11/2004.

- Tipo de Certificado: Persona Física. Soporte Hardware. Clave generada por Usuario
 - Según la DPC “Política de Certificación de Certificado Cameral de Persona Física” versión 1.1.1 con fecha 20-10-2004.
 - Política de Certificado: OID 1.3.6.1.4.1.17326.10.9.2.2.2
 - Tipo de clasificación: PERSONA FÍSICA.
 - Certificado reconocido por el Ministerio de Industria, Turismo y Comercio con fecha 25/11/2004.

- Tipo de Certificado: Persona Jurídica. Soporte Software. Clave generada por PSC
 - Según la DPC “Política de Certificación de Certificado Cameral de Persona Jurídica” versión 1.1.3 con fecha 10-09-2004.
 - Política de Certificado: OID 1.3.6.1.4.1.17326.10.9.4.1.1
 - Tipo de clasificación: PERSONA JURÍDICA.
 - Certificado reconocido por el Ministerio de Industria, Turismo y Comercio con fecha 25/11/2004.

- Tipo de Certificado: Persona Jurídica. Soporte Software. Clave generada por Usuario
 - Según la DPC “Política de Certificación de Certificado Cameral de Persona Jurídica” versión 1.1.3 con fecha 10-09-2004.
 - Política de Certificado: OID 1.3.6.1.4.1.17326.10.9.4.1.2
 - Tipo de clasificación: PERSONA JURÍDICA.
 - Certificado reconocido por el Ministerio de Industria, Turismo y Comercio con fecha 25/11/2004.

- Tipo de Certificado: Persona Jurídica. Soporte Hardware. Clave generada por PSC
 - Según la DPC “Política de Certificación de Certificado Cameral de Persona Jurídica” versión 1.1.3 con fecha 10-09-2004.
 - Política de Certificado: OID 1.3.6.1.4.1.17326.10.9.4.2.1
 - Tipo de clasificación: PERSONA JURÍDICA.
 - Certificado reconocido por el Ministerio de Industria, Turismo y Comercio con fecha 25/11/2004.

- Tipo de Certificado: Persona Jurídica. Soporte Hardware. Clave generada por Usuario
 - Según la DPC “Política de Certificación de Certificado Cameral de Persona Jurídica” versión 1.1.3 con fecha 10-09-2004.

- Política de Certificado: OID 1.3.6.1.4.1.17326.10.9.4.2.2
- Tipo de clasificación: PERSONA JURÍDICA.
- Certificado reconocido por el Ministerio de Industria, Turismo y Comercio con fecha 25/11/2004.
- Tipo de Certificado: Representante. Soporte Software. Clave generada por PSC
 - Según la DPC “Política de Certificación de Certificado Cameral de Representante” versión 1.0.1 con fecha 20-10-2004.
 - Política de Certificado: OID 1.3.6.1.4.1.17326.10.9.3.1.1
 - Tipo de clasificación: PERSONA JURÍDICA.
 - Certificado reconocido por el Ministerio de Industria, Turismo y Comercio con fecha 25/11/2004.
- Tipo de Certificado: Representante. Soporte Software. Clave generada por Usuario
 - Según la DPC “Política de Certificación de Certificado Cameral de Representante” versión 1.0.1 con fecha 20-10-2004.
 - Política de Certificado: OID 1.3.6.1.4.1.17326.10.9.3.1.2
 - Tipo de clasificación: PERSONA JURÍDICA.
 - Certificado reconocido por el Ministerio de Industria, Turismo y Comercio con fecha 25/11/2004.
- Tipo de Certificado: Representante. Soporte Hardware. Clave generada por PSC
 - Según la DPC “Política de Certificación de Certificado Cameral de Representante” versión 1.0.1 con fecha 20-10-2004.
 - Política de Certificado: OID 1.3.6.1.4.1.17326.10.9.3.2.1
 - Tipo de clasificación: PERSONA JURÍDICA.
 - Certificado reconocido por el Ministerio de Industria, Turismo y Comercio con fecha 25/11/2004.
- Tipo de Certificado: Representante. Soporte Hardware. Clave generada por Usuario
 - Según la DPC “Política de Certificación de Certificado Cameral de Representante” versión 1.0.1 con fecha 20-10-2004.
 - Política de Certificado: OID 1.3.6.1.4.1.17326.10.9.3.2.2
 - Tipo de clasificación: PERSONA JURÍDICA.
 - Certificado reconocido por el Ministerio de Industria, Turismo y Comercio con fecha 25/11/2004.
- Tipo de Certificado: Sello Electrónico
 - Según la DPC “PC_Camerfirma_Sello_Electronico” versión 1.1.2 con fecha 03/2005.
 - Política de Certificado: OID 1.3.6.1.4.1.17326.10.11.3
 - Tipo de clasificación: CERTIFICADO PARA COMPONENTE

- ACA

- Tipo de Certificado: Colegiado
 - Según la DPC “Certificados Corporativos Reconocidos de Colegiado” versión 005.0 con fecha 30-10-2006.
 - Política de Certificado: OID 1.3.6.1.4.1.16533.10.2.1
 - Tipo de clasificación: PERSONA FÍSICA.
 - Certificado reconocido por el Ministerio de Industria, Turismo y Comercio con fecha 25/11/2004.

- Tipo de Certificado: Administrativo
 - Según la DPC “Certificados Corporativos Reconocidos de Personal Administrativo” versión 005.0 con fecha 30-10-2006.
 - Política de Certificado: OID 1.3.6.1.4.1.16533.10.3.1
 - Tipo de clasificación: PERSONA FÍSICA.
 - Certificado reconocido por el Ministerio de Industria, Turismo y Comercio con fecha 25/11/2004.

- Tipo de Certificado: Persona Jurídica
 - Según la DPC “Certificados Corporativos de Persona Jurídica” versión 001.0 con fecha 13-07-2006.
 - Política de Certificado: OID 1.3.6.1.4.1.16533.10.5.1
 - Tipo de clasificación: PERSONA JURÍDICA.
 - Certificado reconocido por el Ministerio de Industria, Turismo y Comercio con fecha 25/11/2004.

- ANCERT

- Tipo de Certificado: Notarial Corporativo
 - Según la DPC “CP_CNC” versión 1.6 con fecha 03-52-2006.
 - Política de Certificado: OID 1.3.6.1.4.1.18920.1.3.1.1
 - Tipo de clasificación: PERSONA JURÍDICA.
 - Certificado reconocido por el Ministerio de Industria, Turismo y Comercio con fecha 25/11/2004.

- Tipo de Certificado: Notarial Corporativo de Representación
 - Según la DPC “CP_CNCR” versión 1.5 con fecha 17-05-2006.
 - Política de Certificado: OID 1.3.6.1.4.1.18920.1.3.2.1
 - Tipo de clasificación: PERSONA FÍSICA.
 - Certificado reconocido por el Ministerio de Industria, Turismo y Comercio con fecha 25/11/2004.

- Tipo de Certificado: Notarial Personal
 - Según la DPC “CP_CNP” versión 1.3 con fecha 03-05-2006.
 - Política de Certificado: OID 1.3.6.1.4.1.18920.1.1.1.1
 - Tipo de clasificación: PERSONA FÍSICA.

- Certificado reconocido por el Ministerio de Industria, Turismo y Comercio con fecha 25/11/2004.
- Tipo de Certificado: Notarial Personal de Representación Personal
 - Según la DPC “CP_CNPR” versión 1.1 con fecha 12-01-2005.
 - Política de Certificado: OID 1.3.6.1.4.1.18920.1.1.2.1
 - Tipo de clasificación: PERSONA FÍSICA.
 - Certificado reconocido por el Ministerio de Industria, Turismo y Comercio con fecha 25/11/2004.
- Tipo de Certificado: FEREN
 - Según la DPC “CPS ANCERT_v13” versión 1.3 con fecha 06-03-2006.
 - Política de Certificado: OID 1.3.6.1.4.1.18920.4.1.1.1
 - Tipo de clasificación: PERSONA FÍSICA.
 - Certificado reconocido por el Ministerio de Industria, Turismo y Comercio con fecha 25/11/2004.
- Tipo de Certificado: Certificados para Empleados
 - Según la DPC “CPS ANCERT_v13” versión 1.3 con fecha 06-03-2006.
 - Política de Certificado: OID 1.3.6.1.4.1.18920.4.2.1.1
 - Tipo de clasificación: PERSONA FÍSICA.
 - Certificado reconocido por el Ministerio de Industria, Turismo y Comercio con fecha 25/11/2004.
- Tipo de Certificado: Corporaciones de Derecho Público
 - Según la DPC “CP-CCCDP” versión 1.1 con fecha 22-12-2004.
 - Política de Certificado: OID 1.3.6.1.4.1.18920.3.1.1.1
 - Tipo de clasificación: PERSONA FÍSICA.
 - Certificado reconocido por el Ministerio de Industria, Turismo y Comercio con fecha 25/11/2004.
- Tipo de Certificado: Certificado de Servidor Web
 - Según la DPC “CC_CCP” versión 1.0 con fecha 06-03-2006
 - Política de Certificado: OID 1.3.6.1.4.1.18920.2.1.1.1
 - Tipo de clasificación: CERTIFICADO PARA COMPONENTES
- Firma Profesional
 - Tipo de Certificado: Certificado Reconocido de Colegiado Común
 - Según la DPC “Política de Certificación de Certificados Corporativos Reconocidos. Certificados Reconocidos de Colegiado” versión 1.3 con fecha 19-10-2004.
 - Política de Certificado: OID 1.3.6.1.4.1.13177.10.1.1.2
 - Tipo de clasificación: PERSONA FÍSICA.
 - Certificado reconocido por el Ministerio de Industria, Turismo y Comercio con fecha 25/11/2004.

- Tipo de Certificado: Persona Jurídica
 - Según la DPC “Política de Certificación de Certificados Corporativos Reconocidos. Certificados Corporativos Reconocidos de Entidad o Persona Jurídica” versión 1.0 con fecha 07-04-2006.
 - Política de Certificado: OID 1.3.6.1.4.1.13177.10.1.5.1
 - Tipo de clasificación: PERSONA JURÍDICA.
 - Certificado reconocido por el Ministerio de Industria, Turismo y Comercio con fecha 25/11/2004.

- Tipo de Certificado: Certificado Reconocido de Colegiado con DSCF
 - Según la DPC “Política de Certificación de Certificados Corporativos Reconocidos. Certificados Reconocidos de Colegiado” versión 1.3 con fecha 19-10-2004.
 - Política de Certificado: OID 1.3.6.1.4.1.13177.10.1.1.1
 - Tipo de clasificación: PERSONA FÍSICA.
 - Certificado reconocido por el Ministerio de Industria, Turismo y Comercio con fecha 25/11/2004.

- Tipo de Certificado: Certificado Reconocido de Persona Vinculada con DSCF
 - Según la DPC “Política de Certificación de Certificados Corporativos Reconocidos. Certificados Reconocidos de Persona Vinculada” versión 1.3 con fecha 19-10-2004.
 - Política de Certificado: OID 1.3.6.1.4.1.13177.10.1.2.1
 - Tipo de clasificación: PERSONA FÍSICA.
 - Certificado reconocido por el Ministerio de Industria, Turismo y Comercio con fecha 25/11/2004.

- Tipo de Certificado: Certificado Reconocido de Persona Vinculada Común
 - Según la DPC “Política de Certificación de Certificados Corporativos Reconocidos. Certificados Reconocidos de Persona Vinculada” versión 1.3 con fecha 19-10-2004.
 - Política de Certificado: OID 1.3.6.1.4.1.13177.10.1.2.2
 - Tipo de clasificación: PERSONA FÍSICA.
 - Certificado reconocido por el Ministerio de Industria, Turismo y Comercio con fecha 25/11/2004.

- Banesto
 - Tipo de Certificado: Persona Física
 - Según la DPC “Declaración de Prácticas de Certificación del PSC Banesto Clientes” versión 2.3 con fecha 21-03-2006.
 - Política de Certificado: OID 1.3.6.1.4.1.11076.1.2
 - Tipo de clasificación: PERSONA FÍSICA.
 - Certificado reconocido por el Ministerio de Industria, Turismo y Comercio con fecha 25/11/2004.

 - Tipo de Certificado: Persona Jurídica

- Según la DPC “Declaración de Prácticas de Certificación del PSC Banesto Clientes” versión 2.3 con fecha 21-03-2006.
 - Política de Certificado: OID 1.3.6.1.4.1.11076.1.2
 - Tipo de clasificación: PERSONA JURÍDICA.
 - Certificado reconocido por el Ministerio de Industria, Turismo y Comercio con fecha 25/11/2004.
- Servicio de Certificación de los Registradores
- Tipo de Certificado: Registradores Externos PF Personal
 - Según la DPC “Políticas de Certificación de Certificados Personales”.
 - Política de Certificado: OID 1.2.372.980001.4.2.10080.8930
 - Tipo de clasificación: PERSONA FÍSICA.
 - Tipo de Certificado: Registradores Externos PF Profesional
 - Según la DPC “Políticas de Certificación de Certificados Profesionales”.
 - Política de Certificado: OID 1.3.6.1.4.1.17276.0.2.4.1.1
 - Tipo de clasificación: PERSONA FÍSICA.
 - Tipo de Certificado: Registradores Externos PF Representante
 - Según la DPC “Políticas de Certificación de Certificados Representante”.
 - Política de Certificado: OID 1.2.372.980001.4.2.10080.8930
 - Tipo de clasificación: PERSONA FÍSICA.
 - Tipo de Certificado: Registradores Interno PF Registrador
 - Según la DPC “Políticas de Certificación de Certificados Registrador”.
 - Política de Certificado: OID 1.2.372.980001.4.2.10091.9381
 - Tipo de clasificación: PERSONA FÍSICA

En el documento ‘ANEXO – Tabla Nomenclatura PSCCERT_Usuarios’, que esta disponible en la página de bienvenida de la plataforma, se puede obtener información detallada sobre los atributos de cada certificado de cada PSC que es mapeado en @firma y del que se puede obtener el valor.

10 Publicación de la Información de la Declaración de Prácticas de Validación

10.1 Versiones

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:

1. 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.
2. El Responsable de las prácticas de validación elaborará y mantendrá actualizada la Declaración de Prácticas de Validación.
3. Las Áreas Responsables de los Sistemas de Información mantendrán actualizada la documentación y procedimientos técnicos relacionados con la Declaración de Prácticas de Validación.
4. 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.

10.2 Punto de publicación

Debido al carácter público del presente documentos, éste se encuentra disponible en los siguientes puntos de publicación:

- Página de documentación prevista en la plataforma @firma. URL:

<https://afirma.redinteradministrativa.es/afirma>

- En breve, también estará disponible la información en el portal del Centro de transferencia de tecnologías del MAP, en el área del proyecto @firma:

<http://www.ctt.map.es>

10.3 Responsables

El personal implicado en las prácticas de validación es el siguiente:

- Responsable de la Declaración de Prácticas de Validación.

El Responsable de la Declaración de Prácticas de Validación es la Dirección General de Modernización Administrativa del MAP.

- Responsable de las Prácticas de Validación.

Ejerce funciones de coordinación y control de las prácticas de validación descritas en el presente Documento de Seguridad.

Es una figura con suficiente peso dentro de la Organización para lograr el cumplimiento efectivo de sus funciones respecto a las prácticas de validación.

- Responsable de los Sistemas de Información.

Las Áreas de Sistemas de Información son las responsables de controlar los cambios que deriven en modificaciones de la Declaración de Prácticas de Validación.

11 Responsabilidades legales

11.1 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. La ejecución, interpretación, modificación o validez de la presente Declaración de prácticas se regirá por lo dispuesto en la legislación española vigente.

Normativa de referencia sobre utilización de técnicas electrónicas, informáticas y telemáticas por la Administración General del Estado:

- Firma electrónica:

- Ley 59/2003, de 19 de diciembre, de firma electrónica.
- Real Decreto 1317/2001, de 30 de noviembre, por el que se desarrolla el artículo 81 de la Ley 66/1997, de 30 de diciembre, de Medidas fiscales, administrativas y del orden social, en materia de prestación de servicios de seguridad, por la Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda, en las comunicaciones a través de medios electrónicos, informáticos y telemáticos con las Administraciones Públicas. (Deroga el Real Decreto 1290/1999).
- ORDEN de 21 de febrero de 2000, por la que se aprueba el Reglamento de acreditación de prestadores de servicios de certificación y de certificación de determinados productos de firma electrónica.

- Disposiciones generales:

- LEY 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos.
- ORDEN PRE/1551/2003, de 10 de junio, por la que se desarrolla la Disposición final primera del Real Decreto 209/2003, de 21 de febrero, por el que se regulan los registros y las notificaciones telemáticas, así como la utilización de medios telemáticos para la sustitución de la aportación de certificados por los ciudadanos.
- REAL DECRETO 209/2003, de 21 de febrero, por el que se regulan los registros y las notificaciones telemáticas, así como la utilización de medios telemáticos para la sustitución de la aportación de certificados por los ciudadanos.

- REAL DECRETO 263/1996 de 16 de febrero, que regula la utilización de técnicas electrónicas, informáticas y telemáticas por la Administración General del Estado. (Modificado por el Real Decreto 209/2003, de 21 de febrero).
- LEY 30/1992 de 26 de noviembre, Ley de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común. Art. 38 Registros y Art. 45 Incorporación de medios técnicos.

- Normativa sobre protección de datos de carácter personal:

- LEY ORGÁNICA 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
- 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.

11.2 Responsabilidad

El MAP 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 mismas.

El MAP se compromete a realizar un mantenimiento constante de los servicios de la plataforma de validación.

El MAP pone a disposición de los usuarios la presente declaración de prácticas que podrá consultarse en la/s dirección/es indicadas en el [apartado 7 del presente documento \(publicación de la Información de la Declaración de Prácticas de Validación\)](#) todo lo que se refiere a la propia declaración, en cuanto a su validez y los cambios que en ella puedan efectuarse.

11.3 Limitación de responsabilidades

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

El MAP no se hace responsable de los errores, anomalías o averías que sean debidas a virus informáticos, a fallos o problemas de la red de Internet o a una utilización irregular del Servicio, y en particular de la incorrecta utilización del CLIENTE/ USUARIO.

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

1. Cualquier circunstancia de exoneración definida por la política de certificación de la AC.
2. Cuando el perjuicio causado fuera en el periodo de verificación de las causas de suspensión.
3. Cuando el perjuicio causado fuera en el periodo de actualización de los datos contenidos en la CRL.

4. Estado de Guerra, Sitio y Excepción, ante desastres naturales o cualquier otro caso de Fuerza Mayor.

11.4 Protección de datos de carácter personal

El MAP garantiza la confidencialidad de la información, disponiendo de una adecuada política de tratamiento de la información. El personal está sometido a modelos de acuerdo que deberán firmar todas las personas que tengan acceso a la información confidencial.

Desde el MAP 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.

Por ORDEN APU/793/2008, de 5 de marzo (BOE de 25 de marzo) se incorpora a la relación de ficheros automatizados del Ministerio de Administraciones Públicas, el Fichero Automatizado de Validación de Firma Electrónica de la plataforma @firma.

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.

11.5 Obligaciones de la VA del MAP

La autoridad de validación del MAP 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 ([ver punto 8.1](#)), a los efectos de identificación de usuarios.
- 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.

11.6 Obligaciones de los usuarios

La Autoridad de Validación debe exigir que los usuarios de los certificados acepten las Obligaciones que se describen a continuación, mediante la firma de un Contrato de Usuario en el que se establezcan las condiciones de mismo, así como las circunstancias en las que interactúan la Autoridad de validación y el Usuario:

- a) 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.

- b) Usar las claves criptográficas solamente para aquello que el Contrato de Usuario establece, limitando con ello su uso.
- c) 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 personal que le permite usarla, para evitar que otras personas puedan suplantar su identidad y firmar documentos en su nombre o acceder a mensajes confidenciales.
- d) 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 personal de usuario de este soporte haya podido ser conocido por otro, el usuario debe notificarlo a la Autoridad de validación en un plazo de tiempo razonable, a fin de pedir la revocación o suspensión del certificado, si es el caso, la renovación correspondiente.
- e) Notificar a la Autoridad de Validación cualquier incorrección detectada en el contenido de la solicitud de validación de certificado, así como en cualquier otra situación análoga.
- f) Verificar la validez de los certificados en el momento de realizar cualquier operación basada en los mismos.
- g) 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.

11.7 Obligaciones de terceros

Al hablar de terceros nos estamos refiriendo a los Prestadores de Servicios 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.