Guía de servicios

Plataforma de validación y firma electrónica

Autor:	Ministerio de Hacienda y Administraciones Públicas
Tipo de Documento:	Documento de definición de servicios
Grupo de Trabajo:	@firma
Versión:	3.2
Fecha:	04/04/2016
Fichero:	@firma_guiaservicios_v3.2.docx

Control de Modificaciones

Rev.	**1.0**
Fecha	17-07-2007
Descripción	Documentación inicial

Rev.	**1.1**
Fecha	31-07-2007
Descripción	Borrador inicial

Rev.	**2.0**
Fecha	13-08-2007
Descripción	Primera versión a distribuir

Rev.	**2.1**
Fecha	24-08-2007
Descripción	Mínimas correcciones

Rev.	**2.2**
Fecha	02-01-2009
Descripción	Mínimas correcciones. Se incluyen las versiones XAdES soportadas (4.2.4) y se informa de los nuevos plugins PDF y ODF (4.2.4 y 7.3) y de los servicios que se consideran descontinuados (7.1).

Rev.	**2.3**
Fecha	29-04-2009
Descripción	Mínimas correcciones. Se corrige el listado de servicios web disponibles.

Rev.	**2.4**
Fecha	24-12-2009
Descripción	Se hace referencia a los nuevos servicios DSS.

Rev.	**2.5**
Fecha	28-12-2009
Descripción	Cambios para adecuar a las novedades principales del Cliente 3.0.

Rev.	**2.6**
Fecha	01-03-2010
Descripción	Se actualiza la información de los servicios y los prerrequisitos.

Rev.	**2.7**
Fecha	10-03-2010
Descripción	Se actualiza la información de los prerrequisitos.

Rev.	**2.8**
Fecha	19-07-2011
Descripción	Se incluye una breve mención a que el límite para cualquier petición es de 10 MB. Se incluye como descontinuado el apartado 7.1.C.

Rev.	**2.9**
Fecha	19-12-2011
Descripción	Se actualiza la versión de la Plataforma (5.5). Se hace referencia al uso del servicio DSSAfiramVerify para realizar el upgrade de firmas.

Rev.	**2.10**
Fecha	19-12-2011
Descripción	Se amplía la información sobre el servicio OCSP en el punto 7.5.

Rev.	**2.11**
Fecha	21-02-2012
Descripción	Se adecua el contenido de la información a la nueva estructura de los Ministerios.

Rev.	**2.12**
Fecha	22-03-2012
Descripción	Se reorganiza y actualiza la información.

Rev.	**2.13**
Fecha	18-08-2012
Descripción	Se incorpora la información sobre la aplicación “Firma Fácil”

Rev.	**2.14**
Fecha	05-11-2013
Descripción	Se actualiza la dirección de la web del MINETUR.

Rev.	**3.0**
Fecha	05-06-2014
Descripción	Se reestructura el documento y se actualiza la dirección del CAID

Rev.	**3.1**
Fecha	29-03-2016
Descripción	Correcciones menores

Rev.	**3.2**
Fecha	04-04-2016
Descripción	Se añade información sobre el tamaño admitido de las peticiones WS.

ÍNDICE

1. Introducción

Entre las competencias de las Administraciones Públicas en materia de administración electrónica se encuentra el obtener unos niveles óptimos de calidad, agilidad y rendimiento de los servicios telemáticos que la Administración pone a disposición de los ciudadanos y empresas; conseguir unos niveles de eficiencia en el uso de los recursos públicos; reducir y rentabilizar los costes e inversiones, y mejorar la integración interdepartamental y la simplificación administrativa.

Para conseguir estos objetivos, una de las medidas adoptadas ha sido el impulso del uso de la firma y certificación electrónica. De entre ellas, una de las de mayor trascendencia ha sido la sustitución gradual del Documento Nacional de Identidad actual por el equivalente en formato electrónico, lo que se ha venido en denominar DNI-e.

La introducción de la firma-e y el DNI-e es ya una necesidad en la tramitación telemática de todas las Administraciones públicas, sin embargo, el desarrollo y extensión tecnológica que están teniendo está siendo desigual y pausada en el tiempo. Entre los inhibidores del uso generalizado de estas nuevas técnicas de identificación y firma, está la complejidad tecnológica que hay que introducir en los sistemas de información, los elevados costes e inversiones a realizar o la falta de recursos especializados disponibles en los diferentes organismos Públicos.

Conocedores de estos condicionantes y en el ejercicio de las potestades que tiene atribuidas, el Ministerio de Hacienda y Administraciones Públicas (en adelante MINHAP) 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 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 que así lo requieran.

Desde el punto de vista tecnológico, construye una capa de abstracción de seguridad a nivel de aplicación que desacopla la lógica de negocio de las aplicaciones de la introducción de mecanismos de seguridad a nivel de control de accesos, firma, cifrado, control del no repudio y validez de los certificados, etc.

2. Objetivos

De esta forma, la Plataforma de validación y firma electrónica cubre los siguientes objetivos:

- El objetivo primordial no ha de ser otro que el de impulsar la implantación de la firma-e y el DNI-e mostrando una visión uniforme a los ciudadanos. Toda finalidad diferente de esta no estaría justificada.

- Se reducen los costes en licencias, soporte, infraestructuras, etc por parte de los organismos usuarios.

- Con esta Plataforma se promueven y facilitan una serie de servicios destinados al cumplimiento de las obligaciones de las Administraciones para con los ciudadanos en materia de identificación y autenticación electrónica.

- Poder ofrecer los servicios a cualquier nivel de la Administración: local, autonómico o nacional, y donde todos se vean representados.

- La solución técnica seleccionada es la más idónea para nuestro ámbito de aplicación. Dicha solución se basa en las siguientes premisas:
    - Se trata de una solución nada intrusiva a la hora de integrarse en arquitecturas y soluciones existentes en los organismos.

    - Además de gestionar la validación de los certificados del DNI-e, está abierto a otros de diferentes Prestadores de Servicios de Certificación (PSC): MultiPSC, MultiPolítica, MultiCertificados, MultiFirma o MultiFormatos. Igualmente, se establecerían redes de confianza paneuropeas: BRIDGE-CA. Ello estimula la creación de redes de confianza mutua entre los PSCs acreditados por la Administración y los diferentes organismos públicos usuarios de estos servicios.

    - La administración y evolución del software de @firma será diseñada y articulada por los organismos usuarios.

    - La solución atesora las máximas garantías de seguridad y robustez: certificación de procesos y productos, óptimo rendimiento, alta disponibilidad, portabilidad,...

- El porfolio de servicios a ofrecer han de complementar las capacidades existentes en cada organización, no sustituirlas.

- El nivel de interoperabilidad y reusabilidad óptimo con sistemas.

3. ¿Qué es @firma?

@firma es la solución tecnológica en la que se basa la implementación de la Plataforma de validación y firma electrónica del Ministerio de Hacienda y Administraciones Públicas.

Es una solución basada en software libre, estándares abiertos y en java: servidores web Apache, JBOSS, Sistema Operativo Linux, AXIS, etc.

3.1. ¿Qué requisitos se han de cumplir?

Para acceder a los servicios es necesario disponer de accesibilidad a la Plataforma desde los sistemas de información del Organismo en cuestión a través de la red SARA (Sistema de Aplicaciones y Redes para las Administraciones), que ofrece servicios de intranet entre las Administraciones Públicas. Estos sistemas que soportan los servicios de administración electrónica disponibles para los ciudadanos y empresas, accederán a la Plataforma a través de servicios web implementados en tecnología Microsoft® o Java.

Puede encontrar amplia información en la sección 5.1 de este documento.

3.2. ¿Qué servicios y beneficios ofrece?

Además de determinar la validez de los certificados digitales, dispone de múltiples utilidades de valor añadido, entre las que se encuentran la generación y validación de firmas electrónicas en múltiples formatos, auditoría de las transacciones y documentos firmados, sellado de tiempos o la compatibilidad con certificados digitales generados por múltiples prestadores de servicios de certificación.

Puede encontrar amplia información en la sección 6 de este documento.

En cuanto a los beneficios que ofrece la propuesta de prestación de servicios por a cualquier Administración solicitante, las diferentes aplicaciones de diferentes organismos acceden a los servicios comunes de la Plataforma del MINHAP a través de servicios web u otros protocolos específicos estándar, como OCSP. Otros de los beneficios que lo definen caracterizan son:

- Utilización de los servicios a través de Red SARA.
- Administración delegada para organismos.
- Se habilitan la consulta de reportes mensuales de actividad y transacciones de diferente naturaleza.
- Se dispone de Servicio de Soporte especializado de segundo nivel a organismos usuarios.
- Reducción de costes e inversiones: desarrollo, soporte, plataforma, etc.
- Accesibilidad a últimas versiones y evoluciones de servicios con total transparencia.

3.3. ¿Quién se puede beneficiar de los servicios?

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 Hacienda y Administraciones Públicas se ofrece la ayuda y el soporte necesario para que los Organismos integren estos servicios de certificación de valor añadido en los sistemas de información de Administración Electrónica que admitan autenticación y firma electrónica basada en certificados digitales.

4. Caracterización técnica y de soporte de la Plataforma

4.1. Medidas de seguridad y disponibilidad de los servicios

A continuación se muestran las características de la Plataforma en lo que respecta a la seguridad y disponibilidad:

1. Arquitectura en alta disponibilidad y escalable.

    - Cada uno de los elementos de la arquitectura de servicios se encuentra dimensionado para ofrecer capacidades de, al menos, un 50% superior a las necesidades de rendimiento del uso de los servicios.
    - Se establece una configuración en la que cada elemento se encuentra redundado convenientemente: servidores de aplicaciones, balanceadores, bases de datos, dispositivos seguros de creación de firma, etc.

2. Cuenta con elementos de antivirus, firewalls, sistemas de prevención y detección de intrusos (IPS/IDS), además de las implícitas medidas de seguridad como cifrado de tráfico disponibles en la red SARA de acceso a la Plataforma.

    Igualmente, se han seguido los criterios y guías de seguridad propuestas por el Centro Criptológico Nacional (CCN) del Centro Nacional de Inteligencia (CNI) para la configuración de dichos dispositivos de seguridad, servidores, bases de datos, etc.

3. Utilización sistemas almacenamiento masivo externo SAN de alto rendimiento y disponibilidad y escalable, donde se hospedan todas las transacciones y registros.

4. Utilización de dispositivos seguros de creación de firmas y almacenamiento de claves criptográficas HSM. En dichos dispositivos se emplean para la realización de firmas electrónicas solicitadas por organismos externos usuarios.

5. Centro Espejo de respaldo.
    Se dispone de un centro espejo de contingencias en estado semi activo que entraría en operación completa a ofrecer los servicios de la Plataforma principal de servicios de validación y firma electrónica ante una indisponibilidad grave y longeva en dicho centro.

6. Proceso de acreditación de la Plataforma por el CCN que asegure la adecuación de las medidas de seguridad organizativas, físicas, técnicas, etc. implantadas en la Plataforma. Para ello se dispone del oportuno Análisis y Gestión de Riesgos realizado siguiendo la metodología Magerit ver 2.0 y la herramienta PILAR.

Se dispone de un Acuerdo de Nivel de Servicio (SLA) disponible a través del servicio de Soporte que complementa las medidas implantadas.

4.2. Red SARA

La Red SARA (Sistema de Aplicaciones y Redes para la Administraciones) es una infraestructura tecnológica que permite y garantiza la comunicación entre las distintas administraciones (municipal, autonómica y estatal) además de servir de plataforma de intercambio de operaciones.

Está formada por la Intranet Administrativa, que hoy ofrece un amplio número de servicios que se prestan en cooperación en el ámbito de la Administración General del Estado, sus elementos de incardinación en TESTA II, y los elementos de enlace con las Redes Corporativas de las Comunidades Autónomas. TESTA II es la Red transeuropea que enlaza la Red Corporativa de la Comisión de la Unión Europea, con las de los Estados Miembros, para el soporte de intercambio de datos y cooperación en la prestación de servicios.

La interconexión a la Extranet se realiza a través de lo que se denomina Área de Conexión (AC). Este AC responde básicamente al esquema de una zona desmilitarizada (DMZ) formada por un cortafuegos externo (que, en este caso, conecta con el resto de la red), un servidor donde residen los servicios básicos y un cortafuegos interno.

4.3. Servicio de Soporte (CAID)

La plataforma de @firma dispone un servicio de soporte a los integradores de las Administraciones Públicas para atender las posibles incidencias o anomalías que pudieran ocurrir.

Este servicio está disponiblepara resolver las dudas o consultas de los integradores del sistema a través de los formularios disponibles en la siguiente URL:.
https://soportecaid.redsara.es
Se dispone de un Acuerdo de Nivel de Servicio (SLA) disponible a través del servicio de Soporte que complementa la descripción de los servicios de soporte disponibles.

5. Requisitos de acceso al Servicio

A continuación, se describen cuáles son los requisitos de acceso a los servicios de @firma. Como ya se comentó en un punto anterior de este documento, 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.

5.1. Pasos a dar para la utilización de los servicios

A continuación, se detallan los pasos que el Organismo en cuestión debe dar para solicitar el acceso:

1. El Organismo debe ponerse en contacto con el servicio de Soporte (CAID) de @firma, indicando el Organismo (Ministerio, Comunidad Autónoma o Entidad Local) que desea integrarse en el servicio, así como los datos de contacto del mismo:

   https://soportecaid.redsara.es

   Puede obtener información de los requisitos de acceso y la documentación que es necesario aportar en la solicitud, en la página del a solución en el CTT:

   http://administracionelectronica.gob.es/es/ctt/afirma

   En concreto es necesario aportar el ACL (formulario para el control de acceso)

2. La documentación básica para la integración se compone de:

   a. ACL (formulario para el control de acceso).
   b. Documentación
      i. Pasos iniciales para la integración con @firma.
      ii. Guía de Servicios de @firma.
      iii. Manual del Integrador del Cliente de Firma @firma.
      iv. Manuales de Programación de web service y DSS de @firma.

   También se dispone de unas librerías de integración (Integr@), que pueden descargarse y consultarse desde la página del a solución en el CTT:

   http://administracionelectronica.gob.es/es/ctt/Integra

3. Si es necesaria información adicional, el servicio de Soporte (CAID) se pondrá en contacto con dicho Organismo para informar de los prerrequisitos que son necesarios para iniciar la integración.

4. El Organismo debe devolver el ACL debidamente cumplimentado al servicio de Soporte (CAID) para finalizar el proceso de integración.

5. El servicio de Soporte (CAID) informará debidamente de los parámetros de conexión con los servicios: URL, identificador de aplicaciones,…

5.2. Acceso a los servicios: web service

Un *web service* es una aplicación de negocio publicada como un servicio que puede ser invocado utilizando estándares de Internet e integrado con otros web services. En pocas palabras, es un recurso accesible mediante una URL (URI) que programáticamente devuelve información a los clientes que lo utilizan.

Para acceder a los servicios de @firma, vía web service, es necesario, tal y como se ha descrito en el punto anterior, tener permiso de acceso a la plataforma, así como tener registrada la aplicación que realiza la petición.

Una vez que el usuario tiene acceso al servicio, basta con generar un cliente que sea capaz de invocar al web service con los parámetros necesarios, utilizando para ello un entorno de desarrollo.

En este punto, es necesario tener en cuenta algunas consideraciones para acceso a los web services y su securización:

1. El protocolo de acceso a los WS se define mediante un mensaje de petición y otro de respuesta al mismo.

2. Los interfases XMLSOAP cumplen con el estándar Basic Profile v1.1 del Web service Interoperability (WS-I) de OASIS.

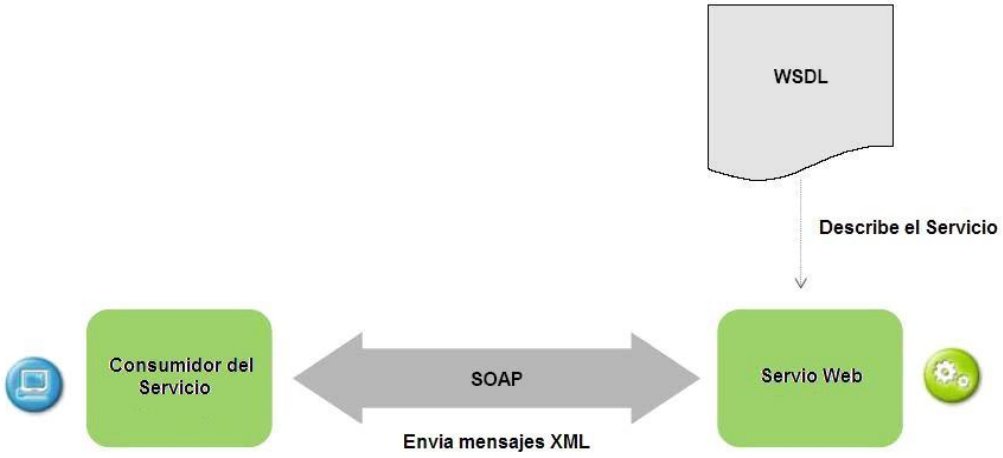
3. Ambos mensajes se intercambian haciendo uso del protocolo XML-SOAP siendo obligatorio que dicha petición sea realizada en codificación “UTF-8” vía http (por el puerto 8080) o https. Las peticiones XMLSOAP en función de la aplicación que realice la misma pueden estar:

    - Securizadas haciendo uso de usuario/password.
    - Firmadas (recomendable).

4. La plataforma devolverá los mensajes SOAP de respuesta firmados haciendo uso del certificado público de la misma (La firma se inserta según en el Binary Security Token según WSS 1.0 de Oasis). Implica la confianza en el certificado público de la plataforma que se proporciona a los organismos.

5.2.1. Caracterización de los servicios de @firma. Uso de los web services.

Actualmente se usan para la integración de aplicaciones y sistemas dispares, gracias a su interoperabilidad, ya que usan XML para describir sus interfaces y codificar los mensajes usados en la comunicación.



La WS-I (Web service Interoperability Organization) es una organización que promueve la interoperatividad de los web services entre plataformas, sistemas operativos y lenguajes de programación. Publica unas guías específicas y recomendaciones de buenas prácticas para el desarrollo y uso de estos servicios. Actualmente, los servicios de @firma cumplen con el perfil *Basic Profile v1.1* (10-abril-2006).

Para lograr comunicar el cliente que solicita la respuesta y el proveedor de servicios, se utiliza el protocolo SOAP (Simple Object Access Protocol) que se trata de un protocolo de mensajería basado en XML para acceso e interconexión de web services.

Un web service responde ante una petición SOAP válida, por tanto es necesario:

1. Conocer la descripción del servicio; para ello obtenemos el WSDL publicado en:

   http://des-afirma.redsara.es/afirmaws/services

2. Crear una petición SOAP. Para ello usaremos un API's de desarrollo.

Para garantizar la interoperabilidad de los web services la plataforma utiliza XML (tratados como string) para definir los parámetros entrada/salida del servicio. Por tanto, el formato de intercambio de documentos entre los organismos que utilicen los servicios de @firma es *SOAP-Document Literal Bare*, es decir, el formato del mensaje de la cabecera SOAP es un XML con los parámetros de la operación invocada encapsulados en varios elementos, implícitos en dicho XML.

5.2.2. La seguridad en los Web service: WS-Security (OASIS).

La tecnología *WS-Security* es un modelo de seguridad en las comunicaciones que suministra un medio para aplicar seguridad a los web services. Originalmente fue desarrollado por IBM y Microsoft, aunque actualmente la iniciativa es coordinada por OASIS.

La versión 1.1 de la especificación de seguridad, WS-Security 1.1, ha sido aprobada en febrero de 2006 como norma internacional para securizar aplicaciones distribuidas y servicios Web. La versión 1.0 fue publicada en abril de 2004.

Este estándar es empleado en la Plataforma por los organismos para determinar el método de autorización de ejecución de los web services. Los métodos empleados son:

- Usuario y password: mediante este método es necesario que las peticiones SOAP realizadas contengan el tag de seguridad "UserNameToken" y que el usuario y password alojados en dicho tag estén registrados para la aplicación que intenta ejecutar el servicio Web.

- Certificado: mediante este método es necesario que las peticiones SOAP realizadas contengan el tag de seguridad “BinarySecurityToken” y estén firmadas por alguno de los certificados registrados para la aplicación que intenta ejecutar el servicio Web. La parte pública de estos certificados, para poder aplicar esta modalidad, ha de ser facilitada a Soporte para la inclusión de la misma en la Plataforma.

6. Servicios ofrecidos por la Plataforma

6.1. Catálogo de servicios

Los servicios ofrecidos a los organismos se pueden catalogar en los bloques que se describen a continuación, basándose la mayoría en la publicación de un catálogo amplio de web services compatible con las tecnologías java y .NET. Todos los web services se encuentran disponibles tanto en castellano como en inglés, facilitando así la integración e interoperabilidad con soluciones existentes en las implantaciones de los organismos usuarios.

Así mismo, la plataforma contempla el uso del estándar Digital Signature Services (DSS) de Oasis, el cual define protocolos de firma, verificación (también firmas longevas) y custodia basados en interfaces XML. Para más información sobre dicho servicio puede consultarse el documento correspondientes ("Perfiles para la adaptación de los Web Services de @firma 5 al protocolo OASIS-DSS").

Actualmente la plataforma @firma admite peticiones con un tamaño máximo de 8 MB.

Los bloques son los siguientes:

6.2. Servicios que ofrece la Plataforma @firma

6.2.1 Servicios de validación.

Se corresponde con todos aquellos servicios orientados a obtener información de certificados y de la validación de certificados y firmas electrónicas. Entre los servicios de validación de certificados X.509 según la RFC 3280, se admite tanto el protocolo OCSP como la invocación de web services específicos.

Se permite realizar una validación completa de la firma electrónica proporcionada a la Plataforma. Como validación completa se entiende:

- Validación de la firma digital contenida en la firma electrónica frente a los datos proporcionados.

- Validación del certificado X.509 empleado y contenido en la firma electrónica. Se validará su integridad, periodo de validez y estado de revocación. Tanto el periodo de validez como el estado de revocación del certificado se comprueban frente a la fecha actual en caso que la firma electrónica no posea sello de tiempo o frente al mismo en caso contrario.

- Obtención de información de certificados. Obtención de los datos de identidad del firmante, así como información adicional del certificado, en una estructura XML homogénea para todos los certificados.

- Soporte del certificado. Se comprueba que el certificado y su emisor sean reconocidos y soportados por la plataforma. Este servicio puede ser empleado para validar tanto las firmas electrónicas generadas por la plataforma o el cliente de firma suministrado por el MINHAP como aquellas ajenas, siempre y cuando su formato sea soportado.

Los web services incluidos son:

- Validación de certificados.
- Obtención de información de certificados.
- Validación de firma electrónica en múltiples formatos: XMLDsig, XAdES, CMS, CAdES, PAdES...

6.2.2 Servicio de upgrade de firma.

Permite la actualización o upgrade de firmas electrónicas a un formato más avanzado, para ello es posible especificar el formato al que se desea extender la firma. Los distintos valores pueden ser: BES, EPEs, T, C, X, X-1, X-2, X-L. X-L-1, X-L-2 y A.

6.2.3 Servicios de firma electrónica (Sólo disponible en el modelo federado).

Engloba todos los servicios relativos a la realización de firmas electrónicas por parte de la Plataforma. Dichas firmas pueden ser de la propia Plataforma o solicitudes de firmas de servidor de los organismos, a partir de certificados hospedados y firmas realizadas en dispositivos seguros de creación de firmas (eje. HSMs).

Este servicio permite a una aplicación cliente realizar, con el certificado de firma de servidor indicado, y siempre dentro del contexto de la plataforma @firma, una firma electrónica. Es decir, la generación de dicha firma se lleva a cabo en la plataforma, de ahí el nombre de firma electrónica servidor.

Es importante resaltar que hay 3 modos de realizar una firma electrónica en servidor:

i. *Firma electrónica servidor simple*:
Es el modo clásico. Se genera una firma electrónica con un formato determinado a partir de unos datos indicados.

ii. *Firma electrónica servidor en paralelo (cosign)*:
Consiste en, a partir de una firma electrónica existente, añadir un nuevo valor de firma al envoltorio que es la firma electrónica en sí.

iii. *Firma electrónica servidor en cascada (countersign)*:
En este tipo de firmas se realiza una firma digital sobre el valor de la firma digital de un firmante concreto, dentro del envoltorio de la firma electrónica. Es decir, es un proceso de aprobación de una firma existente por parte de otro firmante, el cual se incorpora a la misma firma electrónica.

A lo anterior hay que añadir que las firmas se pueden construir en varios formatos: PKCS#7, CMS (compatibilidad con todas sus versiones definidas por la IETF1), XMLSignature Básico, XMLSignature avanzado (XAdES) , y CMS avanzado (CAdES), PDF y PAdES.

Todo lo aplicable en este punto se corresponde con la firma de servidor de la Plataforma, a lo cual hay que añadir las capacidades de firma en servidor disponibles en la librería Integr@ a disposición de los usuarios de la Plataforma que lo requieran, y las capacidades de firma en entornos de usuario, disponibles en el Cliente de @firma.

En cuanto a la Autoridad de sellado de tiempo (TSA) se dispone del servicio web para Solicitar sello de tiempo o un TimeStampReq si se realiza directamente en formato ASN.1

Se pueden consultar el resto de servicios y productos de firma electrónica de la plataforma @firma en la página de la Suite:

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

Actualmente existe un nuevo servicio de firma avanzada siguiendo estándares internacionales basados en perfiles DSS de OASIS, por lo que se recomienda emplear en el modelo federado los servicios de firma en servidor basado en DSS.

En modo servicio, la firma en servidor no se ofrece por parte de la plataforma @firma.

6,2.4 Certificados reconocidos por la Plataforma

La Plataforma @firma valida los certificados digitales reconocidos emitidos por múltiples prestadores de servicios de certificación que se adecuan a lo marcado por la Ley de firma electrónica Ley 59/ 2003, la Ley 11/ 2007 y el RD 1671/ 2009. Los prestadores reconocidos se pueden encontrar en el documento “ANEXO – Proveedores de Servicios de Certificación” publicado actualmente en el PAe (http://administracionelectronica.gob.es/es/ctt/afirma).

Para más información pueden revisar el documento "Anexo - Proveedores de servicios de certificación" para conocer los certificados soportados por los servicios citados y la página https://sedeaplicaciones2.minetur.gob.es/prestadores/

6.2.5 Protocolos de acceso al servicio

Servicios Web

Los Servicios Web (en adelante WS) vienen definidos como un sistema software diseñado para soportar la interacción entre máquinas en una red.

Posee una interfaz descrita en ficheros WSDL (Web Service Description Language). En ellos se describe la definición y descripción de los servicios web, así como otros aspectos como funcionalidad, forma de comunicación y localización. También ofrece un mecanismo para describir las operaciones que realiza un Servicio Web, los formatos de los mensajes que puede procesar, así como los protocolos que soporta.

La interacción con los sistemas se realiza por mensajes SOAP, estándar para el intercambio de mensajes basados en XML, en la forma descrita por su descriptor.

El transporte de los mensajes se realiza vía HTTP serializados en XML junto con otros estándares de la Web.

Se recomienda el uso de los servicios web DSS, ya que siguen los estándares internacionales OASIS y proporcionan servicios avanzados.

El límite de tamaño admitido para las peticiones a los Servicios Web (SOAP) se establece en 12 MB (12.582.912 bytes), incluyendo la codificación en Base64 de los ficheros y/o firmas contenidos en el encapsulado SOAP, no sólo la propia firma o certificado.

OCSP Responder

Se trata de un servidor OCSP multiprestador, según la RFC 2560. Actúa como OCSP responder e indica el estado de revocación de un certificado.

Se trata, pues, de un servicio estándar (RFC 2560) de obtención del estado de un certificado. Presenta muchas ventajas entre las que destacamos que se trata de un método de consulta on-line, así como la fiabilidad del estado del certificado en un determinado instante muy alta.

El servicio OCSP Responder admite la consulta por OCSP de la mayoría de los PSC's soportados disponibles en el ANEXO de Prestadores de Servicios de Certificación publicado en el PAe (https://administracionelectronica.gob.es).

Dentro de las mejoras desarrolladas en la plataforma @firma del MINHAP, se ha evolucionado la funcionalidad del servicio OCSPResponder para que admita la identificación de las peticiones. Esto permite ofrecer un servicio más seguro equiparable a los servicios web ofrecidos por la Plataforma, con una identificación clara de la aplicación usuaria, facilitando la resolución de incidencias y, además, proporcionando a los Organismos usuarios estadísticas más exactas del uso de la Plataforma para aquellas aplicaciones que usan el OCSP como método de validación. Por ello, es necesario que las peticiones OCSP incluyan en el atributo *requestorName* el identificador de aplicación asignado por Soporte @firma en el momento de dar de alta la aplicación usuaria. A continuación se muestra la estructura que tiene una petición OCSP para conocer dónde se ubica dicho atributo en la misma:

```
OCSPRequest     ::=   SEQUENCE {
    tbsRequest                  TBSRequest,
    optionalSignature   [0]     EXPLICIT Signature OPTIONAL }

TBSRequest      ::=   SEQUENCE {
    Version             [0]     EXPLICIT Version DEFAULT v1,
    requestorName       [1]     EXPLICIT GeneralName OPTIONAL,
    requestList                 SEQUENCE OF Request,
    requestExtensions   [2]     EXPLICIT Extensions OPTIONAL }
```

Con el fin de asegurar la no suplantación de la identidad en las peticiones OCSP, las mismas se deben enviar firmadas. Previamente, y para que el servicio reconozca la firma electrónica, será necesario enviar la parte pública del certificado firmante con el que se firmarán las peticiones en el formulario “Plantilla de alta de IPs y Aplicaciones en @firma” o ACL publicado en el PAe.

El servicio OCSP responde ante una petición OCSP válida; para ello es necesario:

1) Un cliente OCSP estándar (RFC 2560).
2) Una petición OCSP que cumpla los requisitos comentados anteriormente.
3) Enviar la petición a:
   a) DESARROLLO: http://des-afirma.redsara.es/servidorOcsp/servidorOCSP
   b) PRODUCCIÓN: http://afirma.redsara.es/servidorOcsp/servidorOCSP

La respuesta del servicio OCSP devolverá el estado del certificado X509 y estará firmada con un certificado público de la Plataforma para propósitos de firma OCSP.

6.2.6 Algoritmos soportados

En la siguiente tabla se representan los algoritmos de resumen soportados por la Plataforma:

	FORMATO DE FIRMA

		PKCS#7	CMS	CAdES	XMLDSIG	XAdES	PADES
ALGORITMO DE HASH	MD2*	☑	☑	☒	☒	☒	☒
	MD5*	☑	☑	☑	☑	☑	☑
	SHA1	☑	☑	☑	☑	☑	☑
	SHA256	☑	☑	☑	☑	☑	☑
	SHA384	☑	☑	☑	☑	☑	☑
	SHA512	☑	☑	☑	☑	☑	☑

** Si bien en algunos formatos es posible utilizar los algoritmos MD2 y MD5, no se recomienda su uso ya que no se considera seguro.*

Un algoritmo de Firma Electrónica se compone de 2 algoritmos: uno asimétrico y un algoritmo de hash, todas las firmas generadas por @firma se realizan utilizando RSA o ECDSA como algoritmo asimétrico mientras que el algoritmo de resumen depende del escenario de firma.

En la siguiente tabla se representa los distintos algoritmos de firma soportados por la Plataforma:

	FORMATO DE FIRMA						
ALGORITMO DE FIRMA		PKCS#7	CMS	CAdES	XMLDSIG	XAdES	PADES
	MD2withRSA*	☑	☑	☒	☒	☒	☒
	MD5withRSA*	☑	☑	☑	☑	☑	☑
	SHA1withRSA	☑	☑	☑	☑	☑	☑
	SHA256withRSA	☑	☑	☑	☑	☑	☑
	SHA384withRSA	☑	☑	☑	☑	☑	☑
	SHA512withRSA	☑	☑	☑	☑	☑	☑

	SHA1withECDSA	☑	☑	☑	☑	☑	☑
	SHA256withECDSA	☑	☑	☑	☑	☑	☑
	SHA384withECDSA	☑	☑	☑	☑	☑	☑
	SHA512withECDSA	☑	☑	☑	☑	☑	☑

** Si bien en algunos formatos es posible utilizar los algoritmos MD2 y MD5, no se recomienda su uso ya que no se considera seguro.*

6.2.7 Modelo Federado

Aquellos Organismos que se encuentren interesados en desplegar en sus instalaciones una autoridad de validación tienen a su disposición la posibilidad de obtener el modelo federado de la Plataforma @firma.

Dicha versión consiste en la cesión del software de @firma del MINHAP para el uso por parte del propio Organismo, beneficiándose de poder configurar la Plataforma ajustándose a sus necesidades.

Para obtener el Modelo Federado deben remitir contactar con el Servicio de Soporte a través del formulario web.

6.3. TSA

Como complemento a los servicios prestados por @firma, se encuentra la TS@, una Autoridad de Sellado de Tiempo puesta a disposición de todas las Administraciones Públicas con el objetivo de ofrecer los servicios de sellado, validación y resellado de sellos de tiempo.

Para más información sobre dicho servicio se puede consultar la siguiente dirección http://administracionelectronica.gob.es/es/ctt/tsa

6.4. Herramientas de firma

6.4.1 Cliente de Firma

El cliente de firma es una utilidad para la firma digital de datos o ficheros. Tiene como característica principal que se ejecuta en el ordenador del cliente (es decir, en el equipo del usuario), no en el servidor web.

Entre otras características, destacan:

1. Está basado en Applets Java (es una aplicación que se ejecuta en el contexto de otro programa, por ejemplo, un navegador web). Éstos se integran en las páginas web a través de JavaScript, que permite invocar a los métodos públicos de la aplicación desde HTML.

2. El cliente hace uso de los certificados digitales X.509 y de las claves privadas asociadas a los mismos que estén instaladas en:
   - el repositorio (*KeyStore*) del navegador Web (Internet Explorer, Mozilla Firefox,…)
   - el dispositivos seguros de creación de firma electrónica (tarjetas inteligentes, dispositivos USB, HSM,…) compatibles PKCS#11 o MS-CSP.

El cliente permite la realización de las siguientes operaciones:

- Firma formularios Web (con y sin adjuntos)
- Firma ficheros binarios
- Firma Masiva, tanto de ficheros binarios como de archivos XML
- Firma Multiformato: CMS, XMLDsig, XAdES, CAdES, PAdES, PDF, ODF
- Co-firma (CoSignature) o Multifirma al mismo nivel.
- Contra-Firma (CounterSignature) o Multifirma en cascada.

El cliente básico se compone de:

1. Clases de la aplicación, agrupadas en ficheros JAR (Java ARchive) almacenados por el instalador en un directorio de usuario.
2. Librerías de sistema (*.dll* en Windows, *.so* en Linux y Solaris y *.dylib* en Mac OS X) almacenadas por el instalador en un directorio de usuario.
3. Ficheros JavaScript, que contienen funciones para la automatización de los procesos de firma.
   - Almacenados en el servidor Web y modificables por los integradores.
   - Muchos de ellos son opcionales y se puede operar sin ellas, pero facilitan los procesos más comunes.
4. Ficheros de configuración.

Puede consultarse la información actualizada del cliente de @firma en la forja de desarrollo colaborativo, en la wiki y en el área de descargas.

http://forja-ctt.administracionelectronica.gob.es/web/clienteafirma

Se ofrece documentación en formato Java (JAVADOC) para los integradores. El JavaDoc se trata de una descripción de la funcionalidad del cliente de firma que proporciona una ayuda en formato Web en la que se detalla qué hace cada uno de los métodos del cliente de firma de los que puede hacer uso el integrador.

Puede descargarse firmado con un certificado del Ministerio, aceptado por los navegadores, desde el área de descargas del PAE, para usuarios de las Administraciones Públicas registrados en el portal:

http://administracionelectronica.gob.es/es/ctt/clienteafirma

El MiniApplet es una aplicación que se ejecuta en cliente. Esto es así para evitar que la clave privada asociada a un certificado tenga que "salir" del contenedor del usuario ubicado en su PC. De hecho, nunca llega a salir del navegador,
el Cliente le envía los datos a firmar y éste los devuelve firmados.

El MiniApplet @firma es Software Libre publicado que se puede usar, a su elección, bajo licencia GNU General Public License versión 2+ (GPLv2) o superior o bajo licencia European Software License 1.1 (EUPL 1.1) o superior.

6.4.2 Cliente Standalone

La versión Standalone del Cliente de Firma permite ejecutarse como una aplicación independiente o aplicación de escritorio, a diferencia de ejecutarse bajo un navegador como hasta ahora.

Es posible encontrar la descarga de la versión Standalone del Cliente de Firma de @firma en el Portal de Administración Electrónica
http://administracionelectronica.gob.es/es/ctt/clienteafirma

así como en la Forja-CTT
http://forja-ctt.administracionelectronica.gob.es/web/clienteafirma

6.4.3 Firma fácil

La aplicación “Firma electrónica fácil con @firma” es otra aplicación de escritorio, que permite realizar de forma muy sencilla, firmas electrónicas avanzadas sobre ficheros locales.

Para simplificar al usuario el proceso, dispone de un mecanismo de selección automática de formato de firma en base al fichero a firmar: "Firma fácil con @firma" está diseñada para utilizar DNI electrónico (DNIe) como dispositivo preferente para la creación de firmas

en sistemas con lector de tarjetas inteligentes instalado, aunque puede hacer uso de cualquier otro certificado instalado en el sistema operativo

Es posible encontrar la descarga de la versión Standalone del Cliente de Firma de @firma en el Portal de Administración Electrónica :

http://administracionelectronica.gob.es/es/ctt/clienteafirma

así como en la Forja-CTT :

http://forja-ctt.administracionelectronica.gob.es/web/clienteafirma

6.4.4 Clientes de firma movil

Se dispone también de aplicaciones para dispositivos móviles (teléfonos y tabletas)

Cliente@Firma Móvil. Integrable de forma transparente para los usuarios del Miniapplet. (BETA). Necesario uso del servidor intermedio (Proxi ClienteMovil). Disponible para plataformas: Android 4.0 y posteriores, iOS 6 y posteriroes, y Windows RT y 8 con interfaz de nueva generación (Metro).

Port@firmas Móvil. (BETA): Integrable con la aplicación Port@firmas de la suite @firma, aunque su funcionalidad es adaptable a otros portafirmas, realizando cambios en el proxi de portafirmas (Proxi PortafirmasMovil). Disponible para Android 4.0 y posteriores.

6.5. Demostrador de @firma

El demostrador de @firma (VALIDe) es un servicio que permite determinar la validez de firmas y certificados digitales. Además, dispone de otras utilidades de valor añadido, entre las que se encuentran la generación y validación de firmas electrónicas en múltiples formatos o la demostración de servicios web de @firma, muy útil para desarrolladores e integradores de la Plataforma.

Es una solución de referencia para cumplir con las medidas de Identificación y autentificación descritas en el Capítulo II de la Ley 11/2007 de Acceso electrónico de los ciudadanos a los Servicios Públicos (LAECSP).

Facilita la creación de redes de confianza y de reconocimiento mutuo de servicios de validación entre autoridades de validación y los prestadores de certificación acreditados así como primera base para cumplir con el plan de acción i2010 en materia de interoperatividad de el IDM (gestión de identidades electrónicas) de la Unión Europea.

En la dirección http://administracionelectronica.gob.es/es/ctt/valide es posible acceder al servicio.

6.6. STORK

Es un servicio para las AAPP que permite la identificación electrónica segura de ciudadanos europeos, y en concreto la aceptación de DNI electrónicos y otras identidades electrónicas que existen en otros países europeos en servicios de administración electrónica. Más información en:
http://administracionelectronica.gob.es/es/ctt/stork.

ANEXO
Conceptos básicos de criptografía y PKI

1. **Criterios de seguridad**

Las aplicaciones que manejan datos de carácter personal deben adoptar una serie de medidas de seguridad desde el punto de vista organizativo y técnico, para crear un entorno seguro para los datos, la información y los sistemas que participan en la misma.

Para ello, se definen los siguientes criterios de seguridad, que serán la base de lo que llamaremos más adelante como *firma digital*:

2. Autenticidad: El receptor del mensaje puede asegurar la identidad del emisor. El emisor puede estar seguro de a quién envía el mensaje. Evita ataques de engaño o suplantación.

3. Confidencialidad: Protección de la información frente a usos no autorizados. Sólo emisor y receptor pueden acceder al contenido del mensaje. Evita ataques de intercepción.

4. Integridad: Protección de la información frente a cualquier tipo de alteración.

5. No repudio: Garantía de que el emisor o receptor no rechazan su envío o recepción.

6. Control de acceso: Protección de los recursos para evitar accesos no autorizados.

1.1. Infraestructura de Clave Pública (PKI)

Podemos definir **criptografía** como la ciencia de escribir con clave secreta para mantener oculta determinada información a accesos no deseados.

Para cifrar los datos, surgen los Algoritmos Simétricos, cuya finalidad es la de cifrar y descifrar mensajes utilizando una misma clave. Como inconveniente principal encontramos la distribución de las claves entre el emisor y el receptor.

Como solución a este problema, surgen los Algoritmos Asimétricos. Este método utiliza dos claves, una para cifrar (encriptar) y otra para descifrar (desencriptar). Las dos claves están relacionadas y cumplen:

1. Los datos cifrados con una clave sólo se descifran con la otra.
2. Con una clave es imposible averiguar la otra.
3. Se cifra con una clave y se descifra con la otra.

Como uso principal está:

- La **FIRMA DIGITAL**, que debe cumplir autenticidad, integridad y no repudio; para ello, cifraremos el mensaje con nuestra clave privada, y los usuarios que deseen verificarla, descifrarán con la clave pública.

- El **CIFRADO** de información, que debe cumplir confidencialidad, integridad y no repudio; para ello, cifraremos el mensaje con la clave pública del receptor, y el receptor será el único que podrá descifrar con su clave privada (por ejemplo, SSL).

La criptografía asimétrica también se denomina Infraestructura de Clave Pública ó PKI.

El uso de esta arquitectura para la firma digital tiene una serie de características, entre las que destacan:

- Tiene por objeto distribuir la clave simétrica de forma segura.
- Está basado en el uso de un par de claves, una pública y otra privada, por cada entidad.
- La clave privada debe permanecer en secreto y bajo el control del usuario. Usarla para cifrar/descifrar es lo que demuestra que la posees y con ello queda garantizada la autenticidad, confidencialidad e identidad.
- La clave pública puede y debe ser libremente distribuida, lo más extensamente.

1.1.1. La Firma Digital

Para la generación y verificación de una firma digital se emplean:

1. Funciones matemáticas de hash o resumen.
2. Criptografía asimétrica.

Para firmar digitalmente, no se cifra todo el mensaje, sino el resultado de aplicar la función de HASH sobre el mismo. El HASH (o DIGEST) es un método matemático que genera un mensaje de longitud fija a partir de un texto original, tenga éste la longitud que tenga. Esta función es irreversible, es decir, a partir de ella no se puede obtener el texto original, pero si cambia cualquier carácter de este texto, el HASH resultante será completamente distinto. Ejemplos de algoritmos de HASH, encontramos el MD5 y el SHA-1.

Es el DIGEST lo que se cifra con la clave privada del emisor para firmar digitalmente y se envía el texto original y el digest cifrado al receptor. Éste descifrará con la clave pública del emisor, contenida en la firma digital, el digest recibido, le aplicará el mismo algoritmo de HASH al texto original, y comparará que ambos digests sean iguales (integridad).

1.1.2. Certificados digitales

Junto con la firma digital, debe facilitarse la clave pública del emisor para poder descifrar el mensaje y comprobar que éste no ha sido alterado. Para ello, existen los certificados digitales.

Un certificado digital es emitido por una Autoridad de Certificación (CA) que garantiza la equivalencia "certificado ←→ persona". Se trata de un certificado en el que se incluyen, entre otros:

1. Identificador único o número de serie del certificado.
2. El algoritmo de firma digital empleado.
3. Datos identificativos de la Autoridad de Certificación.
4. Fechas de expedición y expiración de las claves pública y privada.
5. Clave pública del titular del certificado.

La Autoridad de Certificación firma el certificado con su clave privada, de modo que cualquier persona puede leerlo y comprobarlo utilizando la clave pública de la propia CA (certificado padre o emisor). Al tratarse de una firma digital, se asegura que nadie puede modificarlo, excepto la CA. Por ello, es necesario que en la validación de una firma electrónica, tenemos que comprobar que el certificado firmante pertenece a una CA de confianza, comprobando la firma digital de cada uno de los certificados que conforman la *cadena de confianza* (cada certificado es firmado por su padre hasta llegar al certificado raíz de la CA, en lo que se denomina *cadena de confianza*).

Se almacenan en los navegadores de Internet (IExplorer, Firefox), en ficheros (formato PKCS#12), y en tokens criptográficos (SmartCards, dispositivos USB, HSM,…).

El titular de un certificado puede ser una persona física o jurídica. Además, se emiten certificados a empleados, miembros de asociaciones, empresas, colegios profesionales, ciudadanos,… El uso que se le da a un certificado ha de estar recogido en la Política de Certificación y en el Contrato de emisión suscrito con la CA.

La Autoridad de Certificación (CA) tiene las siguientes características:

1. Es la entidad que emite el certificado, previo visto bueno de la Autoridad de Registro (RA).
2. Proporciona las herramientas y servicios necesarios para gestionar su ciclo de vida: emisión, suspensión y revocación.
3. Las solicitudes de emisión de certificados pasan a ser gestionadas por las Autoridades de Registro.
4. Validar certificados solicitados e informar del estado de certificados.
5. Las garantías y servicios que ofrece a terceros deben quedar reflejadas en su Declaración de Prácticas de Certificación (DPC / CPS). Los requisitos de uso de emisión de certificados quedan reflejados en la Política de Certificación (CP).

Entre las características de la Autoridad de Registro (RA) destacan:

1. Requiere presencia física del solicitante de un certificado en la Autoridad de Registro, donde a través de la documentación pertinente se verificará que el solicitante del certificado y la persona presentada son la misma persona y que la información es verídica.

2. Son numerosas y dispersas geográficamente para facilitar la accesibilidad de los usuarios finales.

3. Son formadas y certificadas por la Autoridad de Certificación (CA) que les proporciona una licencia de funcionamiento.

4. Otras funciones:
   - Informar y asesorar al solicitante.
   - Identificar de forma cierta al solicitante.
   - Realizar copia de la documentación acreditativa presentada.
   - Entregar dispositivo homologado de generación de solicitud de certificado.

En el ámbito de los servicios de certificación y firma electrónica, aquellas entidades, empresas o particulares que reciben un documento electrónico firmado o asumen la identidad de otros a partir de certificados digitales reciben el nombre de Tercero de Confianza (TTP). Entre sus funciones destacan:

1. Decidir los certificados de confianza que admite en firmas.
2. Ha de ser diligente en los procesos de verificación y mantenimiento de los dispositivos de verificación.
3. Ha de custodiar de forma correcta los documentos recibidos que puedan requerir el acceso y verificación por parte de terceros, por ejemplo, en inspecciones tributarias.
4. Ante un conflicto, ha de saber autorizar una firma realizada con anterioridad.

Otro tipo de entidades que participan en este tipo de arquitectura (PKI) son los Emisores de CRL (Lista de Revocación de Certificados – Certificate Revocation List). Éstos actúan en nombre de la Autoridad de Certificación. Por definición, una CRL es una lista de los certificados que han dejado de ser válidos y por tanto, no se puede confiar en ellos. En el proceso de validación de un certificado, se comprueba que el certificado a comprobar no se encuentre en esta lista.

1.1.3. Tipos de firma electrónica

Existen varios criterios según los cuales se pueden distinguir distintos tipos de firma electrónica. A continuación, explicaremos algunos de ellos:

1. Según si el envoltorio de la firma contiene o no el documento a firmar:
    - Attached (ó Implícita): se incluye el documento firmado.
    - Detached (ó Explícita): no se incluye el documento firmado.
2. Según la relación entre las firmas y los documentos:
    - Independientes: se firma un documento por varios firmantes.
    - Envolventes: el digest (o HASH) se forma con la firma anterior.
    - Globales (o de grupo): el digest se forma con la firma y el documento anterior.
3. Según la parte que se firma y la composición del bloque de firma:
    - Envolvente: la estructura de firma incluye el mismo documento.
    - Envuelta: se genera un nuevo documento con el documento inicial y la firma generada.
    - Independiente (ó detached): en contra de los dos casos anteriores, documento y firma están en estructuras independientes.

1.1.4. Formatos de firma electrónica

En función del formato de los elementos firmados, se pueden distinguir varios estándares:

- CMS: Cryptographic Message Syntax
    - Proviene de formato PKCS#7, un formato propietario de una empresa norteamericana (RSA).
    - Recomendación del IETF, RFC 2630.
    - Es especificada en notación abstracta ASN.1.
- XMLdsig: XML Signatures
    - Recomendado por el W3C.
    - Basado y especificado en XML y sus correspondientes esquemas.
    - Permite incorporar varias firmas en un documento, que afecten a diferentes partes del mismo.
- XAdES: XML Advanced Electronic Signatures

- Estandarizado por ETSI TS 101 903. Las versiones soportadas por la Plataforma para la validación de firmas son XAdES v1.1.1, XAdES v1.2.2 y XAdES v1.3.2. Tanto la Plataforma como el Cliente de Firma generan firmas XAdES v1.3.2.
- Permite incorporar información a la firma básica definida por el W3C: time-stamps, certificados de atributos, indicaciones de responsabilidades asumidas al firmar, etc.
- Asegura la longevidad de las firmas (según información incorporada).

- CAdES: CMS Advanced Electronic Signatures

  - Estandarizado por ETSI TS 101 733.
  - Permite incorporar información a la firma básica en CMS definida por IETF RFC 2630.
  - Asegura la longevidad de las firmas (según información incorporada).

- PDF: PDF Signature
  - La ISO 19005-1:2005 define un formato (PDF/A) para documentos electrónicos basados en la Versión PDF 1.4.
-
- Firmas Longevas basadas en PDF o firmas PADES

  - Estandarizado por ETSI TS 102 778
  - Asegura la longevidad de las firmas (según información incorporada).
  -

- ODF: ODF Signature

  - Los documentos ODF son descritos por el estándar ISO26300.
  - La ISO/IEC 26300:2006 define un esquema XML para aplicaciones de ofimática y su semántica.

1.2. Otros protocolos y sistemas utilizados: OCSP y TSA.

1.2.1. OCSP

Online Certificate Status Protocol (OCSP) es un método para determinar el estado de revocación de un certificado digital X.509 usando otros medios que no sean el uso de CRLs. Este protocolo se describe en el RFC 2560 y está en el registro de estándares de Internet.

Los mensajes OCSP se codifican en ASN.1 y habitualmente se transmiten sobre el protocolo HTTP.

OCSP fue creado para solventar ciertas deficiencias de las CRLs. A continuación, se enumeran las ventajas de utilizar OCSP en vez de CRLs:

- OCSP puede proporcionar una información más adecuada y reciente del estado de revocación de un certificado.
- OCSP elimina la necesidad de que los clientes tengan que obtener y procesar las CRLs, ahorrando de este modo tráfico de red y procesado por parte del cliente.
- El contenido de las CRLs puede considerarse información sensible, análogamente a la lista de morosos de un banco.
- OCSP soporta el encadenamiento de confianza de las peticiones OCSP entre los "responders". Esto permite que los clientes se comuniquen con un "responder" de confianza para lanzar una petición a una autoridad de certificación alternativa dentro de la misma PKI.

Para validar el estado de un certificado,

1. Se construye una petición OCSP que contiene, entre otros datos, el número de serie del certificado a validar.
2. La petición se envía al OCSP Responder ubicado en la Autoridad de Certificación.
3. La CA busca en su base de datos el certificado y verifica su estado (si el certificado ha sido revocado, esta información estará contenida en esta base de datos).
4. La CA devuelve una respuesta OCSP que contiene el estado del mismo.
   a. Si el certificado indicado en la petición es "bueno" (good), "revocado" (revoked) o "desconocido" (unknown), la respuesta estará firmada.
   b. Si devuelve un código de error, la respuesta no tiene que estar firmada.

1.2.2. TSA

Una *Autoridad de Sellado de Tiempo* o TSA sirve para certificar la existencia de unos datos concretos en un momento determinado del tiempo.

Para ello, el primer paso del mecanismo consiste en que el usuario de los servicios de sellado de tiempo envía una solicitud al servidor de sellado de tiempo (“Time Stamp Request” en inglés o “TimeStampReq” en [RFC3161]). El segundo mensaje es la respuesta del servidor al solicitante (“Time Stamp Response” en inglés o TimeStampResp en [RFC3161]). Normalmente, esta respuesta contiene un “Time Stamp Token” o TST que es el elemento que sirve para demostrar la existencia de los datos en el tiempo.

La solicitud de sello de tiempo contiene un campo llamado impronta del mensaje (“MessageImprint”) que indica el hash de los datos y el OID del algoritmo de hash.

La respuesta a la solicitud de sellado de tiempo contiene información sobre el estado (correcto o erróneo, descripción del error...) y el TST. Un TST es un ContentInfo (ver [CMS]) de tipo “Signed Data” y contiene el hash de los datos, el momento de firmado y la firma de la TSA. De ésta forma, la TSA garantiza como tercero de confianza que los datos existían en dicho momento.

Hay dos modalidades de utilización de los servicios de la TSA:

1. Notación abstracta ASN.1

Se cumple así con las especificaciones de la IETF RFC3161, pero empleando sintaxis de las peticiones y respuestas en notación abstracta ASN.1 codificado en DER. El protocolo de transporte es http, al igual que en la segunda de las modalidades. El método de envío es POST-http

2. Web service

Diseñados para facilitar la integración con las aplicaciones, utilizando la especificación de mensajes XML-SOAP. Dichos servicios permiten, además, de la solicitud de sellos de tiempos considerados en la modalidad anterior, la validación de un sello de tiempo emitido por la TSA del MINHAP, que verifica tanto la integridad de la misma (no alteración del contenido) como la validez del certificado firmante.
La plataforma soporta el WS Oasis (XML Timestamping Profile of the OASIS Digital Signature Services (DSS) ver. 1.0).

Una TSA necesita una fuente de tiempo de confianza. La TSA del MINHAP está sincronizada (por NTP y mediante Stratum2 con conexión GPS) con el Real Observatorio de la Armada.
El Real Observatorio de la Armada tiene como misión principal el mantenimiento de la unidad básica de Tiempo en España así como el mantenimiento y difusión oficial de la escala "Tiempo Universal Coordinado" (UTC(ROA)), considerada a todos los efectos como la base de la hora legal en todo el territorio nacional (R. D. 23 octubre 1992, núm. 1308/1992).