tecnim@p Sevilla 2006
30 mayo a 2 junio
060.es
24x7x365

Comunicación

288

@FIRMA: PLATAFORMA DE VALIDACIÓN Y FIRMA ELECTRÓNICA

Ismael García Cebada
Gabinete de Administración Electrónica
D.G. Administración Electrónica y Calidad de los Servicios
Consejería de Justicia y Administración Pública
Junta de Andalucía

Palabras clave

Infraestructura de clave pública, PKI, validación, firma electrónica, DNI-e, @firma.

Resumen de su Comunicación

La Junta de Andalucía tiene en funcionamiento desde 2003 una plataforma común para la validación y firma electrónica en todos sus procedimientos telemáticos, conforme a la normativa vigente en materia de firma electrónica y en especial, al Decreto 183/2003, de 24 de junio, que regula los procedimientos telemáticos en la administración andaluza. Mediante un convenio firmado entre la Junta de Andalucía y el Ministerio de Administraciones Públicas se desarrolla la versión 5 de este sistema, que está siendo utilizada como plataforma común de validación de certificados digitales y firma electrónica dentro del plan Conecta. En la presente comunicación se describen las características técnicas de la plataforma @firma, que será utilizada por diferentes administraciones públicas para sus trámites telemáticos dentro del esquema de cooperación del MAP y la Junta de Andalucía, incluyendo la validación del DNI electrónico.

Ismael García Cebada

@FIRMA: PLATAFORMA DE VALIDACIÓN Y FIRMA ELECTRÓNICA

1. Introducción

La Junta de Andalucía establece su compromiso con la modernización y la calidad de sus servicios públicos con el Plan Director de Organización para la Calidad de los Servicios, aprobado en Junio del 2002 por el Consejo de Gobierno, y en el que se establecen, entre otros, los proyectos destinados a sentar las bases de la administración electrónica de la Junta de Andalucía.

Todos los proyectos relacionados con la creación de una infraestructura tecnológica que posibilite la Administración Electrónica se desarrollaron según este Plan Director, y está disponible, desde 2003 una base sólida y firme de elementos que posibilitan que cualquier procedimiento o servicio pueda ponerse al servicio de los ciudadanos/as a través del portal "andaluciajunta.es".

En particular, nos referimos a los proyectos @firma (creación de una infraestructura de clave pública en Andalucía para la autenticación y firma electrónica basada en la utilización de certificados digitales), @ries (Registro Unificado de Entrada/Salida) y notario electrónico (que permite la obtención de sellos de tiempo y la emisión de recibos electrónicos).

Por otro lado y ante la necesidad de establecer un marco legal único se elaboró el Decreto 183/2003, de 24 de Junio, por el que se regula la información y atención al ciudadano y la tramitación de procedimientos administrativos por medios electrónicos (Internet). Con este Decreto se da comienzo a una Administración Electrónica con todas las garantías de seguridad, jurídicas y técnicas, y con una serie de procedimientos (35) y servicios (45) puestos a disposición de los ciudadanos a través de la red.

Desde entonces, se han multiplicado los procedimientos y servicios iniciales. Por poner algunos ejemplos: el pago electrónico y presentación de tributos, la presentación de la solicitud para participar en los concursos de personal, la preinscripción de matrícula universitaria, la solicitud de ayudas de acción social, las notificaciones telemáticas, etc. A la vez que se incorporan nuevos procedimientos, se van mejorando los existentes con nuevas funcionalidades y servicios.

@firma es la solución tecnológica de autenticación y firma electrónica construida por la Junta de Andalucía para dotar de una plataforma común a todos sus servicios y procedimientos telemáticos. Está en funcionamiento desde 2003 y actualmente da soporte a más de doscientos procedimientos y servicios de las consejerías y organismos de la Junta de Andalucía, además de haber sido cedida y estar en funcionamiento en numerosos ayuntamientos, diputaciones provinciales, universidades y otras comunidades autónomas.
El Ministerio de Administraciones Públicas seleccionó @firma como base para la plataforma común de autenticación y firma electrónica dentro del plan Conecta, con la idea de dar servicio a múltiples administraciones y reconociendo toda la variedad de certificados digitales existentes, incluyendo el DNI electrónico. Para ello se firmó un convenio de colaboración entre la Junta de Andalucía y el MAP, estableciendo las bases del desarrollo de la versión 5 de la plataforma @firma.

2. Características técnicas

La plataforma @firma constituye la base tecnológica de los servicios de Firma-e ofrecidos por el MAP a través de su iniciativa para extender el uso del DNI-e y la firma electrónica. La versión actual evolucionada a partir la versión desarrollada por la Junta de Andalucía, es fruto de la colaboración de múltiples Organismos públicos intervinientes en el programa de colaboración y se denomina @firma 5.0.

Para seleccionar @firma como base tecnológica del proyecto, se tuvieron en consideración múltiples con-

dicionantes, entre los que se pueden destacar las siguientes características técnicas de la plataforma desarrollada por la Junta de Andalucía:

• @firma v4 es una solución con una alta base de implantación que se encuentra operativa desde 2003. Dispone de implantaciones en la Junta de Andalucía (más de 200 procedimientos), Junta Castilla León y Consejo General de la Abogacía.
Es por lo tanto una solución con una sólida base de conocimiento

• Mantiene un alta grado de interoperabilidad con las aplicaciones.
Así ofrece sus servicios a través de servicios web u OCSP construidos a partir de estándares.
Como valor añadido, cuenta con recursos de integración de servicios de firma electrónica aplicaciones legacy. Eje: APIs para Oracle Developer, Oracle Form, Visual Basic, ...

• Al tratarse de una solución propiedad de las Administraciones Públicas, desde sus inicios ha habido un creciente interés por publicar información técnica. Ello ha motivado a que actualmente se cuente con una base importante de integradores con conocimientos técnicos sobre @firma.

• Incorporación de Políticas de eFirma (artículo 4 Ley de Firma 59/2003).

Finalmente, otra de las grandes ventajas aportadas por @firma lo constituye el alto nivel tecnológico de sus componentes:

• Solución basada en software libre, estándares abiertos y en J2EE: servidores web Apache, JBOSS, Sistema Operativo Solaris/Linux, AXIS, etc.

• Disponibilidad de Cliente de firma, verificación, validación, ...

• Entorno cliente con múltiples navegadores: Netscape, Mozilla, iExplorer, Firefox, y sistemas operativos (Windows y Linux).

• Sujeción a normas y estándares de ámbito nacional y europeo: EESSI, ETSI, CEN, Directiva y Ley de Firma-e, RFCs, ...

• Alta auditabilidad de la Plataforma: gestión de transacciones de cada módulo, agentes de monitorización, logs de operaciones, ...

• Múltiples formatos de firma: PKCS#7 v 1.5, CMS, S/MIME, XMLSignature, XMLSignature Avanzado (XaDES).

3. Catálogo de Servicios de @firma 5.0

Las nuevas características introducidas en la versión 5.0 de @firma supone la estructuración del producto en 6 módulos que se describen a continuación:

1. Módulo de Gestión y Registro 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.

2. 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.

3. Módulo 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.

4. Módulo de Firma. Centraliza todos los aspectos relativos a los diferentes tipos de firma, integración y gestión de HSM en @firma y adaptación del módulo de custodia al nuevo modelo planteado por el MAP.

5. Módulo de Cifrado. Define un cliente ligero para dar servicio de cifrado a aquellos usuarios finales que lo demanden.

6. Desarrollos Globales. Incluyen todas las tareas globales de mantenimiento de la plataforma: framework WS que cumpla con el WS-I, componente de administración de la plataforma, firma de solicitudes de servicio, Integración con TSA, etc.

En el siguiente apartado se van a enumerar los distintos servicios ofrecidos por la plataforma organizados por los diferentes módulos descritos en este apartado.

1. Módulo de Registro y Gestión de Eventos

Los servicios ofrecidos por este módulo son:

- Auditoría y trazabilidad de todas las transacciones realizadas por la plataforma. 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.

- 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.

2. Módulo Gestión de Prestadores

Los servicios ofrecidos por este módulo son:

- 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.

- Gestión de los distintos tipos de certificados por cada 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.

- Analizador semántico de certificados y mapeo de campos. Por cada tipo de certificado asociado a un PSC, la plataforma permite definir un “certificado tipo” donde se definen aquellos campos de interés para la pla-

taforma. A esto se le denomina mapeado de campos.

- Gestión de Políticas de Confianza. La plataforma permite definir varios mapeos por cada tipo de certificado y asocialos 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 politica seleccionada por cada una de ellas.

- 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.

3. Módulo de Validación

Los servicios ofrecidos por este módulo son:

- 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.

- Validación de certificados X.509 v3 ante un PSC mediante los protocolos http, ftp, LDAP y OSCP. Posibidad de 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.

- Servidor OCSP. 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.

- Reconocimiento y validación del e-DNI emitido por la Dirección General de la Policía, Ministerio del Interior.

- 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.

4. Módulo de Firma

Los servicios ofrecidos por este módulo son:

- 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.

- Firma de Ficheros por Certificado de Organización. 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.

- Firmas realizadas en varios formatos. Este servicio permite realizar firmas electrónicas en varios formatos posibles: PKCS#7, CMS (compatibilidad con todas sus versiones definidas por la IETF), XMLSignature Básico y XMLSignature avanzado.

- Custodia de los 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 de los Elementos de No Repudio de las transacciones de firma incluyendo el documento firmado.
  - 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.

- Integración con un 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 (HSM). De esta forma, se aporta un mayor nivel de seguridad a los certificados de organizaciones ubicados en el Servidor de @firma..

5. Módulo de Cifrado

Los servicios ofrecidos por este módulo son:

- Aplicación Cliente de Cifrado, que permite además de cifrar documentos, validar y firmar en cliente.

6. Desarrollos Globales

Los servicios ofrecidos por este módulo son:

- Herramienta Gráfica de Administración, para gestionar todos los servicios de la plataforma @firma. Contempla la administración delegada a Organismos que registren aplicaciones en la Plataforma de eFirma.

- Comunicaciones entre todas las interfases de la plataforma mediante el estándar XML-SOAP definido por el W3C siguiendo las recomendaciones del "WebServices Interoperability" (WS-I) basado en el Basic Profile v1.1.

- Integración de la plataforma @firma con Autoridades de Sellado de Tiempo (TSA) que sigan el estándar definido para ello por la IETF mediante la RFC 3161.

- Gestión de autorizaciones en todas las solicitudes de servicio realizadas a la plataforma mediante la firma de las mismas en formato XMLSignature.

4. Características funcionales de la solución

A continuación se relacionan la cobertura funcional que han de cumplir los diferentes servicios de seguridad propuestos.

- Reconocimiento de múltiples certificados y PSCs
- Validación de campos de certificados digitales.
- Firma electrónica y verificación de formularios y documentos.
- Módulo de cifrado y descifrado.
- Servicio de custodia y no repudio de Firma-e.
- Utilidades de administración y auditoría.

Integración con otros servicios:

- Autoridad de sincronismo y sellado de tiempos.
- AA y SSO: Autenticación, autorización e identificación única.

Reconocimiento de múltiples certificados y PSCs.

Dado que la certificación del eDNI debe coexistir con los emitidos por otros PSCs tanto españolas como pertenecientes a la Unión Europea, resulta necesario el establecimiento de un mecanismo según el cual se establezca cuales son los Prestadores de Servicios de Certificación cuyos certificados cumplan con los requisitos técnicos establecidos por el MAP y el MITC para su posible utilización en un procedimiento administrativo.

Como premisas normativas se debe destacar que la ley 59/2003 de firma electrónica no permite el establecimiento de restricciones previas en la prestación de servicios pero si define la capacidad de inspección y control por parte del Ministerio de Industria, Comercio y Turismo y la posibilidad de establecimiento de condiciones generales adicionales de forma conjunta entre el Ministerio de Administraciones Públicas y el Ministerio de Industria, Turismo y Comercio.

El manejo de certificados emitidos por diferentes prestadores por parte de los sistemas de los diferentes departamentos y organizaciones de la administración supone diferentes tipos de dificultades derivadas de una complejidad relacionada exponencialmente con el número de PSCs existentes en el mercado entre las que cabe destacar:

- Técnicas:
  - Verificación. Cada aplicación o Departamento debe tolerar todas las posibles excepciones sintácticas y semántica existentes a pesar de la utilización del estándar X.509v3 por parte de los PSCs
  - Conectividad. Cada aplicación o Departamento debe establecer, configurar, y mantener conectividad con los prestadores a través de redes privadas y/o públicas para la verificación on-line del certificado o la descarga de CRLs.
  - Gestión del conjunto de PSCs soportados. Cada aplicación o Departamento debe mantener su lista específica de PSCs soportados.
- Ordenación:
  - Requisitos a los PSCs. Cada Departamento establece los requisitos que debe observar cada PSCs para ser utilizado por sus aplicaciones. Estos requisitos en algunos casos podrían llegar a

diferir con los establecidos por otros Departamentos.

- Islas de Certificación. Las inconsistencias entre las listas de PSCs aceptados entre los diferentes pueden desconcertar a los usuarios en la utilización de certificados electrónicos.

La construcción de una plataforma intermedia, a través de labores de traducción, permite a las aplicaciones el acceso de forma homogénea a la información sintáctica y semántica contenida en los certificados El objetivo final de este módulo parte del proyecto es dotar a la Plataforma de una gestión sencilla, flexible y eficaz de Prestadores adheridos así como de los diferentes Certificados y servicios que estos proporcionen.

Validación de campos de certificados digitales.

Una de las características más importante de los servicios comunes que definimos con estas especificaciones es su capacidad para integrar cualesquiera certificados digitales X.509 ver. 3 de múltiples Prestadores de Servicios de Certificación (PSC) reconocidos: multiPSC. Se han de tener en cuenta las recomendaciones RFC 3280 del IETF para la definición de los certificados de ITU-T X.509 ver. 3 y de los perfiles de certificados listas de revocados de certificados (CRLs) X.509 ver.3.

Mediante este módulo, cualquier aplicación que requiera el acceso a certificados puede comprobar la validez de los certificados y el PSC emisor. Las diferencias entre los certificados emitidos por distintas organizaciones no son triviales, no sólo en la comprobación del estado de revocación, sino que además, los PSC adoptan diferentes criterios a la hora de codificar los campos y/o extensiones que componen los certificados emitidos.

Como es conocido, la posesión de un certificado digital, no garantiza que dicho certificado sea válido en todas sus acepciones. Se puede determinar la validez sintáctica, es decir, que la estructura del certificado en notación abstracta o XML es conforme los estándares. Sin embargo más importante es determinar su validez semántica y en el tiempo, es decir, que el contenido de un campo se corresponde con el tipo de certificado recogido en el almacén de certificados y que esté vigente o no haya sido revocado en el momento de su uso.

Firma electrónica y verificación de formularios y documentos.

Se propone la construcción de un conjunto de componentes y utilidades que ofrezcan una solución completa para la integración de la firma electrónica avanzada, tanto desde el punto de vista lógico como físico. La extensión del uso de la Firma-e hace necesaria la disponibilidad de utilidades y servicios que les garanticen legal y racionalmente la aplicación de esta.

A partir de lo establecido tanto en la Directiva Comunitaria 1999/93/CE para la construcción de Firma-e, como la Ley 59/2003 de Firma-e, se define el marco jurídico necesario para facilitar su aplicación tanto a nivel nacional como europeo.

Los servicios que se han definido en este ámbito han de cumplir con los requisitos de la Firma-e avanzada y reconocida, incluyendo la compatibilidad con la estrategia de introducción del eDNI a partir del uso de dispositivos seguros de creación de firma y emisión de certificados digitales reconocidos por Autoridades de Certificación acreditadas por el Ministerio del Interior. La Firma-e considerada se basa en los procedimientos de clave pública con certificados digitales del tipo X.509 ver. 3.

El objetivo de este módulo es el de establecer un conjunto de facilidades que minimice la barrera tecnológica y el coste del uso de la Firma-e en la aplicaciones.

La Firma-e avanzada permite resolver los siguientes problemas de autenticación de los usuarios, comprobar la integridad y, además, asegurar el no repudio de los documentos firmados. Para ofrecer estas garantías, este módulo se ha de complementar funcionalmente con el resto de módulos: validación de certificados, gestión del sincronismo y sellado de tiempos, cifrado/descifrado, control del no repudio, etc.
Finalmente, con la introducción de componentes cliente de Firma-e, verificación y cifrado/descifrado, se ofrece un conjunto de funcionalidades que permiten a aplicaciones cliente finales la firma de documentos y formularios web desde una página HTML y la verificación de los documentos firmados recibidos del servidor.

Desde el punto de vista técnico, se trata de un componente instalable en el entorno cliente y, consecuentemente, se han de tener en cuenta los aspectos que aseguren la compatibilidad con distintos navegadores y entornos cliente/servidor.

Las funcionalidades aportadas por los componentes son las siguientes:

- Firma de archivos y formularios
- Verificación de firmas, certificados digitales o justificantes de procesos de firma.
- Cifrado y descifrado de elementos
- Control de autenticación y autorización de usuarios en función de perfiles de acceso a aplicaciones y la política de firma elegida.
- Solicitud de sellado de tiempos y verificación de estos.

Módulo de cifrado y descifrado.

Se trata de un módulo de servicio a nivel de servidor, aunque en el componente de cliente se han de disponer de los mecanismos de cifrado que exige el proceso de firma electrónica. Este cifrado es considerado como el instrumento básico a partir del cual se confecciona un "sobre digital" a un destinatario concreto sobre un medio público como Internet.

Servicio de custodia y no repudio de Firma-e.

El servicio de custodia y no repudio tiene como misión garantizar la trazabilidad de las firmas y la utilización a modo de prueba de los registros operacionales de la plataforma.

Utilizando una gestión de workflow de validación se generará un completo registro de actividades de la plataforma, este registro incluirá toda aquella información asociada al momento en el que se realizó la operación y se incluirán elementos para garantizar la integridad, la autoría y el momento temporal.

De esta forma, en el caso de darse algún tipo de discrepancia o incertidumbre en la tramitación de un procedimiento, será posible el cotejo y verificación a través de este servicio.

Utilidades de administración y auditoría.

A fin de construir una plataforma integrada que facilite la gestión y mantenimiento así como la implantación y la reutilización a largo plazo es necesario que el sistema presente una consola de administración única y que esta integre todas las funcionalidades de gestión de la configuración, mantenimiento, estadísticas y auditoria, asociadas a la plataforma.

Integración con otros servicios

Un sistema de firma electrónica utilizado en el ejercicio de potestades no se basa únicamente en la utiliza-

ción de certificados y la verificación de estos en las operaciones, toda tramitación administrativa requiere una sólida gestión de tiempos en las operaciones al estar ligada a plazos de ejecución de actividades.

Así mismo, la firma electrónica provee de herramientas de autenticación que garantizan que el firmante es la persona que dice ser pero no incluye una gestión de autorización, ya que ésta depende del procedimiento o aplicación en el que se este autenticando el usuario.

Es necesario establecer la vinculación existente entre la plataforma de firma y los citados servicios, así como realizar los necesarios desarrollos de integración en este sentido.

Autoridad de sincronismo y sellado de tiempos.

El proyecto de TSA de la Intranet Administrativa se encuentra en la actualidad en una fase muy avanzada de implantación, que, sincronizada con el tiempo marcado por el Real Observatorio de la Armada, cumple con los estándares de sellado de tiempo: ETSI TS 102032: Policy requirements for time-stamping authorities, ETSI TS 101 861 y RFC 3161: Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP) que facilitan la integración.

El objetivo es que la plataforma incluya los servicios de la TSA entre las funciones accesibles de los módulos y librerías con el fin de facilitar a los desarrolladores la construcción de servicios telemáticos que utilicen ambas tecnologías.

De esta manera se posibilita la utilización de las herramientas de contabilidad, administración y auditoría de la plataforma para la monitorización de las peticiones de sellado de tiempo por lo que se obtiene una imagen integral sobre la utilización que los servicios de Administración Electrónica hacen de ambos servicios. Por otra parte, la TSA utilizará los servicios de firma electrónica de la plataforma en la firma y verificación de certificados asociados a su actividad.

AA y SSO: Autenticación, autorización e identificación única.

En la actualidad, se está desarrollando en el MAP un piloto de sistema de identificación única (Single Sign On) dentro del marco de CONECTA (proyecto ED-6 del metaproyecto eDNI).

La integración de la plataforma de firma electrónica con este proyecto permite, por un lado, la inclusión del sistema de autenticación y autorización de la plataforma en un sistema más amplio y generalista y por otro la inclusión de firma electrónica dentro de las posibilidades de identificación del sistema SSO.

Los objetivos de integración que se persiguen en el proyecto incluyen el desarrollo de aquellas funcionalidades que permita a los servicios de la plataforma acceder y ser accedidos por parte del sistema de SSO.