MINISTERIO
DE TRABAJO
Y ASUNTOS SOCIALES

SECRETARÍA DE ESTADO
DE LA SEGURIDAD SOCIAL

GERENCIA DE INFORMÁTICA

Centro de Calidad, Auditoría y

Comunicación TECNIMAP:
Plataforma de Servicios de Seguridad para la GISS

SG-5

C/ Dr. Tolosa Latour, s/n
28041 MADRID
TEL: 91 390 27 18
FAX: 91 390 51 67

Índice

1. INTRODUCCIÓN 3

2. ¿QUIÉNES SOMOS? 3

3. OBJETIVO 3

4. JUSTIFICACIÓN DE LA NECESIDAD 4

5. DESCRIPCIÓN DE LA SOLUCIÓN 6

5.1 ENCUADRE DE LA PLATAFORMA DE SERVICIOS DE SEGURIDAD 6

5.2 ARQUITECTURA DE LA PLATAFORMA DE SERVICIOS DE SEGURIDAD 7

5.2.1 Arquitectura Lógica 7

5.2.2 Arquitectura Física 9

6. CONCLUSIONES 12

C/ Dr. Tolosa Latour, s/n
28041 MADRID
TEL: 91 390 27 18
FAX: 91 390 51 67

1. Introducción

En el mes de Junio de 2007 se ha producido la aprobación de la **Ley 11/2007, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos (LAECSP)**. La Ley consagra la relación con las Administraciones Públicas por **medios electrónicos** como un **derecho de los ciudadanos** y como una **obligación** correlativa para tales **Administraciones**. En su Disposición Final Tercera se especifica como plazo en el que los ciudadanos pueden ejercer plenamente dichos derechos el **31 de Diciembre de 2009,** para el ámbito de la Administración General del Estado. También regulariza el uso de las tecnologías de la información para dar soporte a los procedimientos administrativos entre administraciones públicas y en las relaciones de éstas con los ciudadanos. Además, estamos presenciando la progresiva puesta en circulación del **DNI electrónico** en toda la geografía española.

Esto supone un gran reto para las Tecnologías de la Información y de las Comunicaciones de las Administraciones Públicas en general y de la Administración de la Seguridad Social en particular. La Seguridad Social da servicio a un gran número de empresas, trabajadores y pensionistas motivo por el que maneja unas bases de datos de gran tamaño (Afiliación, Recaudación y Prestaciones), con millones de transacciones diarias. Asimismo, existen más de 1200 oficinas repartidas por toda España (TGSS, INSS, ISM, IGSS, etc.). Esto implica una **gran dificultad y desafío para las Tecnologías de la Información** puesto que hay que adecuar el Sistema de la Seguridad Social para que ofrezca todos sus servicios de manera electrónica con las mismas garantías de nivel de servicio y de seguridad que viene prestando de manera presencial. Hemos de resaltar que actualmente ya se están ofreciendo servicios electrónicos de gran calidad a los ciudadanos y empresas como son el sistema RED (Remisión Electrónica de Documentos) y los servicios de la Oficina Virtual.

2. ¿Quiénes somos?

Dentro de los Servicios Comunes de la Administración de la Seguridad Social se haya la **Gerencia de Informática de la Seguridad Social (GISS)** que tiene entre sus objetivos proporcionar la infraestructura de tecnologías de la información y comunicaciones que sirva de soporte a la labor de servicio de la Seguridad Social a los ciudadanos y empresarios.

Entre los centros dependientes de la GISS se circunscribe el **Centro de Calidad, Auditoría y Seguridad (CCAS)** cuya misión es garantizar la **Seguridad** de las Tecnologías de la Información y de las Comunicaciones de la Seguridad Social así como de la Información gestionada por las distintas entidades de la Seguridad Social.

Ante el nuevo reto que supone la aprobación de la Ley de Acceso Electrónico y la puesta en circulación del DNI electrónico, el **Centro de Calidad, Auditoría y Seguridad (CCAS)** hace la propuesta de una **Plataforma de Servicios de Seguridad para la GISS**, que cubra las nuevas necesidades emergentes relacionadas con la Seguridad de la Información.

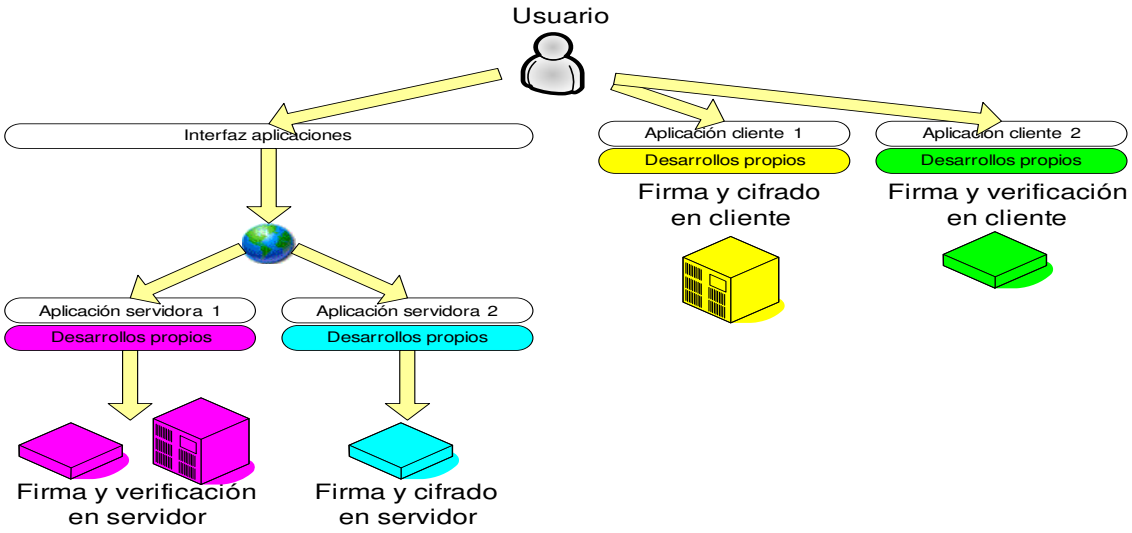
3. Objetivo

La GISS viene ofreciendo servicios electrónicos desde hace tiempo a ciudadanos y empresas. Entre ellos se encuentra el sistema RED (Remisión Electrónica de Documentos) y también los servicios ofrecidos a través de la Oficina Virtual, como por ejemplo la obtención de la Vida Laboral a través de Internet.

C/ Dr. Tolosa Latour, s/n
28041 MADRID
TEL: 91 390 27 18
FAX: 91 390 51 67

Estos servicios electrónicos están implementados por aplicaciones que hacen uso de distintos módulos de seguridad que proporcionan funcionalidades criptográficas, de firma electrónica, verificación de firma, etc. La implementación de estas funcionalidades se ha ido desarrollando a lo largo del tiempo con diversas herramientas. No existe por el momento ningún mecanismo que estandarice los procedimientos para incluir estas funcionalidades en las nuevas aplicaciones que puedan desarrollarse.

De manera esquemática el siguiente dibujo representa la situación actual



Se desea conseguir una situación más uniforme donde existan mecanismos y procedimientos claros para integrar la funcionalidad criptográfica, de firma y verificación de firma en las aplicaciones.

El **objetivo** de la Plataforma de Servicios de Seguridad que propone el Centro de Calidad, Auditoría y Seguridad es el de crear una **plataforma horizontal de servicios** que ofrezca las **funcionalidades de firma, verificación, cifrado, descifrado, sellado de tiempo y validación de certificados a todas las aplicaciones de la Seguridad Social**. Esta plataforma permitirá integrar estas funcionalidades tanto en las aplicaciones existentes como las nuevas que puedan ir apareciendo bajo un único mecanismo y una interfaz común ajustándose a los principales estándares definidos al respecto.

4. Justificación de la necesidad

La Plataforma de Servicios de Seguridad es necesaria para la GISS con el objetivo de que se pueda dar cumplimiento a los requisitos legales, de seguridad y de interoperabilidad siguientes:

- Requisitos legales:

La aprobación de la Ley de Acceso Electrónico establece unos derechos a los ciudadanos que, desde el punto de vista administrativo, se convierten en obligación para la Administración de la Seguridad Social. Entre ellos se hayan el derecho a relacionarse con las Administraciones Públicas por medios electrónicos, a conocer el estado de tramitación de los procedimientos en los que estén implicados, a obtener los medios de identificación electrónica necesarios, a la calidad de los servicios públicos por medios electrónicos, a la garantía de la seguridad y confidencialidad de los datos que figuren en ficheros, sistemas y aplicaciones, a la conservación de los documentos electrónicos que formen parte de un expediente, etc. Es decir, la administración electrónica de la Seguridad Social ha de cumplir las mismas garantías que la Administración presencial y por tanto se hace imprescindible la búsqueda de analogías entre el mundo presencial y el virtual. En particular:

- Firma manuscrita → firma electrónica

C/ Dr. Tolosa Latour, s/n
28041 MADRID
TEL: 91 390 27 18
FAX: 91 390 51 67

- Sello de la oficina → firma electrónica con sellado de tiempo
- Sellado de fecha → sellado de tiempo electrónico
- Almacén de documentos → sistema de custodia de documentos

El objetivo de la GISS es que dichas analogías para la administración electrónica puedan satisfacerse a través de la Plataforma de Servicios de Seguridad, de modo que la Administración de la Seguridad Social logre dar la adecuada respuesta a sus obligaciones con los ciudadanos.

- Requisitos de Seguridad:

Existen diversos riesgos para la Seguridad de los Sistemas de Información de la Seguridad Social: intercepción de comunicaciones, ataques de denegación de servicio, suplantación de identidad, corrupción de datos, manipulación no autorizada de información, no repudio, etc.

Para mantener el sistema seguro es preciso garantizar la **autenticación, el control de accesos, la confidencialidad, la integridad, el no repudio y la disponibilidad.**

- Requisitos de Interoperabilidad:

Es fundamental proporcionar una **plataforma horizontal** que ofrezca **servicios de seguridad a todas las aplicaciones presentes y futuras de la Seguridad Social** ya que no es recomendable que cada aplicación desarrolle los mecanismos de seguridad por su cuenta. Además, es de prever un aumento considerable del número de aplicaciones a desarrollar que ofrezcan servicios electrónicos a los ciudadanos y un aumento ingente de la información intercambiada por estos medios..

Por otra parte, dada la complejidad y variedad de los entornos que se encuentran en los Sistemas de Información de la Seguridad Social y para garantizar la escalabilidad de la Plataforma de Servicios de Seguridad en el futuro, es esencial ajustarse a **estándares abiertos**:

- **X.509**
- **Multi-CA, Multi-Certificado*, Multi-PKI**
- **OCSP**
- Formatos de firma electrónica: **PKCS#7, XMLDSig, XAdEs, CADES**
- **Web Services** (**SOAP, WSDL, UDDI, HTTP**)

* Ha de aceptar todos los certificados reconocidos y estar preparado para la puesta en circulación progresiva del DNI electrónico para que los ciudadanos puedan identificarse electrónicamente.

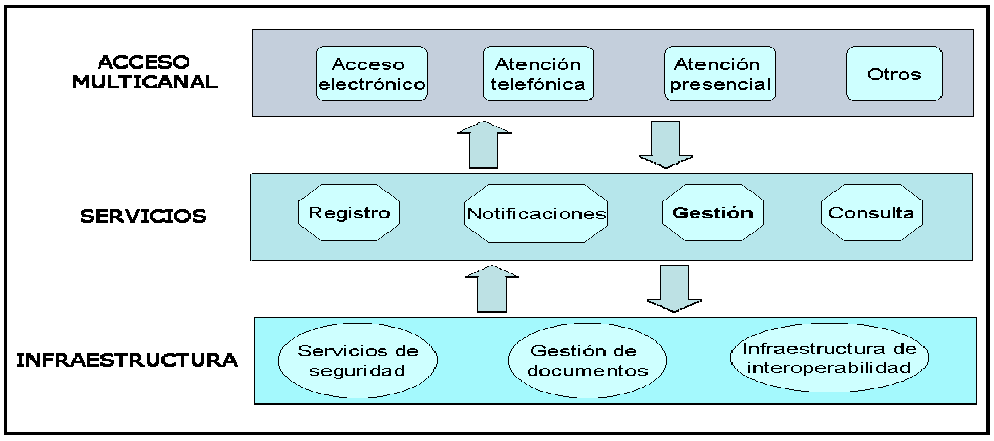
C/ Dr. Tolosa Latour, s/n
28041 MADRID
TEL: 91 390 27 18
FAX: 91 390 51 67

5. Descripción de la solución

5.1 Encuadre de la Plataforma de Servicios de Seguridad

Como ya se ha comentado, para el cumplimiento de los requisitos de la Ley de Acceso Electrónico, es necesario realizar una adecuación de los sistemas de información de la Seguridad Social. Los aspectos más importantes abarcados por dicha ley se traducen en los siguientes requisitos: adaptar los servicios de seguridad para garantizar la generación y verificación de firmas electrónicas con cualquier certificado electrónico reconocido , implementar una aplicación de registro electrónico, implementar una aplicación de custodia de documentos, hacer las adecuaciones necesarias que permitan al ciudadano conocer el estado de cualquier trámite administrativo, soporte multicanal, registro electrónico accesible 24x7, etc.

Se incluyen aspectos que afectan tanto a decisiones estratégicas de tipo gerencial como de tipo tecnológico. El siguiente gráfico muestra un análisis por capas de los componentes tecnológicos necesarios:



A – INFRAESTRUCTURA.

Este constituye el estrato de más bajo nivel sobre el que se asientan los servicios a los ciudadanos, funcionarios y procesos de otras administraciones.

A1. Servicios de seguridad.

Se deben adaptar y construir los servicios de seguridad para dar soporte a las aplicaciones necesarias para dar cumplimiento a la LAECSP. Básicamente, estos servicios serían tres: plataforma para la firma y validación de la firma electrónica, validación de los distintos tipos de certificados y servicio para el sellado de tiempo.

A2. Gestión de documentos electrónicos.

Los procesos administrativos que propone la ley se soportan con aplicaciones de gestión de documentos electrónicos, es más, incluso introduce el concepto de expediente electrónico donde se agrupan todos los documentos que forman parte de un procedimiento.

Para llevar a cabo esta tarea serían necesarios varios componentes, entre ellos un servicio de custodia de los documentos.

La **Plataforma de Servicios de Seguridad** se enmarca dentro estos dos apartados A1 y parte del A2.

B – SERVICIOS.

Esta capa contiene los servicios a los que podrían acceder los interesados y se apoya en los componentes de infraestructura descritos en el punto anterior.

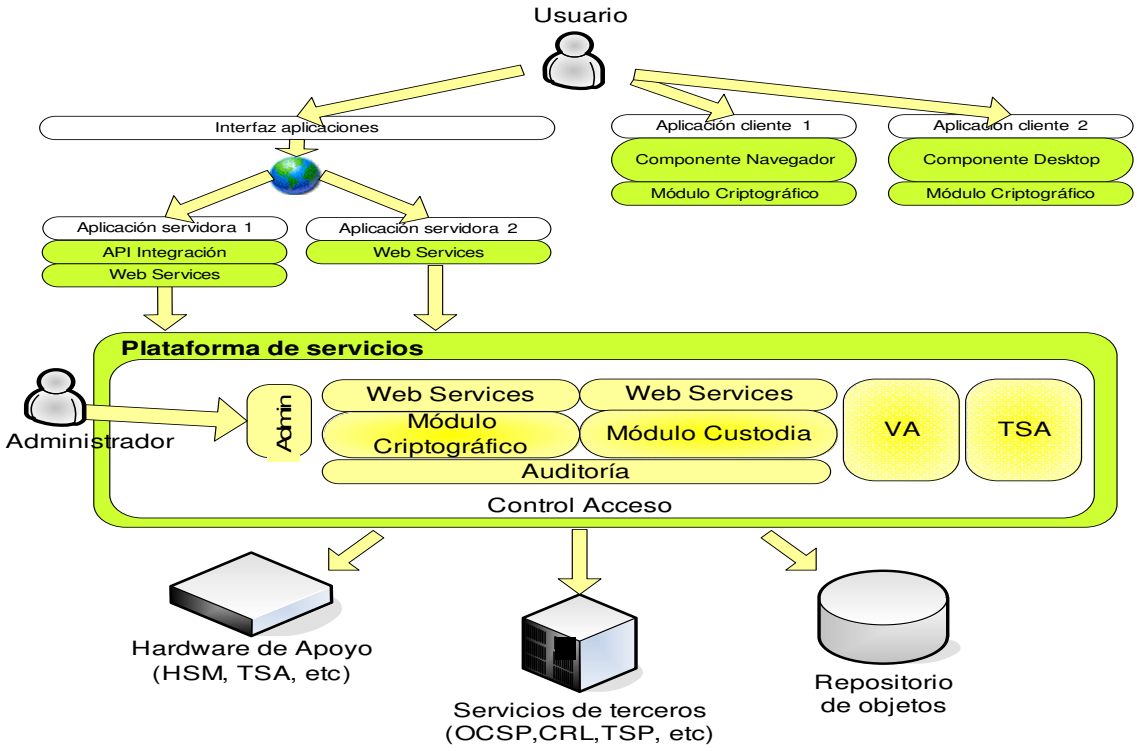
C/ Dr. Tolosa Latour, s/n
28041 MADRID
TEL: 91 390 27 18
FAX: 91 390 51 67

C – ACCESO MULTICANAL.

La ley recoge la necesidad de acceso multicanal a los servicios descritos en el apartado anterior y establece un número mínimo de tipos de acceso, en concreto: presencial, telefónico y puntos de acceso electrónico.

5.2 Arquitectura de la Plataforma de Servicios de Seguridad

El siguiente gráfico muestra la situación objetivo que se desea alcanzar:



Como podemos observar, el conjunto de Aplicaciones de la Seguridad Social se conectan a la Plataforma horizontal de Servicios de Seguridad para hacer uso de las funcionalidades de firma, cifrado, validación de certificados, sellado de tiempo y custodia de documentos..

A lo largo de este apartado se describe **lógica, física y funcionalmente** la **plataforma de servicios de seguridad**. Totalmente orientada a servicios, la plataforma que se expone está basada en estándares y protocolos abiertos y ofrece servicios y/o funcionalidad alrededor del mundo de la firma digital.

5.2.1 Arquitectura Lógica

El siguiente esquema muestra la arquitectura lógica de la plataforma de servicios.

C/ Dr. Tolosa Latour, s/n
28041 MADRID
TEL: 91 390 27 18
FAX: 91 390 51 67

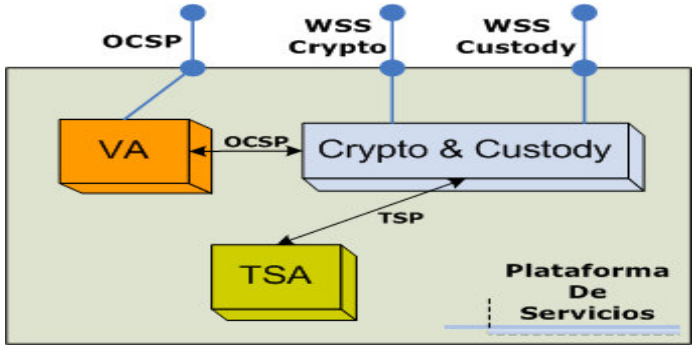


Ilustración 1. Arquitectura Lógica de la Plataforma de Servicios

Como se puede apreciar se distinguen, desde el punto de vista lógico, tres componentes principales:

- **Plataforma de firma y custodia de documentos (Crypto & Custody).** Se trata de un componente que ofrece servicios de firma y validación de documentos, además de la custodia electrónica de los mismos todo ello basado en los principales estándares de firma electrónica, tanto para la firma y verificación, como para la custodia o archivado posterior de los documentos. Para ofrecer algunos de los servicios que proporciona esta infraestructura se apoya en los dos servicios anteriores, el servicio VA para la validación de certificados y el servicio TSA para la generación de sellados de tiempo tanto en el proceso de custodia como en la verificación de firmas cuando así se requiere. Los servicios de esta plataforma tienen una interfaz basada en WSS (Web Services Security, estándar de OASIS).

- **TSA (Time-Stamp Authority),** es la **Autoridad de Sellado de Tiempo**. En esencia es un servicio que ofrece pruebas irrefutables de que un dato existía en un determinado momento. Dentro de la definición de la plataforma de servicios es una tercera parte confiable que los demás servicios usan para establecer evidencia electrónica de que un dato existía en un momento dado. Esta característica puede ser utilizada, por ejemplo, para verificar que la firma digital de un documento fue llevada a cabo antes de que el certificado del firmante fuera revocado o para determinar cuando un documento firmado electrónicamente fue enviado a un servicio con las implicaciones de plazos de entrega que pudiera haber en dicho proceso. Una característica muy importante en este servicio es disponer de una fuente confiable de tiempo. La interfaz de este servicio está basada en el protocolo estándar TSP (Time-Stamp Protocol, RFC 3161).

- **VA (Validation Authority),** es la **Autoridad de Validación**. Como parte de una infraestructura de clave pública (al igual que la TSA) y dentro de los servicios de la plataforma, la VA es el servicio que ofrece las funciones de validación de certificados de tal forma que también actúa como una tercera parte confiable en la que el sistema delega la obtención del estado de revocación de todos los certificados implicados en los procesos de firma de las aplicaciones del sistema. Su uso puede estar indicado, por ejemplo, para comprobar el estado de revocación de un certificado que se ha utilizado para el establecimiento de una conexión segura basada en certificados a un servidor web o para comprobar durante el proceso de verificación de un documento firmado que el certificado del firmante no está revocado. La interfaz de este servicio está basada en el protocolo estándar OCSP (Online Certificate Status Protocol, RFC 2560).

Los tres componentes lógicos y sus interfaces conforman la interfaz de los servicios de la plataforma. Por un lado está la interfaz *OCSP* que proporciona el servicio de la VA, y por otro esta la interfaz WSS que

C/ Dr. Tolosa Latour, s/n
28041 MADRID
TEL: 91 390 27 18
FAX: 91 390 51 67

proporcionan los servicios de la plataforma de firma y custodia, existiendo una por cada tipo de servicio, *Crypto* y *Custody*.

5.2.2 Arquitectura Física

Todos los componentes lógicos identificados con anterioridad, a nivel físico y desde un punto de vista funcional, cumplen requisitos de alta disponibilidad y rendimiento, además de los estándares de las interfaces que publican.

5.2.2.1 VA

La siguiente ilustración muestra como está previsto el despliegue de la infraestructura de la Autoridad de Validación.

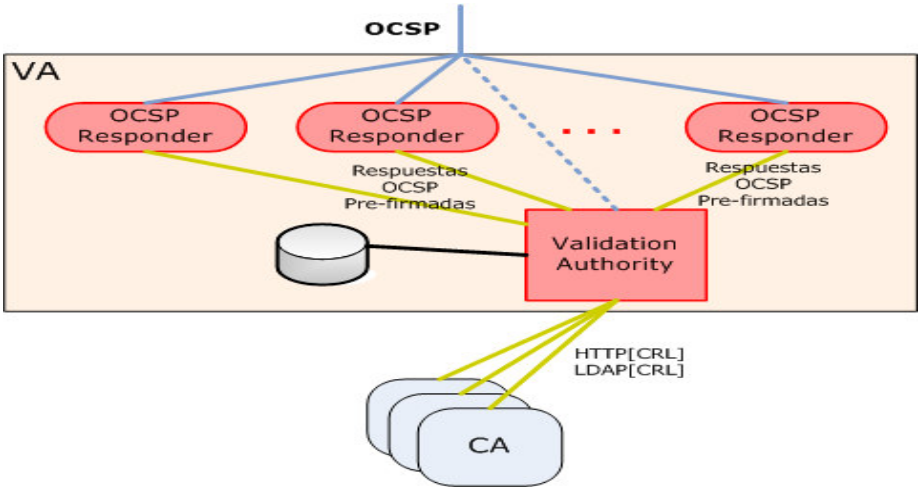


Ilustración 2. Arquitectura VA CoreStreet

Se observan dos niveles diferenciados:

- Validation Authority. Es la Autoridad de validación propiamente dicha. Sus principales funciones son la descarga, vía LDAP o vía HTTP, de CRLs de las autoridades de certificación configuradas como confiables por la plataforma de servicios y la emisión de respuestas OCSP pre-firmadas a los servicios del segundo nivel, *OCSP Responders*. Lo que hace realmente la VA es descargar toda la información de CRLs de forma programada y actualizar su base de datos, para después, también de forma programada, comenzar a publicar respuestas OCSP pre-firmadas que recogen los OCSP Responders.

- OCSP Responders. Son servicios de consulta a peticiones OCSP. Basan su funcionalidad en las respuestas pre-firmadas que ha generado con anterioridad la VA. El sistema se puede dimensionar con tantos de estos servicios como sea necesario, de tal forma que se garantice de cara a los sistemas clientes la disponibilidad de un servicio OCSP para validación de certificados.

C/ Dr. Tolosa Latour, s/n
28041 MADRID
TEL: 91 390 27 18
FAX: 91 390 51 67

Esta arquitectura facilita de por sí el despliegue en entornos distribuidos y con requerimientos de alta disponibilidad y rendimiento, siendo posible, desde un punto de vista funcional, el despliegue de la VA también en alta disponibilidad si así se requiere.

5.2.2.2 TSA

El servicio TSA es un servicio sencillo que recibe peticiones HTTP con TSP embebido. La siguiente ilustración muestra el despliegue de este servicio.

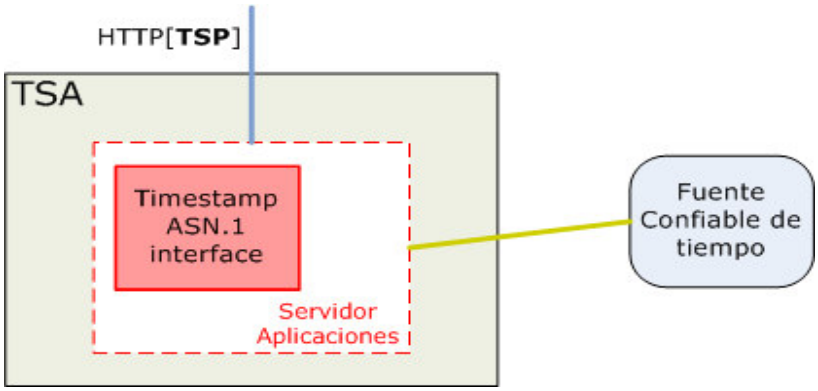


Ilustración 3. Arquitectura Timestamp service

Como requisito para este servicio hay que destacar la necesidad de disponer de una fuente confiable de tiempo.

5.2.2.3 Crypto & Custody

La siguiente ilustración muestra a alto nivel la arquitectura de componentes necesaria para proporcionar la funcionalidad de estos dos servicios.

Ilustración 4. Arquitectura Lógica de los servicios de crypto y custody

C/ Dr. Tolosa Latour, s/n
28041 MADRID
TEL: 91 390 27 18
FAX: 91 390 51 67

Dentro de la arquitectura del producto, el **Módulo Custody** (al igual que el módulo Crypto) presenta una interfaz basada en WSS de OASIS con la posibilidad de utilizar un API de integración basado en J2EE en aquellos casos en los que no se desee ir directamente contra los servicios facilitando así la integración de aplicaciones con los servicios sin necesidad de conocer los entresijos de WSS. Las operaciones disponibles en los servicios y también accesibles desde el API de Integración son las siguientes:

- **Custodia de documentos**. Se llama Custodia de documentos al servicio de la plataforma que permite **preservar cualquier documentación u objeto en una estructura de información (XML) propia del módulo de custodia** y que adicionalmente facilita, en el caso de documentos firmados, **incorporar a esa estructura de información todos los datos relativos a la verificación del documento**, de tal manera que el proceso de archivado se lleva a cabo sobre la estructura de información del módulo. Con este servicio es posible realizar las siguientes operaciones, garantizando en todos los casos la integridad del documento entregado para custodia y la longevidad de las firmas:
  - **Custodia de documentos sin conocer su formato**, tratándolos simplemente como objetos.
  - **Custodia de documentos firmados**, pero cuyo tipo de **firma no tiene un estándar de archivado** de firmas asociado o implementado en la plataforma, por ejemplo PDF.
  - **Custodia de documentos firmados** cuyo tipo de **firma tiene un estándar de archivado** de firmas, pero se desea custodiar el documento siguiendo un estándar específico de archivado.
- **Custodia de firmas**. Se llama Custodia de firmas al servicio de la plataforma que permite custodiar documentos previamente firmados pasando sus firmas al estado de archivado definido por el estándar correspondiente. Actualmente la plataforma soporta la custodia de firmas para documentos XML firmados, llevándose a cabo su archivado según el estándar XAdES, formato XAdES-A.
- **Almacenamiento simple**. El sistema también permite su uso para almacenaje de información sin la aplicación de resellados. Esto permite insertar documentos en el sistema, protegidos por la custodia física (si se dispone de ella) y por el control de acceso proporcionado. Los documentos almacenados de esta forma no son tratados por los procesos de resellado del sistema.
- **Recuperación de documento original**. Esta operación permite devolver el documento u objeto original que se entregó para custodia al sistema.
- **Recuperación de última versión de documento custodiado**. Esta operación permite recobrar el documento u objeto entregado para custodia, pero embebido en el documento de custodia que se guarda en los repositorios de la plataforma.

Todo **documento** entregado a los servicios de **custodia** tiene asociado un **identificador único** en el sistema. Éste identificador se retorna tanto en las llamadas en el API de Integración como en los acuses de recibo que puede generar el servicio de custodia cuando se le entrega un documento.

Además de las operaciones descritas, el módulo Custody presenta las siguientes características:

- **Custodia de políticas junto a los documentos**. Se garantiza la persistencia en el tiempo, no sólo de los documentos firmados, sino también de sus políticas.
- **Resellado automático de documentos firmados**. Se proporciona al documento validez a lo largo del tiempo en base a los resellados programados desde la Administración.
- **Soporte a múltiples repositorios** de forma simultánea. Selección dinámica de los repositorios en base a reglas definidas en la administración de la plataforma.
- **Recuperación de documentos**. Devolución de documentos custodiados en base a un identificador único. Posibilidad de recuperación del documento en su formato original o en su formato de custodia.

C/ Dr. Tolosa Latour, s/n
28041 MADRID
TEL: 91 390 27 18
FAX: 91 390 51 67

- Posibilidad de definir las **políticas de Retención, Acceso y Resellado** de documentos de forma flexible a través de la administración centralizada. Desde la misma también se gestiona el histórico de políticas generado.
- Definición de tipos o categorías de documentos. La definición de un tipo o categoría de un documento implica agrupar bajo una categoría las políticas que van a aplicarse para su custodia, incluido el repositorio donde se llevará a cabo la custodia.
- Revisión automática de configuración. Se detectan caducidades o anomalías en los certificados y se notifica en forma de alertas que podrán ser consultadas en el módulo de Auditoría.

6. Conclusiones

La Plataforma de Servicios de Seguridad es determinante para que la Seguridad Social cumpla el reto que supone la puesta en práctica de la Ley de Acceso Electrónico satisfaciendo los derechos de los ciudadanos en fecha requerida (31 de enero de 2009) así como para el uso masivo del DNI electrónico.

Esto facilitará un mayor acercamiento de los ciudadanos y empresas a la Seguridad Social, ofreciendo una mejora sustancial del servicio que las Administraciones Públicas prestan al ciudadano.

Las ventajas de la Plataforma de Servicios de Seguridad son:

- Garantizar el mismo **nivel de seguridad** en la Administración Electrónica de la Administración de la Seguridad Social que en la Administración Presencial.
- Alta **eficiencia** para grandes volúmenes de petición, haciendo frente a la futura demanda de acceso electrónico de los ciudadanos.
- Soporte a los procedimientos administrativos entre administraciones públicas y en las relaciones de éstas con los ciudadanos.
- **Alta disponibilidad**.
- Abierto a todo tipo de certificados reconocidos, incluyendo el DNI electrónico.
- **Altamente escalable** gracias al uso de estándares abiertos.
- **Custodia de todo tipo de documentos**.

C/ Dr. Tolosa Latour, s/n
28041 MADRID
TEL: 91 390 27 18
FAX: 91 390 51 67