CARPETA CIUDADANA

App Factory

Guía de integración con el Centro de mensajes.

Modalidad I: Servidor

AUTOR	App Factory SGAD
ÁREA	App Factory - SGIDA
PROYECTO	Carpeta Ciudadana - Centro de mensajes
LUGAR DE REALIZACIÓN	App Factory SGAD
NOMBRE DEL DOCUMENTO	Guía de integración con el Centro de mensajes de Carpeta Ciudadana. Modalidad I: Servidor

Control de Versiones del Documento

VERSIÓN	AUTOR	FECHA	DESCRIPCIÓN
1.0	App Factory SGAD	28-10-2024	Versión inicial
1.1	App Factory SGAD	16-01-2025	Cambio del formato de fechas de UNIX-Timestamp a ISO-8601.
1.2	App Factory SGAD	30-01-2025	Correcciones de formato. Se ha añadido: • Ejemplo de generación de objetos JWS en pseudo-código. • Política de renovación de certificados. • Aclaración sobre el uso del remitente. • Objeto AVISO_ENV de la consulta de estado de un aviso. Corregidos los campos incluidos en el servicio de envío de mensaje para incorporar los campos de remitente (*nombreOrganismo* y *dir3Organismo*).

Índice

RELACIÓN DE GRÁFICOS

RELACIÓN DE TABLAS

1 INTRODUCCIÓN

Dentro de su estrategia general y con el objetivo de mejorar la interacción y comunicación entre los ciudadanos y la Administración Pública, se ha desarrollado el Centro de Mensajes en Carpeta Ciudadana. Esta funcionalidad busca, a través de un nuevo mecanismo de comunicación más directo y simplificado, el envío de mensajes personales y avisos push a los ciudadanos desde cualquier Organismo público.

El Centro de mensajes de Carpeta Ciudadana permite a los ciudadanos recibir mensajes sobre el estado de sus trámites con diferentes Organismos públicos, en un único espacio. Estos avisos informan sobre temas que puedan resultar de interés, y no se trata en ningún caso de notificaciones oficiales de las Administraciones, que se comunicarán a través de las vías habituales.

Este servicio tiene el objetivo de enviar avisos personales a ciudadanos concretos y no avisos masivos sobre noticias de interés.

Este servicio ofrece importantes ventajas tanto para los Organismos públicos como para los ciudadanos. Para los ciudadanos, el Sistema de Avisos facilita la gestión de sus trámites al concentrar los mensajes en un solo lugar. Esto les permite realizar un seguimiento en tiempo real de los cambios en sus expedientes, sin tener que consultar múltiples plataformas o realizar llamadas, ahorrando tiempo y esfuerzo. La posibilidad de personalizar los avisos según los Organismos de interés contribuye a una experiencia más adaptada a las necesidades de cada ciudadano. Además, la constante actualización de la información permite a los ciudadanos actuar con rapidez cuando se requiere su intervención, lo que mejora la eficiencia y reduce la incertidumbre asociada a la espera de respuestas.

Para los Organismos públicos, el Centro de mensajes amplia la capacidad de comunicación con los ciudadanos a través de un canal más cercano, intuitivo y adaptado a la movilidad, ampliando el espectro de personas informadas, por ejemplo, en el envío de actualizaciones sobre los expedientes. Esto reduce la carga administrativa al automatizar los mensajes y permite liberar recursos para tareas de mayor prioridad. También se reducen los costes operativos, ya que se minimiza el uso otros métodos tradicionales por los ciudadanos (teléfono, asistencia presencial o correos electrónicos) y se puede automatizar el envío de avisos. Al proporcionar información clara y puntual, el sistema favorece una relación más transparente y positiva con los ciudadanos, lo que contribuye a una mayor satisfacción con los servicios públicos y mejora la percepción de la Administración.

En conjunto, el Centro de mensajes de Carpeta Ciudadana contribuye a una gestión más eficiente tanto para los ciudadanos como para las Administraciones, facilitando el acceso a la información y promoviendo una comunicación más ágil y directa.

Este documento describe las especificaciones de la API para el envío de avisos personales a los ciudadanos que lo hayan autorizado, así como los Servicios Web que se han desarrollado desde el equipo de Carpeta Ciudadana.

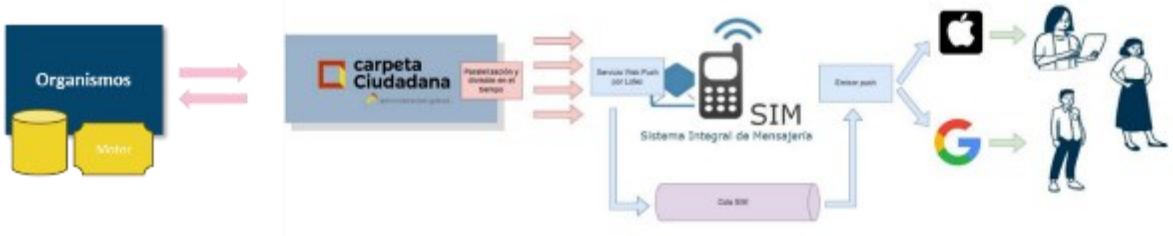


Figura 1.- Diagrama general del funcionamiento

2 REQUISITOS PARA LA INTEGRACIÓN DE ORGANISMOS

2.1 Cumplimentación y firma del documento de integración.

Para formalizar la integración de un servicio dependiente de un Organismo con el centro de mensajes será necesario cumplimentar y firmar un formulario que recoge la información necesaria para gestionar la integración. Entre otros datos se deberá proveer de la parte pública del certificado con el que se va a establecer la confianza back-to-back, y otros datos administrativos. Se hará llegar el formulario PDF a rellenar a los Organismo interesados en la integración, o se publicará cuando se disponga de él junto con el resto de documentación técnica de integración.

A continuación, se indican las consideraciones más relevantes respecto a la modalidad y la identificación del servicio del Organismo.

Modalidad

El centro de mensajes es compatible con dos modos de integración, la modalidad dual como cliente y servidor y la modalidad de cliente puro:

- Modalidad I: Cliente-Servidor.

  En esta modalidad, cubierta en este documento, el Organismo debe consumir servicios desplegados en el CM-CC (Centro de Mensajes de Carpeta Ciudadana) actuando como cliente y desplegar en su infraestructura una API (actuando como servidor) para que CM-CC comunique de forma proactiva cada cambio solicitado por los ciudadanos. Esta modalidad es más compleja y está pensada únicamente para Organismos con un número muy elevado de usuarios o que, por sus reglas de negocio, requieran la actualización inmediata de los usuarios que se den de alta o baja del servicio.
- Modalidad II: Cliente

  La modalidad II, cubierta en otro documento, sólo requiere que el Organismo desarrolle en su infraestructura el cliente que consuma la API expuesta por CM-CC, tanto para consultas de cambios solicitados por los ciudadanos como para el envío de

avisos. Esta modalidad de integración ligera está pensada para la mayoría Organismos ya que es mucho más sencilla a costa de tener que gestionar la sincronización de las tablas de usuario de forma periódica.

En el formulario será necesario indicar claramente la modalidad elegida.

Identificación del Organismo y servicio

El Organismo debe cumplimentar todos los campos de identificación del propio Organismo y de los servicios que se deseen integrar con el sistema de avisos del CM-CC.

Se debe tener en cuenta que los campos relativos a las interfaces del servicio en Carpeta Ciudadana se corresponden con las etiquetas y campos de texto que se emplearán en las aplicaciones web y móvil de Carpeta ciudadana para identificar el servicio del Organismo.

En la figura siguiente se ilustra a modo de ejemplo cómo se muestran los campos correspondientes al nombre y descripción del servicio para el servicio de la Dirección Electrónica Habilitada única o DEHú.

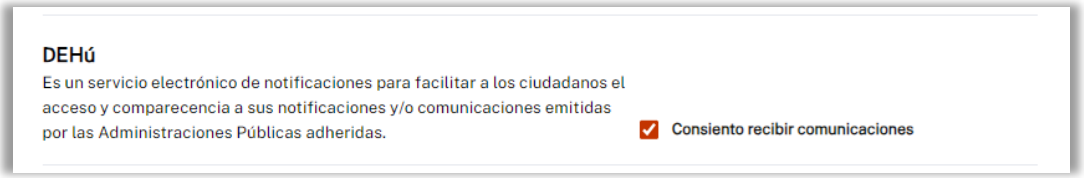


Figura 2.- Ejemplo de gestión de consentimientos para DEHú en Carpeta Ciudadana.

2.2 Provisión y gestión de certificados

El Organismo debe aprovisionar un certificado digital que quedará vinculado en el CM-CC al servicio correspondiente del Organismo. Durante la configuración de la integración, el Organismo deberá facilitar la parte pública y el número de serie del certificado, utilizando los medios acordados entre ambas partes.

Cuando el certificado esté próximo a caducar, el Organismo y el CM-CC establecerán de manera conjunta los plazos y el protocolo para su renovación. La renovación implicará registrar un nuevo certificado, que coexistirá con el original en el CM-CC antes de que se efectúe el cambio en el servicio del Organismo.

Será responsabilidad exclusiva del Organismo vigilar los plazos de caducidad de sus certificados y notificar al equipo de CM-CC para iniciar el proceso de renovación.

2.3 Responsabilidades del Organismo

El desarrollo, mantenimiento y gestión de las infraestructuras y aplicaciones propias necesarias para la integración con el Centro de Mensajes de Carpeta Ciudadana (CM-CC) será responsabilidad exclusiva del Organismo. Esto incluye la implementación de los servicios, la

seguridad de las comunicaciones, la gestión de certificados y cualquier otro aspecto técnico vinculado a la integración.

Aunque el equipo del CM-CC podrá proporcionar asesoramiento y orientación durante el proceso de integración, esta asistencia no exime al Organismo de su plena responsabilidad sobre el correcto funcionamiento y la gestión de su infraestructura.

3 INTERACCIONES ENTRE SISTEMAS:

A continuación, se detallan los flujos de comunicación entre los sistemas de los distintos Organismos y el Centro de Mensajes de Carpeta Ciudadana.

Para gestionar todas las comunicaciones entre un Organismo integrado en el sistema de mensajería y el Centro de Mensajes, Carpeta ciudadana expone una API REST con dos, y se requiere que el Organismo desarrolle otra API REST con tres servicios indicados.

Figura 3.- API Rest del Centro de mensajes

La gestión de consentimientos se realiza en tres servicios. Que permiten el alta, la actualización y la consulta.

- Alta consentimiento usuario: Este servicio permite a un usuario autorizar a recibir avisos personales por parte de un Organismo.
- Verificación datos usuario: Permite a carpeta ciudadana consultar el estado del consentimiento de un ciudadano concreto. Se plantea su uso solo con fines de auditoría y no como parte del flujo estándar.
- Actualización estado consentimiento: Este servicio permite la actualización de las autorizaciones por parte de los ciudadanos.

Los mensajes se gestionan mediante dos servicios, uno para el envío de un mensaje y otro para la consulta del estado de un mensaje.

- Envío de mensajes: Este servicio verifica el consentimiento del usuario y los dispositivos habilitados antes de almacenar el mensaje en la bandeja de avisos y solicitar a SIM el envío de avisos push. Devuelve un identificador único para consultas posteriores.
- Consulta de estado de mensaje: Permite consultar el estado de un mensaje previamente enviado, utilizando el identificador único devuelto por el servicio de envío.

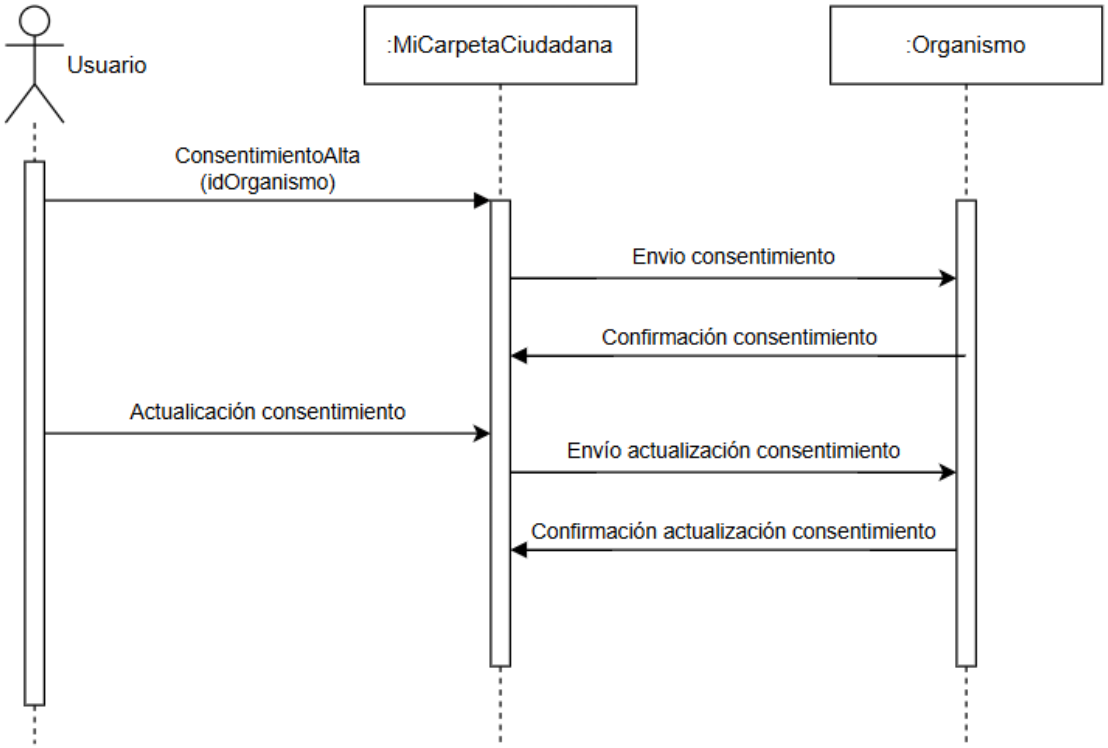


Figura 4.- Secuencia de alta y actualización de consentimientos para avisos de un Organismo.

La figura 4 muestra el diagrama de secuencia correspondiente a los procesos completos de solicitud de alta y actualización (baja) del usuario para recibir mensajes y avisos desde el Organismo, incluyendo la consulta desde el Organismo de las modificaciones de altas y bajas.

El diagrama de secuencia de la figura 5 representa las interacciones entre sistemas en el envío de mensajes y la consulta del estado de un mensaje, incluyendo las interacciones entre el Centro de mensajes y la plataforma de mensajería SIM para el envío de avisos PUSH.

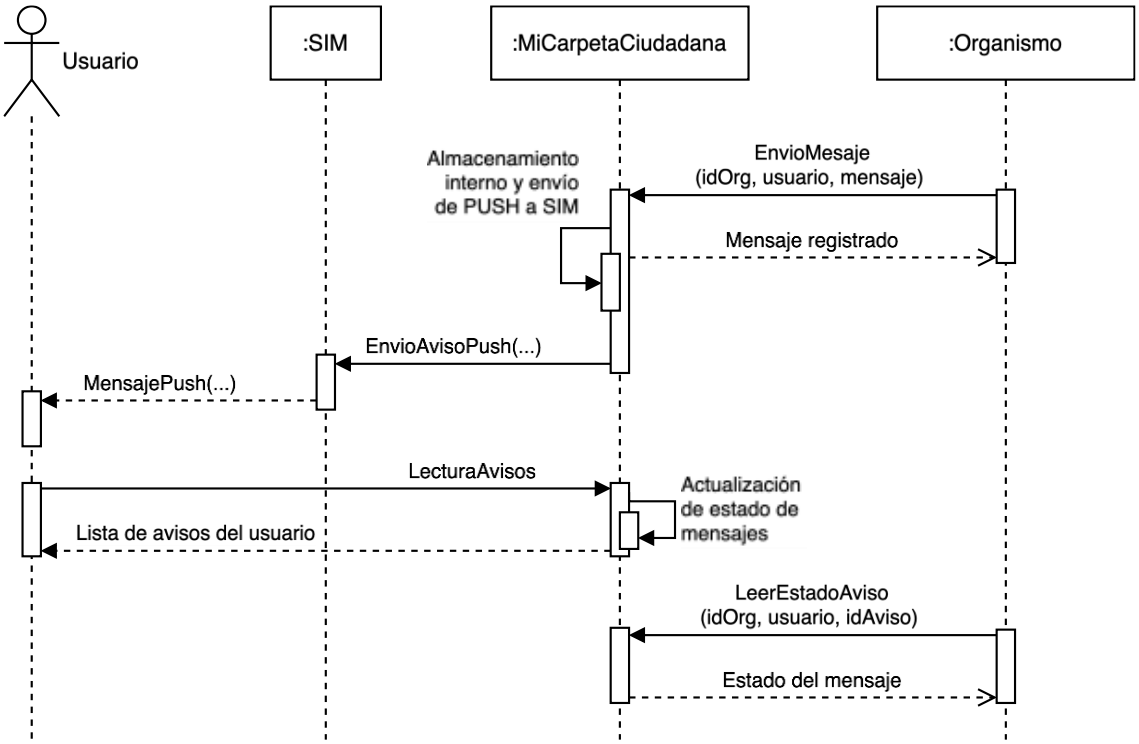


Figura 5.- Secuencia de envío y consulta de avisos.

4 ARQUITECTURA GENERAL DEL SISTEMA

Desde una perspectiva de alto nivel, la arquitectura del Centro de Mensajes sigue un modelo basado en la interoperabilidad de sistemas. Los Organismos son responsables de configurar sus sistemas internos y desarrollar las soluciones necesarias para conectarse con la API del Centro de Mensajes. Una vez integrados, los Organismos pueden enviar avisos que son procesados por el Centro y distribuidos a los ciudadanos suscritos a través de la Carpeta Ciudadana.

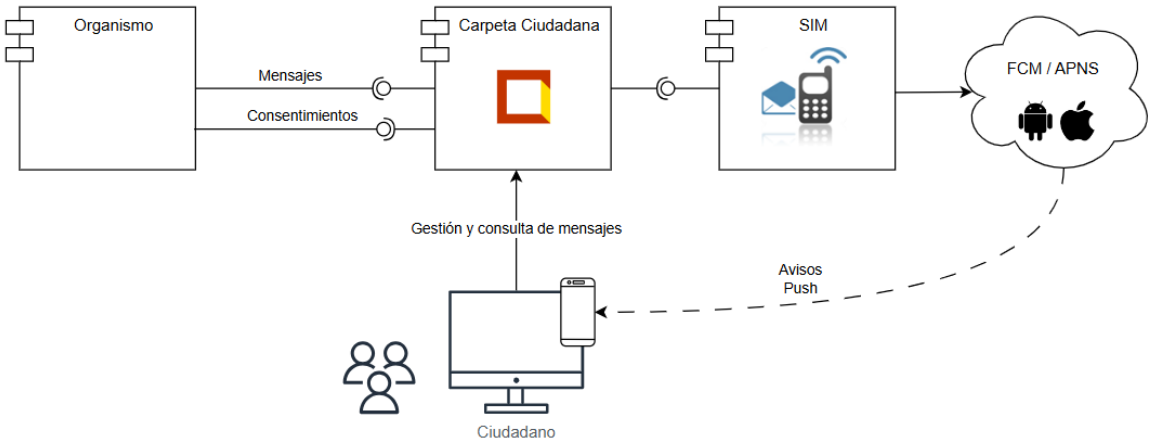


Figura 6.- Diagrama general del sistema

El Centro de Mensajes de Carpeta Ciudadana es una plataforma centralizada que permite a los ciudadanos recibir avisos y mensajes de Organismos públicos.

Los ciudadanos gestionan sus suscripciones desde Carpeta Ciudadana, seleccionando qué Organismos pueden enviarles mensajes.

La integración de los Organismos se realiza mediante dos API que permiten la consulta y actualización de los datos de los ciudadanos, así como el envío de avisos de manera segura.

El Centro de Mensajes también está integrado con SIM (Sistema Integral de Mensajería), lo que permite gestionar los dispositivos habilitados para el envío de avisos push en web y plataformas móviles.

Los Organismos solo deben conectarse al Centro de Mensajes a través de la API, ya que éste actúa como intermediario con SIM y con Carpeta Ciudadana para la distribución de mensajes.

Esta arquitectura garantiza una comunicación eficiente, con los debidos controles de seguridad y privacidad, permitiendo a los Organismos centrarse en la configuración y mantenimiento de sus propios sistemas internos.

5 REQUISITOS DE SEGURIDAD:

Este apartado cubre los requisitos de seguridad para la integración, incluyendo autenticación, autorización de los Organismos, cifrado de información y protección de datos.

Las comunicaciones se realizarán a través de canales seguros (**TLS/HTTPS**) basados en la confianza del certificado del servidor, garantizando la encriptación de los datos compartidos.

Autenticación y Autorización

Para autenticar y autorizar las solicitudes de los Organismos, cada solicitud deberá ser firmada digitalmente con el certificado del Organismo, y verificada por el Centro de Mensajes usando la clave pública del mismo certificado. Este proceso se implementará mediante el estándar JWS (RFC-7515: https://datatracker.ietf.org/doc/html/rfc7515#section-7.2.2.), que permite firmar y serializar peticiones JSON.

El Organismo deberá proporcionar un certificado digital confiable, ya sea de tipo RSA o de curva elíptica (EC), que deberá haber sido registrado previamente en Carpeta Ciudadana junto con su identificador único.

Proceso de Firma de Solicitudes

1. Generación de la cabecera

Se crea una cabecera JSON que incluye el tipo de token, el algoritmo de firma, la marca de tiempo actual, y el identificador del certificado:

```
{
```

```
  "typ": "JOSE",
  "alg": "RS256",
  "timestamp": "2025-01-13T14:23:19.766+01:00",
  "kid": "numero_serie_certificado"
}
```

Esta cabecera se codifica en Base64URL.

2. Codificación del cuerpo de la solicitud:

El cuerpo de la solicitud (payload), que incluye los datos a transmitir, se codifica en Base64URL. Ejemplo de cuerpo:

```
{
"idServicio": 33,
"fechaHoraDesde": "2025-01-13T14:23:19.766+01:00",
}
```

3. Generación de la firma:

La cabecera y el cuerpo codificados se concatenan usando un punto "." y se firma usando la clave privada del Organismo. El resultado de la firma también se codifica en Base64URL.

4. Empaquetado en JWS:

El mensaje firmado se estructura en formato JWS como:

```
{
  "protected": "<cabeceraBase64URL>",
  "payload": "<cuerpoBase64URL>",
  "signature": "<firmaBase64URL>"
}
```

Un ejemplo final del objeto JWS sería:

```
{
  "protected": "eyJ0eXAiOi...",
  "payload": "ewogICJhdmlzby...",
  "signature": "R2GarXn8..."
}
```

5. Pseudocódigo de generación del objeto JWS

A continuación, se ejemplifica la generación del objeto JWS mediante un sencillo pseudo código:

```
// Codificar la cabecera en Base64URL
```

```
cabeceraBase64URL = base64UrlEncoder (cabecera);

// Codificar el cuerpo en Base64URL
cuerpoBase64URL = base64UrlEncoder (cuerpo);

// Concatenar cabecera y cuerpo con un punto (.)
mensaje = cabeceraBase64URL + "." + cuerpoBase64URL;

// Firmar el mensaje concatenado con la clave privada
firma = firmaConClavePrivada (mensaje, clavePrivada);

// Codificar la firma en Base64URL
firmaBase64URL = base64UrlEncoder (firma);

// Construir el objeto JWS
JWS = {
   "protected": cabeceraBase64URL,
   "payload": cuerpoBase64URL,
   "signature": firmaBase64URL
};
```

Aún no siendo operativo este pseudocódigo debe servir para aclarar el proceso de generación del objeto JWS que se usará en cualquier comunicación con el centro de mensajes.

6. Envío del JWS

El JWS se enviará en el cuerpo de la solicitud con el tipo de contenido `application/jose+json`.

Validación de Solicitudes en el Centro de Mensajes

Al recibir la solicitud, el Centro de Mensajes verifica la firma mediante los siguientes pasos:

- Validación de que a marca de tiempo es anterior al momento actual y tiene una antigüedad menor a 30 segundos.
- Obtención de la clave pública del certificado del Organismo a partir del identificador en la cabecera.
- Verificación de la autenticidad de la firma.

Si la validación es correcta, el contenido, es decir, la solicitud subyacente en el payload se procesa y se devuelve la información correspondiente.

Nota sobre reintentos y la marca de tiempo

En caso de fallos de comunicación o interrupciones, es importante reconstruir la solicitud con una nueva marca de tiempo antes de realizar reintentos, ya que las solicitudes con marcas de tiempo caducadas serán rechazadas.

Todas las marcas de tiempo se formatearán mediante ISO-8601, incluyendo los milisegundos.

Métodos HTTP empleados

Aunque algunos servicios del sistema, como las consultas de estado de los mensajes, podrían implementarse mediante métodos **GET** en base a su naturaleza, se ha decidido optar por el uso exclusivo de **métodos POST** en todos los servicios con el objetivo de maximizar la seguridad del sistema.

El uso del estándar **JWS (RFC-7515)** implica que cada solicitud firmada contiene una cantidad significativa de información, lo que puede dar lugar a objetos JSON de considerable tamaño. Dado que el método **POST** permite el envío de un cuerpo (body) en la solicitud, es el método más adecuado para enviar el objeto JWS completo. Esto garantiza que la información se transmite de manera segura y eficiente, ya que los objetos JSON firmados (JWS) se incluirán en el cuerpo de la solicitud y no en la cabecera del mensaje.

Por otro lado, el estándar HTTP prohíbe el uso de un cuerpo en las solicitudes **GET**, indicando que, en estas solicitudes, los parámetros deben enviarse en la URL. Desde el punto de vista de la seguridad, incluir información sensible en la URL presenta riesgos significativos, como la posibilidad de que dicha información quede registrada en logs de sistemas intermedios, proxies, o servidores de red, lo que podría comprometer la confidencialidad de los datos.

Debido a estos factores, **todas las solicitudes al Centro de Mensajes utilizarán el método POST**, incluyendo en el cuerpo de la solicitud el objeto JWS.

El contenido del cuerpo deberá tener el tipo de contenido especificado como **'application/jose+json'**, que es el formato adecuado para las solicitudes que contienen objetos JWS firmados.

En resumen, el uso exclusivo de **POST** contribuye a una mejor gestión de la seguridad y privacidad de las comunicaciones, evitando la exposición innecesaria de datos y permitiendo un manejo más seguro del intercambio de información firmado y autenticado entre los sistemas.

Política de renovación de certificados

Para evitar interrupciones en el servicio debido a la caducidad de los certificados, tanto el centro de mensajes como los organismos permitirán la coexistencia de dos certificados correspondientes al otro extremo. Esto facilita que, durante el periodo cercano a la caducidad de un certificado, los clientes puedan cambiar gradualmente el certificado utilizado para firmar las solicitudes, pasando del certificado antiguo al nuevo. Una vez que el certificado antiguo caduque, se eliminará de ambos extremos, quedando únicamente el nuevo certificado.

Evidentemente este proceso se deberá notificar con la suficiente antelación y no debe iniciarse hasta que el certificado esté registrado en ambos extremos, guardando la parte privada en el sistema que actúa como cliente y la parte pública en la máquina que actúa como servidor.

6 DESCRIPCIÓN FUNCIONAL

6.1 Servicios desarrollados por los Organismos

En esta sección se describe el comportamiento de la gestión de consentimientos perteneciente al centro de mensajes. Los métodos descritos en esta sección deben ser desarrollados por los Organismos conforme a las especificaciones indicadas para que posteriormente desde carpeta ciudadana se les indique que usuarios desean recibir avisos.

Mediante este desarrollo se permite que los usuarios indiquen su deseo de recibir avisos procedentes de los diferentes Organismos integrados. La gestión de consentimientos es un paso necesario para poder recibir, posteriormente, avisos en carpeta ciudadana, debido a que es aquí donde se verifica si el ciudadano ha dado su consentimiento para recibir mensajes de forma activa y si dispone de un dispositivo móvil al que enviar los avisos push.

Estos avisos push que recibirá el usuario trataran información personal del usuario por lo que el sistema no está pensando para unos avisos globales informativos desde los Organismos.

Para ello desde Carpeta Ciudadana se ha desarrollado una interfaz que permite a los ciudadanos indicar qué avisos quieren recibir.

Una vez que el usuario ha seleccionado los avisos y pulsado el botón “Guardar”, se almacena la configuración del usuario en la base de datos de carpeta ciudadana y se realiza una petición a los servicios web de los diferentes Organismos integrados en la que se les informa de que dicho usuario desea recibir sus mensajes.

Así mismo, en este momento, se comprueba que el usuario tenga algún dispositivo dado de alta en SIM al que poder enviarle avisos push. Sino solo podrá visualizar los mensajes en el centro de mensajes.

En caso de que no lo hubiera, se informaría a dicho ciudadano que para recibir las push debe tener algún dispositivo registrado en SIM. Para realizar este registro se debe utilizar la aplicación móvil de Carpeta Ciudadana.

Para esta funcionalidad están involucrados tres métodos

- Registrar consentimiento Usuario. Es el método principal que se describe en detalle. Corresponde con el flujo **Registrar consentimiento Usuario.**
- Verificación datos usuario. Método Auxiliar que permite consultar si un usuario es notificable. Se utiliza como auditoria y es necesario únicamente para verificar errores con usuarios, no se utiliza para el envío de mensajes. Corresponde con el flujo **Verificación datos usuario.**
- Actualización estado consentimiento. Método auxiliar que permite a un usuario dar de baja el consentimiento. Corresponde con el flujo **Actualización estado consentimiento.**

Estos métodos se describen en detalle a continuación:

Alta consentimiento Usuario

Se describe a continuación la funcionalidad del servicio web del Organismo mediante el cual se les informa cuando un usuario ha aceptado recibir avisos personales de su parte:

- Un usuario dentro de carpeta ciudadana autoriza a recibir avisos personales por parte de un Organismo.
- Carpeta ciudadana llama al WS del Organismo para informarle la decisión del usuario.
- Se envía la documentación del usuario al Organismo, para que la almacene y pueda empezar a enviar avisos.
- Se recibe una respuesta por parte del Organismo para saber si ha recibido y almacenado la información correctamente.

A continuación, se describe el flujo:

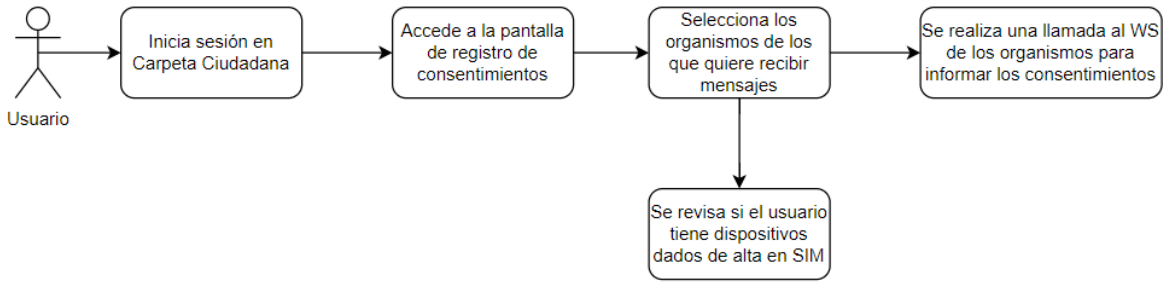


Ilustración 1- Registrar consentimiento Usuario

Para ello:

- El servicio web enviará una petición post al Organismo con la siguiente información:
  - Documentación (DNI, NIE, NIF pasaporte) del ciudadano
  - Id servicio: Identificador único del servicio de carpeta ciudadana
  - Id registro: Identificador del dispositivo

Un ejemplo de petición sería:

```
{
  "documentacion":"99999999R",
  "idServicio":"33",
  "idRegistro":"1auprquc3na6gepnav8vsng9j8gt6g26AA"
}
```


- El servicio Web del Organismo enviará la siguiente respuesta:
  - CodRespuesta: Código de la respuesta
  - Mensaje que especifica si se ha podido realizar la comunicación correctamente.

El ejemplo de respuesta valida de este servicio web sería:


```
{
  "codRespuesta": 0,
  "textoRespuesta":"Información del usuario guardada"
}
```


Verificación datos usuario

Se describe a continuación la funcionalidad del servicio web de carpeta ciudadana que llama a un servicio web del Organismo para saber si un usuario en concreto ha aceptado recibir mensajes push de dicho Organismo:

- Carpeta ciudadana llama al WS del Organismo para saber si un usuario ha aceptado recibir mensajes de dicho Organismo.
  - Se envía la documentación del usuario cuyo consentimiento se quiere consultar.
- Se recibe respuesta por parte del Organismo.

A continuación, se describe el flujo:

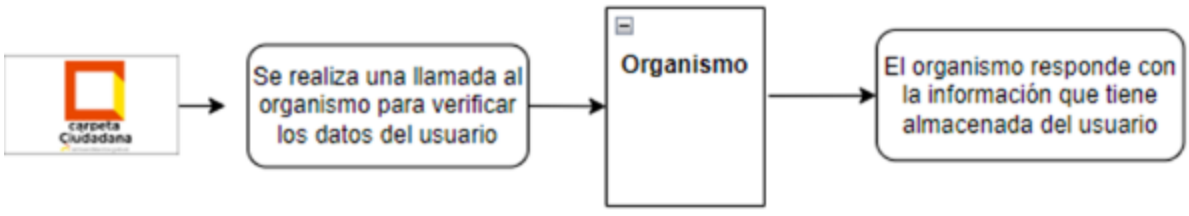


Ilustración 2 - Verificación datos del usuario

Para ello:

- El Web Service enviará una request al Organismo con los siguientes parámetros:
  - Documentación del usuario cuyo consentimiento se quiere consultar.
  - Id servicio

Ejemplo de petición del servicio web:

```
{
  "documentacion": "99999999R",
  "idServicio":"33"
}
```

- El servicio Web lo siguiente al Organismo que le llamó:
  - CodRespuesta: Código de la respuesta.
  - Mensaje que especifica si se ha dado el consentimiento o no.
  - Estado: indica el estado del consentimiento (activado/desactivado)

Ejemplo de repuesta del servicio web

```
{
  "codRespuesta": "0",
  "textoRespuesta":"Usuario encontrado",
  "estado": true
}
```

Actualización estado consentimiento

Se describe a continuación la funcionalidad de la llamada al web service del Organismo para informar la baja de un usuario al servicio de avisos personales:

- Un usuario decide retirar su consentimiento a un Organismo para recibir avisos personales por su parte.
- El WS de carpeta ciudadana llama al WS del Organismo para informar la baja de dicho usuario.
- Se le envía al Organismo la documentación del usuario que se ha dado de baja
- El WS de carpeta ciudadana espera la respuesta por parte del Organismo para saber si la baja se ha producido exitosamente.

A continuación, se describe el flujo:

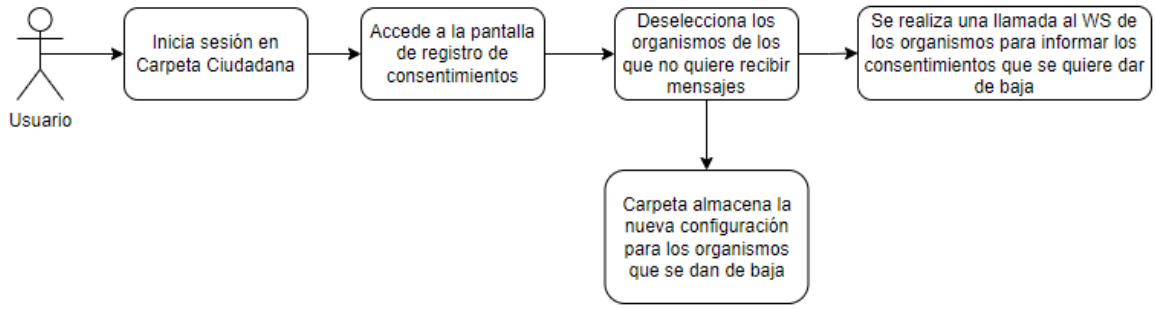


Ilustración 2 - Actualización estado consentimiento

Para ello:

- El Web Service enviará una petición post al Organismo con la siguiente información:
  - Documentación (NIF, NIE …) del ciudadano
  - Id servicio: Identificador único del servicio de carpeta ciudadana
  - Id registro: Identificador del dispositivo

Ejemplo de petición

```
{
  "documentacion":"99999999R",
  "idServicio":"33",
  "idRegistro":"1auprquc3na6gepnav8vsng9j8gt6g26AA"
}
```

- El servicio Web del Organismo enviará la siguiente respuesta:
  - CodRespuesta: Código de la respuesta
  - Mensaje que especifica si se ha podido realizar la comunicación correctamente.

```
{
  "codRespuesta": "0",
  "textoRespuesta":"Usuario dado de baja",
}
```

Para evitar posibles errores, desde carpeta ciudadana se realizan reintentos de envíos de usuarios registrados en el Organismo que no se hubieran podido informar tanto para el caso de alta del usuario como de baja. Desde el equipo de carpeta ciudadana se ha desarrollado un job para tal efecto que reintenta diariamente la comunicación hasta que se consiga informar.

6.2 Servicios desarrollados por Carpeta

Como se ha comentado anteriormente, el objetivo de este desarrollo es proveer a los Organismos, que deseen integrarse con Carpeta Ciudadana, de un mecanismo para enviar mensajes a los usuarios.

Para esto entra en juego la segunda parte de este desarrollo, que son los servicios desarrollados por carpeta ciudadana

Una vez realizada esta integración, los usuarios de Carpeta Ciudadana podrán recibir avisos push en su móvil, a través del sistema de mensajería SIM, y consultarlos en el centro de mensajes tanto de la web como de la aplicación móvil de Carpeta Ciudadana.

Esta interfaz permitirá al usuario ver todos los avisos recibidos, filtrarlos por categoría y fecha, y marcar como leídos aquellos mensajes que ya no desee visualizar.

En el centro de mensajes se mostrarán tanto los mensajes emitidos por los Organismos, sobre los que versa este documento, como los mensajes genéricos emitidos por los administradores de la web.

Es importante tener en cuenta que para que un usuario pueda recibir mensajes de los Organismos debe haber dado previamente su consentimiento, lo cual está explicado en el

documento anteriormente mencionado “CC-Especificaciones Avisos Personales Servicios web desarrollados por los Organismos”.

Para esta funcionalidad están involucrados dos métodos:

- Envío de avisos personales. Método principal que permite el envío de mensajes a los usuarios, se corresponde con los flujos de envío de mensajes.
- Obtención de avisos personales. Método auxiliar que permite consultar por un aviso en concreto, se corresponde con los flujos de obtención de mensajes.

Se describen a continuación:

Envío de avisos personales

Se describe a continuación la funcionalidad del servicio web de carpeta ciudadana encargado del envío de mensajes avisos (avisos push) a los ciudadanos que hayan dado su consentimiento:

- Un Organismo que deseé enviar un aviso personal a un ciudadano en concreto se conecta a carpeta ciudadana y llama al WS de avisos personales.
- Se envía la información pertinente a través del WS.
- Carpeta Ciudadana se encarga de guardar el aviso en base de datos para mostrarlo en el interfaz del centro de mensajes y se lo envía a SIM.
- SIM envía el aviso al ciudadano especificado que esté dado de alta en Carpeta Ciudadana.
- Si SIM no pudiera enviar el aviso, este se guarda en una base de datos de Carpeta Ciudadana. Posteriormente se realiza el reintento de envio a través de un job, asegurando por parte de Carpeta la comunicación. De esta forma no es necesario que el Organismo realice ningún tipo de reintento.

A continuación, se describe el flujo:

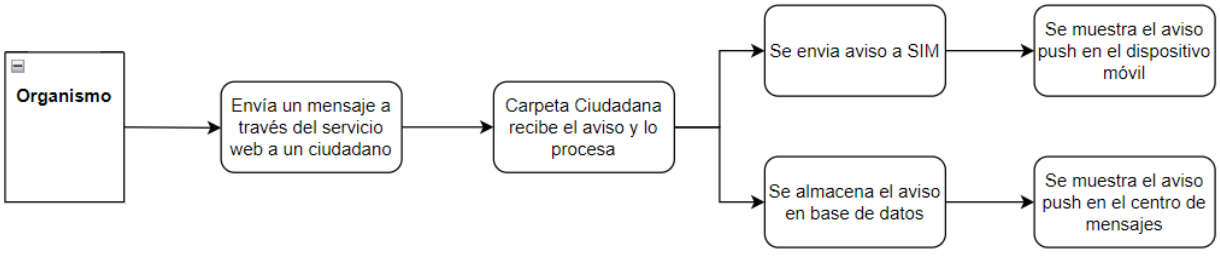


Ilustración 3- Flujo de envío de mensajes

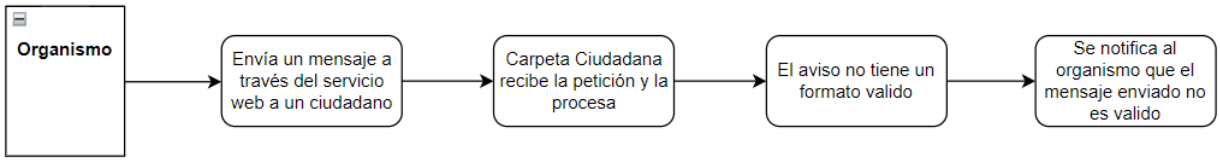


Ilustración 4 - Flujo de envío de mensajes – Error

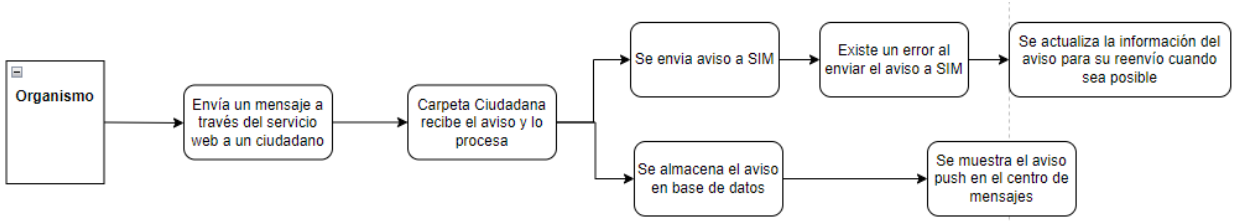


Ilustración 5 - Flujo de envío de mensajes - Error envío SIM

Para ello:

El Web Service recibirá una request por parte del Organismo con los siguientes parámetros en el cuerpo de la request:

- Id servicio
- Tipo de aviso. Indica el mecanismo de envío al usuario. Los valores pueden ser: 1 - push, 0 - solo centro de mensajes, 2 – ambos.
- Id usuario. Documentación (DNI, NIE, NIF…) del ciudadano
- Ámbito (opcional)
- Fecha de caducidad del aviso: (Opcional) Fecha a partir de la cual se deja de mostrar el aviso dentro de la interfaz de carpeta Ciudadana.
- Título del aviso y sus traducciones
- Información y sus traducciones
- nombreOrganismo: Nombre que se desea que aparezca en el centro de mensajes.
- dir3Organismo: Identificador del organismo que se desea marcar como remitente.

El servicio Web para el envío de avisos personales devolverá lo siguiente al Organismo que le llamó:

- Código del mensaje: 0 si todo fue bien, 1 si el usuario no dio su consentimiento para recibir avisos de este Organismo.
- Mensaje que especifica si se ha podido o no enviar el aviso.
- Id Aviso: apartado que devuelve la ID del aviso si el aviso se ha podido enviar.

Un ejemplo de petición válida sería:

```
{
   "idServicio": "33",
   "tipoAviso": 2,
   "idUsuario": "99999999R",
   "ambito": "Trabajo y prestaciones",
   "fechaCaducidad": "2025-01-31",
   "nombreOrganismo": "SGAD",
   "dir3Organismo": "E04995903",
   "aviso": {
      "titulo": "Título de ejemplo",
      "mensaje": "Contenido del mensaje de ejemplo,
      "traducciones": {
        "eu": {
```

```
            "titulo": "Adibideko titulua",
            "informacionEu": "Adibideko mezuaren eduki",
          },
          "en": {
            "titulo": "Example title",
            "informacionEu": "Adibideko mezuaren eduki",
          },
          "gl": {
            "titulo": "Título de exemplo",
            "informacionEu": "Contido do mensaxe de exemplo",
          },
          "ca": {
            "titulo": "Títol d'exemple",
            "informacionEu": "Contingut del missatge d'exemple",
          }
          "va": {
            "titulo": "Títol d'exemple ",
            "informacionEu": "Contingut del missatge d'exemple"
          }
        }
      }
}
```


Un ejemplo de respuesta devuelta por el servidor sería:


```
{
   "codRespuesta": 0,
   "textoRespuesta": "Notificación tramitada",
   "idAviso": 202
}
```


Obtención de avisos personales

Se describe a continuación la funcionalidad del servicio web de carpeta ciudadana encargado de obtener un aviso personal que se haya enviado previamente:

- Un Organismo que deseé consultar un aviso previamente enviado llama al WS de avisos personales.
- En la llamada, especifica la ID del aviso que quiere recuperar y el documento del usuario al que se envió.
- El servicio web de Carpeta Ciudadana consulta la base de datos en busca del aviso utilizando la información aportada por el Organismo devuelve el aviso si ha sido encontrado en la base de datos o un error en caso contrario.
- La utilidad de este método es que se devuelve un campo estado que indica si el usuario ha leído o no el mensaje en la web de Carpeta Ciudadana.

A continuación, se describe el flujo:

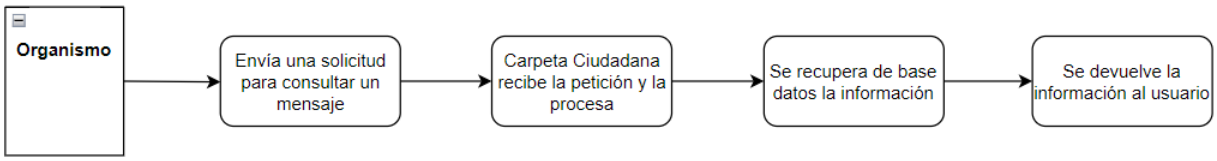


Ilustración 6 – Flujo de obtención de mensajes.

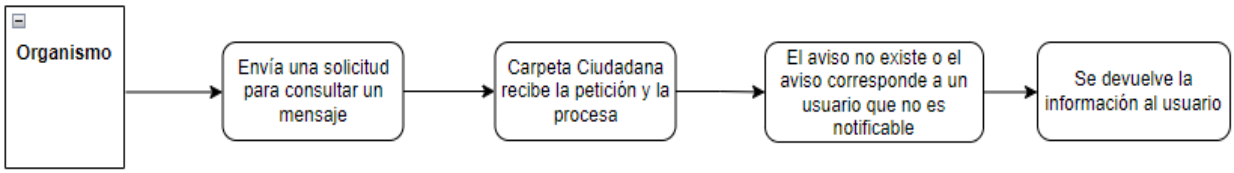


Ilustración 7 - Flujo de obtención de mensajes – Error

Para ello:

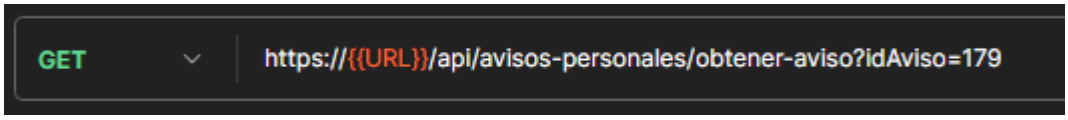
El Web Service recibirá una request por parte del Organismo con los siguientes parámetros en el cuerpo de la request:

- Id del aviso que se desea consultar.

El servicio Web lo siguiente al Organismo que le llamó:

- Código del mensaje: 0 si todo fue bien, 1 si el aviso no pudo ser encontrado.
- Mensaje que especifica si se ha podido o no encontrar el aviso.
- Datos: apartado que devuelve el aviso solicitado en caso de haberlo encontrado. Si no se encuentra, devuelve el valor “Null”

Un ejemplo de petición valida seria:




```
{
  "idServicio": 33,
  "idAviso": 179
}
```

Un ejemplo de respuesta valida seria:

```
{
   "codRespuesta": 0,
   "textoRespuesta": "Mensaje recuperado correctamente",
   "idAviso": 202,
   "fechaRegistro": "2024-10-22",
   "estado": 1,
   "datos": {
      "idServicio": "33",
```

```
        "tipoAviso": 2,
        "idUsuario": "99999999R",
        "ambito": "Trabajo y prestaciones",
        "fechaCaducidad": "2024-12-31",
        "nombreOrganismo": "SGAD",
        "dir3Organismo": "E04995903",
        "aviso": {
            "titulo": "Título de ejemplo",
            "mensaje": "Contenido del mensaje de ejemplo,
            "traducciones": {
                "eu": {
                  "titulo": "Adibideko titulua",
                  "informacionEu": "Adibideko mezuaren eduki",
                },
                "en": {
                  "titulo": "Example title",
                  "informacionEu": "Adibideko mezuaren eduki",
                },
                "gl": {
                  "titulo": "Título de exemplo",
                  "informacionEu": "Contido do mensaxe de exemplo",
                },
                "ca": {
                  "titulo": "Títol d'exemple",
                  "informacionEu": "Contingut del missatge d'exemple",
                }
                "va": {
                  "titulo": "Títol d'exemple",
                  "informacionEu": "Contingut del missatge d'exemple"
                }
            }
        }
    }
}
```


Anotación sobre la identificación del remitente de los avisos personales

El centro de mensajes sabe qué servicio u organismo he enviado el mensaje ya que este se identifica en la cabecera del mensaje JWS. Aún así se incluyen otros dos campos de identificación del remitente para dar mayor flexibilidad a los organismos emisores de forma que puedan concretar o acotar más el servicio emisor en caso de necesidad.

Estos otros dos campos adicionales son los campos “nombreOrganismo” y “dir3Organismo”. La lógica que se implementa en el centro de mensajes es la siguiente:

Si se incluye el campo “nombreOrganismo”, de forma independiente al valor incluido en el campo “dir3Organismo” y a la identificación del emisor del mensaje, se mostrará como remitente el servicio identificado en dicho campo.

Si no se indica el remitente en el campo “nombreOrganismo” y sí que se incluye un código DIR3 válido en el campo “dir3Organismo”, independientemente de la identificación del emisor del mensaje, se mostrará como remitente el servicio identificado con dicho código en los servicios comunes de DIR3.

Finalmente, si no se incluye ninguno de estos dos campos, se marcará como remitente el servicio emisor del aviso con el nombre que se haya registrado en el centro de mensajes en el proceso de alta del servicio (documentación de alta en el servicio).

Con esta lógica se busca dar más flexibilidad a los organismos para que puedan informar mejor a los ciudadanos identificando claramente el servicio o departamento responsable del aviso. Como ejemplo podemos tomar el caso de un ayuntamiento; con estos campos se puede indicar qué concejalía es la responsable del trámite o de la información incluida en el mensaje.

Anexos

ANEXO I – ESPECIFICACIÓN DE LOS SERVICIOS WEB DEL CENTRO DE MENSAJES

API Rest: Parámetros comunes a todos los servicios web

Todas las solicitudes deben incluir los parámetros específicos de cada tipo de solicitud en un objeto JWS.

En la cabecera http de todas las solicitudes se debe indicar el tipo de contenido que para JWS debe ser:

```
Content-Type: application/jose+json
```

Tabla 1.- Solicitud genérica en formato JSW

Parámetros de entrada en la solicitud JSW			
CAMPO	**TIPO**	**DESCRIPCIÓN**	**COMENTARIOS**
protected	String	Cabecera de la solicitud.	Obligatorio. Incluye el objeto HEADER codificado en Base64URL.
payload	String	Cuerpo de la solicitud	Obligatorio. Incluye el objeto JSON con los parámetros específicos de la solicitud codificado en Base64URL.
signature	String	Firma digital de la solicitud	Obligatorio. Incluye la firma digital de la concatenación mediante un punto de la cabecera y el cuerpo, ambos en Base64URL, a su vez codificada la firma en Base64URL.

El objeto HEADER incluye los campos siguientes:

Tabla 2.- Objeto cabecera de JSW

Campos del objeto "HEADER" de JWS			
CAMPO	**TIPO**	**DESCRIPCIÓN**	**COMENTARIOS**
typ	String	Tipo de objeto	Obligatorio. Será "jose", acrónimo de JavaScript Object Signing and Encryption.
alg	String	Identificador del algoritmo usado para generar la firma	Obligatorio. Se debe acordar qué algoritmo usar por defecto. (RS256).
timestamp	String	Marca de tiempo de la solicitud.	Obligatorio. Fecha y hora de la solicitud en formato SCSPv3, es decir ISO 8601 (por ejemplo: "2025-01-13T14:23:19.766+01:00"). Debe ser anterior al momento actual y no puede ser anterior a 30 segundos respecto a la hora actual.
kid	String	Identificador único del certificado usado para la firma	Debe coincidir con el identificador registrado en el centro de mensajes para el certificado. (Número de serie del certificado).

Servicio Web: Envío de nuevo mensaje

URL: <#URL_BASE>/mensaje/envio **Tipo**: POST

Tabla 3.- Parámetros de entrada del servicio web: mensaje/envio

Parámetros de entrada			
CAMPO	**TIPO**	**DESCRIPCIÓN**	**COMENTARIOS**
idServicio	Integer	Identificador del servicio del Organismo.	Obligatorio.
tipoAviso	Integer	Indicador del tipo de aviso se desea enviar.	Obligatorio. Valores: 0 - Centro de mensajes 1 – PUSH 2 – Ambos.
idUsuario	String	Identidad del ciudadano al que se quiere notificar	Obligatorio. Puede ser DNI, pasaporte, NIE o NIF.
ambito	String	Ámbito del aviso para su contextualización en Carpeta Ciudadana	Opcional. Se escoge entre un conjunto predefinido de valores.
fechaCaducidad	Date	Fecha de caducidad del aviso	Opcional. Formato YYYY-MM-DD. No puede ser anterior a la fecha actual.
nombreOrganismo	String	Identificador del remitente tal como se mostrará en la interfaz de usuario.	No tiene por qué coincidir con el nombre oficial, se busca informar al ciudadano sobre el remitente.
dir3Organismo	String	Identificador del remitente en base al código DIR3.	Si el código no es válido se obvia este campo.
aviso	Obj: **AVISO**	Objeto de tipo aviso	Obligatorio

Tabla 4.- Parámetros de salida del servicio web: mensaje/estado

Parámetros de salida			
CAMPO	**TIPO**	**DESCRIPCIÓN**	**COMENTARIOS**
codRespuesta	Integer	Código de respuesta de la petición	Puede ser: 0 – Todo correcto Valor ≠ 0 – Error
textoRespuesta	String	Mensaje de la respuesta	Indica si la solicitud se ha procesado correctamente o el error en caso contrario.
idAviso	Integer	Identificador del aviso	Devuelve el idAviso si todo ha ido bien o un null si algo ha fallado.

Tabla 5.- Objeto aviso

Campos del objeto "AVISO"			
CAMPO	**TIPO**	**DESCRIPCIÓN**	**COMENTARIOS**
titulo	String	Título del aviso	Obligatorio.
mensaje	String	Contenido del mensaje	Obligatorio.

Campos del objeto “AVISO”			
CAMPO	**TIPO**	**DESCRIPCIÓN**	**COMENTARIOS**
traducciones	Object - **TRADS**	Objeto conteniendo el contenido del aviso en las lenguas cooficiales e inglés.	Opcional.

Tabla 6.- Objeto traducciones

Campos del objeto “TRADS”			
CAMPO	**TIPO**	**DESCRIPCIÓN**	**COMENTARIOS**
eu	Object – **AVISO_TRAD**	Objeto con el contenido del aviso traducido al eusjera	Opcional.
en	Object – **AVISO_TRAD**	Objeto con el contenido del aviso traducido al inglés	Opcional.
gl	Object – **AVISO_TRAD**	Objeto con el contenido del aviso traducido a gallego	Opcional.
ca	Object – **AVISO_TRAD**	Objeto con el contenido del aviso traducido a catalán	Opcional.
va	Object – **AVISO_TRAD**	Objeto con el contenido del aviso traducido a valenciano	Opcional.

Tabla 7.- Objeto aviso_traducido

Campos del objeto “AVISO_TRAD”			
CAMPO	**TIPO**	**DESCRIPCIÓN**	**COMENTARIOS**
titulo	String	Título del aviso	Obligatorio. Si se incluye la traducción, esta debe estar completa incluyendo los dos campos.
mensaje	String	Contenido del mensaje	Obligatorio. Si se incluye la traducción, esta debe estar completa incluyendo los dos campos.

Servicio Web: Consulta de estado de un mensaje

URL: <#URL_BASE>/mensaje/estado **Tipo**: POST

Tabla 8.- Parámetros de entrada del servicio web: mensaje/estado

Parámetros de entrada			
CAMPO	**TIPO**	**DESCRIPCIÓN**	**COMENTARIOS**
idAviso	Integer	Identificador del aviso	Devuelve el idAviso si todo ha ido bien o un null si algo ha fallado.

Tabla 9.- Parámetros de salida del servicio web: mensaje/estado

Parámetros de salida			
CAMPO	**TIPO**	**DESCRIPCIÓN**	**COMENTARIOS**
codRespuesta	Integer	Código de respuesta de la petición	Puede ser:

Parámetros de salida			
CAMPO	**TIPO**	**DESCRIPCIÓN**	**COMENTARIOS**
			0 – Todo correcto Valor ≠ 0 – Error
textoRespuesta	String	Mensaje de la respuesta	Indica si la solicitud ha sido procesada correctamente, en caso contrario indica el motivo
idAviso	Integer	Identificador del aviso	Devuelve el idAviso si todo ha ido bien o un null si algo ha fallado.
estado	Integer	Indicador del estado del mensaje	Los valores posibles son: 0 – Enviado. 1 – Entregado. 2 – Leído. 3 – Error.
fechaRegistro	Date	Fecha de registro del aviso	Formato YYYY-MM-DD.
datos	Object – **AVISO_ENV**	Contenido del aviso registrado en el centro de mensajes	Coincide con el objeto enviado en la solicitud de envío de mensaje.

Tabla 10.- Objeto Aviso Enviado – Coincide con el objeto usado en el envío de avisos

Campos del objeto "AVISO_ENV"			
CAMPO	**TIPO**	**DESCRIPCIÓN**	**COMENTARIOS**
idServicio	Integer	Identificador del servicio del organismo.	Obligatorio.
tipoAviso	Integer	Indicador del tipo de aviso se desea enviar.	Obligatorio. Valores: 0 - Centro de mensajes 1 – PUSH 2 – Ambos.
idUsuario	String	Identidad del ciudadano al que se quiere notificar	Obligatorio. Puede ser DNI, pasaporte, NIE o NIF.
ambito	String	Ámbito del aviso para su contextualización en Carpeta Ciudadana	Opcional. Se escoge entre un conjunto predefinido de valores.
fechaCaducidad	Date	Fecha de caducidad del aviso	Opcional. Formato YYYY-MM-DD. No puede ser anterior a la fecha actual.
nombreOrganismo	String	Identificador del remitente tal como se mostrará en la interfaz de usuario.	No tiene por qué coincidir con el nombre oficial, se busca informar al ciudadano sobre el remitente.
dir3Organismo	String	Identificador del remitente en base al código DIR3.	Si el código no es válido se obvia este campo.
aviso	Obj: **AVISO**	Objeto de tipo aviso	Obligatorio

Servicio Web: Alta consentimiento Usuario

URL: <#URL_BASE>/consentimiento/alta **Tipo**: POST

Tabla 11.- Parámetros de entrada del servicio web: consentimiento/alta

Parámetros de entrada			
CAMPO	**TIPO**	**DESCRIPCIÓN**	**COMENTARIOS**
documentacion	String	Documentación que acredita la identidad del ciudadano.	Obligatorio. Puede ser DNI, pasporte, NIE o NIF.
idServicio	String	Id del servicio de carpeta ciudadana	Obligatorio
idRegistro	String	Identificador del dispositivo	Obligatorio

Tabla 12.- Parámetros de salida del servicio web: consentimiento/alta

Parámetros de salida			
CAMPO	**TIPO**	**DESCRIPCIÓN**	**COMENTARIOS**
codRespuesta	Integer	Código de respuesta de la petición	Puede ser: 0 – Todo correcto Valor ≠ 0 – Error
textoRespuesta	String	Mensaje de la respuesta	Indica si la solicitud se ha procesado correctamente o el error en caso contrario.

Servicio Web: Verificación datos usuario

URL: <#URL_BASE>/consentimiento/consulta **Tipo**: POST

Tabla 13.- Parámetros de entrada del servicio web: consentimiento/consulta

Parámetros de entrada			
CAMPO	**TIPO**	**DESCRIPCIÓN**	**COMENTARIOS**
documentacion	String	Documentación que acredita la identidad del ciudadano.	Obligatorio. Puede ser DNI, pasporte, NIE o NIF.
idServicio	String	Id del servicio de carpeta ciudadana	Obligatorio
idRegistro	String	Identificador del dispositivo	Obligatorio

Tabla 14.- Parámetros de salida del servicio web: consentimiento/consulta

Parámetros de salida			
CAMPO	**TIPO**	**DESCRIPCIÓN**	**COMENTARIOS**
codRespuesta	Integer	Código de respuesta de la petición	Puede ser: 0 – Todo correcto Valor ≠ 0 – Error
textoRespuesta	String	Mensaje de la respuesta	Indica si la solicitud se ha procesado correctamente o el error en caso contrario.
consentimiento	Boolean	Estado del consentimiento del usuario	True si el consentimiento está activo, false en caso contrario

Servicio Web: Actualización estado consentimiento

URL: <#URL_BASE>/consentimiento/actualizacion **Tipo**: POST

Tabla 15.- Parámetros de entrada del servicio web: consentimiento/actualizacion

Parámetros de entrada			
CAMPO	**TIPO**	**DESCRIPCIÓN**	**COMENTARIOS**
documentacion	String	Documentación que acredita la identidad del ciudadano.	Obligatorio. Puede ser DNI, pasporte, NIE o NIF.
idServicio	String	Id del servicio de carpeta ciudadana	Obligatorio
idRegistro	String	Identificador del dispositivo	Obligatorio

Tabla 16.- Parámetros de salida del servicio web: consentimiento/ actualizacion

Parámetros de salida			
CAMPO	**TIPO**	**DESCRIPCIÓN**	**COMENTARIOS**
codRespuesta	Integer	Código de respuesta de la petición	Puede ser: 0 – Todo correcto Valor ≠ 0 – Error
textoRespuesta	String	Mensaje de la respuesta	Indica si la solicitud se ha procesado correctamente o el error en caso contrario.

Códigos de respuesta funcionales

Tabla 17.- Códigos de respuesta y error funcionales

Código de respuesta	Descripción	Comentarios
0	Solicitud ejecutada con éxito.	La solicitud se ha procesado correctamente.
1	Error de autorización del Organismo	El Organismo, alguno de los campos que lo identifican o el elemento sobre el que se consulta (p.e. el estado de un aviso) no se corresponden con el certificado empleado en la firma de la solicitud, por lo que no se autoriza la consulta.
1	Error de salida	La solicitud se ha procesado correctamente pero no se pueden devolver resultados. En una consulta de usuarios indica que el rango solicitado está vacio. En la consulta del estado de un aviso, indica que el aviso no se encuentra.
2	Error: Usuario no válido	El usuario referenciado en la solicitud no existe o ha revocado su consentimiento al Organismo.
3	Error: Posible desactualización de la base de datos	El rango solicitado en la búsqueda de modificaciones de usuarios excede el rango almacenado. El Organismo debe iniciar un proceso de reconciliación de bases de datos.
4	Error: Parámetros no válidos	Indica que alguno de los parámetros empleados en la solicitud no es válido o que falta algún parámetro obligatorio.

Códigos de respuesta HTTP

Tabla 18.- Códigos de respuesta y error http

Código de respuesta	Descripción	Comentarios
200 – OK	Solicitud ejecutada.	La solicitud se ha procesado correctamente. La respuesta puede contener errores funcionales pero el contenido JWS es correcto y está firmado con un certificado de Organismo válido.
400 – Bad Request	Error: Solicitud no válida	Este error indica que la solicitud no es válida, bien porque falte alguno de los campos del objeto JWS o porque la marca de tiempo se considere desfasada.
401 - Unauthorized	Error: Firma no válida	Este error indica que no se ha podido verificar la autenticidad de la firma digital del contenido.
403 - Forbidden	Error: Recurso no permitido	El Organismo está intentando acceder a un recurso no permitido.
404 – Not Found	Error: El recurso solicitado no existe	El recurso no existe o la url está mal formada.
408 – Request Timeout	Error: El servicio ha tardado demasiado en responder.	El servidor no ha recibido la solicitud completa en un tiempo permitido, o ha tardado demasiado en procesarla.
409 – Conflict	Error: Se ha producido en conflicto en el acceso a los datos	Se ha producido un conflicto al intentar procesar una solicitud, generalmente debido a que los datos han cambiado en el tiempo transcurrido.