

Documento técnico

Manual integración Habilita Servicios web con WS-Security

Versión: 1.20

Fecha de la versión: 14/09/2021



Madrid, 14 de septiembre de 2021

Elaborado por la Secretaría General de Administración Digital

© Ministerio de Asuntos Económicos y Transformación Digital

NIPO: Pendiente de asignación.

ÍNDICE

1. OBJETO	3
2. DESCRIPCIÓN DE FUNCIONES DEL CATALOGO	4
2.1. Área de gestión de usuarios.....	4
2.1.1.Comprobación de permiso para procedimiento SIA	4
2.1.2.Comprobación de permiso para procedimiento SIA por tipo	4
2.1.3.Obtención de fichero de consentimiento de ciudadano	4
3. FUNCIONAMIENTO DE LOS SERVICIOS WEB	5
3.1. Área de gestión de usuarios.....	5
3.1.1.Comprobación de permiso para procedimiento SIA	5
3.1.2.Comprobación de permiso para procedimiento SIA por tipo	6
3.1.3.Obtención de fichero de consentimiento de ciudadano	7
4. INTEGRACIÓN CON WS-SECURITY	11
4.1. Ejemplos de integración	11
4.1.1.SoapUI.....	11

1. OBJETO

El presente documento describe el catálogo de servicios web que se ha implementado para exponer a las aplicaciones que los usen las funcionalidades del entorno de Habilita

Este catálogo de servicios web implementa la especificación de seguridad WS-Security. Éste es un protocolo de comunicaciones que suministra un medio para aplicar seguridad a los Servicios Web. Del mismo modo WS-Security incorpora características de seguridad en el encabezado de un mensaje SOAP, trabajando en la capa de aplicación, garantizando de esta manera la seguridad extremo a extremo.

De modo que, el estándar WS-Security define una especificación que implementa una serie de mejoras al marco de trabajo de mensajería SOAP con el objetivo de mejorar la protección de los mensajes.

Para ello, se basa en dos mecanismos esenciales:

- La integridad y confidencialidad de los mensajes.
- Autenticación de un mensaje individual.

En la [sección 4](#) del presente documento se detalla la configuración necesaria para el uso del catálogo de servicios web bajo la especificación WS-Security.

2. DESCRIPCIÓN DE FUNCIONES DEL CATALOGO

2.1. Área de gestión de usuarios

2.1.1. Comprobación de permiso para procedimiento SIA

Esta función del catálogo de servicios web permite saber si un funcionario está o no habilitado para poder tramitar un determinado procedimiento.

2.1.2. Comprobación de permiso para procedimiento SIA por tipo

Esta función del catálogo de servicios web permite saber si un funcionario está o no habilitado para poder tramitar un determinado procedimiento. Es igual que la función anterior pero pudiendo precisar el tipo de habilitación por el que queremos buscar.

2.1.3. Obtención de fichero de consentimiento de ciudadano

Esta función del catálogo de servicios web devuelve el pdf firmado electrónicamente en base 64 de un consentimiento de un ciudadano para su identificación y autenticación por parte de un funcionario habilitado para la realización de un trámite

3. FUNCIONAMIENTO DE LOS SERVICIOS WEB

3.1. Área de gestión de usuarios

3.1.1. Comprobación de permiso para procedimiento SIA

- Nombre del Servicio:

isUserHabilitadoForProc();

- XML de llamada:

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:hab="http://habilita.ws.sgad.es">
  <soapenv:Header/>
  <soapenv:Body>
    <hab:isUserHabilitadoForProc>
      <hab:nif_or_nie>?</hab:nif_or_nie>
      <hab:codSIAProc>?</hab:codSIAProc>
    </hab:isUserHabilitadoForProc>
  </soapenv:Body>
</soapenv:Envelope>
```

- Explicación relleno de parámetros:

Lo primero que se debe rellenar es el identificador sin guiones (DNI o NIE) del funcionario, dicho valor irá asignado dentro de la etiqueta <hab:nif_or_nie>.

A continuación se ha de rellenar el código SIA del procedimiento, y dicho valor se asignará dentro de la etiqueta <hab:codSIAProc>.

- Condiciones:

Esta función únicamente revisa aquellas habilitaciones que se hayan asignado al funcionario habilitado recibido, y que además estén aprobadas y activas. Y de dichas habilitaciones comprueba si alguna de ellas está asociada al procedimiento SIA que se ha recibido como parámetro, es decir en última instancia devuelve si el funcionario puede o no tramitar un determinado procedimiento.

- Tabla detalle parámetros de entrada:

Parametro	Valor	Tipo
nif_or_nie	DNI o NIE del funcionario a consultar (Sin guiones)	Obligatorio
codSIAProc	Código numérico del procedimiento en SIA	Obligatorio

- XML de respuesta válida (El funcionario Sí está habilitado para hacer el trámite):

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <soapenv:Body>
    <isUserHabilitadoForProcResponse xmlns="http://habilita.ws.sgad.es">
      <isUserHabilitadoForProcReturn>
        <funcionarioHabilitadoForProc>true</funcionarioHabilitadoForProc>
        <habilitaError xsi:nil="true"/>
      </isUserHabilitadoForProcReturn>
    </isUserHabilitadoForProcResponse>
  </soapenv:Body>
</soapenv:Envelope>
```

- XML de respuesta no válida (El funcionario NO está habilitado para hacer el trámite):

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <soapenv:Body>
    <isUserHabilitadoForProcResponse xmlns="http://habilita.ws.sgad.es">
      <isUserHabilitadoForProcReturn>
        <funcionarioHabilitadoForProc>false</funcionarioHabilitadoForProc>
        <habilitaError>6-Funcionario no habilitado para
procedimiento</habilitaError>
      </isUserHabilitadoForProcReturn>
    </isUserHabilitadoForProcResponse>
  </soapenv:Body>
</soapenv:Envelope>
```

3.1.2. Comprobación de permiso para procedimiento SIA por tipo

- Nombre del Servicio:

isUserHabilitadoForProcByType();

- XML de llamada:

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:hab="http://habilita.ws.sgad.es">
  <soapenv:Header/>
  <soapenv:Body>
    <hab:isUserHabilitadoForProcByType>
      <hab:nif_or_nie>?</hab:nif_or_nie>
      <hab:codSIAProc>?</hab:codSIAProc>
      <hab:tipoHab>?</hab:tipoHab>
    </hab:isUserHabilitadoForProcByType>
  </soapenv:Body>
</soapenv:Envelope>
```

- Explicación relleno de parámetros:

Lo primero que se debe rellenar es el identificador sin guiones (DNI o NIE) del funcionario, dicho valor irá asignado dentro de la etiqueta <hab:nif_or_nie>.

A continuación se ha de rellenar el código SIA del procedimiento, y dicho valor se asignará dentro de la etiqueta `<hab:codSIAProc>`.

Por último hay que rellenar el tipo de Habilitación por el que estamos buscando, dicho valor irá asignado dentro de la etiqueta `<hab:tipoHab>` y podrá contener 1, 2 o 3, valores numéricos correspondientes a la siguiente relación por tipo:

- IDENTIFICACION_Y_FIRMA(1)
- COPIA_AUTENTICA_DE_ENTRADA(2)
- COPIA_AUTENTICA_DE_SALIDA(3)

3.1.3. Obtención de fichero de consentimiento de ciudadano

- Nombre del Servicio:

`getConsentFileForCitizen ()`;

- XML de llamada:

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:hab="http://habilita.ws.sgad.es">
  <soapenv:Header/>
  <soapenv:Body>
    <hab:getConsentFileForCitizen>
      <hab:nif_or_nie_funcionario>?</hab:nif_or_nie_funcionario>
      <hab:nif_or_nie_ciudadano>?</hab:nif_or_nie_ciudadano>
      <hab:codSIAProc>?</hab:codSIAProc>
    </hab:getConsentFileForCitizen>
  </soapenv:Body>
</soapenv:Envelope>
```

- Explicación relleno de parámetros:

Lo primero que se debe rellenar es el identificador sin guiones (DNI o NIE) del funcionario, dicho valor irá asignado dentro de la etiqueta `<hab:nif_or_nie_funcionario>`.

A continuación se debe rellenar también el identificador sin guiones (DNI o NIE) del ciudadano. En este caso el valor se asigna dentro de la etiqueta `<hab:nif_or_nie_ciudadano>`.

Para finalizar se ha de rellenar el código SIA del procedimiento, y dicho valor se asignará dentro de la etiqueta `<hab:codSIAProc>`.

- Condiciones:

Esta función únicamente revisa aquella habilitación más reciente que se haya asignado al funcionario habilitado recibido, y que además esté aprobada, activa y vigente. Y comprueba si dicha habilitación está asociada al procedimiento SIA que se ha recibido como parámetro. Para finalizar comprueba si existe algún consentimiento firmado para el ciudadano recibido como parámetro dentro de la habilitación.

- Tabla detalle parámetros de entrada:

Parametro	Valor	Tipo
nif_or_nie_funcionario	DNI o NIE del funcionario a consultar (Sin guiones)	Obligatorio
nif_or_nie_ciudadano	DNI o NIE del ciudadano a consultar (Sin guiones)	Obligatorio
codSIaproc	Código numérico del procedimiento en SIA	Obligatorio

- XML de respuesta válida (Se ha encontrado un consentimiento firmado por el funcionario para ese ciudadano en ese trámite):

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <soapenv:Body>
    <getConsentFileForCitizenResponse xmlns="http://habilita.ws.sgad.es">
      <getConsentFileForCitizenReturn>
        <habilitaError xsi:nil="true"/>
        <idConsentimiento>121</idConsentimiento>

        <pdfConsentFirmadoDigitalmente>JVBERi0xLjQKJ</pdfConsentFirmadoDigitalmente>
      </getConsentFileForCitizenReturn>
    </getConsentFileForCitizenResponse>
  </soapenv:Body>
</soapenv:Envelope>
```

- XML de respuesta no válida (Error 1 – Funcionario no encontrado):

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <soapenv:Body>
    <getConsentFileForCitizenResponse xmlns="http://habilita.ws.sgad.es">
      <getConsentFileForCitizenReturn>
        <habilitaError>1 - Funcionario no encontrado.</habilitaError>
        <idConsentimiento xsi:nil="true"/>
        <pdfConsentFirmadoDigitalmente xsi:nil="true"/>
      </getConsentFileForCitizenReturn>
    </getConsentFileForCitizenResponse>
  </soapenv:Body>
</soapenv:Envelope>
```


- XML de respuesta no válida (Error 2 – Procedimiento SIA no incluido en Habilita):

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <soapenv:Body>
    <getConsentFileForCitizenResponse xmlns="http://habilita.ws.sgad.es">
      <getConsentFileForCitizenReturn>
        <habilitaError>2-Procedimiento SIA no incluido en
Habilita.</habilitaError>
        <idConsentimiento xsi:nil="true"/>
        <pdfConsentFirmadoDigitalmente xsi:nil="true"/>
      </getConsentFileForCitizenReturn>
    </getConsentFileForCitizenResponse>
  </soapenv:Body>
</soapenv:Envelope>
```

- XML de respuesta no válida (Error 3 – Falta algún valor de parámetro en la entrada):

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <soapenv:Body>
    <getConsentFileForCitizenResponse xmlns="http://habilita.ws.sgad.es">
      <getConsentFileForCitizenReturn>
        <habilitaError>3-Falta algún valor de parametro en la
entrada.</habilitaError>
        <idConsentimiento xsi:nil="true"/>
        <pdfConsentFirmadoDigitalmente xsi:nil="true"/>
      </getConsentFileForCitizenReturn>
    </getConsentFileForCitizenResponse>
  </soapenv:Body>
</soapenv:Envelope>
```

- XML de respuesta no válida (Error 4 – DNI o NIE mal formateado):

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <soapenv:Body>
    <getConsentFileForCitizenResponse xmlns="http://habilita.ws.sgad.es">
      <getConsentFileForCitizenReturn>
        <habilitaError>4- DNI o NIE mal formateado.</habilitaError>
        <idConsentimiento xsi:nil="true"/>
        <pdfConsentFirmadoDigitalmente xsi:nil="true"/>
      </getConsentFileForCitizenReturn>
    </getConsentFileForCitizenResponse>
  </soapenv:Body>
</soapenv:Envelope>
```

- XML de respuesta no válida (Error 5 – Código procedimiento SIA mal formateado):

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <soapenv:Body>
```

```

    <getConsentFileForCitizenResponse xmlns="http://habilita.ws.sgad.es">
      <getConsentFileForCitizenReturn>
        <habilitaError>5 - Codigo procedimiento SIA mal
formateado.</habilitaError>
        <idConsentimiento xsi:nil="true"/>
        <pdfConsentFirmadoDigitalmente xsi:nil="true"/>
      </getConsentFileForCitizenReturn>
    </getConsentFileForCitizenResponse>
  </soapenv:Body>
</soapenv:Envelope>

```

- **XML de respuesta no válida (Error 6 – Funcionario no habilitado para procedimiento):**

```

<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <soapenv:Body>
    <getConsentFileForCitizenResponse xmlns="http://habilita.ws.sgad.es">
      <getConsentFileForCitizenReturn>
        <habilitaError>6 -Funcionario no habilitado para
procedimiento.</habilitaError>
        <idConsentimiento xsi:nil="true"/>
        <pdfConsentFirmadoDigitalmente xsi:nil="true"/>
      </getConsentFileForCitizenReturn>
    </getConsentFileForCitizenResponse>
  </soapenv:Body>
</soapenv:Envelope>

```

- **XML de respuesta no válida (Error 7 - No se ha encontrado ningún consentimiento firmado):**

```

<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <soapenv:Body>
    <getConsentFileForCitizenResponse xmlns="http://habilita.ws.sgad.es">
      <getConsentFileForCitizenReturn>
        <habilitaError>7-No se ha encontrado ningun consentimiento firmado por
el funcionario para ese ciudadano en ese tramite.</habilitaError>
        <idConsentimiento xsi:nil="true"/>
        <pdfConsentFirmadoDigitalmente xsi:nil="true"/>
      </getConsentFileForCitizenReturn>
    </getConsentFileForCitizenResponse>
  </soapenv:Body>
</soapenv:Envelope>

```

4. INTEGRACIÓN CON WS-SECURITY

La invocación de los servicios web de Habilita puede realizarse por medio de WS-Security. Los endpoints serán los siguientes:

Preproducción: <https://pre-habilita.redsara.es/HabilitaServerWS/services/HabilitaWS?wsdl>

Producción: <https://habilita.redsara.es/HabilitaServerWS/services/HabilitaWS?wsdl>

Certificados

La aplicación invocante deberá disponer de un certificado para su uso y proporcionar un certificado raíz e intermedio de extensión .cer o .crt para que Habilita pueda disponer de la cadena de confianza.

La invocación de servicios web sin especificar cabecera de seguridad, devolverá la respuesta “WSDoAllReceiver: Request does not contain required Security header”.

Mientras el certificado no esté incluido en el almacén de certificados de Habilita la invocación de los servicios web devolverá la siguiente respuesta aunque esté bien configurado en la aplicación cliente: “WSDoAllReceiver: The certificate used for the signature is not trusted”.

4.1. Ejemplos de integración

4.1.1. SoapUI

A continuación se explica la configuración a realizar en la herramienta SoapUI para invocar los servicios web de Autentica.

NOTA: Por cuestiones de seguridad, es necesario proveer a Habilita de la clave pública del certificado con el que se firmarán las peticiones o llamadas al servicio web. Esto es necesario para establecer la relación de confianza entre los dos sistemas. Este fichero se proveerá mediante apertura de incidencia (soporte.habilita@correo.gob.es) o a través de correo electrónico.

Se puede obtener más información en la propia página de ayuda de SoapUI:

<https://www.soapui.org/soapui-projects/ws-security.html>

Para realizar este manual se han utilizado las versiones 4.6.1 y 5.3.0

- Se accederá a las propiedades del proyecto (doble clic sobre el mismo u opción del botón derecho “Show Project View”).
- Pestaña “WS-Security Configurations”
- Pestaña “Keystores”. Se añade el archivo .keystore que está integrado en los servicios web de Habilita
 - Source: [...] *\nombre del almacen donde esta el certificado.p12*
 - Status: OK (valor que indica SoapUI si la contraseña introducida es correcta).
 - Password: [.....]

- Pestaña “Outgoing WS-Security Configurations”: se añade una nueva configuración especificando un nombre único, ej. “outgoing_habilitaws” y se completan los siguientes datos:
 - Default Username/Alias: [en blanco]
 - Default Password: [en blanco]
 - Actor: autenticaSig
 - Must Understand: [Seleccionado]
- En el apartado inferior se añade una nueva entrada WSS (WSS Entry) seleccionando el tipo “Signature” en la ventana de diálogo “Add WSS Entry”.
- Se rellena la siguiente configuración de la entrada “Signature”
 - Keystore: *nombre del almacen donde esta el certificado.p12*
 - Alias: alias del certificado con el que se firma la petición
 - Password: [.....]
 - Key Identifier Type: BinarySecurityToken
 - Signature Algorithm: <default> (no es necesario añadir nada, pero si lo fuera, se seleccionaría la opción <http://www.w3.org/2000/09/xmldsig#dsa-sha1>)
 - Signature Canonicalization: <default>(no es necesario añadir nada, pero si lo fuera, se seleccionaría la opción <http://www.w3.org/2001/10/xml-exc-c14n#>)
 - Digest Algorithm: <default>(no es necesario añadir nada, pero si lo fuera, se seleccionaría la opción <http://www.w3.org/2000/09/xmldsig#sha1>)
- Se crea una nueva petición y se completan los datos correspondientes. Es imprescindible poner a “true” la propiedad “Strip Whitespaces” de la petición.
 En cualquier caso, si se ejecuta en este momento, se mostrará el siguiente error:

<soapenv:Fault>

<faultcode>soapenv:Server.generalException</faultcode>

<faultstring>WSDoAllReceiver: Request does not contain required Security header</faultstring>

<detail>

<ns1:hostname

xmlns:ns1="http://xml.apache.org/axis/">sacaedesse01.redsara.es</ns1:hostname>

</detail>

</soapenv:Fault>

Así que para poder ejecutar la petición se tienen dos opciones

- Añadir la cabecera con el botón derecho.
 - Se añade la cabecera WS-Security con el botón derecho “Outgoing WSS” → “Apply outgoing_asistentews” de tal forma que ocurren dos cosas
 - Se añade una cabecera “<soapenv:Header><wss:Security...”

- Se modifica el elemento “<soapenv:Body>” para añadir dos atributos “wsu:Id” y “xmlns:wsu”
- Se ejecuta la petición y se muestra el siguiente error:


```
<soapenv:Fault>

  <faultcode>soapenv:Server.generalException</faultcode>

  <faultstring>WSDoAllReceiver: security processing failed; nested exception is:

    org.apache.ws.security.WSSecurityException: The signature verification
    failed</faultstring>

    <detail>

      <ns1:hostname
xmlns:ns1="http://xml.apache.org/axis/">sacaedesse01.redsara.es</ns1:hostname>

    </detail>

</soapenv:Fault>
```

Se debe a que la petición que se genera con el SoapUI está tabulada y debe estar en una misma línea (a partir del elemento <soapenv:Body>). Esto es así porque el XML que se envía puede tener caracteres de fin de línea dentro del elemento Body que en este caso no acepta SoapUI.

- Si se coloca todo en una misma línea y se ejecuta, seguirá produciéndose el mismo error porque la cabecera ws-security se ha generado para una petición tabulada, así que con el botón derecho se selecciona la opción “derecho “Outgoing WSS” → “Remove all outgoing wss”, se vuelve a añadir la cabecera como se ha visto antes y se vuelve a ejecutar la petición, de tal forma que se obtendrá una respuesta del servicio web.

Esta forma de agregar la cabecera es dependiente de la petición realizada, es decir, si se cambia algún atributo para realizar otra petición, la cabecera WS-Security ya no coincidirá con la petición modificada, por lo que se mostrará la incidencia “The signature verification failed”

- Añadir la cabecera con la opción inferior “Auth” (“Auth” en la versión 5.3.0)
 - En la versión 4.6.1 pulsamos sobre la opción “Auth” y se abre un formulario:
 - Authorisation Type: Global HTTP Settings
 - Outgoing WSS: outgoing_asistentews
 - En la versión 5.3.0 pulsamos sobre la opción “Auth” y se abre un formulario:
 - Authorization: Basic
 - Outgoing WSS: outgoing_asistentews
 - Se ejecuta la petición y devolverá resultados de la invocación siempre y cuando el elemento “<soapenv:Header>” no tenga contenido .

La ventaja de esta forma de invocar la petición con SoapUI es que la cabecera WS-Security se genera dinámicamente de tal forma que si se cambia algún dato de la petición la cabecera seguirá siendo correcta y la petición se ejecutará correctamente.