

**Manual de Instalación y Explotación**

*Cl@ve2 - Monitorización*

**Solución de Monitorización (Cl@ve 2)**

Versión 14/11/2018

Control de Modificaciones

|  |  |
| --- | --- |
| Documento nº: | Cl@ve-Monitorizacion-InstalcionExplotacion-MAN |
| Revisión: | 001 |
| Fecha: | 14/11/2018 |

|  |  |
| --- | --- |
| Rev. | 001 |
| Fecha | 14/11/2018 |
| Descripción | Versión inicial del documento |

Control de Distribución

|  |  |
| --- | --- |
| Documento nº: | Cl@ve-Monitorizacion-InstalcionExplotacion-MAN |
| Revisión: | 001 |
| Fecha: | 14/11/2018 |

Propiedad del documento:

Este documento pertenece al Gobierno de España y posee un carácter de público para uso y distribución en ámbitos autorizados por este mismo, según se recoge en la declaración de privacidad.

Declaración de privacidad:

El contenido de este documento está sujeto al protocolo de libre distribución dentro del entorno definido para el contexto.

Copias Electrónicas:

La distribución de este documento ha sido controlada a través del sistema de información.

Copias en Papel:

La vigencia de las copias impresas en papel está condicionada a la coincidencia de su estado de revisión con el que aparece en el sistema electrónico de distribución de documentos.

El control de distribución de copias en papel para su uso en proyectos u otras aplicaciones es responsabilidad de los usuarios del sistema electrónico de información.

**INDICE GENERAL**

[1 Objeto 7](#_Toc531197155)

[2 Alcance 7](#_Toc531197156)

[3 Siglas 8](#_Toc531197157)

[4 Documentos de Referencia 8](#_Toc531197158)

[5 Introducción 9](#_Toc531197159)

[6 Recursos hardware 9](#_Toc531197160)

[6.1 Configuración mínima y recomendada 9](#_Toc531197161)

[6.2 Conectividad 9](#_Toc531197162)

[6.3 Otras Restricciones 10](#_Toc531197163)

[6.4 Recursos software 10](#_Toc531197164)

[6.4.1 Estructura de la distribución 10](#_Toc531197165)

[6.4.2 Restricciones técnicas 10](#_Toc531197166)

[7 Instalación y configuración del software 11](#_Toc531197167)

[7.1 Despliegue del modelo de datos 11](#_Toc531197168)

[7.2 Compilación y generación de binarios 11](#_Toc531197169)

[7.3 Configuración del entorno de ejecución 11](#_Toc531197170)

[7.3.1 Parámetros JVM 12](#_Toc531197171)

[7.3.2 Configuración componente SAMLEngine 13](#_Toc531197172)

[8 Monitorización plataforma Cl@ve 13](#_Toc531197173)

[8.1 Actuaciones previas 13](#_Toc531197174)

[8.1.1 Gestión de los correos para las alarmas 13](#_Toc531197175)

[8.1.2 Gestión del temporizador 14](#_Toc531197176)

[8.1.3 Gestión de las alarmas 14](#_Toc531197177)

[8.2 Agente eIDAS 15](#_Toc531197178)

[8.2.1 Gestión de la plataforma Cl@ve 15](#_Toc531197179)

[8.2.2 Gestión del servicio de Cl@ve 15](#_Toc531197180)

[8.2.3 Formato de las peticiones 16](#_Toc531197181)

**ÍNDICE DE FIGURAS**

**No table of figures entries found.**

# Objeto

Es objeto del presente documento especificar y detallar el procedimiento de instalación y configuración del componente Monitoriz@ para la monitorización del Sistema de Identificación Cl@ve, así como las instrucciones para su uso y explotación.

# Alcance

Los objetivos que cubre este documento son los siguientes:

* Describir el proceso de instalación y configuración del componente Monitoriz@ para la monitorización de las plataformas, detallando lo siguiente:
  + Configuración del entorno de despliegue.
  + Configuración del entorno de desarrollo.
  + Tareas adicionales post instalación.
  + Requisitos de instalación.
  + Parámetros de configuración del componente.
* Detallar las instrucciones de uso del componente Monitoriz@ para la monitorización de las plataformas.

# Siglas

|  |  |
| --- | --- |
| **HTTP** | *Hypertext Transfer Protocol* |
| **HTTPS** | *Hypertext Transfer Protocol Secure* |
| **SAML** | *Security Assertion Markup Language* |
| **URL** | Uniform Resource Locator |
| **WAR** | *Web Application Archive* - Archivo de aplicación web |

# Documentos de Referencia

|  |  |
| --- | --- |
| **Manual de Monitoriz@** |  |
| **Analisis\_Requisitos\_sol monitorizacion** |  |
|  |  |

# Introducción

La solución de monitorización del sistema de identificación Cl@ve 2 emplea y se basa en la plataforma Monitoriz@, inicialmente desarrollada para la monitorización del núcleo de la plataforma @firma. De este modo, ha sido necesario ampliar las capacidades de monitorización de Monitoriz@, implementando nuevos agentes de monitorización que permitan la generación y envío de peticiones SAML a los diferentes componentes del Sistema Cl@ve 2 objeto de monitorización, además de su configuración.

Inicialmente las funcionalidades que serán objeto de monitorización son las siguientes:

* Acceso a eIDAS desde pasarela.
* Autenticación mediante certificado electrónico.

# Recursos hardware

## Configuración mínima y recomendada

|  |  |
| --- | --- |
| Requisitos Hardware Mínimos | |
| Procesador | * Número de CPU: 1. * Clock-speed > 2,5GHz. * Arquitectura de 64-bits. |
| RAM | 2 Gb |
| Disco duro disponible | 512Mb |

|  |  |
| --- | --- |
| Requisitos Hardware Recomendados | |
| Procesador | * Número de CPU: 2. * Clock-speed > 2,5GHz. * Arquitectura de 64-bits. |
| RAM | 4 Gb |
| Disco duro disponible | 2 Gb |

## Conectividad

La siguiente tabla recopila los requisitos de comunicación de Monitoriz@.

|  |  |
| --- | --- |
| Requisitos Comunicación | |
| Sistema de Gestión de Base de Datos | Debe poder tener conectividad con el Sistema de Gestión de Base de Datos que aloje la base de datos donde Monitoriz@ persistirá la información de las entidades gestionadas. |
| Pasarela Cl@ve | Debe poder invocar remotamente, mediante HTTP/S, el envío de la petición SAML desde el componente Pasarela que, posteriormente, provoca la redirección a un IdP. |
| IdP @firma | Debe poder invocar remotamente, mediante HTTP/S, el envío de la petición SAML mediante la que se solicita la validación del certificado del ciudadano a la plataforma @firma (IdP Cl@ve). |
| Otros sistemas monitorizados | Debe poder invocar remotamente, mediante HTTP/S, los servicios publicados por otros sistemas monitorizados. |

## Otras Restricciones

Este apartado recopila otras restricciones hardware a satisfacer para la correcta ejecución del componente Proceso Java. Estas son las siguientes:

Uso de almacenes de certificados. En caso de requerir el uso de lectores de tarjetas criptográficas, el equipo o máquina donde se instale el componente proceso Java deberá disponer de los puertos o interfaces exigidos por el lector para el acceso a los certificados.

## Recursos software

### Estructura de la distribución

La distribución binaría del sistema es empaquetada en dos archivos war que presentan la estructura y organización habitual de una aplicación web Java. El primero de ellos, denominado monitoriza-web, implementa XXX. Este tiene las vistas en el directorio WEB-INF/clases/templates. Este incluye las vistas para Clave…

Por su parte, el segundo war, monitoriza-afirma-status-app, incluye la logíca necesaria para la invocación de los diferentes servicios de monitorización….XXX. Este componente incluye los agentes de monitorización de Clave….

### Restricciones técnicas

Las siguientes tablas recogen, por categorías, los requisitos y restricciones sobre el software necesario.

|  |  |
| --- | --- |
| Requisitos Software | |
| JVM | * Java Virtual Machine 1.8.X * Extensión criptográfica no limitada de políticas de seguridad instalada. |
| API’s, librerías y frameworks de terceros | Bouncy Castle v1.46 (provider, KIX/CMS/EAC/PKCS/OCSP/TSP/OPENSSL y SMIME).  SAML Engine  etc |
| Base de datos |  |
| Otros |  |

# Instalación y configuración del software

## Despliegue del modelo de datos

XXX

## Compilación y generación de binarios

Tal y como se ha comentado anteriormente, la solución de monitorización de Cl@ve está basada en Monitoriz@. Sin embargo, ha sido necesario una serie de adaptaciones sobre este sistema de forma que se integre y pueda invocar la lógica necesaria para monitorizar Cl@ve. Esta lógica se encuentra agrupada en los siguientes módulos del sistema:

* **monitoriza-clave-status-app**. Componente jar que implementa el agente de monitorización de Cl@ve, aportando al sistema la capacidad de poder efectuar peticiones HTTP que incorporen una petición SAML como parámetro (AuthnRequest), y, opcionalmente, aportar un certificado electrónico de usuario a la misma, empleado al establecer el canal seguro de comunicación. Es integrado en el war monitoriza-afirma-status-app.
* **monitoriza-clave-web**. Componente web que incorpora a Monitoriz@ las interfaces de usuario necesaria para la definición y configuración de plataformas tipo “Cl@ve”.

La gestión, compilación y construcción del sistema se lleva a cabo mediante Maven, siendo su organización la habitual de un proyecto Java Web Maven (v3.x), donde se establece un proyecto padre que agrupa y define configuración, recursos, plugins y dependencias comunes.

No obstante, previo a la compilación y generación de los binarios, es necesario instalar en el repositorio local Maven, o en un gestor de repositorio Maven corporativo (por ejemplo, Artifactory), los artefactos cuyas dependencias no pueden ser resueltas automáticamente (distribuidos junto a fuentes y binarios del componente). Estos son los siguientes:

ENUMERAR DEPENDENCIAS

## Configuración del entorno de ejecución

La configuración del sistema será efectuada en base a archivos de propiedades y archivos XML, algunos de ellos requeridos por el propio componente y otros por las diferentes API’s, librerías y frameworks empleados por el proceso.

A continuación, se enumerarán aquellos archivos nuevos incorporados a Monitoriz@ por el agente de monitorización de Cl@ve, o aquellos que requieren algún tipo de modificación para el correcto funcionamiento del agente. Consultar la documentación de Monitoriz@ para conocer en más detalle los archivos globales del sistema.

### Parámetros JVM

Directorio bin:

Ilustración 3 Configuración de tomcat

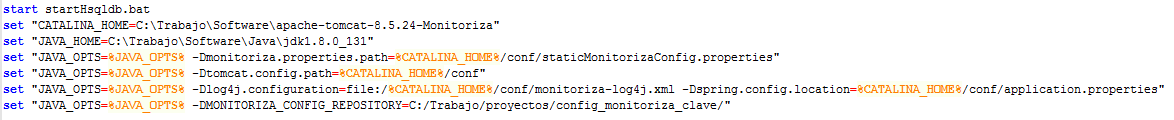
* Catalina.bat/.sh: Es el archivo de ejecución para el despliegue de la herramienta.

Ilustración 4 Configuración de catalina

* startHsqldb.bat: Archivo de creación de la base de datos.

Directorio conf:

* **application.properties:** Contiene la configuración de conexión con la base de datos, propiedades de thymeleaf, los directorios de lenguaje multiidioma, etc.
* **Monitoriza-log4j.xml:** Configuración de log4j.
* **staticMonitorizaConfig.properties:** Contiene las propiedades estáticas de la herramienta Monitoriz@.
* **Catalina.properties:**
* **Directorio certificate:** Certificado SSL utilizado en el cliente monitoriz@.
* **Directorio database:** Contiene propiedades de la configuración de la base de datos HsqlDB.
* **Directorio messages:** Contiene los message del multiidioma.

Directorio lib:

Contiene las librerías que la herramienta de despliegue necesita para el despliegue de la herramienta Monitoriz@, en nuestro caso el fichero jar de la base de datos.

### Configuración componente SAMLEngine

Se encuentran los parámetros de la petición SAML. Todos estos parámetros son heredados de la herramienta de cl@ve, el único fichero que debemos tener en cuenta es:

* **SignModule\_Monitoriza.xml:** Se encuentran los parámetros de la petición SAML, estos son los atributos estáticos definidos en la petición.
  + **check\_certificate\_validity\_period:** Validación del periodo del certificado.
  + **disallow\_self\_signed\_certificate:** Rechazar certificado autofirmado.
  + **signature.algorithm:** Firma del algoritmo.
  + **signature.algorithm.whitelist:** Lista de algoritmos de firma entrantes de la lista blanca separados por ;.
  + **response.sign.assertions:** Afirmaciones de signo de respuesta.
  + **keyStorePath:** Ruta del almacén de certificados.
  + **keyStorePassword:** Contraseña del almacén de certificados.
  + **keyPassword:** Clave del almacén de certificados.
  + **Issuer:** Editor.
  + **serialNumber:** Número de serie.
  + **keyStoreType:** Tipo del almacén de certificados.

# Monitorización plataforma Cl@ve

## Actuaciones previas

### Gestión de los correos para las alarmas

Se procede a dar de alta los correos necesarios para las notificaciones realizadas por las alarmas.

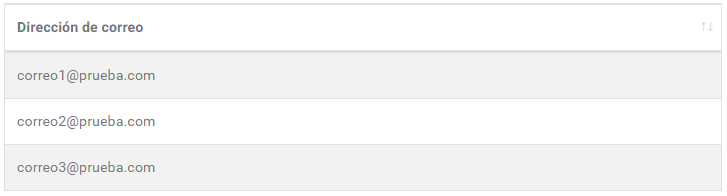
* **Dirección de correo:** Inserción del correo electrónico. En este caso, se van a añadir una serie de correos electrónicos de prueba.

Ilustración 5 Listado de correos electrónicos

### Gestión del temporizador

Se procede a dar de alta el temporizador o el tiempo transcurrido entre una petición del servicio y la siguiente.

* **Nombre:** Se indica el nombre identificativo del temporizador.
* **Frecuencia:** Se establece en formato HH:mm:ss la frecuencia de repetición del servicio.

Ilustración 6 Listado de temporizadores

### Gestión de las alarmas

Se procede a dar de alta la alarma que se produce en el caso de haber alguna incidencia en los servicios que posteriormente se van a crear, estas alarmas envían a los correos añadidos la incidencia ocurrida en el transcurso de la operación.

* **Nombre:** Se indica un nombre identificativo de la alarma a añadir.
* **Tiempo de bloqueo:** Tiempo en el que se almacenan las alarmas producidas en ese transcurso.
* **Correos degradados:** Correos a los que se enviaran las notificaciones en el caso de producirse una degradación del servicio (aumento del tiempo de degradado, el cual se establecerá en el servicio).
* **Correos caídas:** Correos a los que se enviaran las notificaciones en el caso de producirse una caída del servicio.

Ilustración 7 Formulario Alarmas

## Agente eIDAS

### Gestión de la plataforma Cl@ve

Procedemos a dar de alta la plataforma perteneciente al agente de monitorización de Cl@ve.

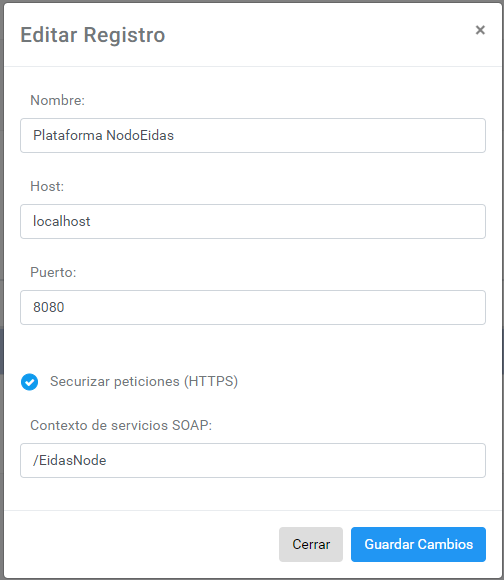
* **Nombre:** Se indica el nombre de la plataforma de Cl@ve, no es significativo.
* **Host:** Se indica el host de la plataforma de Cl@ve, en este caso se le indica “localhost” debido a que nos encontramos en el entorno de desarrollo local.
* **Puerto:** Se indica el puerto de la plataforma Cl@ve, en este caso se le indica el puerto en el que se encuentra desplegado mediante Wildfly.
* **Securizar peticiones(HTTPS):** En el caso de las peticiones a través de eIDAS siempre se realizaran mediante HTTPS, por lo que se marca la opción.
* **Contexto de servicios HTTP:** Se indica el contexto en el que se encuentra el agente a monitorizar.

Ilustración 8 Formulario Plataforma eIDAS

### Gestión del servicio de Cl@ve

Se procede a dar de alta el servicio que realizara la monitorización del agente de eIDAS.

* **Nombre:** Se indica el nombre que tendrá el servicio.
* **Plataforma:** Identifica la plataforma a la que se va a conectar el servicio. Se selecciona la plataforma creada anteriormente.
* **Tipo de Servicio:** Identifica el tipo de servicio según la plataforma seleccionada, en este caso solo tenemos un tipo de contexto que es HTTP.
* **Endpoint:** Punto de la dirección URL en el que se encuentra el agente de monitorización de eIDAS.
* **Timeout:** Tiempo de conexión del servicio.
* **Timer:** Identifica el temporizador con el que se va a controlar el servicio. Se selecciona un temporizador creado anteriormente.
* **Umbral degradado (milisegundos):** Establece el tiempo en milisegundos el umbral máximo del tiempo de la petición del servicio.
* **Umbral perdido (%):** Establece el porcentaje máximo de peticiones perdidas de la petición de servicio.
* **Alarma:** Identifica la alarma que saltara en el caso de producirse un problema en la petición de servicio. Se selecciona una alarma creada anteriormente.
* **Archivo de peticiones en formato ZIP:** Se establece el archivo ZIP que contiene la petición XML del servicio.

### Formato de las peticiones

El agente para la monitorización de Cl@ve 2 desarrollado requiere el envío de peticiones HTTP que incorporen un parámetro, denominado SAMLRequest, que informe una petición SAML. Esta petición SAML debe ser generada dinámicamente, en tiempo real, por lo que las peticiones de los servicios de monitorización para Cl@ve no se corresponderán con peticiones SAML precargadas, sino con un archivo, con formato XML, que configure ciertos aspectos, tanto de la construcción y envío de la petición HTTP, como de la generación de la generación SAML.

La estructura de este archivo puede observarse mediante el siguiente archivo XML:

|  |
| --- |
| <?xml version="1.0" encoding="UTF-8"?>  <mcl:ClaveAgentConf  xmlns:mcl="urn:es:gob:monitoriza:invoker:http:conf:messages:1.0.0"  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"  xsi:schemaLocation="urn:es:gob:monitoriza:invoker:http:conf:messages:1.0.0 generationRequestClaveTypes.xsd ">  <mcl:connection>  <mcl:proxy>  <mcl:host>localhost</mcl:host>  <mcl:port>8888</mcl:port>  <mcl:user>usuario</mcl:user>  <mcl:password>12345</mcl:password>  </mcl:proxy>  <mcl:authenticationMutual>  <mcl:passwordKeyStore>G5cp,fYC9gje</mcl:passwordKeyStore>  <mcl:typeKeyStore>jks</mcl:typeKeyStore>  <mcl:path>C:\\Trabajo\\Software\\CertificadosPruebas\\PF\_ACTIVO\_EIDAS.p12</mcl:path>  </mcl:authenticationMutual>  </mcl:connection>  <mcl:request>  <mcl:httpRequest>  <mcl:headers>  <mcl:param>  <mcl:id>parametroH1</mcl:id>  <mcl:value>valorH1</mcl:value>  </mcl:param>  <mcl:param>  <mcl:id>parametroH2</mcl:id>  <mcl:value>valorH2</mcl:value>  </mcl:param>  </mcl:headers>  <mcl:params>  <mcl:param>  <mcl:id>parametro1</mcl:id>  <mcl:value>valor1</mcl:value>  </mcl:param>  <mcl:param>  <mcl:id>parametro2</mcl:id>  <mcl:value>valor2</mcl:value>  </mcl:param>  </mcl:params>  </mcl:httpRequest>  <mcl:samlRequest>  <mcl:assertionConsumerServiceURL>http://localhost:8080/Proxy2/ServiceProvider</mcl:assertionConsumerServiceURL>  <mcl:SPApplication>SPApp</mcl:SPApplication>  <mcl:providerName>DEMO-SP\_NIF</mcl:providerName>  <mcl:SPType>public</mcl:SPType>  <mcl:attributes>  <mcl:attribute>familyName</mcl:attribute>  </mcl:attributes>  </mcl:samlRequest>  </mcl:request>  </mcl:ClaveAgentConf> |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Nombre | Tipo | Padre | Campo obligatorio | Descripción |
| claveAgentConf | String | **-** | Si | Petición hacia la pasarela de cl@ve. |
| connection | **ConnectionType** | **claveAgentConf** | No | Configuración de la conexión de la petición. Opcional. |
| request | **RequestType** | **claveAgentConf** | No | Configuración de la petición. Opcional. |
|  | | | | |
| proxy | **ProxyConfType** | **connection** | No | Configuración del proxy. Opcional. |
| authenticationMutual | **authenticationMutualType** | **connection** | No | Configuración de la autenticación mutua. Opcional. |
|  | | | | |
| host | String | **proxy** | Si | Identificador del host. |
| port | String | **proxy** | Si | Identificador del puerto. |
| user | String | **proxy** | Si | Identificador del usuario. |
| password | String | **proxy** | Si | Identificador de la contraseña. |
|  | | | | |
| path | String | **authenticationMutual** | No | Dirección del almacenamiento de las claves. Opcional. |
| base64 | String | **authenticationMutual** | No | Base64 del almacenamiento de las claves. Opcional. |
| passwordKeystore | String | **authenticationMutual** | Si | Contraseña del almacenamiento de las claves. |
| typeKeystore | String | **authenticationMutual** | Si | Tipo del almacenamiento de las claves. |
|  | | | | |
| httpRequest | **httpRequestType** | **request** | No | Configuración de la peticion http. Opcional. |
| samlRequest | **samlRequestType** | **request** | Sí | Configuración de la petición Saml encapsulada en la patición HTTP. |
|  | | | | |
| headers | **ParamsType** | **httpRequest** | No | Configuración de los otros parámetros. Opcional. |
| params | **ParamsType** | **httpRequest** | No | Configuración de los otros parámetros. Opcional. |
|  | | | | |
| param | **paramsType** | **headers** | Si | Un parámetros de la relación de parámetros. |
|  | | | | |
| id | String | **param** | Si | Identificador del parámetro. |
| value | String | **param** | Si | Valor del parámetro. |
|  | | | | |
| assertionConsumerServiceURL | String | **samlRequest** | Si | Dirección del servicio de confianza de la petición Saml. |
| SPApplication | String | **samlRequest** | Si | Dirección destino de la petición Saml. |
| providerName | String | **samlRequest** | Si | Nombre del proveedor de la petición Saml. |
| SPType | **SPRequestType** | **samlRequest** | No | Tipo del proveedor del servicio de la petición Saml. |
| attributes | **AttributesType** | **samlRequest** | No | Listado de atributos. |
|  | | | | |
| attribute | **AttributeType** | **attributes** | Si | Un atributo de la relación de atributos. |
|  | | | | |
| SPRequestType | public, private | | | |
| AttributeType | familyName, firstName, dateOfBirth, personIdentifier, legalName, legalPersonIdentifier | | | |

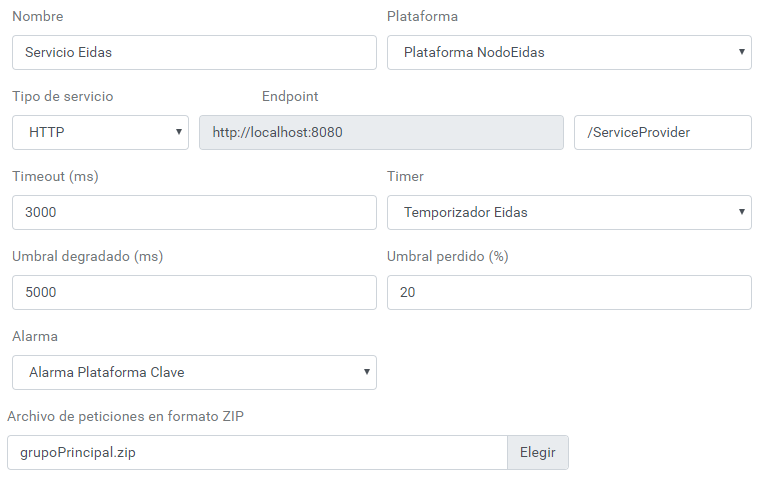


Ilustración 9 Formulario Servicio eIDAS