HEINSOHN
BUSINESS TECHNOLOGY

ASOFONDOS

ASOFONDOS
Instructivo de uso de API de Seguridad

Contenido

1. Alcance

En el presente documento explica el modelo de seguridad definido para interactuar con nuestros servicios web:

2. Términos y Definiciones

Los parámetros POST en esta solicitud son explicados a continuación:

grant_type= en el llamado al servidor usamos el tipo password grant. Es decir, se debe incluir en este parámetro el valor "password".

client_id= es el identificador público de la aplicación o sistema que está realizando el consumo del servicio de token.

client_secret= para aplicaciones o sistemas externos es requerido que envíe una llave de seguridad asignada previamente (mecanismo definido y no explicado en este documento).

username= (opcional) En caso que existan usuarios con diferentes niveles de acceso, se solicitará el envío del usuario específico para acceder al recurso.

password=(opcional) contraseña asociada al username.

3. Esquema de seguridad para acceder a recursos del Sistema

Como esquema de seguridad para el acceso a estos servicios se usará un mecanismo de consulta de token y posteriomente en el servicio de negocio (recurso) se deberá incluir dicho token en las cabeceras de petición y será válido durante el tiempo de la vigencia definida para acceder al recurso (por default está en 5 minutos pero puede ser parametrizado). El API de Token se encuentra expuesto como parte del api del Sistema de los fondos de pensiones en la siguientes URL:

Pre-Producción
https://pre.sistema.com.co/api/sistema/oauth/token/v1 ¨* Son de ejemplo y no existen en este momento
Producción
https://sistema.proveedor.com.co/api/sistema/oauth/token/v1 * Son de ejemplo y no existen en este momento

3.1Campos de entrada al servicio generación de token

En el presente numeral se detallan los campos de entrada del servicio de generación de token, estos campos deben ser enviados como cabecera de la petición:

Nombre del campo en el header	Descripción del campo	Tipo de Dato	Longitud	Restricciones	Obligatorio
grant_type	Solo se debe incluir la palabra password en su valor.	String	15		S
client_id	Identificador de la entidad cliente entregado previamente.	String	10		S
client_secret	Clave de aplicación del	String	20		S

	cliente que consume los servicios. Asignada previamente.				
username	Usuario de servicio para la autenticación	String	15		S
password	Clave asociada al usuario de servicio	String	20		N

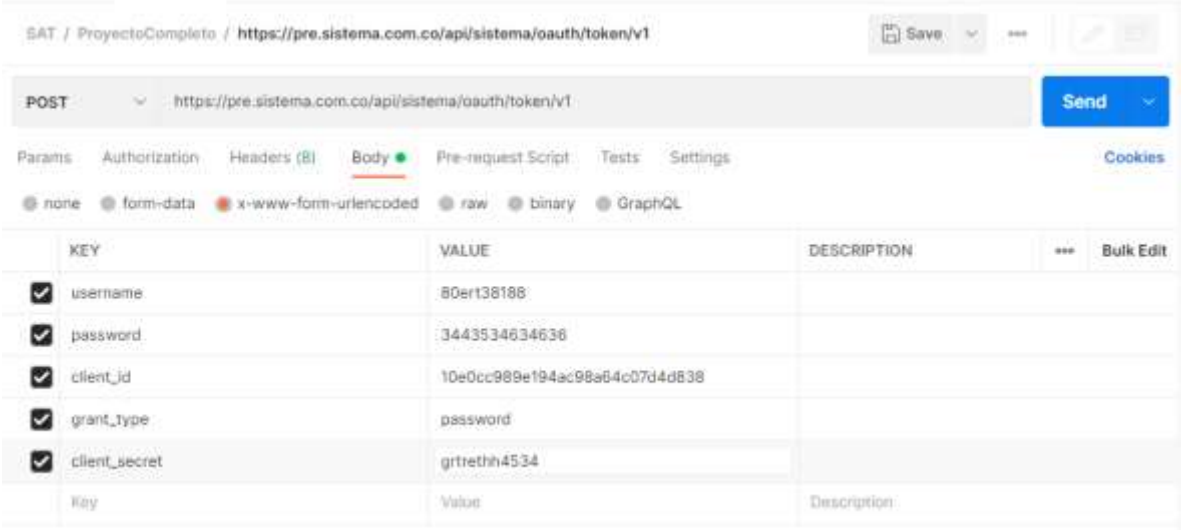
3.2Campos de salida al servicio generación de token

En el presente numeral se detallan los campos de entrada del servicio de generación de token:

Nombre del campo en el header	**Descripción del campo**	**Tipo de Dato**	**Longitud**	**Restricciones**	**Obligatorio**
access_token	Token de acceso	String	128	Solo se retorna cuando la autenticación es correcta	N
token_type	Tipo de token entregado	String	15	Solo se retorna cuando la autenticación es correcta corresponde al tipo de token entregado	N
expires	Timestamp del tiempo de expiración del token	String	30	Solo se retorna cuando la autenticación es correcta. Fecha de expiración en formato “yyyy-MM-dd'T'HH:mm:ss.SSSXXX” con zona horaria "America/Bogota" Ej: "2021-09-21T09:57:12.481-05:00"	N
error	Error presentado	String	25	Este campo solo se entrega cuando se genera error en la autenticación este error puede ser de credenciales (grant-error), o error interno (internal-error).	N
error_description	Descripcion del error	String	200	Este campo se entrega cuando el camp error no viene vacío con la descripción del error.	N

3.3Ejemplo consumo del servicio generación de token

Este recurso provee una interface REST para el intercambio de información en formato JSON con operaciones POST, su definición técnica en Open API 3.0.1 se encuentra en el archivo anexo “openapi.yaml”, a continuación, se muestra un ejemplo de un request y response usando la herramienta postman:



3.4Configuración de cabeceras de seguridad en la petición de reporte al SAT

En seguida se incluye un ejemplo de la cabecera especifica para la parametrizacion de seguridad que requiere ser incluida en el request de las operaciones de reporte al servicio de negocio (recurso) que se quiera acceder:

4. Historia de Cambios

.

Fecha	Versión	Descripción	Autor
10/08/2021	1.0	Versión Inicial	XXXX XXX

5. Aprobaciones

Fecha	Nombre	Firma
<ddmmaa>	<Nombre revisor>	

6. Bibliografía de referencia

https://www.oauth.com/oauth2-servers/map-oauth-2-0-specs/