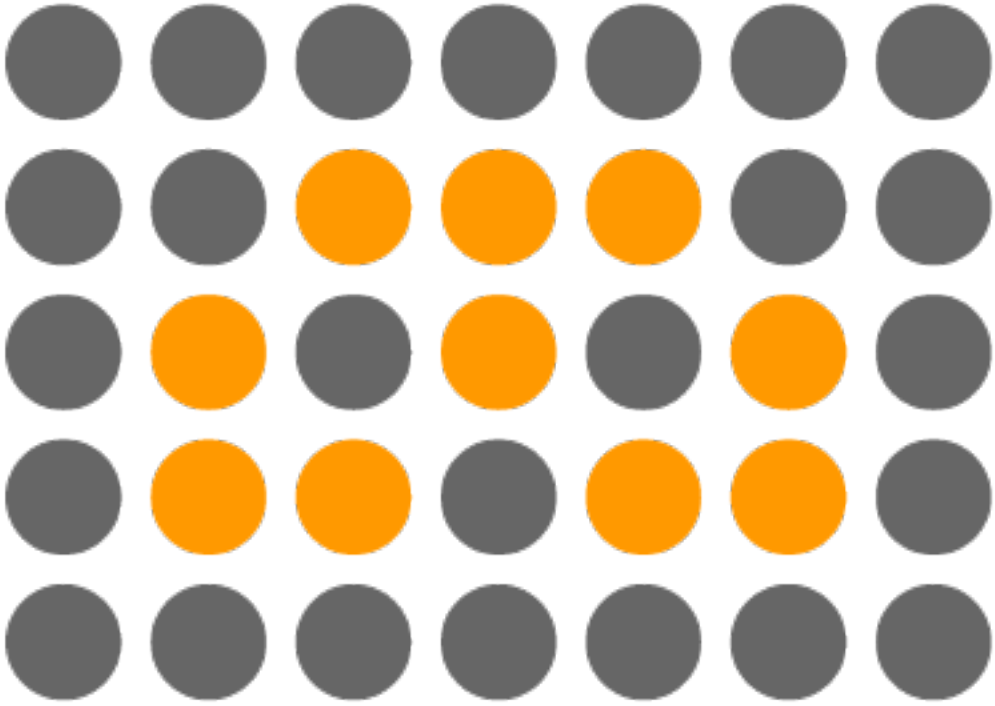

SERVICIO DE

2FA (AUTENTICACIÓN DE DOS FACTORES)

Y

OTP (TOKEN DE UN SOLO USO)

HTTPS/API

Versión: 1.2
Última Actualización: 5/05/2017
Uso: Público

INDICE

Contenido

API HTTP/s SERVICIO DE 2FA y OTP

1.--- INTRODUCCIÓN

API de integración de servicios de autenticación mediante envío de token por SMS y/o VOZ.

Mediante este sistema se consigue la comunicación desde servidores y/o aplicaciones externas a los servidores de MENSATEK utilizando el protocolo HTTP ó HTTPs para los servicios de 2FA (Two Factor Authentication) y OTP (One time password) para aumentar la seguridad de acceso y validación de usuarios. El proceso básico de comunicación es el siguiente: MENSATEK recibe la petición GET o POST del servidor externo según los parámetros especificados a continuación y procesa la petición.

2.--- COMPATIBILIDAD Y VERSIONES

Versión 1.0 – 1.2: Última actualización 2017. Se recomienda la actualización a versión 1.2.

3.--- SERVIDORES PARA PETICIONES

Las peticiones se pueden realizar por HTTP o HTTPs (conexión segura) y los parámetros pueden ser enviados en peticiones GET o POST.

Datos peticiones HTTP:

Servidor: **http://api.mensatek.com/v5/** (para puerto 80 –puerto HTTP por defecto-)
Servidor **http://api.mensatek.com:3377/v5/** (para puerto 3377)
Puerto: 80 ó 3377 (utilice 3377 si piensa que puede conectarse a través de proxies).

Datos peticiones HTTPs (seguras):

Servidor: **https://api.mensatek.com/v5/** (para puerto 443 -SSL por defecto-)
Servidor **https://api.mensatek.com:3378/v5/** (para puerto 3378)
Puerto: 443 ó 3378 (utilice 3378 si piensa que puede conectarse a través de proxies).

4.--- DATOS IMPORTANTES A TENER EN CUENTA

Conexiones en vacío:

Es importante tener en cuenta que una conexión errónea de forma repetida será tratada por el sistema como spam y podrá llegar a bloquear temporalmente la conexión.

Es conveniente evitar realizar repetidas conexiones con datos erróneos o conexiones rápidas 'en vacío' (sin realizar envíos) con los mismos datos.

Método GET o POST:

GET: (cambiar función.php por la función que se desee –ver más abajo las funciones-)
http://api.mensatek.com/v5/funcion.php?Correo=tucorreoregistrado@tudominio.com&Passwd=TuPContraseña&Variables=.....

Si las peticiones se realizan en el método GET (ver nota posterior), es importante realizar un UrlEncode a todos los parámetros:

Es conveniente codificar las peticiones url, por ejemplo:

- En php:

  "?Correo=".urlencode(Correo)."&Passwd=".urlencode(Passwd).

- En java:

  "?Correo="+URLEncoder.encode(Correo)+"&Passwd="+URLEncoder.encode(Passwd)

- Etc…

POST: (cambiar función.php por la función que sea –ver más abajo las funciones-)

/v5/funcion.php
HTTP/1.1
Host: api.mensatek.com
Correo=tucorreoregistrado@tudominio.com&Passwd=TuPContraseña&Variables=.....

Es conveniente utilizar método POST en cualquiera de estas opciones:

1. Si estima que la longitud de mensaje más variables incluidas en la petición supera los 2048 caracteres. Las peticiones GET, por estándar, tienen limitación de 2048 caracteres como máximo.
2. Si las peticiones son seguras ya que con el método GET las variables incluidas en la petición no quedan encriptadas.
3. En general, recomendamos utilizar el método POST.

Si utiliza método POST: En este método se codifican automáticamente las peticiones por lo que no necesita funciones urlencode pero debe asegurarse de que utiliza un set de caracteres utf8. La forma de conocer si está utilizando codificación/set de caracteres correcto es enviar mensajes con caracteres especiales como ñ o el carácter €, si aparecen correctamente en el móvil destino, está utilizando la codificación correcta. En caso contrario, tiene dos soluciones sencillas:

1.- Utilizar funciones utf8_encode en cada parámetro enviado.

2.- Guardar el fichero de su script o aplicación en formato utf8 (la mayoría de los editores permiten ‘guardar con codificación ‘utf8’).

Respuesta de las peticiones:

La mayoría de las funciones disponen de un parámetro denominado 'Resp'. Este parámetro define el formato de la respuesta que se devolverá. Puede ser TXT, JSON, XML o no definido.

Se recomienda siempre definir este parámetro ya que todas las funciones, por compatibilidad con versiones anteriores de la API, responden por defecto (si no se define este parámetro) tal y como lo hacían en versiones antiguas. En estos resultados de versiones de API anteriores se obvian algunas de las variables que se incluyen en esta versión de la API y que consideramos importantes para facilitar la integración e información de la cuenta.

En los ejemplos incluidos siempre se tiene en cuenta que ha definido el parámetro. Si está trabajando directamente con versiones de la API posteriores a 2016, asumiremos que ha definido el parámetro en todas las peticiones.

5.--- FUNCIONAMIENTO NORMAL DEL SERVICIO

OTP. ONE TIME PASSWORD:

1.- La aplicación/web solicita un móvil o fijo al usuario para validar una operación (transferencia, firma, consentimiento, etc…

2.- La aplicación o web realiza una petición a la función 'Envío de OTP' en Mensatek

3.- La aplicación o web solicita al usuario que introduzca el token/PIN recibido en su móvil o fijo especificado

4.- La aplicación o web realiza una petición a la función 'Validar OTP' en Mensatek

5.- Si el resultado es correcto, el proceso se ha validado.

2FA. AUTENTICACIÓN DE DOS FACTORES:

Normalmente, en el registro, se valida mediante OTP (funcionamiento previsto anteriormente) un móvil o fijo que queda guardado en la base de datos de usuarios registrados junto a los datos del usuario.

A partir de entonces, en cada autenticación/acceso del usuario o en cada validación de operaciones (por ejemplo transferencias en un banco):

1.- La aplicación/web solicita autentica al usuario tal y como se hace normalmente (usuario / contraseña).

2.- Si la autenticación es correcta (o cuando se vaya a autorizar una operación) La aplicación o web

realiza una petición a la función ‘Envío de OTP’ en Mensatek

3.- La aplicación o web solicita al usuario que introduzca el token/PIN recibido en su móvil o fijo especificado

4.- La aplicación o web realiza una petición a la función ‘Validar OTP’ en Mensatek

5.- Si el resultado es correcto, el proceso se ha validado.

6.--- FUNCIONES

6.1.- ENVÍO DE OTP

Objetivo:

Envío de OTP.

Petición a:

https://api.mensatek.com/v5/peticionotp.php

Parámetros GET o POST:

- Correo: String con el correo del usuario que envía (en MENSATEK).
- Passwd: String con la contraseña del usuario que envía (en MENSATEK).
- Destinatario: (String) Móvil o Fijo al que se envía la OTP, de la forma PrefijoTelefono (Ej:346000000)
- AppId: (integer Opcional) Es el identificador de la Aplicación que envía la petición. Le permite identificar y validar los mismos teléfonos en distintas aplicaciones desde un mismo usuario.
- Mensaje: (String Opcional) Mensaje que se envía. Debe contener el string [CODE] que será sustituido por el código generado. (muy recomendado utilizar funciones urlencode en caso de peticiones GET). Si no se especifica, se envía uno por defecto.
- Remitente: (String Opcional) Es el teléfono, nombre de la empresa o persona que envía. ATENCIÓN: Si es alfanumérico el Máximo es de 11 caracteres.
- Long: (Integer opcional) Longitud del código a enviar. Por defecto 4. Este valor debe estar comprendido entre 3 y 10.
- Tipo: (Integer opcional). Valor entre 1 y 4. Significado de valores:

- 1 (por defecto): Código sólo números
- 2: Sólo letras (mayúsculas)
- 3: Letras mayúsculas y números
- 4: Letras mayúsculas, minúsculas y números.

- MaxIntentos: (Integer opcional). Número de intentos fallidos antes de invalidar el código. Por defecto 3 (0=ilimitados).

- Validez: (integer opcional) Tiempo en segundos en los que el código es válido y puede validarse. Por ejemplo 3600 para una hora, 1800 para 30 minutos, 24horasx60minutosx60segundos=86400 para un día, etc… Por defecto 3600 (una hora).

- ValidarDestino: (integer opcional)

  - 0: No validar
  - 1: Validar el número y enviar sólo si el móvil o teléfono es válido, no está dado de baja y está operativo en ese momento. En caso contrario, notificar el motivo para que el usuario revise y escriba el número correcto (Debe solicitar la activación de esta opción en su cuenta a soporte antes de utilizarlo).

- Fail2Voice: (integer opcional) 0 por defecto, si se activa (valor 1) se validarán los fijos por voz. El destinatario recibirá una llamada de voz con una locución con el código generado.

- Unicode: (integer opcional)
  - 0: (por defecto) Alfabeto GSM3.38 (ver apéndice para caracteres incluidos)
  - 1: Unicode. Se puede utilizar cualquier idioma o carácter en los mensajes.

- Resp: (String) Tipo de respuesta a mostrar.

  Posibles valores:

  - TXT: salida texto. Ejemplo:

```
Res:1;
id:12;
Cred:12345.67;
```

  - JSON: Respuesta en formato json. Ejemplo:

```
{
      "Res":1,
      "Id":27,
      "Cred":19808.45,
}
```

- XML: Respuesta en formato XML. Ejemplo:

```
<?xml version="1.0"?>
<result>
 <Res>1</Res>
 <Id>12</Id>
 <Cred>12345.67</Cred>
</result>
```

Respuesta:

DEVUELVE: string de la respuesta de la página:

- Res:Número

Significado del Número:

1 correcto, Token enviado.

-1 Error de autenticación

-2 No hay créditos suficientes.

-3 No ha enviado un teléfono/móvil en la llamada.

-4 El remitente debe ser de, al menos, 3 caracteres

-5 Debe incluir la plantilla del mensaje a enviar con el código y éste debe incluir [CODE] que será sustituido en el mensaje final por el PIN/OTP de validación.

-6 El tipo debe ser 1 (sólo números), 2 (sólo letras), 3 (Letras mayúsculas y números) ó 4 (letras mayúsculas, minúsculas y números)

-7 La longitud del código a generar debe estar entre 3 y 10 caracteres

-8 El destinatario no es válido

-9 El destinatario no está disponible (apagado o fuera de cobertura)

-10 El destinatario no existe (dado de baja)

-11 El destino es un fijo, para enviar y validar el código debe utilizar el parámetro Fail2Voice=1

-12 No ha podido enviarse el mensaje. Contacte con soporte.

-13 El número máximo de intentos debe ser 0 (ilimitado) o un número menor que 10.

-14 Error en el envío, contacte con soporte

-15 La validez debe estar entre 5 minutos (valor 5minutosx60segundos=300) y 72 horas (valor 72horasx60minutosx60 segundos=259200)

- Id:identificador

Significado del identificador:

Se refiere a un identificador (numérico o string) de la petición sobre un mismo código de APP.

- Cred:Número (Float) de créditos restantes del usuario en MENSATEK.

6.2.- *VALIDAR OTP*

Objetivo:

Validar el token introducido por el usuario.

Petición a:

https://api.ensatek.com/v5/validarotp.php

Parámetros GET o POST:

- Correo: String con el correo del usuario que envía (en MENSATEK).
- Passwd: String con la contraseña del usuario que envía (en MENSATEK).
- Destinatario: String Móvil o fijo al que se refiere la petición en formato PREFIJONúmero. Por ejemplo 34600000000
- AppId: (Integer opcional) Identificador de la aplicación a la que se refiere la petición.
- Codigo: (String) Con el Token introducido por el usuario y que debemos validar.
- Resp: (String) Tipo de respuesta a mostrar.

  Posibles valores:

  - TXT: salida texto. Ejemplo:

    ```
    Res:1;
    ```

  - JSON: Respuesta en formato json. Ejemplo:

    ```
    {"Res":"1"}
    ```

  - XML: Respuesta en formato XML. Ejemplo:

    ```
    <?xml version="1.0"?>
    <result>
     <Res>1</Res>
    </result>
    ```

DEVUELVE: string de la respuesta de la página:

- Res:Número con el resultado

  Significado del Número:

  1 Validación correcta (Token válido para la appId). Se incluyen en la respuesta, adicionalmente, dos parámetros:

  - FechaValidado: Fecha en formato YY-MM-DD HH:mm:ss en que se ha producido la validación
  - Intentos: Intentos realizados hasta validación.

  -1 Error de autenticación

  -2 No existe una petición con estos datos.

  -3 No ha especificado el móvil/fijo en Destinatario

  -4 La validez del código ha expirado.

  -5 Código ya validado. Se incluye Fecha de validación en la respuesta (parámetro Fecha adicional en la respuesta)

  - *Fecha: Fecha en la que el código fue validado.*

  -6 Número máximo de intentos fallidos superados (se ha intentado validar erróneamente más veces de las indicadas en MaxIntentos en la petición a la función peticionotp.

  -7 El token debe tener entre 3 y 10 caracteres de longitud

  -8 Código incorrecto/Validación incorrecta.

  -9 Destinatario incorrecto.

6.3.- OBTENCIÓN DE REPORT DE PETICIONES OTP

Objetivo:

Obtención de report del listado de peticiones realizadas en un periodo dado.

Petición a:

https://api.mensatek.com/v5/reportotp.php

Parámetros GET o POST:

- Correo: (String) con el correo del usuario que envía (en MENSATEK).
- Passwd: (String) con la contraseña del usuario que envía (en MENSATEK).
- FechaDesde: (String opcional) Formato YY-MM-DD HH:mm Fecha de inicio del report. Si no se especifica el rango de fechas se ajusta al mes anterior.
- FechaHasta: (String opcional) Formato YY-MM-DD HH:mm Fecha de fin del report. Debe especificarse un rango inferior a un mes. Si no se especifica se ajusta a un mes posterior a la fecha especificada en FechaDesde.
- App: (integer opcional) Identificador de la aplicación. Por defecto 0.
- Formato: (string opcional) Formato en el que se descarga el report. Posibles valores.
    - CSV (por defecto)
    - EXCEL
- Resp: (String) Tipo de respuesta a mostrar en caso de que exista algún error. Posibles valores:
    - TXT: salida texto. Ejemplo:

```
Res: -1;
```

    - JSON: Respuesta en formato json. Ejemplo:

```
{"Res":"-1"}
```

- XML: Respuesta en formato XML. Ejemplo:

```
<?xml version="1.0"?>
<result>
        <Res>-1</Res>
</result>
```

Respuesta:

Sin errores: Descarga de fichero CSV o EXCEL (según se especifique):

Contenido:

Listado de peticiones OTP y resultados.

Errores:

- -1: Error de Usuario/contraseña
- -2: Error en los parámetros enviados
- -3: No tiene permiso
- -4: FechaHasta debe ser mayor que FechaDesde y el rango máximo debe ser un mes.

ANEXO 1. CARACTERES

Los caracteres permitidos en el mensaje son los incluidos en el estándar GSM 3.38. Debe tener en cuenta que el € ocupa dos caracteres (se envía como combinación de dos) y que los acentos cerrados no están en el estándar (excepto el de la é) por lo que, si se incluyen, se cambiarán por el carácter más similar.

Los caracteres admitidos en el estándar se incluyen en la tabla inferior, los de la tabla de extensión ocupan dos caracteres y los de la primera (Básica) ocupan 1 carácter.

Para el remitente le aconsejamos:

1.- Sólo números (un móvil o fijo en formato internacional, p.e. +34600000000) hasta 15 números
2.- Sólo letras y números y carácter subrayado hasta 11 caracteres. P.e. MiRemitente

Set de caracteres Básico (ocupan 1 carácter)

	0x00	0x10	0x20	0x30	0x40	0x50	0x60	0x70
0x00	@	Δ	SP	0	¡	P	¿	p
0x01	£	_	!	1	A	Q	a	q
0x02	$	Φ	"	2	B	R	b	r
0x03	¥	Γ	#	3	C	S	c	s
0x04	è	Λ	¤	4	D	T	d	t
0x05	é	Ω	%	5	E	U	e	u
0x06	ù	Π	&	6	F	V	f	v
0x07	ì	Ψ	'	7	G	W	g	w
0x08	ò	Σ	(	8	H	X	h	x
0x09	Ç	Θ	)	9	I	Y	i	y
0x0A	LF	Ξ	*	:	J	Z	j	z
0x0B	Ø	ESC	+	;	K	Ä	k	ä
0x0C	ø	Æ	¸	<	L	Ö	l	ö
0x0D	CR	æ	-	=	M	Ñ	m	ñ
0x0E	Å	ß	.	>	N	Ü	n	ü
0x0F	å	É	/	?	O	§	o	à

Tabla de Extensión de caracteres.(ocupan 2 caracteres)

	0x00	0x10	0x20	0x30	0x40	0x50	0x60	0x70
0x00					|			
0x01								
0x02								
0x03								
0x04		^						
0x05							€	
0x06								
0x07								
0x08			{					
0x09			}					
0x0A	FF							
0x0B		SS2						
0x0C				[				
0x0D	CR2			~				
0x0E				]				
0x0F			\					