Guía técnica de un proceso de validación OTP por SMS

Ref. 20110901 - Guía y recomendaciones

9 de noviembre de 2020 v1.2

Índice

info@labsmobile.com

1 Introducción

En este documento se describen las recomendaciones y buenas prácticas en una integración con la plataforma SMS de LabsMobile para un uso de proceso de validación con códigos OTP vía SMS.

Este tipo de proceso de validación y verificación se identifica como un uso frecuente por las características inherentes a este métodos de comunicación: inmediatez, universalidad, identificable.

La validación OTP se puede aplicar a multitud de entornos y tipos de software como aplicaciones móviles, redes sociales, plataformas web, transacciones económicas, etc.

A continuación se presenta una serie de consejos, protocolos y diferentes técnicas que se han observado recomendables y beneficiosas en numerosas integraciones de este tipo de procesos.

1.1 Proceso de validación OTP SMS

En los últimos años se ha generalizado el SMS como vía de comunicación para la validación y verificación de usuarios.

Los objetivos del proceso de validación pueden ser diversos. Los más comunes son:

- Verificación del teléfono móvil de un usuario.
- La identificación de accesos a aplicaciones (procesos 2FA).
- Doble verificación en ciertas acciones o procesos (transacciones económicas, cambios de configuración clave, etc.).
- Identificación o asociación de un usuario con un teléfono móvil.
- No duplicidad o multiplicidad de cuentas de usuario.
- Procesos de recuperación de contraseña.

Para este tipo de proceso de validación LabsMobile dispone de dos soluciones que se pueden utilizar de forma indistinta. Se describen a continuación sus ventajas e inconvenientes.

1.2 API JSON

LabsMobile dispone de una API SMS generalista con la que se pueden enviar mensajes SMS con llamadas REST de tipo POST y variables codificadas en el cuerpo de la llamada HTTP en formato JSON.

Funcionalidades básicas: *Enviar SMS*, *Consultar estado SMS*.

Ventajas:

- Compatible con cualquier entorno de programación.
- Ejemplos de código, soporte y multitud de recursos online.
- Control de todo el proceso y configuración por parte del cliente.
- Es posible consultar el estado de cualquier mensaje enviado y actuar en consecuencia.
- Esta API es muy similar a otras plataformas SMS y por tanto es fácil intercambiar la API JSON por cualquier otra API SMS de cualquier plataforma o utilizar diversos proveedores por destino o intereses comerciales.

Inconvenientes:

- Es necesario construir todo el proceso de validación almacenando una base de datos de códigos OTP generados.

Recursos:

- Documentación y ejemplos de código: https://apidocs.labsmobile.com/
- Tutorial de primeros pasos para una integración SMS API JSON: https://www.labsmobile.com/es/tutoriales/integra-tu-aplicacion-con-nuestra-api.

1.3 API OTP

LabsMobile ha creado una API específica para la creación y gestión de códigos OTP y para procesos de validación como los que se describen en este documento.

Funciones: *Enviar nuevo código*, *Reenviar código*, *Validar código*.

Ventajas:

- Se incrementa la seguridad del proceso ocultando los códigos OTP en la plataforma LabsMobile.
- Simplifica el proceso de validación sin tener que generar o guardar los códigos OTP.
- Compatible con cualquier entorno que pueda generar llamadas REST HTTP/GET.

Inconvenientes:

- API con funciones no estándar que añaden un periodo de aprendizaje o adaptación.
- No es posible cambiar o consultar algunos detalles del proceso (formato del código OTP, estado o entrega de los mensajes enviados).

Recursos:

- Manual y ejemplos de uso: https://www.labsmobile.com/es/api-sms/versiones-api/otp.

2 Seguridad y autenticación

El primer paso crear una integración para un proceso de validación OTP SMS con LabsMobile es crear una cuenta de usuario en https://www.labsmobile.com/.

Con una cuenta es posible implementar un proceso de validación ya sea con la API JSON o con la API OTP descritas en el apartado anterior. En ambos casos es necesario adoptar algunas medidas de seguridad descritas a continuación.

2.1 Token API

La primera medida de seguridad es utilizar como contraseña un *token API* que se puede generar en el panel de control de la cuenta (apartado *Mi cuenta —> Seguridad y contraseñas*) creada en la plataforma LabsMobile.

Estos *token API* no comprometen la contraseña general de la cuenta y se pueden generar y deshabilitar en cualquier momento. Es recomendable cambiar el valor del token API cada 3-6 meses.

2.2 Cifrado SSL

Es importante utilizar siempre las URLs de la API con el protocolo HTTPS para el cifrado de los datos y variables enviados.

2.3 Filtro por dirección IP

En las *Preferencias* de la cuenta creada en la plataforma LabsMobile es posible configurar una o varias direcciones IP válidas para realizar envíos o llamadas a la API SMS.

Una vez configurado este filtro por dirección IP no será posible realizar ningún envío desde cualquier origen que no esté presente en el listado de direcciones IP. Cualquier intento de envío o conexión ajeno a estas direcciones IP será bloqueado y generará error.

2.4 Conexión API

Las llamadas o peticiones a la API (API JSON o API OTP de LabsMobile) se deben realizar siempre desde el backend o servidor de datos. En ningún caso se debe realizar la conexión directamente desde la interfaz de usuario (web o app).

El principal motivo es no comprometer los datos sensibles (contraseñas, métodos de generación/almacenamiento de códigos, etc.) y centralizar las peticiones para una mejor gestión y control.

Para el envío de un código OTP (y también para su posterior validación) es necesario pasar la petición y datos del usuario desde la interfaz al backend mediante algún método tecnológico como llamada AJAX, petición HTTP/POST, socket, etc. Posteriormente el backend debe gestionar las peticiones a la API de LabsMobile y controlar el proceso de validación. Recomendamos consultar el diagrama del proceso que se encuentra al final de este documento.

3 Interfaz de usuario

A continuación se presentan algunas recomendaciones relacionadas con la interfaz de usuario en un proceso de validación OTP.

3.1 Introducción del número móvil y validaciones

Es importante crear una interfaz clara y sencilla para que el usuario introduzca su número de teléfono móvil. Es recomendable:

- Que exista sólo un campo en la interfaz de usuario. Eliminar cualquier otro campo, opción o acción para concentrar la atención del usuario en el proceso de validación.
- En este campo sólo debe ser posible introducir dígitos (eliminar cualquier otro símbolo).
- Añadir el prefijo de país con una selector de país a ser posible en formato bandera. Preseleccionar por defecto el país más frecuente o detectar el país del usuario.
- Validar el teléfono introducido por el usuario. Si no se ha introducido un formato de número móvil correcto mostrar un error y permitir que el usuario modifique el valor del teléfono.

Se recomienda la adopción de alguna de las siguientes librerías:

- Interfaz de campo móvil y país: https://intl-tel-input.com/
- Validación del formato móvil por país: https://github.com/google/libphonenumber.

3.2 Instrucciones y ayuda

El usuario debe recibir unas instrucciones claras que le guíen durante el proceso de validación. A continuación se presentan unos textos de ejemplo en función del estado del proceso en el que se encuentra el usuario.

- Pantalla de introducción del teléfono.

> *Introduce tu teléfono móvil y recibirás un código por SMS.*

- Error en el formato del teléfono.

> *El teléfono no corresponde con un teléfono móvil válido para [PAÍS]. Ruego compruebes y modifiques el número y país seleccionado.*

- Una vez se ha introducido un teléfono válido y se ha enviado el código OTP por SMS.

> *Busca en tu Inbox SMS. Hemos enviado un código por SMS a tu teléfono móvil. Introduce en el campo siguiente el código de 4 dígitos recibido.*
> ***IMPORTANTE**: comprueba que tienes cobertura GSM/llamadas para recibir mensajes SMS.*

- Pasados unos pocos segundos (3s-6s) añadir un mensaje de espera.

> *Han pasado 6 segundos desde el último envío. En **24 segundos** podrás reenviar un nuevo código por SMS.*

- Mensaje de método de comunicación alternativa cuando se han agotado los intentos.

> *Se han agotado los intentos permitidos. Ruego te pongas en contacto con nosotros en **support@labsmobile.com** o +**34938132933**.*

4 Elementos del proceso

En un proceso de validación OTP SMS intervienen algunos elementos básicos que deben cumplir unos requisitos o para los que se enumeran unas recomendaciones en este apartado.

4.1 Código OTP

El código OTP es el elemento principal del proceso y se recomienda que cumpla las siguientes características:

- Código numérico (sólo dígitos).
- Longitud de entre 4 y 6 dígitos.
- Mantener el mismo código para un mismo usuario y proceso de validación. Por tanto, cualquier mensaje enviado a un número (incluidos todos los intentos) deben tener el mismo código OTP.

4.2 Texto del mensaje

El texto del mensaje SMS enviado en una validación OTP (en todos los intentos) debería respetar los siguientes aspectos:

- El texto del mensaje debe ser lo más corto y conciso posible.
- El código se debe localizar al inicio del texto del mensaje. A ser posible entre las 3 primeras palabras. De esta forma se podrá reconocer de forma fácil incluso en las previsualizaciones o notificaciones del mensaje SMS.
- Es recomendable identificar al remitente del mensaje o proceso de validación. Esta identificación se puede hacer en el remitente o en el texto del mensaje.
- Es recomendable identificar los intentos en el texto del mensaje.

Ejemplos:

```
<#> 3823 es tu codigo de validacion en nuestra app Kiwoko
```

```
El codigo 3823 valida tu acceso en labsmobile.com solicitado el
2020-11-01 10:33 GMT+2
```

```
PayPal: codigo 381223 para la validacion de tu ultima transaccion.
Este codigo caducara en 10 minutos.
```

4.3 Política de intentos

Si el primer envío de código OTP por SMS no llega a su destino, es recomendable establecer una política de intentos finitos con algunas especificaciones.

- Se debe establecer un tiempo mínimo entre intentos. Es decir, la opción de enviar un nuevo código no puede estar disponible hasta después de entre 20 y 40 segundos. Se recomienda mostrar al usuario el número de segundos restantes hasta que el siguiente intento esté habilitado.
- El número máximo de intentos debe estar entre 1-3 mensajes.
- Una vez alcanzado el número máximo de intentos es recomendable mostrar algún método alternativo de comunicación como email o teléfono de soporte.
- Consultar el estado de los mensajes SMS enviados a un usuario o número:
    a) Enviado: mensaje sin estado final, procesado y comunicado al operador local. La espera hasta el siguiente intento se puede ampliar ya que pueden existir episodios de congestión o incidencia temporal.
    b) Entregado: mensaje confirmado como entregado al dispositivo de destino. Establecer una política máxima de 1-2 intentos mostrando un mensaje al usuario que reinicie su dispositivo y compruebe su configuración y cobertura.
    c) Rechazado/No entregable: error de entrega normalmente porque el número no es correcto. Forzar al usuario a cambiar de número de teléfono.
- Establecer una validez de cada código OTP generado de entre 10-30 minutos. Pasado este intervalo de tiempo el código OTP ya no es válido y el usuario deberá iniciar el proceso de validación.

info@labsmobile.com

5 Diagrama del proceso