

SMS Finder - Análise OSINT do luxfysms.app

Investigação técnica para identificar os provedores de SMS utilizados pela plataforma **luxfysms.app** (dP SMS - Plataforma Inteligente de Marketing Digital).

Resumo Executivo

A plataforma luxfysms.app utiliza **três provedores de SMS** em conjunto, com o **Onbuka** como provedor primário. A descoberta foi feita através de análise do bundle JavaScript da aplicação (/assets/index-DX_F-_pt.js , 2.6 MB), que revelou campos de configuração, endpoints de API e referências diretas aos provedores.

Provedor	Papel	Referências no Código
Onbuka	Primário	73+ referências
EIMS	Secundário (3 contas)	Múltiplas instâncias
SMPP (kftel.hk)	Gateway terciário	Servidores dedicados

Metodologia

Técnicas de OSINT (Open Source Intelligence) utilizadas:

Técnica	Ferramenta	O que revelou
Análise de código-fonte (HTML)	<code>curl</code> + inspeção manual	Framework, meta tags, scripts externos
Análise de bundle JavaScript	<code>curl</code> + <code>grep</code> por keywords	Provedores SMS, endpoints, credenciais config
DNS Reconnaissance	<code>dig</code> , <code>nslookup</code>	Nameservers, ausência de MX/TXT/SPF
HTTP Header Analysis	<code>curl -sI</code>	Cloudflare, cookie leak <code>lovable.app</code>
SSL/TLS Inspection	<code>openssl s_client</code>	Google Trust Services, cert details
IP Intelligence	<code>ipinfo.io</code> , <code>ipapi.co</code>	Cloudflare anycast, geolocalização
WHOIS / Reverse DNS	<code>whois</code> , <code>host</code>	Registrador Dynadot, sem rDNS
Web Search (OSINT)	Múltiplos motores de busca	Presença online mínima
API Probing	<code>curl</code> em endpoints comuns	API pública Supabase documentada

Provedores de SMS Identificados

1. Onbuka (Provedor Primário)

- **Website:** onbuka.com
- **Endpoint API:** `api.onbuka.com`
- **Autenticação:** API Key + API Secret + App ID (hash MD5)
- **Referências no código:** 73+
- **Campos de configuração encontrados:**

```
onbuka_api_key
onbuka_api_secret
onbuka_app_id
```

Onbuka é um provedor de SMS internacional focado em rotas wholesale/grey para envio em massa. A quantidade massiva de referências no código indica que é o gateway principal para envio de mensagens.

2. EIMS (Provedor Secundário)

- **Tipo:** Gateway SMS com múltiplas contas
- **Autenticação:** Account + Password
- **Instâncias configuradas:** 3 contas independentes
- **Campos de configuração encontrados:**

```
eims_account      / eims_password    / eims_servers
eims_account_1    / eims_password_1  / eims_servers_1
eims_account_2    / eims_password_2  / eims_servers_2
eims_account_3    / eims_password_3  / eims_servers_3
```

A existência de 3 contas sugere redundância e balanceamento de carga entre diferentes rotas EIMS.

3. SMPP Gateway (Provedor Terciário)

- **Protocolo:** SMPP (Short Message Peer-to-Peer)
- **Servidor principal:** `smpp.kftel.hk:20003` (Hong Kong)
- **Domínio fallback:** `biapts.bio`
- **IPs de servidores:**

IP	Porta	Função
43.249.30.190	20003	SMPP Produção
85.195.119.206	20003	SMPP Backup
147.93.10.215	—	Provedor SMS (Produção)
191.96.224.109	3000, 9999	Gateway SMS (Dev/Teste)

Infraestrutura Completa

Stack Tecnológico

CLOUDFLARE (CDN/WAF)		
IP Anycast: 185.158.133.1		
CF-Ray: BSB (São Paulo)		
FRONTEND (SPA)		
React 18 + Vite + Tailwind CSS		
shadcn/ui + Radix UI + Lucide Icons		
React Flow (editor visual de fluxos)		
i18next (internacionalização pt-BR)		
Construído com: Lovable.dev (no-code IA)		
BACKEND		
Supabase (PostgreSQL + Edge Functions)		
Projeto: pikphkcxjtvukdcolviv		
Auth: GoTrue (Supabase Auth)		
Functions: public-api, elevenlabs-voices		
PROVEDORES SMS		
Onbuka	EIMS	SMPP (kftel.hk)
(73+ ref)	(x3)	porta 20003
ANALYTICS		
Tinybird (flock.js) + Facebook Pixel		
Pixel ID: 1062729962007816		

Detalhes de Infraestrutura

Componente	Serviço	Evidência
CDN/WAF	Cloudflare	Header <code>server: cloudflare</code> , cookie <code>__cf_bm</code>
Hosting	Lovable.dev	Cookie <code>Domain=lovable.app</code> , path <code>/lovable-uploads/</code>
Backend	Supabase	Endpoint <code>pikphkcxjtvukdcolviv.supabase.co</code>
DNS	Dynadot	NS <code>ns1.dyna-ns.net</code> , <code>ns2.dyna-ns.net</code>
SSL	Google Trust Services	Cert CN=luxfysms.app, issuer WE1, ECDSA 256-bit
Analytics	Tinybird + Meta	Script <code>~flock.js</code> , Facebook Pixel
TTS/Voz	ElevenLabs	Edge function <code>elevenlabs-voices</code>

Domínios Associados

Domínio	Relação
<code>biapts.bio</code>	Domínio padrão/fallback do gateway SMPP
<code>clnik.bio</code>	Provedor alternativo
<code>nourishco.online</code>	Domínio parceiro/afiliado
<code>personbonusx.com</code>	Domínio parceiro
<code>veja30hs.pro</code>	Domínio parceiro
<code>lovable.app</code>	Plataforma de build (Lovable.dev)

API Pública Descoberta

Base URL: `https://pikphkcxjtvukdc0lviv.supabase.co/functions/v1/public-api`

Versão: 1.1.0

Endpoints Disponíveis

Método	Endpoint	Descrição
POST	<code>/sendsms</code>	Enviar mensagens SMS
GET	<code>/balance</code>	Consultar saldo da conta
GET	<code>/status/{id}</code>	Verificar status de SMS enviado
GET/POST	<code>/campaign</code>	Listar/criar campanhas
GET/PUT/DELETE	<code>/campaign/{id}</code>	Gerenciar campanha específica
GET	<code>/logs</code>	Visualizar logs de envio
GET	<code>/health</code>	Health check do serviço

Evidências Técnicas

Como o Onbuka foi descoberto

O bundle JavaScript principal (`/assets/index-DX_F-_pt.js` , 2.6 MB) contém 73+ referências ao Onbuka, incluindo:

- Campos de configuração do painel admin (`onbuka_api_key` , `onbuka_api_secret` , `onbuka_app_id`)
- Referência à documentação: “onbuka.com - Autenticação MD5”
- Endpoint de API: `api.onbuka.com`

Como o EIMS foi descoberto

No mesmo bundle JS, foram encontrados campos de configuração para 3 instâncias independentes do EIMS, com padrão de nomenclatura `eims_account_N` / `eims_password_N` / `eims_servers_N`.

Como o SMPP foi descoberto

Referências diretas ao servidor `smpp.kftel.hk:20003` e IPs de servidores SMPP (`43.249.30.190` , `85.195.119.206`) foram encontrados no bundle JS, junto com 10+ referências ao protocolo SMPP.

Como o Lovable.dev foi descoberto

O header HTTP `Set-Cookie` contém `Domain=lovable.app` — um vazamento de cookie que revela que a aplicação foi construída e está hospedada na plataforma Lovable.dev. Além disso, o favicon está em `/lovable-uploads/`.

Como o Supabase foi descoberto

O bundle JS contém referências ao projeto Supabase `pikphkcxjtvukdcolviv`, incluindo URLs de Edge Functions e configuração de autenticação GoTrue.

Identidade da Plataforma

Campo	Valor
Nome	dP SMS
Subtítulo	Plataforma Inteligente de Marketing Digital
Autor	dP
Twitter/X	@dP_oficial
Idioma	pt-BR (Português Brasileiro)
Público-alvo	Marketing digital / SMS em massa
CNPJ	Não encontrado publicamente

Funcionalidades Identificadas

Além de SMS em massa, a plataforma oferece:

- **Call Center com IA:** Sistema de chamadas com IVR (Interactive Voice Response)
- **Agentes de IA:** Configuração de agentes automatizados para chamadas
- **Editor de Fluxos:** Interface visual (React Flow) para criar fluxos de comunicação
- **Gestão de Campanhas:** Criação, monitoramento e análise de campanhas
- **Importação de Contatos:** Upload via CSV
- **Logs em Tempo Real:** Monitoramento de envios e chamadas
- **TTS (Text-to-Speech):** Integração com ElevenLabs para síntese de voz
- **Link Tracking:** Analytics de links com rastreamento de cliques

Segurança Observada

- HTTPS obrigatório (HSTS 1 ano com includeSubDomains)
- Cloudflare WAF/DDoS protection ativo

- Credenciais armazenadas com criptografia no banco (`*_encrypted`)
 - Source maps desabilitados em produção
 - Detecção de WebDriver/bots automatizados
 - Sem vazamento de API keys no código-fonte público (chaves no banco)
-

Conclusões

1. **O provedor principal de SMS é o Onbuka** (`onbuka.com`), um gateway internacional de SMS em massa com foco em rotas wholesale, identificado por 73+ referências no código-fonte.
 2. **EIMS é o provedor secundário**, com 3 contas independentes configuradas para redundância e balanceamento de carga.
 3. **SMPP via kftel.hk** atua como gateway terciário, com servidores em Hong Kong e Europa.
 4. A plataforma foi construída com **Lovable.dev** (plataforma no-code com IA), usa **Supabase** como backend, e está protegida por **Cloudflare**.
 5. Além de SMS marketing, a plataforma inclui funcionalidades de **call center com IA** e **síntese de voz** (ElevenLabs).
 6. A descoberta foi possível primariamente pela **análise do bundle JavaScript** — um arquivo de 2.6 MB que, por ser uma SPA (Single Page Application), contém toda a lógica da aplicação no lado do cliente, incluindo referências a provedores e configurações.
-

Análise realizada em 06/02/2026 utilizando técnicas de OSINT (Open Source Intelligence).