interactive digital media

ENTERPRISE WHITEPAPER

The A2P SMS Guide

What enterprises need to know about application-to-person messaging: technology, regulation, best practices and vendor selection — in twelve pages.

First edition published 2024

Current revision — February 2026

ABOUT THIS GUIDE

A practical reference for enterprise messaging

First released in 2024 and refreshed for 2026, this guide compresses two decades of operational experience in application-to-person (A2P) SMS into a working reference — for the people who actually run or choose messaging programmes.

The 2026 revision refreshes regulatory references, updates market data, expands the security section to reflect the rise of Artificially Inflated Traffic (AIT), and revises the vendor-selection criteria to match what enterprise buyers are actually asking in RFPs today.

Contents

A note on vendor mentions. This is a vendor-published guide. Where specific vendors are named — including IDM itself and our sister company AnyMessage — we identify them clearly and explain why. The criteria and frameworks are written to be useful regardless of which vendor a reader ultimately chooses.

CHAPTER 01

A2P SMS and how it works

A working definition, why SMS still dominates in 2026, and the end-to-end chain every message travels from application to handset.

A working definition

Application-to-Person (A2P) SMS is any text message sent from software to a mobile subscriber. The application can be a CRM, a banking core, an e-commerce platform, an authentication service or an IoT backend; the person is any mobile subscriber with a device capable of receiving SMS. The counterpart is **Person-to-Person (P2P)** — two humans texting each other. The split is not just terminology: it determines pricing (A2P termination rates are materially higher than P2P), routing (A2P should flow over registered commercial routes, not grey routes), regulation (consent, sender-ID and opt-out rules apply to A2P), and SLA expectations (delivery receipts, fallback routing, 24/7 support).

Why SMS still dominates in 2026

SMS is the only business messaging channel that works on every mobile phone, in every country, without an app, without a data connection, without a login and without a platform owner's policy review. When a bank needs to deliver an OTP to 200 countries in under three seconds, nothing else reliably does the job.

~98%	<3s	100%	0
OPEN RATE	**TYPICAL LATENCY**	**DEVICE COVERAGE**	**APP INSTALLS**
within minutes of delivery	A2P to handset, global avg.	any SIM-enabled phone	no data connection needed

The end-to-end delivery chain

An A2P SMS traverses four to six distinct systems between originating application and recipient handset. Each hop is an opportunity for routing, filtering or failure — and each is where a serious messaging operator earns its fee.

1 · App	2 · API	3 · Hub	4 · Carrier	5 · Handset
CRM / core / auth	HTTP/REST or SMPP	routing, HLR, firewall	SMSC, SS7/ Sigtran	delivery + DLR

Inside the hub, every message goes through number validation, HLR/MNP lookup to determine the number's *current* home network (Mobile Number Portability means the original prefix is often misleading), route selection, content and compliance filtering, and firewall inspection for AIT and impersonation patterns. Once routed, the message is handed to a terminating carrier's SMSC over SMPP or SS7/Sigtran, and delivery receipts (DLRs) flow back as evidence of delivery.

WHAT "CARRIER-GRADE" ACTUALLY MEANS

When a vendor claims to be "carrier-grade," they are usually making claims about four things: GEO-redundant infrastructure with real-time replication, direct SS7/Sigtran connectivity to operators, 24/7 NOC monitoring with sub-minute alerting, and SLA-backed uptime of 99.9% or better. Ask for evidence of all four — not a brochure, but live dashboards and reference calls.

CHAPTER 02

Core use cases

The five workloads that drive roughly 90% of global A2P volume — and what each one demands from the channel.

O

OTP & 2FA authentication

Largest single use case by volume. Sub-three-second delivery, near-100% deliverability, no tolerance for message loss. The single most AIT-targeted traffic type; dedicated premium routes required. Avoid URLs in OTP messages — many operators filter them as phishing.

T

Transactional notifications

Delivery tracking, payment confirmations, appointment reminders, travel updates. Lower latency priority than OTP, higher volume. Enterprises increasingly move these from email to SMS to cut inbound call volume — a 1¢ SMS beats an €8 support call.

M

Marketing & CRM

Highest compliance bar. Requires explicit GDPR-compliant opt-in in the EU, prior express written consent under TCPA in the US, DLT template registration in India. Consider pairing with RCS/ WhatsApp where opt-in exists — SMS handles what those channels cannot reach.

C

Customer service & two-way

Inbound SMS, keyword commands (STOP, HELP, STATUS), short codes, conversational flows. Often the SMS leg of a richer WhatsApp or RCS conversation — SMS as universal fallback rather than primary channel.

I

M2M / IoT

Device-originated signalling: vehicle telematics, smart meters, alarm systems, POS terminals. Low per-device volumes, large fleets. Deterministic delivery, long validity periods and international roaming support typically required.

+

Emerging patterns

Voice-OTP fallback for markets where SMS is blocked, flash-call verification (restricted in the EU since 2023), and increasingly AI-driven two-way service bots sitting behind short codes or long numbers.

OPERATIONAL RULE OF THUMB

Never route OTP traffic over the same carrier path as marketing traffic. Different latency tolerances, different firewall profiles, different fraud exposure. Keep them separate in your platform and in your SLAs.

CHAPTER 03

Regulation & compliance

The four overlapping regulatory regimes that apply to every enterprise A2P message — and a practical compliance baseline for 2026.

A2P compliance is four overlapping regimes that apply to different aspects of the same message: **consent and privacy** (who gave permission, how, for what purpose); **content** (restricted categories per country); **sender identification** (what appears on the handset, and whether it has been registered where registration is required); and **delivery window and frequency** (time-of-day rules, Do-Not-Disturb registries).

Europe — GDPR, ePrivacy and national variants

Inside the EU, commercial A2P SMS is governed primarily by GDPR (Regulation 2016/679) and the ePrivacy Directive (2002/58/EC). The core rule: **prior, specific, informed and freely given consent is required before direct-marketing SMS can be sent**, with a narrow "soft opt-in" exception under ePrivacy Article 13(2) for existing customers of similar products. Transactional messages — OTPs, delivery notifications, appointment reminders for requested services — typically rely on legitimate interest or contractual necessity rather than explicit marketing consent. The critical line is purpose: a "your package is here" SMS that ends with "50% off your next order" is a marketing message.

National implementations add teeth. Germany's UWG §7 sets administrative fines up to €300,000 per violation and double-opt-in is the de-facto standard. France's CNIL requires explicit opt-in and a clear opt-out keyword in every message. The UK's PECR substantially mirrors ePrivacy with active ICO enforcement. Italy's Garante and Spain's AEPD have both issued seven-figure fines for A2P marketing without consent.

> **Where IDM and AnyMessage fit.** For enterprises whose primary requirement is EU/EEA data residency, full GDPR-aligned processing, German-hosted infrastructure and a legal entity inside the EU for DPA purposes, IDM and its sister company **AnyMessage** are among the vendors specifically set up for that constraint. Several strong EU-based providers exist — we do not claim to be the only option — but for buyers where EU compliance is a non-negotiable selection criterion, IDM and AnyMessage together meaningfully shorten the shortlist.

North America, India and beyond

The US runs on three rails: **TCPA** (47 USC §227) sets the consent baseline with statutory damages of $500–1,500 per message; the **CTIA Messaging Principles** are a carrier-enforced code on content and opt-in/opt-out handling; **10DLC** requires brand and campaign registration with The Campaign Registry for A2P from long numbers. Canada layers on CASL, which is closer to the EU standard than TCPA. India operates the most technically advanced regime in the world — every commercial SMS must use a pre-registered template tied to a registered sender ID on the DLT platform; non-compliant messages are blocked at the network firewall. UAE, Saudi Arabia, Qatar and a growing list of Gulf and African regulators operate sender-ID whitelists with mandatory registration.

A practical compliance baseline

- ✓ Documented opt-in for every number: source, timestamp, consent scope.
- ✓ Honour opt-out keywords (STOP and local equivalents) within one message cycle.
- ✓ Enforce time-of-day restrictions automatically per destination country.
- ✓ Register sender IDs and templates in every jurisdiction that requires it.
- ✓ DPA in place with the messaging provider for EU traffic; data-residency confirmed.

✓ Audit trail — message content, metadata and DLRs retained per legal basis.

CHAPTER 04

Security & anti-fraud

Grey routes, SIM boxes, Artificially Inflated Traffic and the firewalls that defend against them — the fraud patterns that define enterprise messaging risk in 2026.

A2P fraud is not an edge case. Industry estimates place global operator revenue loss from grey routes and related fraud in the single-digit billions of US dollars annually, with enterprise losses from AIT alone climbing into the hundreds of millions. The direct cost (paying for messages that never reach real users) is compounded by second-order damage: collapsed conversion rates, regulatory exposure where traffic routes through non-compliant intermediaries, and reputational harm when grey-route delivery fails publicly.

The three fraud patterns that matter

Grey routes deliver A2P traffic while misclassifying it as P2P, avoiding the higher termination rate and the operator's compliance controls. Pricing is dramatically cheaper — sometimes 70–80% below clean A2P — and deliverability looks fine initially, then degrades as operator firewalls learn the patterns. **SIM-box fraud** uses hardware loaded with consumer SIMs to re-originate incoming A2P as local P2P, defrauding the operator of the termination fee and destroying sender-ID branding along the way. **Artificially Inflated Traffic (AIT)** — also called SMS pumping — is the pattern that has grown most aggressively since 2022: malicious actors operate pools of phone numbers and feed them into enterprise sign-up and OTP flows, collecting a share of the termination fee while the enterprise pays for messages nobody legitimate ever wanted.

AIT WARNING SIGNS — MONITOR CONTINUOUSLY

Sudden spikes in OTP requests from number ranges or countries you do not market in. Unusually high delivery rates combined with unusually low onward conversion (people "receive" the OTP but never complete sign-up). Clustering on specific MNC/MCC combinations. Account-creation velocity beyond realistic human behaviour. A modern messaging-side firewall should detect all of these.

The SMS firewall as operational defence

F

Traffic classification

Identifies A2P, P2P, spam and grey-route traffic in real time based on content, origination and pattern. Drops or surcharges traffic that does not match its declared class.

C

Content filtering

Blacklists, whitelists, keyword rules, per-country content policies, URL reputation lookups. Enforces regulator-mandated restrictions automatically.

V

Velocity & anomaly detection

Flags sender-ID impersonation, unrealistic request rates, geographic clustering and number-range concentration consistent with AIT.

R

Revenue assurance

Reconciles traffic class against terminating rates, ensuring A2P pays A2P rates and that grey-route leakage is captured before it becomes a dispute.

IDM's IMT-HUB® firewall — and firewalls from any credible hub operator — expose this layer to enterprise customers as well as operators, meaning enterprises can set their own AIT tolerances and get alerted in real time when patterns emerge. Any modern vendor evaluation should probe firewall capabilities in detail.

CHAPTER 05

Vendor selection

Nine criteria that actually separate good A2P providers from bad ones, and the questions to put in every RFP.

#	CRITERION	WHAT TO PROBE
1	**Coverage & route quality**	Direct operator connections vs. via sub-aggregators. Proportion of traffic on direct, A2P-approved routes. Evidence, not claims.
2	**GSMA OC certification**	Is the hub OC-certified? If not, which OC hub does it terminate through?
3	**Deliverability & DLR quality**	Per-country SLAs. Real operator-sourced receipts or fabricated? Live dashboards available?

#	CRITERION	WHAT TO PROBE
4	**Firewall & AIT protection**	What detection runs on outbound traffic? What controls can you configure? Commercial remedy for AIT losses?
5	**Compliance & data residency**	Where is data processed and stored? DPAs, ISO 27001, SOC 2? EU/EEA hosting? Sender-ID registration services?
6	**Channels & RCS readiness**	SMS plus Voice, RCS, WhatsApp, email? Unified orchestration or separate tools? Fallback logic configurable?
7	**Platform & integration**	SMPP, HTTP/REST, webhooks, SDKs. Throughput per account. Sandbox. Docs quality.
8	**SLA & commercials**	Uptime SLA, credit structure, per-country pricing transparency, contract flexibility.
9	**Support model**	24/7/365 NOC? Named account management? Incident-response SLA? Language coverage?

Eight questions for every RFP

1. List your direct operator connections vs. sub-aggregator connections, by country.
2. Are you a GSMA OC certified SMS hub? If not, which OC hub do you route through?
3. Show live deliverability dashboards for our destination countries, last 90 days.
4. Describe your AIT detection architecture and remedy if we are hit using your platform.
5. For EU traffic, confirm contracting entity, hosting location, and provide your DPA.
6. What is your RCS roadmap, which operators can you send to, and how does SMS fallback work?
7. Provide per-country uptime, latency and deliverability SLAs plus the credit structure.
8. Describe 24/7 support: who answers the phone at 03:00 on a Sunday, and the escalation chain.

IDM and AnyMessage — where we fit honestly. Our sweet spot is enterprises and operators who need **carrier-grade routing, GSMA OC compliance, EU/EEA data residency, and a named support relationship** — where those attributes matter more than the number of tangential channel integrations. For buyers who primarily need EU compliance, we are one of several strong options; for buyers with truly global omnichannel needs and EU compliance as a secondary requirement, IDM and AnyMessage should be compared directly with the global CPaaS players using the criteria above.

ABOUT THE PUBLISHER

interactive digital media GmbH

IDM is a German cloud communication service provider founded in 2003 and headquartered in Lübeck. Our proprietary **IMT-HUB®** platform, now in its fourth generation, is one of approximately 40 GSMA Open Connectivity (OC) certified SMS hubs worldwide. We serve enterprises, mobile operators and service providers across every major industry, with infrastructure hosted entirely in Germany. Since 2024, IDM has been part of the **United Capital / AnyMessage group**; our sister company AnyMessage operates complementary messaging infrastructure, and together we represent a European messaging group with particular strength in regulated, compliance-sensitive deployments.

20+	200+	1,000+	~40
YEARS	**COUNTRIES**	**OPERATORS**	**GSMA OC HUBS**
of operating experience	reachable on our network	directly or via OC	IDM is one of them

Who we serve

IDM serves enterprise clients across banking, automotive, healthcare, research, retail, tourism and the public sector, together with carrier partners across the EU, GCC and international hub networks. Because messaging is mission-critical for many of our clients, we name specific references only with prior written consent and on a case-by-case basis — available on request under NDA.

TALK TO US

If this guide raised questions about your current messaging operation, your compliance posture, or your vendor set — we are happy to talk, whether or not a commercial conversation ever follows. Enterprise enquiries: **sales@i-digital-m.com**. Carriers, aggregators and resellers: **partners@i-digital-m.com**. Or call **+49 (0)451 31 70 21-0**.

Let's start the conversation

Excellence in Cloud Communication Services

Sales & general enquiries

INTERACTIVE DIGITAL MEDIA GMBH

✉ sales@i-digital-m.com

☏ +49 (0)451 31 70 21-0

Partner Program

CARRIERS · AGGREGATORS · RESELLERS

✉ partners@i-digital-m.com

☏ +49 (0)451 31 70 21-0

Online

WEBSITE & CUSTOMER PORTAL

🌐 www.i-digital-m.com

☏ +49 (0)451 31 70 21-0

Headquarters

interactive digital media GmbH · Moislinger Allee 9d · 23558 Lübeck · Germany

Presences in London (UK) and New Delhi (IN) · Part of the United Capital / AnyMessage group