A Buying Guide To Choose a Secure SMS Provider

exotel | Whitepaper

Table of contents

The Thriving Business of SMS

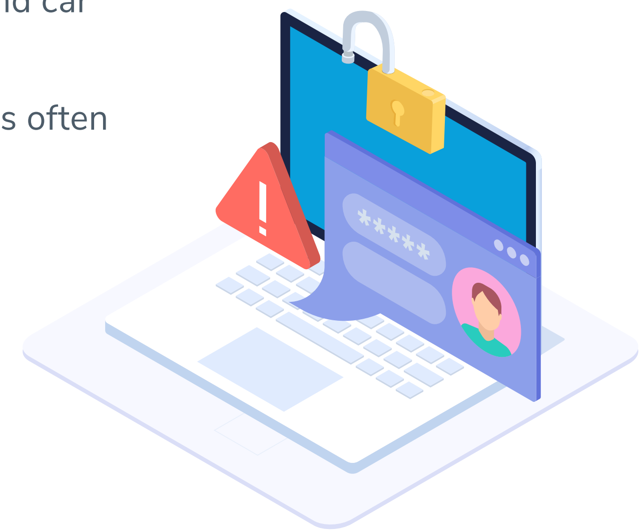
Over the years, modern AI- and automation-enabled messaging channels are only rising in popularity, taking direct aim at text-based channels like SMS. But SMS has cemented its position as a vital communication channel because it offers speed of delivery and certain failsafe measures.

Today, a host of new players have democratised the range of SMS services and capabilities to suit evolving market needs with the help of modern tech. While most of these providers can facilitate SMS communication well, few can guarantee the security of your customer data. In fact, some have just the basic protocols and nothing comprehensive. Of course, this data is your businesses' competitive advantage.

This whitepaper shares best practices you can follow while choosing a reliable, safe, yet effective SMS service partner.

Average Open Rate of SMS : 98%

Growing Security Vulnerabilities in SMS



Try refreshing your memory. If you recently enquired to buy a loan or a second-hand car from certain businesses, were you surprised when you got a call from a competing business soon after your conversation? Even if you haven't, our potential customers often come to us with these concerns. There are high chances that your SMS provider is knowingly or unknowingly leaking your data to other parties.

There are two downsides to this: unauthorised sharing of personal customer data could put you in legal trouble, and loss of competitive advantage i.e. handing business data over to your rivals.

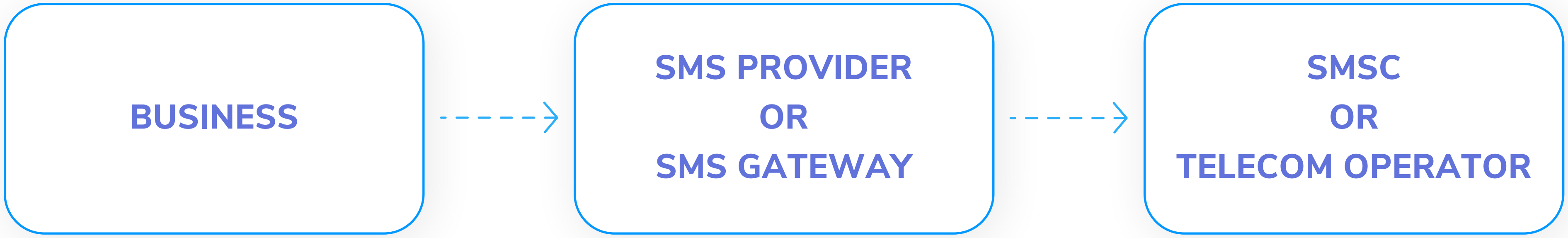
The explosion of the SMS market is partly to blame. It has birthed a number of SMS providers whose security practices exclude key data privacy protocols or regular tests to plug platform or infrastructural loopholes. Additionally, some intentionally create backdoors in their tech framework to monetise your customer data.

Recent News

A leaky database of SMS text messages exposed contact details and security codes. TechCrunch

SMS provider TrueDialog leaves a billion entries of highly sensitive data unprotected COMPUTERWORLD

A Bulk SMS Journey: Involves Multiple Players



BUSINESS

SMS PROVIDER
OR
SMS GATEWAY

SMSC
OR
TELECOM OPERATOR

Requiring SMS Services

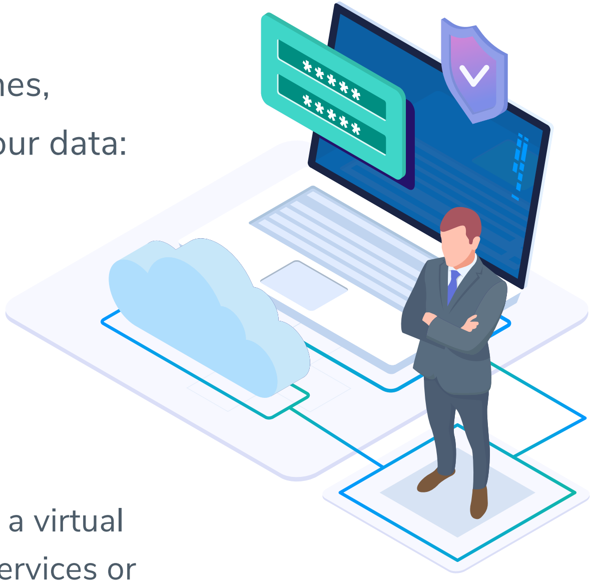
Has infra to schedule SMS

Short Message Service Centre or Telecom players

P.S: Sometimes, gateways that directly work and comply with SMSC protocols of mobile operators take on the role of aggregators as well.

The data protection protocols you need

The journey of sending bulk SMS to your customers is not that straightforward, after all. This increases the chances of data breaches, requiring the following protocols and infrastructure to safeguard your data:



1 Network Security Protocols

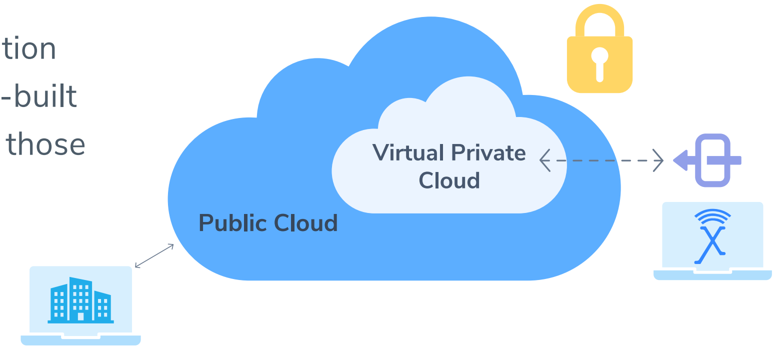
Applies to data residing in a cloud space.

Virtual Private Cloud (VPC)

The data you send to an SMS service provider can be well secured using a virtual private cloud. It is offered by a public cloud provider like Amazon Web Services or Microsoft Azure, and is a highly-secured space with the following access protocols:

Entry points - Access to the VPC is moderated by a server called a bastion host. It interfaces with external networks like the Internet. It comes pre-built with two firewalls filtering requests from the "outside world" and from those made inside its secure space.

Access controls -Designated personnel from the SMS gateway are provided with secure keys that allow them to interface with data inside the virtual private cloud.



Access restrictions - Authorising personnel does not mandate access to the entire space of the SMS service or gateway provider's VPC. Rather, administrators can share limited to full access based on the personnel's clearance level to access required data.

Activity logs - All nature of access requests, including details of personnel entering secure spaces are recorded in a log. They can be sent to a central server from which administrators can use them for reporting purposes.

2 Data at Rest Protocols

Physical equipment like a server at a data centre can be illegally accessed. Or, the VPC's dashboard can be accessed, by stealing an endpoint device like a laptop. That's where "at-rest encryption" comes into play, keeping data unreadable even if an unauthorised party can access it. This feature allows only those with the right digital key for the server to decrypt the data.

3 Data in Transit Protocols

This applies to data being transmitted between two endpoints. The data turns to 'at rest' once the transfer completes.

API authentications

Typically, businesses interact with an SMS service provider or gateway using Application Programming Interfaces or APIs. Called RESTful or REST APIs, they come with authentication authorisations of their own. In addition, they can be configured to suit the nature of every businesses' enterprise stack or specific security requirements.

The Transport Layer Security (TLS)

Hypertext Transfer Protocol (HTTP) is a common term and a form of Transmission Control Protocol (TCP) offering logic for text-based data to be transferred digitally. But it can't fully protect the data from being accessed by unauthorised personnel. If it's your customer's data, it can be misused. With TLS as an added security layer (essentially converting HTTP to HTTPS, what you see besides URL bars on browsers), data is encrypted en route to its next point in the SMS lifecycle. While latency or delay in transmission might increase, it is certainly worth the wait.

4 Key Tests

These best practices help your service provider look beyond its security blind spots.

Third-party audits

You build trust is built when data security practices are certified through external specialists. Vendors must allow them to independently scan entities like networks or entry points and look for vulnerabilities. In addition, internal teams like platform engineering can regularly organise random security tests.

PEN (penetration) tests

While audits are to test vulnerabilities, PEN tests are meant to find which parts can break or be deliberately broken into when a forceful or brutal attack is made on your infrastructure. For instance, at Exotel, we openly challenge our customers to conduct PEN tests and come back with any threats they detected.

ISO 27000

According to iso.org, the ISO/IEC 27000's family of standards aims at "providing requirements for an information security management system to manage the security of assets such as financial information, intellectual property, or information entrusted by third parties." There are 114 controls under this family.

A Cloud Communication Platform as a Comprehensive Solution

Using standalone SMS providers increases the chance of security risks. This is because of the lack of standards on their platforms, especially around data integrity. However, a cloud communication platform (CCP) stands in a league of its own, offering:

Channel Choice - An agile CCP can easily support changing customer engagement patterns by deploying the right suite of channels while sharing data insights to improve CX.

Reliability - Choose a cloud communication platform that has seamlessly supported enterprises during times like a peak sale season. Compare uptime rates across providers to make an informed choice.

Security Compliance - The CCP follows required practices that are up-to-date to fend off any threats to its platform.

Platform Flexibility - The platform must be agile to work with the tech architecture of your business. That helps to integrate key channels onto your app or web portal. As a result, data silo issues are resolved.

Customer Engagement - You can get the most when your CRM, helpdesk and cloud communication platform works as a tightly-knit unit, generating personalised customer recommendations.

Does Your Provider Offer These Parameters Too?

SMS Service providers or gateways must be at the top of their game. This is not just with cloud-centric security, but with other aspects of their business as well. Specifically, the aspects that could pose a threat to your SLA-governed data. Let's take a quick look:

Product Security

Providers must be mindful when changes are made to the hardware, applications or tech configurations. In addition, enabling two-factor authentication for account access by employees and customers has become the norm. Finally, strict security guidelines during product development must supplement all the other guidelines mentioned in this whitepaper.

Added Cloud and Network Security

Asset management, especially planning, acquisition, maintenance and disposal of information assets must be standardised. Ensure your provider wipes all confidential data upon disposal or works with trusted vendors when purchasing equipment.

People Security

Security governance must be hard-coded into the culture of the provider you go with. They should cultivate best practices around periodical Information Security sessions and have stringent background checks when a new employee is hired.

Physical Security

Workplace security standards cannot be compromised. Ensure the regulated entry of authorised employees through biometric scanning and the use of security cameras to prevent any unwanted facility break-ins.

Disaster Recovery

Ensure your provider maintains activity logs backed up in multiple cloud locations. This feature is usually called "server redundancy". This ensures business continuity despite any unwanted cloud blackout from a single server or a cybersecurity attack that can wipe your data from any backup instance.

Why should you consider Exotel?

Exotel is one of Asia's leading cloud communication platforms. In fact, we work with some of the largest companies in Asia including Ola, Go-Jek, and HDFC on the cloud telephony side of the business. Through our SMS services vertical, we serve businesses like Dunzo and Zivame.

While we offer all the above protocols and standards, here is also why you could consider Exotel as a powerful & safe SMS gateway.

More Robust SMS Routes

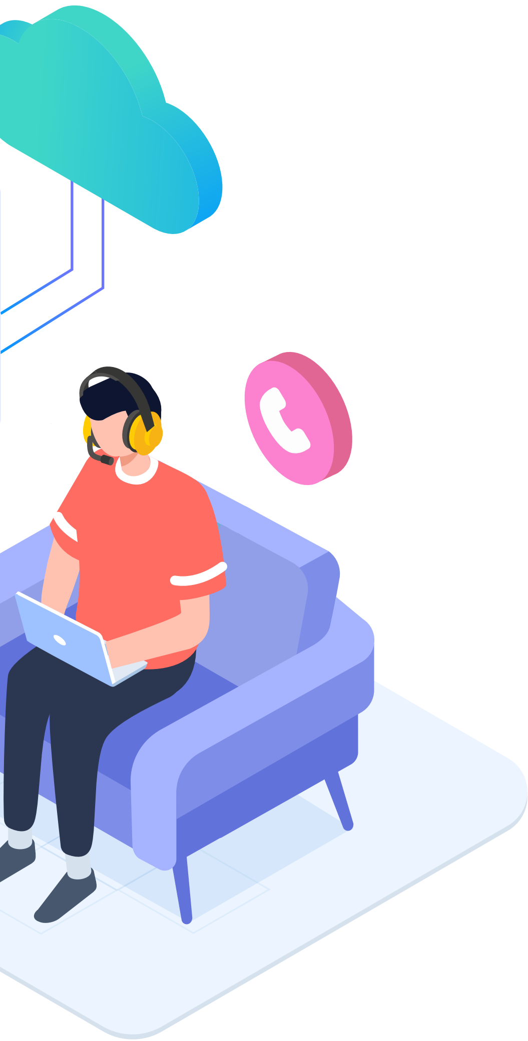
We use reliable, and in few cases, dedicated SMS pipes to deliver messages. They bypass traditional routes that are prone to get clogged.

SLAs With Customers

Our SLAs promise no leakage of customers data through our systems or the entities we work with, except telecom operators who have strong data security practices of their own.

Low Latency

By using reliable data transfer pipes, our delivery timelines usually hover between 3-8 seconds, another key industry standard. We promise delivery rates of 94%.



Personalisation

Set up SMS campaigns for tailored sales events within minutes with our intuitive user interfaces.

Affordability

Get all these benefits at competitive rates so you drive maximum ROI from your spend.

Scrubbing Compliance

We've made it extremely easy to comply with TRAI guidelines and DLT template scrubbing with resources to help you every step of the way.

Flexibility

Working on the REST format, our OTP SMS APIs are highly programmable to work with your enterprise tech stack and generate key insights on performance.

Book a Demo