TRUSTED PROVIDER

Essential checklist for choosing the right messaging provider

When choosing the right messaging provider, it's important to ensure they cover all your essential messaging needs while meeting security and compliance requirements. Make sure a provider is the right fit for you by asking these essential questions:

Messaging value chain	Is the supplier directly connected to the MNO for each destination? If not, what is their delivery chain?	Significantly lower price points for non-direct solutions can indicate the use of SIM farms, grey routes, AIT blending, or message trashing. Additional hops in the chain increase the risk of this happening as visibility decreases. Support tends to be worse for multi-hop solutions, as more parties would need to be involved in escalation processes.
Feature support	Which type of sender ID is supported and delivered to the handset?	Limited sender ID support may suggest that an overwrite is being used to bypass a filter and go undetected. It may also suggest a SIM farm is in use.
Feature support	Are handset delivery receipts supported?	If handset delivery receipts are not supported, it may suggest that the supplier is trying to hide the true deliverability and capacity metrics. It also suggests that non-trusted routes are being used, such as SIM farms. This can potentially be an indication of message trashing.
Feature support	What encoding and concatenation support is available?	No concatenation support suggests that a SIM farm or alternative non-trusted route is being used. However, there are end networks that don't support all encoding. There are direct connections that don't support real handset delivery receipts due to regulatory/privacy rules in the country.
Capacity	What type of throughput is offered for this particular solution?	Low-cost solutions often come with limited throughput that is shared across many customers. This can lead to message delays. It's important to note that there are other factors that could affect throughput, including operator throughput specifications and vetting. However, the right provider with great carrier relationships can help navigate these complexities.
Service requirement	What support does the provider offer for two-way messaging?	If two-way messaging is required, you will need to use inbound numbers, preferably in each market where you intend to offer service. You can also use numbers that can be reached internationally, but this will require your customers to pay extra costs. The availability and terms for acquiring inbound numbers differ between suppliers and geographical markets, so the provider should outline their prices and delivery time for each market you're interested in.
Service requirement	What content support does the provider offer to ensure the messages are delivered?	Message length: SMS standard allows for messages of up to 160 characters. However, it is possible to send longer messages with concatenated SMS. Language: The languages supported by an SMS supplier are mainly determined by the character sets they accept. There are different character sets used to represent different alphabets and writing systems, and your provider must accept character sets that support the languages you communicate in.
Service support	What support does the provider offer?	Sinch provides 24-hour dedicated support with engineers, as well as commercial teams covering all time zones. We strive to solve any issues/ enquiries as quickly as possible.

Sinch: A trusted provider for your messaging needs

When choosing a messaging partner, pay attention to whether they follow industry best practices and requirements – this will help protect your business.

Security and compliance are non-negotiable. Any mishandling of customer data or failure to comply with regulations **can lead to severe legal consequences and reputational damage**.

We believe all companies communicating with their customers using SMS should do the following:

Know your supplier	Is your messaging provider a signatory of Mobile Ecosystem Forum's Business SMS Code of Conduct? Has it been awarded the Trust in Enterprise Messaging badge? Is your messaging provider connected directly to mobile network operators?
Know your messaging delivery chain	Ask your suppliers to disclose how they route your business messaging traffic for delivery to your customers on a destination network-by-destination network basis. Ensure your supplier contract specifies your right to ask your supplier to provide proof from the mobile network operator that a direct connection is in place.
Know your data protection risks	Back-to-back contracts along the length of the message delivery chain are key to ensuring that the described route is authorized, legal, and that all relevant parties are accountable. Brief your Data Protection Officer and make sure all contracts include personal data management requirements.
Audit your suppliers	Use a testing service to establish how your business messages are sent.

Strong security and compliance standards

Choose a messaging provider who prioritizes compliance with local laws and regulations, maintains a network of data centres in various locations, and upholds GDPR and CCPA standards. Their distinct certifications will not only enhance data security, but also give your customers confidence in your commitment to protecting their sensitive information.

At Sinch, we're **GDPR** and **CCPA compliant**, **MEF Code of Conduct approved**, and we proudly hold **PCI** and **ISO27001 certifications**. Those aren't just acronyms to us – they represent our unwavering commitment to the highest standards of security and compliance.