secure trust in rich business messaging

Unless service providers and brands get verification right — and soon — fraudsters will exploit RBM chatbots the way they do text messaging and other digital channels.

consumer trust is key for RBM to live up to its potential

The stakes for conversational commerce continue to rise. With the adoption of Rich Business Messaging (RBM) chatbots entering the fold, Juniper Research[1] estimates online and physical retailers will save $439 million annually in customer service expenses and drive $112 billion in retail sales by 2023. Realizing those savings and the increased sales, however, is dependent on one fundamental element: trust.

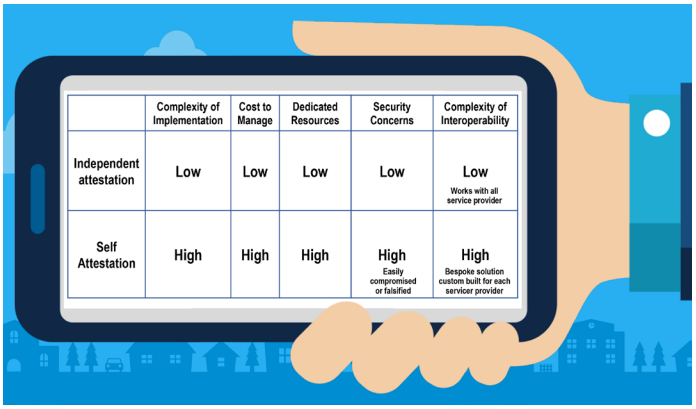
To establish and maintain consumer trust, the mobile ecosystem is counting on an industry-standard framework that authenticates and verifies the identity of each business that is using Rich Communication Services (RCS) chatbots to engage consumers. That's no easy task considering that RBM is an open ecosystem for businesses of all types and sizes. As a result, huge volumes of business chatbots will be active on each service provider network at any given time.

Even with a framework in place, businesses and service providers have to decide on the best way to verify the identity of a business. Two main options have emerged: self-attestation or independent attestation.

verification 101

Digital signatures are used in a wide variety of e-commerce, banking, enterprise, government and other applications to verify the identities of people and companies accessing their systems. This proven approach is among the reasons why they're also an ideal way for service providers to verify the trustworthiness of business senders using their communications channels to engage consumers.

A digital signature uses a private key that's decoded against a matching public key, which is linked to a business or other organization via a digital certificate. These key pairs require participants to invest in a robust Public Key Infrastructure (PKI) policy to secure and scale that mechanism. To use digital signatures for RBM, service providers have two options: They can allow brands or messaging service providers to self-sign their digital identities, each under a unique certificate, or have a neutral, trusted third party sign these digital identities on their own certificate as an attestation of the business' authenticity. Each option has its pros and cons for wireless service providers.



	Complexity of Implementation	Cost to Manage	Dedicated Resources	Security Concerns	Complexity of Interoperability
Independent attestation	Low	Low	Low	Low	Low Works with all service provider
Self Attestation	High	High	High	High Easily compromised or falsified	High Bespoke solution custom built for each servicer provider

[1]https://www.juniperresearch.com/press/press-releases/chatbot-interactions-retail-reach-22-billion-2023

self-signing:

Is self-signing as easy, inexpensive and effective as it initially appears?

considerations for service providers

Some service providers may be willing to trust self-signed certificates from businesses that they already have relationships with. This presumes the businesses are adequately securing their private key so no other entity can impersonate them. However, the business may need to share this key with application providers that will send messaging content on their behalf. This may require sharing these keys with multiple partners further exposing the keys to potential compromise. And what about all of the businesses they don't have relationships with? If identities are self-signed what keeps fraudsters from impersonating a legitimate business sender? Under the self-attestation model, two verification model would need to be maintained.

Having a certificate used for digital signatures by every business sender either requires service providers to invest in a rigorous Certificate Policy or allows for bespoke certificate policies maintained by each of the business senders, which may differ in significant ways. Is it reasonable that a wireless service provider can be a relying party for all these potentially different policies and still maintain certainty in the authenticity of all these business senders? There are also many technical components and procedures to create, manage, renew and revoke these certificates and manage the vast inventory of public certificates, which wireless service providers will likely need to support in this model.

considerations for businesses

Businesses will need to work with multiple service providers to serve all of their customers, as they already do with SMS and voice calls. Since digital signatured are unique to each service provider, there is added complexity that may make it impractical and unsustainable. It is also expensive, even for their application provider partner, to set up a secure PKI to manage the lifecycle for the private/public key pairs used in digital signatures for every business customer.

Businesses and their application provider partners that want to issue their own verification must balance the different opinions and requirements believed to be sufficient for verification. This is further complicated because some application provider partners may verify only the customer's payment instrument while others may use various data sources to thoroughly verify a customer's identity (i.e. Know Your Customer (KYC). The lack of consistency for processes, procedures and education dilutes the credibility of self-issued certificates and self-attestation.

Businesses, unfamiliar with the service provider's PKI-compliant procedures, will also need to rely heavily on application provider partners to navigate these processes for each service provider.

our take

The self-signing model appears to be faster and less expensive to implement but appearances can be deceiving. To accept self-signed certificates used to digitally sign chatbot identities, service providers must implement a system to verify that those businesses are operating under a robust and accepted Certificate Policy and root of trust before they rely upon those digital signatures. This creates an extraordinarily complex undertaking for the ecosystem, with each service provider potentially operating with a massive number of bespoke PKIs and tens of thousands of participating businesses.

Any initial savings quickly evaporates as RBM interactions scale up, making this bespoke PKI system increasingly expensive to maintain. The ROI is weak because no matter how much a service provider spends on supporting a diverse PKI environment, the system will provide only local verification. The rest of the ecosystem may not accept a self-signed certificate for the same reason no country will accept a traveler with a homemade passport: Neither is backed by an authoritative entity that has thoroughly vetted each user's identity.

Finally, if the private key used for any one self-signer was compromised, it would enable a bad actor to sign a number of fraudulent chatbots. If the root certificate for the signer were compromised, hundreds of falsified certificates could be shared amongst bad actors. That could be a massive setback for consumer trust in RBM. Service providers will invest heavily to manage that vulnerability and likely will need to pass that cost on to the business senders and their application provider partners.

independent attestation:

Will a verification authority reduce complexity and vunerability?

considerations

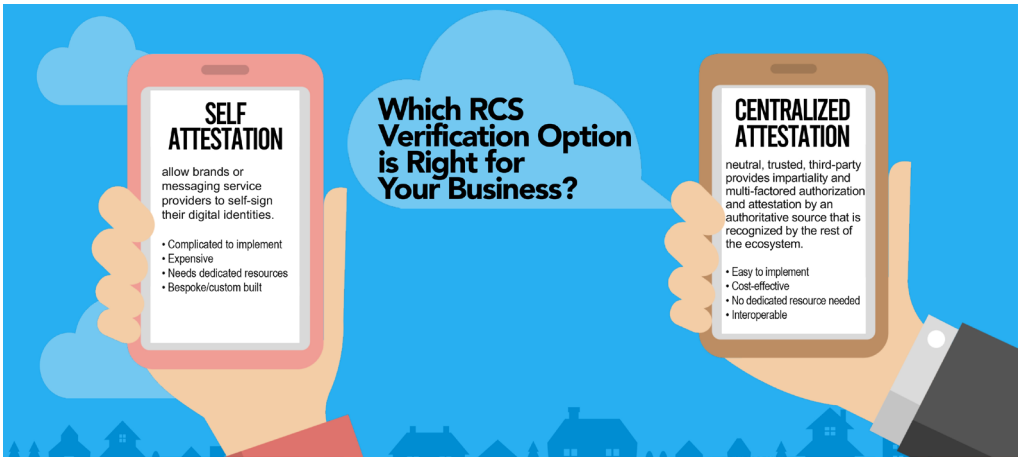
An independent third-party Verification Authority provides impartiality and multi-factored authorization and attestation by an authoritative source that is recognized by the rest of the ecosystem.

A Verification Authority reduces fraud risk by providing a neutral set of eyes to validate a brand and its authorized chatbots. It provides the kind of comprehensive protection that each wireless service provider cannot necessarily achieve with internal checks and balances in a model with self-signing by business senders. For example, a Verification Authority has the resources necessary to identify fraudsters masquerading as brands that a service provider already works with. Absent independent verification, a service provider may inadvertently onboard some of those imposters, especially as RBM's popularity grows, leading to a growing number of nefarious new chatbot requests entering the ecosystem. A Verification Authority is much better suited to accommodate the necessary security, at scale.

our take

The ideal Verification Authority should be a neutral party with proven experience providing authentication services for other types of applications, such as voice calls to combat illegal robocalling. This experience demonstrates that it has the deep knowledge and the necessary components to operate digital signatures under a PKI in a secure and trusted manner. This helps avoid risks such as compromised root certificates resulting in hundreds of falsified signing certificates shared amongst bad actors.

One potential downside of using a Verification Authority is having to pay for the digital signatures generated that attest to the business's authenticity. However, service providers will not incur these costs themselves and this expense is negligible for business senders: between 0.1% and 1.0% of the cost per year to engage their audiences. The alternative where a business entity or their application provider partner implements the lifecycle requirements for a fully secure PKI is significantly more expensive in comparison to avoiding the cost of independent verification.



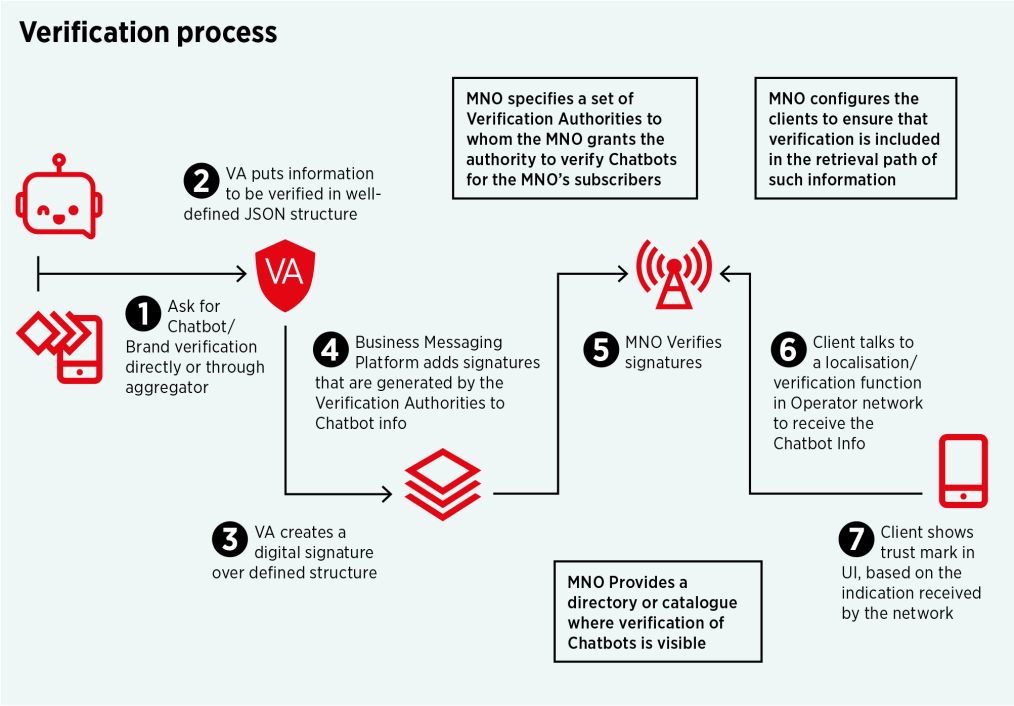
[2] https://en.wikipedia.org/wiki/Know_your_customer

verification authority models

The GSMA's RCS Verified Sender initiative is an industry effort to ensure that RBM avoid the spoofing and other fraud types that afflict SMS. It establishes trust in business-to-consumer messaging by providing a framework that verifies the business sender's identity.

RCS Verified Sender includes an independent Verification Authority that would be responsible for authenticating the identity of businesses. The Verification Authority would also verify the chatbots used by the business and would register the information in a system that shares the business' logos and other enhanced sender ID information with each participating platform provider.

This information would be digitally signed by the Verification Authority, which will help mitigate the risk of spoofing or impersonation of chatbots by fraudsters. Verified Sender content could then be presented to the consumer with an icon, such as a trust mark, to further emphasize that the sender has been verified. The service provider would also deliver this information with the sender's business name and logo so recipients could feel more confident that the business is legitimate and that the content is authentic while, in parallel, business senders can leverage brand loyalty.



iconectiv TruReach Intel

iconectiv® is helping lead the GSMA Verified Sender initiative. This role includes numerous contributions to the GSMA industry specifications and related documents based on providing decades of expertise in helping service providers and businesses with tools for ensuring consumer trust in other forms of communications, including voice calls and Application-to-Person (A2P) SMS.

iconectiv TruReach Intel provides Verification Authority services, as well as a variety of additional tools to help the RBM ecosystem manage verification at scale. It's a neutral and secure service that helps distinguish those business messages that are coming from verified senders. Those messages can then be presented to consumers as legitimate and authenticated. The solution is very efficient for business senders connecting to numerous service providers.

Service providers can use this software as a service (SaaS) solution to allow businesses access to their networks where messages and chatbots from legitimate businesses can be authenticated and verified. TruReach Intel also supports voice calls and SMS, making it a comprehensive solution for building and maintaining consumer trust with omnichannel engagement.

get it right, right from the start

Messaging application chatbot spoofing, SMS phishing ("smishing"), email spearfishing and illegal robocalling all show that consumer trust is hard to win and easily lost. History also shows that for every technology, fraudsters always find new loopholes to exploit. The most effective response is an industry-wide, collaborative and continually vigilant effort designed to make it as difficult as possible for fraud to occur.

As a new technology, RBM has a unique opportunity to build a technological and business-process foundation to minimize vulnerabilities from the outset. By leveraging a centralized Verification Authority as the foundation for ensuring trust in RBM communications, the ecosystem can protect consumers, legitimate businesses and the RCS market opportunity.

about iconectiv

Your business and your customers need to access and exchange information simply, seamlessly and securely. iconectiv's extensive experience in information services and its unmatched numbering intelligence helps you do just that. In fact, more than 2B people count on our platforms each day to keep their networks, devices and applications connected. Our cloud-based Software as a Service (SaaS) solutions span network and operations management, numbering, trusted communications and fraud prevention. For more information, visit www.iconectiv.com.
Follow us on Twitter and LinkedIn.

make the connection.

For more information about iconectiv, contact your local account executive, or you can reach us at:

+1 732.699.6800

info@iconectiv.com

www.iconectiv.com