RCS Verified Sender

Product Feature Implementation Guideline

March 2019

RCS VERIFIED SENDER

About the GSMA

The GSMA represents the interests of mobile operators worldwide, uniting more than 750 operators with over 350 companies in the broader mobile ecosystem, including handset and device makers, software companies, equipment providers and internet companies, as well as organisations in adjacent industry sectors. The GSMA also produces the industry-leading MWC events held annually in Barcelona, Los Angeles and Shanghai, as well as the Mobile 360 Series of regional conferences.

For more information, please visit the GSMA corporate website at www.gsma.com. Follow the GSMA on Twitter: @GSMA.

This is a Non-binding Permanent Reference Document of the GSMA

Copyright Notice

Copyright © 2018 GSM Association

Disclaimer

The GSM Association ("Association") makes no representation, warranty or undertaking (express or implied) with respect to and does not accept any responsibility for, and hereby disclaims liability for the accuracy or completeness or timeliness of the information contained in this document. The information contained in this document may be subject to change without prior notice.

Antitrust Notice

The information contained herein is in full compliance with the GSM Association's antitrust compliance policy.

Contents

1 Introduction

Overview

Before the advent of Rich Communications Services (RCS), a phone number was the only identifier for branded messages. As it would be unlikely for the number to be in the recipient's contacts, this makes it difficult for users to verify whether they are actually dealing with the brand in question, potentially prompting them to ignore messages or even report the number as spam. This also led to opportunities for misbehaviour such as "smishing" (SMS phising).

One of the new features of RCS Business Messaging is the ability to verify senders. Once the brand has been verified by a Verification Authority (e.g. specialised entities who offer this service in other sectors, Mobile Network Operators (MNOs) themselves, Chatbot Platform providers, etc), their logo will show at the top of the conversation, along with their official brand name, brand colour and a User Interface (UI) indication to designate the verification status, for example a check mark.

For this verification to be validated, the party operating the Chatbot is checked to ensure that it is entitled to use the name and logo associated with the Chatbot. By including the indication in conversations and search results, brands can ensure their communications are more secure, providing a greater sense of trust for their customers.

Opportunity

RCS is a distributed ecosystem with interconnected parties, with operator messaging being a trusted and well-known service. The ecosystem relies on trust in other parties; one party not being sufficiently diligent could potentially harm the entire ecosystem.

Brands already use trust-marks on internet and over-the-top (OTT) services. Having something similar available to operators is a hygiene factor that will help to retain and enhance trust in operator messaging.

MNOs believe that fraud takes an average of 9.4% of Application to Person (A2P) revenue[1]. Spam and SMiShing are becoming a concerning issue which could potentially put MNO messaging at risk. SMS remains an important element of the messaging ecosystem, but it does not allow the recipient to confirm the identity of the sender. This can now be addressed under RCS.

Scope

This document considers the use cases, business model and business architectural considerations implicit in the deployment of RCS Sender Verification. It seeks to provide guidelines on how to deploy and realise the concepts defined in Universal Profile v2.2. The Sender Verification process ensures that the attributes, for example name and logo, associated to the Chatbot address match the party that is authorised to use that address and results in an indication to the user that this is the case

It should be noted that the Sender Verification feature requires the Chatbot Address to not be susceptible to spoofing. Spoofing prevention is handled by internal procedures in the MNO network and the Chatbot Platform, however, these are out of scope of this document.

[1] What MNOs think about A2P Messaging. An A2P Monetisation Study by Mobile Ecosystem Forum, November 2018

2 Feature Architecture

Universal Profile version 2.2 introduces the concept of Verification Authorities that verify whether the Chatbot is entitled to use the name and logo that are shown to the user in the UI. If a Verification Authority that is trusted by the operator has verified a Chatbot, the UI will show an indication to the user that the Chatbot has been verified. In the case that Chatbots are not verified, or have been verified only by Verification Authorities that are not trusted by the operator, they will remain available to the user, but the verified indication will not be shown in the UI.

Actors and Roles

Before going into the details of the Sender Verification process it is worth briefly looking at the ecosystem entities, partners and 3rd parties and describing their functions, roles and, responsibilities within the value chain.

Brands

A brand is the commercial entity interacting with the customer, and as such, wants to be verified as a business message sender. A brand needs to provide all of the information necessary for the verification process. This would be shared directly to the entity performing the verification role or through an independent aggregator.

Aggregators and Messaging Partners

Aggregators and messaging partners provide connectivity, hosting and simplify aggregation services towards RCS Business Messaging Platforms. RCS Business Messaging Platforms are traditionally provided by operators or can be hosted by a 3rd party provider. Messaging partners can offer further hosting services and tools, like Chatbot Platforms, which can also support the design and development of Chatbots.

Aggregators and messaging partners may be responsible for collecting analytic data for the brand they represent on behalf of the Verification Authority, as a first stage of verification. However, for the criteria defined in Appendix B to be fulfilled, some direct communication between the Verification Authority and the brand is required.

Verification Authorities

A Verification Authority could be, but is not limited to, a commercial business, for example verification companies from the internet world, an operator or a government department.

The Verification Authority determines whether the Chatbot to be verified is entitled to use the name and logo that it provides in the Chatbot Information, according to the criteria defined in Appendix B. Proof of verification is in the form of a digital signature that is provided to the Business Messaging Platform. A successful verification confirms that the Chatbot is allowed to represent the identity that their name and brand icon represent.

Business Messaging Platforms

The RCS Business Messaging Platform enables brands and aggregators to connect to operator RCS services and exchange rich messages with users. The RCS Business Messaging Platform function and role in the verification process, is to add the signature that it receives from the verification authority to the Chatbot information, which is transferred to the MNO network.

Mobile Network Operators (MNOs) – RCS Service Provider

RCS is an operator service. They grant the right to a Verification Authority to verify on their behalf. An MNO can specify a number of Verification Authorities that they grant this responsibility to and the GSMA, on behalf of its members, plans to publish and maintain a list where the approved verification authorities are visible, along with the MNO that has granted them this right. This makes it easier for brands and aggregators to find the minimum set of verification authorities that might be used for the networks where they want their Chatbot to be considered verified.

The MNO confirms whether the signature(s) provided by the Verification Authorities matches the Chatbot Information. If it does, the MNO provides an indication to the client that the Chatbot has been verified. To do this, the MNO must configure the client to ensure that requests for Chatbot Information are routed to a function where the signature of the Verification Authorities can be verified.

Clients or Messaging Application

Clients are the messaging applications in users' devices. Clients that receive the verification indication from the MNO, will show an indication in the UI that the Chatbot has been verified. Clients should also be able to show which party verified the Chatbot and when the verification will expire.

Clients that are not configured to route their request for Chatbot Information to the MNO network or that do not receive a verification indication from the network for a Chatbot, will not show an indication in the UI that the Chatbot was verified. This will assist the verification ecosystem to mature avoiding potential negative security concerns.

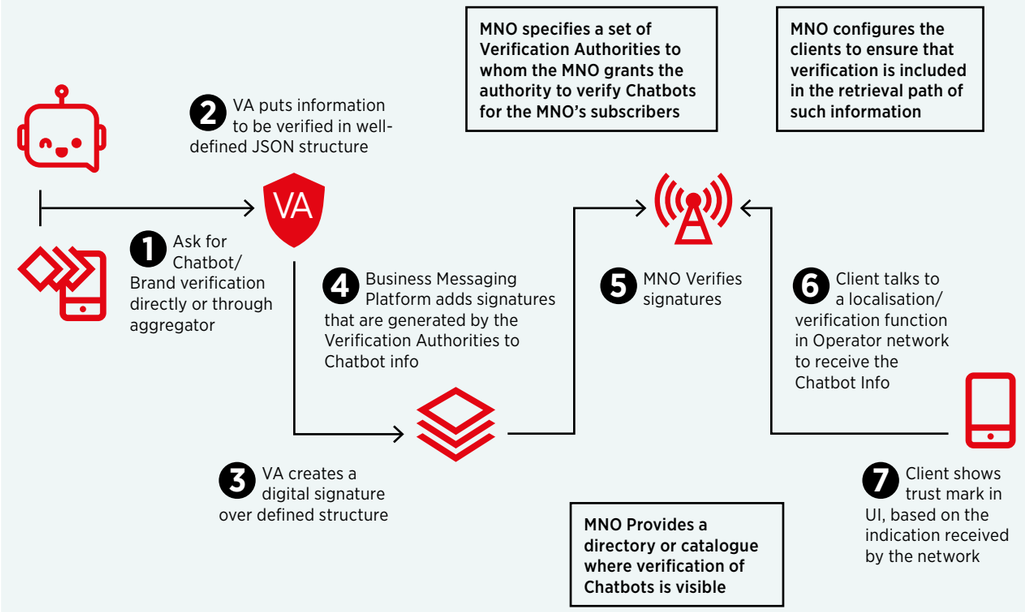
Process

The process for the Chatbot/brand verification is defined in the Rich Communication Suite 8.0 Advanced Communications Services and Client Specification (RCC.07). See Appendix A.

Criteria for verification

A set of criteria that is accepted as a common baseline is necessary to ensure consistency and to help build trust amongst all players in the ecosystem. Even if there is an established process that is accepted by all, trust is a necessary ingredient for Sender Verification to work and to be able to achieve interoperability among solutions. The suggested criteria can be complemented or substituted by equivalent established business practices. See Appendix B.

Verification process



3 Deployment Options

The previous section describes all roles as separate – however when deploying the solution, they can potentially be merged and performed by one party, especially for roles that are new to the ecosystem.

For example, an MNO could take on the role of the RCS Business Messaging Platform provider and/or Verification Authority or an RCS Business Messaging Platform provider might want to take on the role of the Verification Authority. It is recommended that the role of the Verification Authority is an independent party, fully aligning with the role as defined in Universal Profile 2.2, otherwise this could lead to issues when scaling the ecosystem. Chatbots would need to be verified by a number of Verification Authorities to ensure that they are marked as verified to all users in the countries/regions where they intend to be active.

In cases where an MNO's RCS Business Messaging network is hosted by a third party, we have seen that the Business Messaging Platform may take up the role of the Verification Authority. This is a merging of roles and can still follow the necessary steps for a full verification. However, it is only advisable for an ecosystem at its infancy; as soon as the RCS Business Messaging ecosystem starts scaling, a full implementation of the recommended process should be selected. In any case, as with any verification authority, the MNO has the right to perform due diligence checks to ensure that it is satisfied by the criteria that are checked.

Independent Verification Authorities could be companies that perform a similar role in other sectors, national authorities or an entity that is created for this reason. In certain cases, MNOs could look at selecting a centralised verification authority at country or even regional level.

The number of authorities used by MNOs will depend on the market and region. It is expected that the list of MNO-trusted Verification Authorities is unlikely to change frequently (after a ramp-up period). MNOs in certain regions could be aligned when selecting Verification Authorities, to try to avoid fragmentation and making the process less cumbersome for brands and aggregators. What becomes important is to align the processes that are followed by Verification Authorities, enabling mutual trust between entities and helping the system become interoperable.

4 Considerations

Liability

Where the liability lies within the Sender Verification process will depend on where the fraud would eventuate, existing contracts between parties, and whom the Chatbot is “verified by”. The liability will also cascade, based on the aforementioned factors.

Cost of verification

Who pays for the verification and how much it will cost remains to be defined. As the ecosystem develops, existing players may be willing to perform the tasks for the verification process for free to attract brands. However, in an ecosystem at scale that cannot be the case, similarly to the World Wide Web ecosystem, the entities performing the verification will have to be paid for their services. The GSMA does not expect these fees to be higher than the fees for a website verification.

Transition to P2A

For Person to Application (P2A) verification it is very important in the discovery process for users to discern whether a Chatbot is related to the brand that they want to contact. This means that the verification status of Chatbots has to be shown in the Chatbot directory and search results. This will follow a similar process as the one described in Appendix A.

Different companies may use the same brand name, e.g. when active in different regions or countries. This means that there may be cases (for example franchised businesses) where the same name is allocated to different Chatbots, where they all pass the verification criteria.

5 Conclusions and Recommendations

Sender Verification is a key RCS feature that can drive the adoption of RCS business messaging through increased trust. For major brands, it presents significant value in brand management and provides additional fraud and security protection for products and services.

The verification ecosystem includes multiple roles, which adds to the complexity of implementation. It might be required that a step-by-step approach is taken. At the same time, a commitment by all ecosystem players to the specification is crucial to avoid fragmentation, which would hinder interoperability and the establishment of trust in the RCS ecosystem. In such a varied environment, the importance of a common approach and criteria for verification is vital.

The GSMA will next shift its focus to identifying entities that could play the role of the Verification Authority at country and regional levels. The aim is to publish a list of available authorities in the next 12 months for easier roll-out of the feature.

For brands

Verified sender provides a good means to discern a brand's Chatbots from any party attempting to impersonate the brand. Brands are therefore recommended to have their Chatbots verified. This will ensure that users expect to see the verification mark in the UI when communicating with a brand that they value and be suspicious of attempts at malicious behaviour when it's not there.

With verified sender on top of the increased security that it offers over SMS, RCS becomes a great candidate for any messaging that requires secure communication, e.g.it could be used to replace SMS for 2-factor authentication. Brands in markets where RCS has launched and has significant market coverage could consider using RCS for these purposes.

For implementations

For an immediate roll-out of the feature, the ability to show a check-mark in the client should be prioritised so that users get used to seeing the verification check-mark when communicating with a brand.

Operators and RCS Business Messaging platforms should prioritise the introduction of the verification in their implementation to allow the associated UI indications to be shown to their subscribers. This can happen without a full implementation of the specification described above. However, the GSMA will be making the full implementation of the feature a requirement for future accreditation of device and platform providers in the future.

MNOs who roll-out the Sender Verification feature are also advised to educate end users on the meaning of "verified by". This can vary from a notification when the user encounters it for the first time to a full campaign. This would ensure that end users are aware of the importance of the verification status.

Appendix

Appendix A

The steps for the verification process are summarised below:

1. The Chatbot/brand asks to be verified
2. Verification authority puts information to be verified in well-defined JSON structure
   a. Name, Signature/Hash of icon file, Chatbot Address (called Service ID)
3. Verification authority creates a digital signature over defined structure
4. Verification Authority's signature is added by Chatbot Platform to Chatbot Info
   a. i.e. also Chatbot Platform needs to accept Verification Authority
5. Client request for Chatbot Info request is routed to a localisation/verification function in operator network
   a. Function verifies signature and compares verified data to actual Chatbot Info
   b. Provides verified/not-verified indication to the client
   c. NOTE: actual verification process is network internal and operator may take short cuts
6. Client shows trust mark in UI based on indication received from network

Note: The process for search results will be similar, but the Service Provider Directory is used instead of the localisation function

Signature creation and verification are based on public/private key cryptography. The MNO (service operator) needs to have the Verification Authority's public key for verification.

Any change of the Chatbot brand icon, the Chatbot service name and the Chatbot Service ID shall require a renewal of the verification. Changes in other areas of the Chatbot Information shall not require renewal of the verification.

The verification status shall have a validity period and shall have to be renewed after expiry if representation of the trust mark is still required.

For more details on how the process works please see footnote[2].

Appendix B

Verification Authorities should validate and verify the following criteria to ensure consistency in providing verified status to brands and Chatbots:

- Name of organisation
- Company registration details
- Address
- 2FA of publically listed contact number for business
- Government-issued identity of the requestor
- Business headed letter to confirm authorisation to set up service, use of brand logo etc.
- Prove Chatbot name is linked to business and does not contravene trademark or copyright issues (e.g. copy of a registered trademark certificate or details of a registration that can be verified on a register)
- Verification that company has permission to use brand (group entity verify child entity or child entity has group entity approval) – Child brands might need to be re-verified as they might not fully represent their parent entity
- MNO to provide authorisation for verified bot (optional, subject to commercial arrangements)
- If Chatbot name of verified Chatbot is locked, when Chatbot name is changed, a re-verification process will need to take place.

[2] For more details on how the process works please refer to RCC.07 3.6.3.2.1 and 3.6.4.2 on www.gsma.com

Definitions and Abbreviations

Definitions

Term	Description
A2P	Application to Person messaging is uni-directional message where there is no expected reply from the recipient. A2P messaging includes but is not limited to marketing messages, appointment reminders, notifications and pin codes.
Aggregators and messaging partners	Companies that offer a variety of value-added services to enterprises – not the least is messaging connectivity into multiple wireless providers.
Business Messaging Platform	Enabler layer to enrich communication between businesses (content and service providers) and MNO messaging users
Chatbot Discoverability	The mechanism for the customer to discover Chatbots, Plugins and Chatbot Platforms provided by a third-party, an MNO, or a combination (MNO hosted platform on a third party).
Chatbots	A service provided to users whose output is presented in a conversational form and which provides some kind of value to the users. Often a piece of software interfacing with one or more users aiming to simulate intelligent human conversation.
Chatbot platform	A system that provides a mechanism for Chatbot developers to create and register Chatbots, which can then be exposed to the users connected to the platform through a messaging system.
Chatbot Profile Information	Additional information provided by the Chatbot to the user that allows the user to e.g. contact the Brand operating the Chatbot over other channels, or better understand what the purpose of the Chatbot is or what the Brand operating the Chatbot does.
Content Owner	Any company or organisation who has a message or content they want to get to any user.
P2A	Communication initiated by the end user.
Sender Verification	RCS feature that enables to verify that the party operating the Chatbot is entitled to use the Chatbot Name (e.g. the brand that it includes) and Chatbot Logo. The Verification is linked to Chatbot Address i.e. it guarantees that the party operating the bot at that address may use the name and logo.
SMiShing	SMS Phising – Sending text message(s) to an individual's mobile phone in an attempt to get them to divulge personal information. Could include a security attack in which the user is tricked into downloading a Trojan horse, virus or other malware onto his cellular phone or other mobile device.
Spam	Mobile message, which is sent to a customer, which the sender does not have the permission of the recipient to send. Therefore, in the context of this document it refers to unsolicited RCS and SMS messages of a commercial nature.
Verification Authorities	A provider of verification for Chatbots. Verification Authority is responsible for verifying and validating brands and chatbots against specific criteria.

Abbreviations

Term	Description
A2P	Application to person
GSMA	GSM Association
MNO	Mobile Network Operator
OTT	Over The Top
P2A	Person to Application
RBM	RCS Business Messaging
RCS	Rich Communication Services
SMS	Short Message Service
UI	User Interface
VA	Verification Authority

Find out more at
www.gsma.com

GSMA HEAD OFFICE
Floor 2
The Walbrook Building
25 Walbrook
London EC4N 8AF
United Kingdom
Tel: +44 (0)20 7356 0600
Fax: +44 (0)20 7356 0601