MEF

FUTURE OF MESSAGING PROGRAMME

RCS Business Messaging

BEST PRACTICES

Implementation guidelines to support the effective launch of A2P & P2A messaging services

June 2019

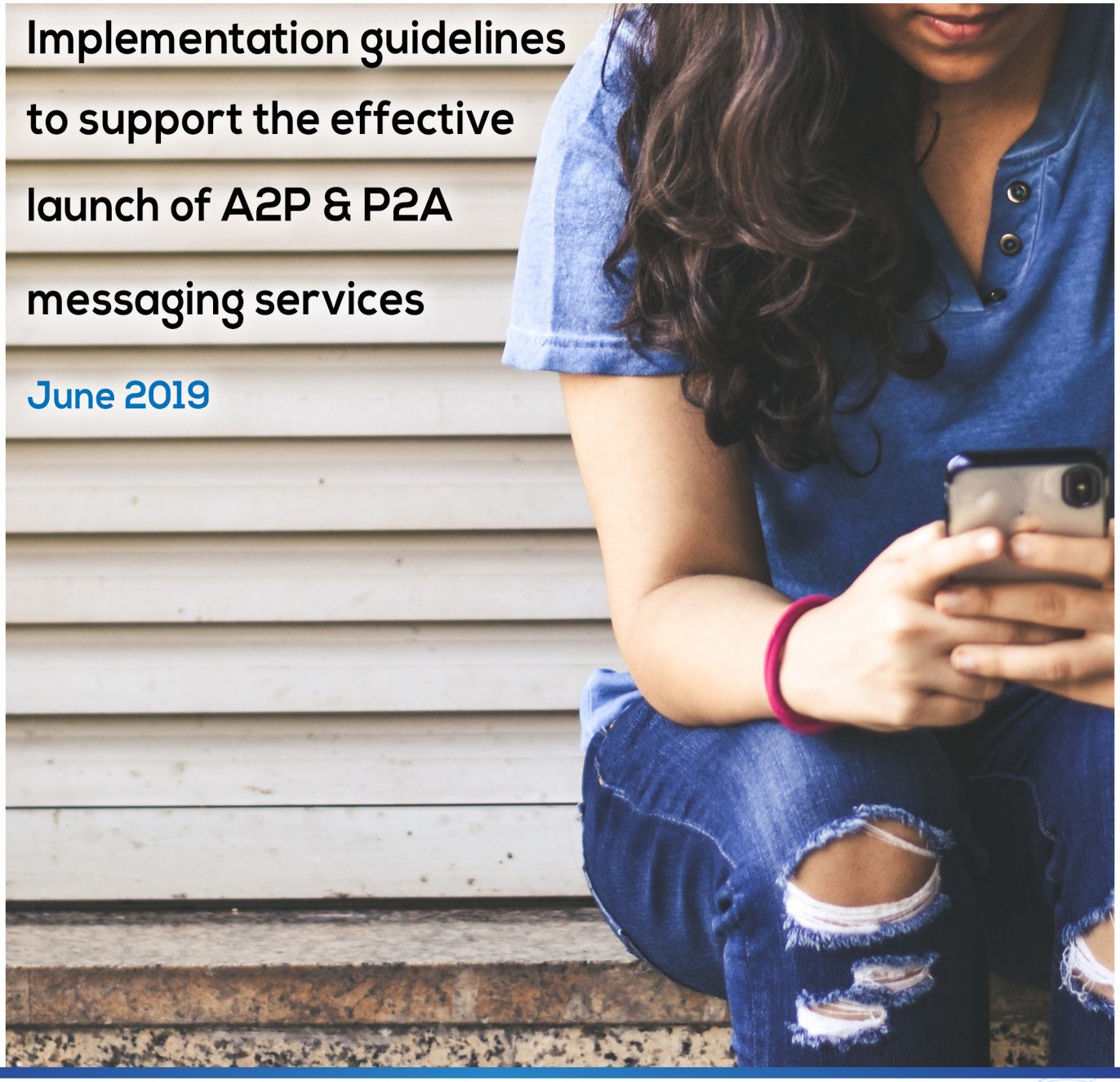

TABLE OF CONTENTS

Executive Summary

Overview

The mobile industry is rolling out a new messaging platform for personal and business communications: Rich Communications Services (RCS). Its business use cases are particularly interesting as the interactive features of RCS enable both application-to-person (A2P) as well as person-to-application (P2A) messaging.

RCS Business Messaging (RCS BM) builds on strong fundamentals: the success of A2P SMS services; it has support from leading players in the industry including mobile operators, Google and the Android ecosystem, as well as device makers, messaging and solution providers. However, implementation is complex due to the fragmentation of its ecosystem.

Competing services to RCS, including OTT platforms such as Apple Business Chat, WeChat and WhatsApp, rely on single stakeholders that define the commercial approaches. RCS as an open standard, is less rigid and has more options. While RCS will benefit from the creativity and differentiation that open standards developed by multiple stakeholders bring, lack of alignment on some fundamental options could seriously limit its scalability and effectiveness.

These guidelines aim to provide a framework for the technical and business options for deploying RCS BM and streamline the processes for a successful launch of RCS business messaging. They provide best practices generated from the experiences of MEF's members who represent the full value chain from enterprises to the enablers and service providers in the messaging industry.

We believe that providing guidance and simplification will enable a faster and more efficient launch of A2P and P2A messaging via RCS.

Introduction to RCS Business Messaging

RCS is a messaging technology standard. Its features, detailed in Universal Profile 2.0[1] of the RCS specification, include several advantages for business messaging such as sender brand and logo, sender verification, message-received and message-read statistics, rich media including image and video carousels and suggested-reply buttons. It also includes innovations to help mitigate spam and fraud in business messaging.

Commercial deployment of RCS is accelerating with 75 networks currently live and an additional 90 launches by the end of 2019 estimated, including seven markets where all MNOs will be supporting RCS. [2] RCS is forecast to be the world's largest messaging platform by 2020 with an estimate of $18 bn spend on business messaging via RCS by 2023.[3]

Key Recommendations

The guidelines provide recommended best practices across seven key areas and are summarised below.

[1] https://www.gsma.com/futurenetworks/rcs/rcs-documentation/
[2] GSMA forecast
[3] Mobile Squared research

COMMERCIAL TEMPLATES

The introduction of RCS BM with its enhanced functionalities to support conversational commerce and improve consumer engagement can substantially increase the value-add of messaging for enterprises, digital marketing agencies and other Message Service originators. It provides an opportunity to evolve the commercial models for business messaging from its traditional commodity-based single message delivery rates towards other models prevalent in the digital marketing and internet marketing industries.

Trials of new charging models by the MNOs and the business messaging community including trials of hybrid models (where usage and success fee can be mixed) at launch, even if the operator community is not ready, will help accelerate learning and adoption.

1. **Charging Principles**
   A minimum 'common approach' should be adopted for a **period of 12 months from launch to provide a transition period from A2P SMS models and to encourage conversational messaging (P2A).** The following should be supported:
   a. **Per message charging**
   b. **Per session charging** with the standard implementation as recommended with a **24-hour response window and a 4-hour session duration**

2. **Common Definitions**
   MEF encourages the use of its standardised definitions for charging models.

3. **Business Messaging and User Charges**
   a. **Charging for Metadata.** At a minimum, the cost of downloading RCS metadata for the business profile (e.g. branding of conversation) should be free to the end user
   b. **MNOs should free rate the end user receiving RCS traffic for business communication**. It is in the interest of the industry to avoid bill shock to users.

4. **Early Access to Charging Tools**
   MNOs should act as soon as possible to establish charging on an introductory basis for A2P RCS to allow market testing and development

INTERCONNECTION

RCS is a network of multiple mobile operators' services, to make the service truly accessible all of these operators would have to support business messaging. Universality was a crucial element for the success of SMS, and it should be offered by RCS as soon as possible.

1. **Technical Support/Compatibility**
   MNOs and vendors should launch Universal Profile 2.0.

2. **Commercial Interconnection**
   Each MNO, Hub and Messaging Solution Provider should map its path for universal reach. Overall, a target of 100% interconnectivity for A2P and P2P traffic should be in place from day one. The use of hubs is an important tactical solution to achieve universal reach.

3. **Separation of P2P and A2P Traffic**
   MNOs should adopt usage policies which mandate separate interconnection routes for A2P and P2P traffic and exclude A2P traffic from the P2P channel; routing P2P traffic via the NNI and A2P traffic via a MaaP gateway. Continued monitoring of the NNI interface for grey route A2P traffic is advised.

4. **Additional improvements in traffic routing**
   - Access to a central database identifying the MNO serving a particular MSISDN (where one exists) to be accessible to non-Operators as well as Operators
   - Access to be granted at a commercially feasible rate to non-Operators
   - Where a central database does not exist, treatment of any data charges incurred while trying to find the correct MNO should be agreed and communicated in a common way; at a minimum at a national level

PERMISSION MANAGEMENT

Regulation and good business practices require all businesses to acquire permission to send messages from their customers.

1. **Enterprise Opt In - Inclusion of RCS in terms and conditions**
   We encourage enterprises to include an explicit reference to RCS ("RCS communication" or "mobile data messaging") in any terms and conditions relating to data collection as soon as possible (e.g. MEF templates).

2. **MNO – Simplifying End User Charges**
   MNOs should position RCS as a technical upgrade to SMS and ensure there is clarity on end user data charges – making additional opt in redundant. SMS thrived in its simplicity; MNOs should allow for the enterprise to cover the cost to the recipient of the messages. Alternatively, enterprises should consider implicit acceptance of data charges already agreed by users in their terms and conditions. (e.g. MMS or email)

3. **P2A Consent**
   If the end user is already known to the enterprise, another opt-in should not be required for first time bot interaction. However, an end user contacting an enterprise via P2A RCS (via a chatbot) does not automatically give consent to be sent A2P messages at later date – the enterprise should request permission to send further messages in the future.

4. **Opt- Out**
   The same procedure as SMS should be offered to opt out of receiving RCS messages and similarly, an unsubscribe list of end users who have asked not to receive RCS business messages should be maintained

FRAUD PREVENTION

RCS presents higher security mechanism than SMS. However, the fight with fraud is a continuous one.

1. **Fraud – A Continuous Fight**
   It is imperative that fraud prevention is built into the processes from day one.
   a. RCS Network Providers and MaaP providers should **develop effective policies and procedures** for detecting and blocking fraudulent messages.
   b. MNOs and MaaP providers should routinely include an **RCS Firewall** as part of their requirements within their RCS tender / purchase process.

2. **Industry must support a unified sender verification process**

   Brand registration in a verified sender programme is an important enabler in establishing secure communication and fighting fraud. The service should become a hygiene factor, readily available at low cost for all enterprises. To facilitate this, MNOs should appoint a common verification authority across all networks, at a minimum nationally.

   a. Financial Enterprises (bank, credit cards) and other enterprises at high risk of phishing and spoofing fraud should implement Verified Sender ID as a priority (see Fraud Prevention section for details)
   b. Messaging Solution Providers should encourage enterprises to adopt sender verification across its customer base.
   c. Sender verification should be easy and low-cost so that small businesses can also implement if needed
   d. Steps should be taken by sender verification services to ensure the chatbot equivalent of cyber-squatting is prevented, and that a single verification is valid across all jurisdictions
   e. There should be either a unique national / regional verification authority, or a common level of rigour in every verification process, and mutual recognition should be agreed between verification authorities.

f. Withdrawal of verified status from a verified business should only be done due to a lack of trust in the identity of the enterprise

3. **User Fraud Reporting**
   There should be an agreed mechanism for end-users to report abuse in RCS (similar to Spam reporting tools).

4. **Education**
   Proactive education and awareness should be offered to the users for all messaging fraud, and specifically for the new RCS multimedia threats.

SPAM PREVENTION

Spam has been generally deterred in SMS, by its pay per message models. However, spam has negatively affected the other messaging platforms – and consequently their A2P markets. RCS should be rolled out with a clear intention to avoid Spam.

1. **Proactive Permission Management**
   Induction process required by MNO's and messaging platform to educate all enterprises. **Launch Checklist** to include details on permission management. **Fair use policy** specifying appropriate levels of communications.

2. **User Control- Standard Commands**
   A set of common commands used for SMS messaging should be used to give and retrieve communication permission via RCS messages across a specific language/market (e.g. "Stop")

3. **Rogue P2P Traffic Monitoring**

4. **Sharing of information on Rogue Senders**

5. **Blocking Rogue Senders.**

REPORTING

In digital marketing reporting data is a critical. The success of RCS will be dependent on how quickly it will establish a superior return on investment on other solutions. This can only be provided by data reporting that is consistent and transparent.

1. **Consistent MNO reporting**
   a. Reporting by MNOs to messaging companies should be consistent across all networks to enable consistent reporting to enterprises.
   b. MNOs should strive to provide the greatest possible level of information on receiving and opening of messages.

2. **Enterprise – Single Data Source**
   The enterprise should have a single point to receive all stats for the campaign. Reporting is a key differentiation for each messaging solution provider, it should not be left as an afterthought.

3. **Data Privacy**
   All data concerning a customer's interaction with an enterprise should be made secure and private. The chain of data processing needs to be secured.

4. **Local Regulations**
   Local data protection regulations must always be adhered to for both data protection data storage.

CHATBOT QUALITY CONTROL

The availability of many chatbots for conversational messaging will be a key the attraction of RCS However, it is recommended that some level of controls/guidance will be required to guarantee minimum usability and avoiding malicious usage.

1. MNOs / MaaP platform providers should adopt a **common quality review process for chatbots** coming onto their platform to ensure a minimum level of quality safety and user-friendliness is achieved in all RCS chatbots.
2. This should be a **single review process**; MaaP providers and MNOs should agree which stakeholder will be responsible for quality in order that messaging providers do not have to pass multiple quality reviews.
3. **Messaging Solution providers** should play a key role in the value chain to test chatbot quality and confirm suitability according to the common quality review
4. **Federation models** will allow MNOs to accept other chatbots already vetted by other MNOs. This will make for quicker scaling up in the market.
5. Development of the chatbot **quality review process should grow organically** as more chatbots come on stream. It need not be developed in its entirety before MNOs go live with RCS BM.

Best Practices for RCS Business Messaging

COMMERCIAL TEMPLATES

BACKGROUND

Part of the success of the SMS model has been its simple pricing model based on a per message charge. However, this could be also seen as a limitation; per-message charging commoditises the service leading to an emphasis on lower cost rather than improved service. Conversational commerce assumes multiple messages are being exchanged between enterprise and its customers or potential customers and per-message charging could discourage enterprises from using RCS for conversational commerce.

A significant issue with per-message pricing is that it does not capture the real value created for the enterprises in helping them achieve their KPI targets nor distinguish between them e.g. an appointment reminder is arguably less valuable than a buying decision. Stakeholders in the messaging value chain are perceived as a cost line provider by the enterprise, not as value-adding partners.

RCS is an opportunity to develop a new premium segment to complement, and in some cases, supersede A2P SMS. Commercial models should reflect the ability to enable higher-value customer engagement for brands and enterprises e.g. discovery, purchase and support and RCS BM should be considered alongside other high-value digital marketing services e.g. banner advertising and search.

RCS Message Delivery - Commercial Models for Consideration

MODEL	DESCRIPTION	CONSIDERATIONS
Per Session	Individual messages between an enterprise and a customer are bundled into a conversation 'session' and the session is the billable event, not the individual messages. This allows the enterprise to make full use of conversational chatbots and RCS in order to form a better relationship with the customer.	Having a consistent definition of a session is crucial so that there is a consistent charging basis within countries and to a lesser extent within regions.
Per Megabit	Based on data, is an alternative to per-message pricing	RCS messages can vary widely in file size and thus in cost to the MNO to deliver, and potentially to the end user, so pricing to enterprises would need to reflect that.

Access Based	Where the enterprise pays a set amount to send unlimited messages to some or all of the MNO's customers for a set period of time.	This model has been successfully deployed by OTT messaging providers e.g. Viber.
Outcome Based (or Success Based)	Where the enterprise pays for a certain outcome which may be a website visit, a purchase, a registration etc. and not for the number of messages they send to achieve that outcome	Scaling this model is challenging for the MNO billing system configuration and interconnecting with other networks. It may be that outcome-based charging is offered by business messaging companies (and MNOs moving up the value-chain to offer some of the same services as business messaging companies) based upon a per-message or per-session charge paid by the messaging provider to the MNO of the message recipient.

In addition to the delivery of RCS business messages, RCS BM also opens up new revenue opportunities in relation to preferential placement, search results and directories as well as chatbot creation and management. However, this is not the focus of these guidelines and they will be reviewed be reviewed in a separate paper.

KEY PRINCIPLES

Drawing on previous experience with SMS and MMS as well as the models for IP business messaging the following characteristics should be considered mandatory for any RCS BM commercial template:

A. **Universal** – the commercial models should be broadly adopted by RCS BM service providers and MNOs to enable brands to contact all their customers regardless of which mobile network they use. Alignment within countries is crucial, alignment across countries is desirable.
B. **Simple –** the charging basis should balance flexibility with the need to avoid creating too many options which confuse the enterprise purchasing the service and necessitate complex and expensive development e.g. in the operators billing systems.
C. **Transparent** – a brand should be able to understand and assess the cost and potential value of a campaign before committing to it.
D. **Attributable** – Sharing of real time delivery data is a key benchmark to enable delivery and conversion optimisation. Digital marketers need to be able to attribute campaign success for each channel and adapt campaigns accordingly.

<table>
<tr><th>RCS BM CHARGING MODEL</th><th>DEFINITION</th><th>PROS</th><th>CONS</th></tr>
<tr><td rowspan="2">Per- message</td><td>Charge for every message sent to a user / received by a user</td><td>Simple
Ideal for e.g. notifications, broadcast messages, 2-factor authentication
Predictable for outbound messaging
Implemented in current MNO billing systems</td><td>Commoditises channel
Discourages conversational commerce
Reduces revenue potential
Could drive ever-larger file size unless caps or volume charges added</td></tr>
<tr><td colspan="3">Recommended Implementation: Per message charging (A)

Charging is calculated on the number of RCS messages delivered to the inbox of users. MNOs should support one or more of the following models in respect of customer data charges:

Whitelisting: All RCS BM data traffic is whitelisted; sender just pays to send the message (Note: May be a net neutrality impact depending on jurisdiction. If the MNO is already free-rating WhatsApp or other social media data charges, then it should be ok to free-rate RCS data charges)
Free-to-end-user model: The end users cost of data to download the file is bundled with the per message price. The RBM per-message price could be tiered to allow for different file sizes
End-user-pays model: The end user pays for the data to download the file and the sender just pays to send the message. A max file size and pre-download file-size warning may be used to prevent bill shock. This approach may be of interest for premium content (Note: other similar services e.g. WhatsApp, WeChat are totally free to the end user on networks where unlimited social media app data charges are included in the customers bundle. Having the end user incur a charge to receive an enterprise’s messages may be detrimental for RCS adoption).</td></tr>
</table>

<table>
<tr><td></td><td colspan="3"></td></tr>
<tr><td>Per-session</td><td>A single rate for unlimited message traffic over a given time period (e.g. 4 hours) once a session has been initiated.</td><td>• Relatively simple
• Supports the conversational model (although a conversation may in practise comprise of multiple sessions)
• Can be easily supported by MNO billing systems</td><td>• Commoditises channel
• It could encourage excessive messaging from enterprise during session time to optimise cost</td></tr>
<tr><td></td><td colspan="3">Recommended implementation: Per A2P session charging (B)

An A2P session is considered initiated when:

(i) an enterprise has sent a message to an end user and the end user has responded in a way that requires a follow-up from the enterprise, within a set response window (e.g. 24 hours) of the original message (A2P)
(ii) an end user sends a message to an enterprise to which the enterprise responds, and the end user then messages the enterprise again within a set response window (P2A).
(iii) A session allows for unlimited messages between an enterprise and a user for a period of time (e.g. 4 hours) after the session initiation.

Other recommendations:
• There is no suggested limit to the size of messages in an active session; however, MNOs may feel free to incorporate a size limit.
• In combination with the subscriber’s data charge being included in what the enterprise pays, the MNOs should have a fair usage policy allowing them to block messages from a specific bot so that they are protected in case an enterprise sends very high amounts of data.</td></tr>
</table>

Access Model / Per customer model	An enterprise pays to send unlimited messages to a customer within a time period	• Very simple • Values and monetises the customer relationship of the MNO	• Commoditises channel • Might encourage abuse / excessive messaging • Could go against regulations in certain countries (e.g. Germany)
Per megabyte	An enterprise pays for the data traffic it generates to send traffic to multiple users, potentially with a daily cap and an extra charge for exceeding the cap.	• Flexibility to support short messages, sessions and very large file sizes	• Commoditises channel to a degree • Might encourage abuse / excessive messaging
Success Based Fee/ Revenue Share	An enterprise agrees a payment for a specific result from the campaign e.g. per new customer sale / click on page	• Optimises the value of the channel • Applies native digital marketing models – which enterprises are familiar with	• May require change in MNO processes to scale, although this will reduce over time • Challenges in measurement and adapting MNO billing systems • Time and complexity of contract negotiations • Challenge in verification of reported outcomes

BEST PRACTICES

1. **Charging Principles**

   A minimum 'common approach' should be adopted for a **period of 12 months from launch to provide a transition period from A2P SMS models and to encourage conversational messaging (P2A).** The following should be supported:

   a. **Per message charging**

   b. **Per session charging** with the standard implementation as recommended (see below) with a **24-hour response window and a 4-hour session duration**

MNOs may also consider new charging models in addition to the common approach.

The business messaging community should offer new charging models including hybrid models (where usage and success fee can be mixed) at launch even if the operator community is not ready in order to engage in trials.

2. **Common Definitions**

   MEF encourages the use of its standardised definition for charging models.

3. **Business Messaging and User Charges**
   a. **Charging for Metadata.** At a minimum, the cost of downloading RCS metadata for the business profile (e.g. branding of conversation) should be free to the end user and not impact their data bundle
   b. **MNOs should free-rate end user receiving RCS traffic for A2P business communication.** It is in the interest of the industry to avoid bill shock to users.

4. **Early Announcement of Charging**

   MNOs should act as soon as possible to establish charging on an introductory basis for A2P RCS to allow market testing and development

NOTES

1. Optimum session duration is likely to vary greatly over different products and services. Flexibility and a variety of session lengths is the best long-term scenario, but a single session length and response window initially will allow enterprises, business messaging companies and MNOs to gain the practical experience required to optimise in the future.

2. MEF's RCS Roundtables which bring together MNOs, business messaging providers and critically enterprises, brands and digital agencies will help support knowledge sharing on the trial & development of new commercial models enabled by RCS
3. Cost Per Click. As many of the new charging models seek to emulate the cost per click advertising model, it is worth considering how cost-per-click works. See Annex.

INTERCONNECTION

BACKGROUND

One of the defining strengths of SMS messaging is its reach; SMS messages are delivered across every mobile device and network in the world. However, this global interconnection has also provided opportunities for commercial exploitation and bad practices such as grey routes and spamming that have negatively impacted commercial terms and customer experience. It's important that RCS Business Messaging acknowledges and mitigates these issues from the outset to ensure RCS is a safe, secure and successful channel for enterprise communication.

A key issue linked to interconnect is the use of grey routes. The RCS Universal Profile 2.0 specification outlines the following:

- RCS business messages follow a completely different process for identification of the traffic as compared to the P2P traffic
- Business messaging features (i.e. colours, logo, Rich Cards, carousels etc.) are only available on the handset when the incoming message is tagged as a Business Message
- Most live RCS networks do not route business messaging traffic over the NNI between networks, allowing P2P traffic only to cross the NNI. Business traffic accesses the network via a gateway controlled by the Operator.
- Some businesses may attempt to send business messages without any of the features of RCS business messaging in order to save money but normal monitoring of NNI traffic to detect imbalances is key to preventing this. In any case it is likely that the end user, seeing the message as being visibly different to a legitimate RCS Business message (No logo, no sender verification, no brand, no carousel or rich card) will treat the message as spam and disregard and / or report it.
- However, monitoring of P2P RCS traffic via the NNI is still recommended.

KEY PRINCIPLES

A. **Universal Coverage** - For RCS to be recognised by end users as a trusted channel, customers and enterprises alike will have to be assured with a high degree of certainty that an RCS message is going to reach the intended recipient.

B. **Interoperability** – While the service architecture of RCS is more complex and innovative than that of SMS, with hosted solution players taking a greater role in delivering services and hubs accelerating interconnectivity, it is key that all ecosystem stakeholders see that universal service requires interconnection and interoperability between all RCS Universal-Profile-compliant systems.

BEST PRACTICES

1. **Technical Support for U.P. 2.0**
   MNOs and vendors should launch Universal Profile 2.0. If they are already live on a previous version, they should upgrade as soon as possible to unlock the monetisation potential of RCS BM.

2. **Commercial Interconnection**

Each MNO, Hub and Messaging Solution Provider should map its path for universal reach. Overall, a target of 100% interconnectivity for A2P and P2P traffic should be in place as soon as possible. The use of hubs is important tactical solution to achieve universal reach. This requires MNOs to either connect to at least one RCS messaging hub. They should also terminate all traffic coming from hubs; or become hubs themselves (setting interconnect rates with other MNOs).

3. **Separation of P2P and A2P Traffic**
   MNOs should adopt usage policies which mandate separate interconnection routes for A2P and P2P traffic and exclude A2P traffic from the P2P channel; routing P2P traffic via the NNI and A2P traffic via a MaaP gateway that ensures the traffic is coming from a source that has a commercial arrangement with the network. Traffic differentiation can be done via the A2P tag in file headers. Continued monitoring of the NNI interface for grey route A2P traffic is advised, however.

4. **Improvements in traffic routing**
   - Access to a central database identifying the MNO serving a particular MSISDN (where one exists) to be accessible to non-Operators as well as Operators
   - Access to be granted at a commercially feasible rate to non-Operators
   - Where a central database does not exist, treatment of any data charges incurred while trying to find the correct MNO, should be agreed and communicated in a common way at least at a national level

NOTES

1. In addition to agreeing interconnect rates for A2P traffic, MNOs should consider implementing a cross carrier charging for P2P RCS. If the channel is not generating any revenue it can become a magnet for fraud. Furthermore, if the channel is not revenue generating it will be difficult for MNOs to justify spending internally to clean up the channel at a later date.

PERMISSION MANAGEMENT

BACKGROUND

Under the Telephone Consumer Protection Act (TCPA) in the United States and similar legislation including the General Data Protection Regulation (GDPR) in the EU and other local data privacy laws, enterprises need to ensure they have consent prior to communicating with its customers or prospective customers.

However, ambiguity exists about what customers have actually consented to, and what that means. If a specific technology is named in the consent, does that mean that other technologies require a separate consent? If the cost of receiving the message to the end user is different to other technologies but consistent with competing business messaging providers, is a new consent required? Enterprises, messaging companies, MNOs and indeed regulators need a common approach to opt-in, to enable RCS to move forward.

KEY PRINCIPLES

A. **Legal compliance** - the approach adopted must comply with all local regulatory requirements
B. **Operational efficiency** - the approach needs to maximise the value of the consented opt-ins and minimise the requirement to seek new opt-ins
C. **Positive end user impression** - the approach needs to be accepted by the end users as benefiting their customer experience and reflect any concerns about being targeted by spam

BEST PRACTICES

1. **Enterprise opt In - Inclusion of RCS in terms and conditions**
   Encourage enterprises to include an explicit reference to RCS in any terms and conditions relating to data collection as soon as possible.
   Business messaging companies should advise enterprises to update their terms and conditions to include the term “RCS communication” or “mobile data messaging” as a channel, with an additional clarification that standard data charges may apply.
   Example:
      i. **Terms and conditions. “I agree to receive information / marketing communications / third party via mobile data message services (including but not limited to SMS/RCS/MMS). Charges may apply as per your standard operator data services”.**
      ii. Enterprise may also consider more generic, non-specific language to cover any communication channel they use or may use in the future e.g. to cover AI-driven services including voice chatbots.

2. **MNO - Ensure there is clarity on end user data charges**
   a. ***MNOs position RCS as a technical upgrade to SMS* and ensure there is clarity on end user data charges** – making additional opt in redundant**.** The same originating company, network and client on the recipients’ device are used as with SMS. Therefore, if an end-user has already given consent to receive SMS or MMS messages, they can also be sent an RCS message as long as:

i. The MNO allows the enterprise to cover the cost to the recipient of downloading any attachments or files as part of their pricing; OR
ii. The message includes clear text such as: “This is an RCS message: charges apply for data usage as per your standard operator charges”.
iii. The MNO otherwise ensures the end user is not charged for message without their knowledge.

b. *Implicit acceptance of data charges.*
   i. If the customer has also opted to receive e-mail or MMS messages or generically “mobile data messaging” they have agreed to receive messages for which a small cost of data for downloading the message will be added to their bill or decremented from their data bundle (assuming it is not an unlimited bundle). Therefore, the enterprise does not require a separate opt-in, nor does it need to cover the cost of end user downloads to send RCS messages.

3. Guidance on consent process for P2A

a. If the end user is known to the enterprise, another opt-in should not be required for first time bot interaction.
b. However, an end user contacting an enterprise via P2A RCS does not automatically give consent for that enterprise to contact him/ her.
c. Similarly, an end user contacting an enterprise via P2A RCS (via a chatbot) does not automatically constitute opt-in to A2P messages– explicit permission should be received from the end user.

4. Opt Out – Consistency with SMS

The same ability to opt out of receiving RCS messages and the accompanying procedures to remove end users from a permissions list that exist for SMS should also be maintained for RCS messaging with the overriding principle it should be an easy and not an obfuscated process.

FRAUD MANAGEMENT AND PREVENTION

BACKGROUND

Fraud is an issue for RCS as it is for any messaging channel. Typically messaging fraud falls into two categories; Consumer Fraud including spam, originator spoofing, phishing, malware, access hacking, etc. usually with the intention of getting access to an end users credit card, identity or other data, and Network Fraud or Commercial Manipulation such as Grey Routes, Global Title Faking, SIM farms, Artificial Traffic Inflation and MaaP compromise where the intent is to send messages, which may be legitimate in themselves, without paying for them. (See MEF's A2P Messaging Fraud Framework for more details).

As adoption of RCS BM accelerates the ecosystem has a unique opportunity to implement best practices that prevent and limit fraud from launch. U.P 2.0 specifications contain technical provisions for fraud prevention, primarily Sender Verification, but to date concrete implementation guidelines for the specification have not been adopted and implemented by all players. Indeed, Sender Verification currently does not have a unified solution with separate initiatives being sponsored by some mobile operators, Google, CTIA and some aggregators with no guidelines in place on interoperability between verification solutions.

It should be noted the RCS is by design not end-to-end encrypted. While RCS messages are fully encrypted outside the MNO environment, and no evidence exists to suggest RCS is more prone to fraud than other channels, as human-engineering is still overwhelmingly more common than technically sophisticated man-in-the-middle attacks, the RCS ecosystem should ensure that the security of RCS is both maximised and well-communicated to enterprises and end users alike.

KEY PRINCIPLES

A. **Confidence** End users should have a high degree of confidence that when a message is tagged in the inbox as coming from a verified sender, it is a legitimate message
B. **Simple Verification Process** At least nationally, and preferably regionally or internationally the process for an enterprise to become a Verified Sender should be robust, cost-effective, rapid and transferable across messaging companies, MaaP platforms and mobile networks, avoiding the need to re-verify multiple times.
C. **Verification** The question of whether Sender Verification should be optional, or mandatory is under active debate across the business messaging ecosystem. It is noted that sender verification is mandatory for Apple Business Chat and WhatsApp and arguably a 'hygiene factor' for business messaging. MEF's Future of Messaging Programme's Fraud Working Group will continue to consult with stakeholders in the ecosystem in the future.
D. **Branding** The visual representation of a verified sender should be clear and well-understood to the end user

BEST PRACTICES

1. **Fighting Fraud - A Continuous Fight**
   It is imperative that fraud prevention is built into processes from day one. No communication service is free from fraud.

a. RCS Network Providers and MaaP providers should **develop effective policies and procedures** for detecting and blocking fraudulent messages. These policies and procedures should be reviewed regularly.
b. MNOs and MaaP providers should routinely include an **RCS Firewall** as part of their requirements within their RCS tender / Purchase process. Firewalls should always be used to ensure the integrity of the source and destination of the content. It is important to ensure firewalls are appropriately maintained and configured
c. Traffic access should be split with only P2P traffic going over NNI and all RCS BM traffic going over a MaaP gateway
d. MNOs should work closely with messaging providers to ensure the security integrity of the whole channel

2. **Industry to support a unified sender verification process**

   Brand registration in a verified sender programme is an important enabler in establishing secure communication and fighting fraud. The service should become a hygiene factor, readily available at low cost for all enterprises. To facilitate this, MNOs should appoint a common verification authority at least nationally.

   a. Financial Enterprises (bank, credit cards) and other enterprises at high risk of phishing and spoofing fraud should implement Verified Sender ID as a priority
   b. Messaging Solution Providers should encourage enterprises to adopt sender verification across its customer base.
   c. Steps should be taken by sender verification services to ensure the chatbot equivalent of cyber-squatting is prevented, and that a single verification is valid across all jurisdictions
   d. There should be either a unique national / regional verification authority, or a common level of rigour in every verification process and mutual recognition agreed between verification authorities.
      i. Sender verification authorities should agree peering arrangements based on a common standard of verification and common acceptance and de-listing policies.
      ii. MNOs verifying brands should apply the same level of rigour in verification as is agreed between verification authorities at a national / regional level.
   e. Withdrawal of verified status from a verified business should only be done due to a lack of trust in the identity of the enterprise

3. **User Fraud Reporting**

   There should be an agreed mechanism for end-users to report abuse in RCS (similar to Spam reporting tools).

4. Education

Proactive education and awareness should be offered to the users for all messaging fraud, and specifically for the new RCS multimedia threats.

a. Sender Verification will only be effective if end users are aware of it.
    i. MNOs should develop a standardised position to explain RCS BM, sender verification, how it is rendered in the User Interface and what it means, to be sent to all RCS end users Similar developments (I.e. the introduction of https) have taken many years to become generally understood by end users.
    ii. End users should also be advised that the principle of “buyer beware” always applies – if any interaction with an enterprise via RCS seems irregular and suspicious, end users should exercise caution.
b. Educating local regulators and law enforcement is essential
c. Operators and business messaging companies should also undertake education of brands and marketers on the necessity to make sure their own structures and security are robust; they will be trusted by the end users and could be compromised from within.

NOTES

1. MEF’s Code of Conduct for A2P SMS is a self-regulatory code that could be evolved to include principles specific to the RCS channel and a dedicated Fraud Framework mapping the RCS ecosystem
2. The sharing of data on fraudulent attacks and known fraudulent message deliverers across the industry helps to tackle fraud. It requires a collaborative approach between all stakeholders in the value chain including brand and merchants. The sharing of such data needs to be done carefully so as not to misrepresent or libel a company or individual. As yet there is no central registry of fraud attacks e.g. a grey list (potential fraud) or blacklist (of confirmed fraud incidents (Note: MEF is currently examining the feasibility and value of establishing and maintaining such lists on behalf of the industry).
3. As RCS messages can be sent from a variety of devices, potentially many without a SIM, that extra level of authentication provided by the physical SIM will not be present.

SPAM PREVENTION

BACKGROUND

Spam is a major issue for all business-to-consumer communications channels. The first spam SMS messages were sent within months of the commercial launch of SMS. The presence of spam is shown to reduce the engagement and response activity from a user. SMS response indicators remain higher than email and most other OTT platforms thanks to the relatively lower amount spam in the system.

Originally the per-message charging nature of SMS shielded users from receiving the high volume of unwanted / bulk messages. The fight against spam is ongoing as the industry works to establish A2P SMS as a quality enterprise communication medium (e.g. self-regulation /code of conducts, grey route blocks etc).

A Spam message is defined in MEF's Fraud Framework as one which is sent to a consumer, which the sender does not have the permission of the recipient to send. This can include:

- Aggressive marketing without consent by a legitimate business
- Violation of acceptable use, poor communication and/or poor implementation of opt-out process by a legitimate business

KEY PRINCIPLES

A. **Performance**. RCS has been marketed as an evolution of SMS, so it is important for it to replicate the same KPIs for response time or interaction levels.
B. **New points for spam attacks.** Some MNOs are offering P2P traffic for RCS charged by data traffic (analogous to OTT services such as WhatsApp). Rogue players could use P2P messages to introduce bulk messages, avoiding the quality control in place for A2P services.
C. **Regulation**: Spam is illegal under multiple regulatory frameworks, these actors' risk significant fines.
D. **Education:** MNOs and messaging companies have a role to play in educating enterprises to the long-term negative effects on their business of Spam and help them ensure they have effective Opt-in/ Opt-out policies and procedures in place

BEST PRACTICES

1. **Proactive Permission Management.**
   Often Spam is not a designed malicious communication, but the results of bad internal permission management practices. The industry should highlight the long-lasting damage that spam introduces to the brand as well as to the channel in the medium/long term as well as the risk of infringing regulatory requirements.
   a. **Induction process**. MNOs and messaging providers should offer permission management guidance to brands and enterprises adopting RCS Business Messaging. (Note: MEF could provide a template for RCS Permission Management as a standard shared information, T&Cs templates). Permission management needs to be adopted culturally and regulation such as GDPR has

helped highlight best practices. While many enterprises will be well versed in permission management it is worth making permission management part of the routine induction process in the launch phases of RCS.

b. **Launch checklist** should include the existence of opt-in and opt out policies and mechanisms.
c. **Fair use policy:** Appropriate levels of communication (amount and frequency) should be comparable to human behaviour and not necessarily linked to a hard-numerical value. However, it could be beneficial if MNOs and business messaging companies on a national or regional basis to agree informally what a 'normal' level of communications is and communicate a common understanding to enterprises.

2. User Control- Standard Commands

The industry should make end users feel empowered and avoid the perception of Spam. A set of common commands should be used to give and retrieve communication permission via messages across a specific language/market (e.g. 'STOP' or "ADD ME", "SUSPEND"). Where available the "Opt In – Opt Out" commands should be the same as the existing common SMS commands.

2. **Rogue P2P Traffic Monitoring**. The sending of business messages purporting to be consumer messages to achieve a lower cost per message by taking advantage of low consumer interconnect rates between networks are to be prevented
    a. **A2P Traffic Flagging**. All actors should make sure that RCS Business messages are always flagged as such in the message header
    b. **P2P Traffic Policing**. Spam is today primarily detected automatically based on message volume and velocity. Machine learning and AI technologies can examine message content to further differentiate spam from legitimate messaging – especially P2P messaging.
3. **Sharing of information on Rogue Senders** The sharing of data on known spam senders is a significant benefit to all members in the business messaging ecosystem but as yet no central grey list (of potential spammers) or black list (of confirmed spammers), open to all members of the ecosystem to query, exists. Information should be shared between all stakeholders on spam-senders and spam blocking, on a like for like basis rather than as a profit-centre. (Note: MEF could examine/facilitate the feasibility and value of establishing and maintaining such lists on behalf of the industry).
4. **Blocking Rogue Senders**. Spam is dealt with in several ways by RCS;
    a. End users can block the sender on their device and report the sender of the spam to their network.
    b. MNOs can block the sender at the network level.
    c. The Messaging as-a Platform (MaaP) provider or Chatbot host (where that is a separate entity to the network provider) can block the spam sender.
    d. Potentially RCS hubs could also play an active role in spam detection and prevention.
5. **Sender ID Verification** While primarily an anti-fraud device, sender verification will also have a positive contributory effect on spam by increasing traffic transparency. Sender ID verification would not affect rogue senders using P2P.
6. **Spoofing:** Where carriers provide the valuable service of collapsing and linking an enterprise's dedicated Short Code with their Verified RCS Sender ID into one message thread, controls should be put in place to detect/prevent spoofed SMS arriving into an enterprise branded message thread

REPORTING

BACKGROUND

The increased level of reporting data on the success of a campaign is one of the main advantages RCS has over SMS and MMS. Currently enterprises receive only basic reporting statistics on SMS campaigns (such as message delivered by terminating network). RCS allows to move towards more complex digital marketing solutions.

The RCS Universal Profile specifications make it feasible to gather details including:

- Details of the recipients who received the message (date, time, etc.)
- Details of the recipients who opened the message
- Details of the recipients who replied to the message
- Details of the recipients who engaged in a session with the chatbot
- Navigation within the chatbot (carousel, chips, etc)

However, the information about the full customer journey through a chatbot experience is distributed across the players in the ecosystem. Maximising the value of RCS data, and thus realising the value this provides to enterprises, requires a commitment to sharing of data across the ecosystem.

The data owners in the ecosystem can be viewed as:

- Enterprise
- Messaging Company
- MaaP Platform administrator

STAKEHOLDER	ENTERPRISE	MESSAGING COMPANY	MAAP PLATFORM ADMIN
Data available	# sessions ending in a completed purchase # sessions abandoned during purchase	Session duration # Messages sent # Responses received # Sessions initiated # Clicks per chip/ button # clicks/ carousel card # clicks/ carousel position	Visibility of chatbot in directory (P2A) Views Impressions Clicks Searches by category Time/message received Time/ message opened Location/ message opened
Data required	All data pertaining to customer journey through the chatbot	Most popular tags in directory search # impressions # sessions ending in successful purchases Searches by category	

		Time/message received Time/ message opened Location/ message opened	
Purpose	Chatbot content improvement	Chatbot design improvement Campaign planning improvement	

KEY PRINCIPLES

A. **Rich Reporting:** RCS can and should differentiate as a premium service by offering enterprises the richest set of statistics on end user responses possible
B. **Cost efficiency:** The effort by the business messaging company of capturing additional statistics should be rewarded.
C. **Consistency:** A common set of parameters for reporting by MNOs to messaging provider should be agreed across all networks.

BEST PRACTICES

1. **Consistent MNOs reporting**
   Reporting by MNOs to messaging companies should be consistent across all networks to enable consistent reporting to enterprise.
   MNOs should strive to provide the greatest possible level of information on receiving and opening of messages.

2. **Enterprise – Single Data Source**
   The enterprise should have a single point to receive all stats for the campaign; MNOs should report to the business messaging company, not direct to the enterprise (unless they have a direct relationship with enterprise).

3. **Data Privacy**
   All data concerning a customer's interaction with an enterprise should be made secure and private. The data should be available to the enterprise and not shared, distributed, etc., without full anonymisation so that any individual consumer's data and activity cannot be compromised.

4. **Local Regulations**
   Local regulations including GDPR as well as data protection and data storage regulations from other countries must always be adhered to.

RCS CHATBOT QUALITY APPROVAL

BACKGROUND

It is in all stakeholders' best interest to ensure RCS remains a trustworthy and secure channel that provides an enhanced end-user experience.

MNOs have a duty of care to ensure that the services represent their brand, values and quality, recognising that RCS is defined as an operator service. One way to do this is for the MNOs to limit (or not) the accessibility of chatbots to their users, via discovery mechanisms or interconnection. There are a number of options available:

A. Restrict users to visit chatbots that are known and vetted by the MNO
B. Support users to visit chatbots already vetted by other MNOs (with similar criteria)
C. Support free access to all chatbots, including those not vetted by MNOs.

A wider offering of chatbots will be a key driver for success of RCS. Too much quality control would slow uptake, whereas too little control introduces fraud or bad user experience to the channel. The role of quality control cannot sole rest on the MNOs and the full value chain should adopt best practices.

The following areas have been initially identified as part of the RCS Chatbot lifecycle and alignment is required in relation to each stakeholder's role and responsibilities:

- Chabot Design and business functional purpose
- Quality and Technical Assurance
- Technical deployment
- End-user Quality of Experience (QoE)
- Privacy & Data security

Keeping in mind the core goal of preserving trust and customer experience; services under development for RCS BM should consider relevant measures in order to:

- Avoid rolling out services with dysfunctional behaviour that that directly impacts the core functionality of the Chabot and/or the smartphone performance.
- Avoid unintentional and intentional spams or potential storm-like attacks due to the Chabot technical design setup
- Avoid unintentional charges linked to misinformation in the chatbot (e.g. direct carrier billing, or device-based payment initiated on wrong or misleading information)
- Prevent services from aggressively engaging end-customers directly impacting RCS end-user experience.
- Further help detecting and preventing new fraudulent activities or behaviours.

Similar to the development of mobile apps, OS providers such as Apple and Android take a strong proactive stance ensuring the apps available to end customers are truly meant to tackle their business purpose and perform as expected. This is aimed at preserving their customer experience guidelines and avoiding possible fraudulent functionality. As the RCS ecosystem further develops, it is envisioned that similar "RCS business directories" or

"Marketplace arenas" will likely take a role in moderating and ensure the services made available are seen as fit for purpose for consumer use by their respective stakeholders.

TYPE OF RCS CHATBOTS

In developing quality indicators, the various types of RCS services should be considered, some of which maybe basic "send only" services that are ported from the SMS channel and some of which offer a full conversational ability.

The acceptance of an RCS Chatbot can be eased by classifying them

1. **Send Only**: This RCS service primary use case is sending messages to the user, it is the easier form of a chatbot based on information being sent to the users (e.g. sport results, news headlines). Send only are simple in nature and require less oversight. However, they do not represent an RCS conversational media and some operators might decide not to include them in their discovery/directory.

2. **General Conversation**: The Service will support two-way conversation, using either predefined responses (a "button bot") or using a set of keywords for navigation and interaction. The main question to be addressed here **is response time (latency**) for the conversation. The chat should not hang for unusual time for a response/confirmation (e.g. more than 1 minute). Guidance and feedback would be enough to self-manage this area.

3. **Advanced Conversational Chatbot:** These chatbots include advanced options such as:
    a. Payment
    b. User's Data Access (photo, video, address) book
    c. Location Data

    These RCS Chatbots should be **tagged** and should be reviewed more closely by the value chain as they are more likely to be abused.

RCS STAKEHOLDERS ROLES & RESPONSIBILITIES

The following section will expand on each of the areas below and suggests a RACI approach to assign the RCS stakeholders responsibility:

- Chabot Design and business functional purpose
    - Application technical design to comply with the business ambitions or service requirements coming from the Enterprise.
    - Brand - Implementation of visual elements into the technical design in order to portray the desired look and feel in accordance to respective brand guidelines
- Quality and Technical Assurance
    - Test and procedures to ensure a fully working application which is also able to meet its intended business purpose.
- Deployment
    - Campaign Planning and technical rollout of the application into a respective region or market.
- End-user Quality of Experience
    - Looking after the constantly improving QoE to ensure customer satisfaction when interacting with the service
- Privacy & Data security

- Procedures to handle customer's data shared within the Designed Service in accordance to regulatory and customer data protection.

RCS stakeholder's overview:

- Business
  - Brand design
  - Developer
- Messaging or Solution Provider
- MaaP Providers MNO

R= Responsible, A= Accountable, C= Consulted, I=Informed

	BUSINESS / BRAND DESIGN	BUSINESS / DEVELOPER	MESSAGING / SOLUTION PROVIDER	MAAP PROVIDER	MNO
Application technical design, compliance w/ business goals of the Enterprise	C	A	R	I	I
Brand - Implementation of visual elements into the technical design in order to portray the desired look and feel in accordance to respective brand guidelines	A	C	R	I	I
Chabot Design and business functional purpose	A	A	R	I	I
Test and procedures to ensure a fully working application which is also able to meet its intended business purpose.	A	A	R	C	I
Campaign Planning and technical rollout of the application into a respective region or market	A	A	R	C	C
End-user Quality of Experience Looking after the constantly improving QoE to ensure customer satisfaction when interacting with the service	C	A	R	C	I
Privacy & Data security Procedures to handle customer's data shared within the Designed Service in accordance to regulatory and customer data protection.	C	R	C	I	I

BEST PRACTICES

1. MNOs / MaaP platform providers should adopt a **common quality review process for chatbots** coming onto their platform to ensure a minimum level of quality safety and user-friendliness is achieved in all RCS chatbots.
2. This should be a **single quality review process**; MaaP providers and MNOs should agree which stakeholder will be responsible for quality and the details thereof. Business Messaging companies should not have to pass multiple quality reviews.
3. **Messaging Solution providers** should play a key role in the value chain to test chatbot quality and confirm suitability according to the common quality review
4. **Federation models** will allow mobile operator to accept other chatbots vetted by other operators. This will make for quicker scaling up in the market.
5. Development of the chatbot **quality review process should grow organically** as more chatbots come on stream. it need not be developed in its entirety before MNOs go live with RCS BM.

Definitions

Table of acronyms and technical terms

ACRONYM / TERM	EXPLANATION
A2P	Application-to-Person Messages sent from an application to a device for a person to read
Chatbot, or bot	An application designed to manage a conversation with a user using natural language interaction and interactive options.
Excessive Messaging	Brands which have valid opt-ins from their customers need to ensure they do not send too many messages as they run the risk of the customer perceiving their communications as 'spam'. The 'right' number is a judgement for each individual brand. Excessive messages are technically not spam as the enterprise has an opt-in, but excessive messaging can have a negative impact on consumer perception of business messaging.
Grey Route	Used as a way to avoiding paying the correct charges, or to avoid paying any charge for message termination.
Hub / Messaging Hub	Hubs provide national and international connectivity for RCS services.
IP	Internet Protocol
KPI	Key Performance Indicator
Long Code / Long Number)	In contrast to a short code, this is a traditional format mobile number, also known as a virtual mobile number (VMN) or dedicated phone number MSISDN. It is a reception mechanism used by businesses to send & receive SMS messages and voice calls. While a Short Code can be sometimes shared by multiple brands, Long Codes tend to be unique to businesses.
MaaP	Messaging as a Platform The term is often used to refer to - A paradigm shift in business messaging from a simple exchange of text messages exchange to new forms of interactive multimedia conversations deeply integrated in commerce, payment, service fruition. - *(By extension)* the service platforms that support MaaP services
Metadata	The data [information] that provides information about other data. In RCS metadata can refer to the information that is used to pre-populate an RCS business chat (e.g. logo, description) – this is silently downloaded once receiving a message.
MMS	Multi-media Message Service
MNO	Mobile Network Operator
NNI	Network-to-Network Interface

OTT	Internet messaging solutions providing a service on mobile devices without going through the MNO billing system
P2A	Person-to-Application. Messages sent from a person to interact with an application interface. Also known as conversational messaging.
P2P	Messages sent between users for personal communication.
Phishing	A form of criminal activity combining Spam, Spoofing and social engineering techniques to pretend to be a trustworthy entity, in order to gain access to online systems, accounts or data such as credit card, banking information or passwords, for malicious reasons.
RCS	Rich Communication Services A communication protocol devised by GSMA to transport advanced multimedia messaging across mobile operators and to compatible devices.
RCS BM	RCS or Rich Business Messaging is the implementation of communication services by businesses using RCS. Also known as RCS Enterprise Messaging or Rich Business Messaging (RBM)
Sandbox Area	A testing environment that offers access to a full business process, but via an untested platform in order to use for experimenting. Sandboxes replicate at least the minimal functionality needed to accurately test the programmes or code under development
SMS	Short Message Service
Short Code	Short digit sequences that are used to address messages in the Multimedia Messaging System and SMS systems of mobile network operators.
Spam	A Spam message is one which is sent to a consumer, which the sender does not have the permission of the recipient to send. Spam is commonly commercial in nature.
Universal Profile 2.0	The GSMA's Universal Profile is a single, industry-agreed set of features and technical enablers developed to simplify the product development and global operator deployment of RCS. It contains core features such as capability discovery, chat, group chat, file transfer, audio messaging, video share, multi-device, enriched calling, location share, live sketching and rich cards.

Definitions of Stakeholder Roles

ROLE	DEFINITION
Mobile Network Operator	Service owner / channel delivery
Messaging as a Platform Provider	The solution to exchange of text messages across multiple channels in interactive multimedia formats. Enables conversations between end users and businesses these can be deeply integrated in commerce, payment, service fruition.
RCS Hub	Provides interconnection functionality needed to extend the reach of RCS to multiple MNOs
Messaging Providers	Enables enterprises to reach consumers via messaging channels
Solution Providers including: • Customer engagement platforms • Chatbot Developers • Campaign Management tools	Developing and operating tools & services for businesses to communicate with their consumers
Security Providers	Provide services to the messaging value chain to prevent and protect against fraud
Businesses Enterprises, Brands, Digital Marketing Agencies, SMEs	Business users of RCS
Consumers	End User of RCS

About

About the Guidelines

These guidelines were developed as part of MEF's Future of Messaging Programme during H1 2019.

A series of one-on-one interviews with MEF members and industry stakeholders were carried out by David O'Byrne on behalf of MEF to identify the key areas that would benefit from clarification and industry recommendations. The recommended best practices were then developed and discussed by the Programme's Market Development Working Group.

The goal was to agree a framework for the technical options for deploying RCS Business Messaging and to help streamline the processes for a successful launch of A2P & P2A services.

It is a living document with updates to reflect the ongoing roll out of RCS as well as make further recommendations on RCS BM critical success factors area such as Discovery.

About MEF

Established in 2000, the Mobile Ecosystem Forum is a global trade body that acts as an impartial and authoritative champion for addressing issues affecting the broadening mobile ecosystem. As the voice of the mobile ecosystem it provides its members with a global and cross-sector platform for networking, collaboration and advancing industry solutions. The goal is to accelerate the growth of a sustainable mobile ecosystem that delivers trusted services that enrich the lives of consumers worldwide.

About MEF's Future of Messaging Programme

Launched in 2015, MEF's Future of Messaging Programme is a dedicated industry programme that promotes a competitive, fair and innovative market for mobile communication between businesses and consumers. Programme participants represent different regions and stakeholder groups working collaboratively to:

- Produce and publish best practice frameworks, papers and tools to accelerate market clean-up and limit revenue leakage
- Educate buyers of messaging solutions
- Promote business messaging as a premium and trusted channel
- Drive knowledge across the ecosystem of new platforms, technologies and procedures to address the evolving messaging landscape
- Develop the value-chain to support new use cases

Contributors

We would like to acknowledge and thank the following companies for their active contribution to shaping these Guidelines:

- 3C Interactive
- Apprentice Valley
- AT&T
- Deutsche Telekom
- GSMA
- IMImobile
- Infobip
- MMDSmart
- MobileSquared
- Openmarket
- Orange
- RDcom
- SAP
- Sinch
- Telefonica
- Telenor
- Tyntec

Annex

Cost-Per-Click

Overview

Search engine advertising platforms utilise a maximum cost-per-click model for determining the ad position and the final cost-per-click in relation the user's search query. The first factor to contribute towards the cost-per-click is the maximum price one is willing to pay-per-click. Bids can be set at an individual keyword level or at an ad group level. If the keyword has higher buyer intent, then this will result in it attracting higher bids and more competitors within the auction, thus raising the estimated cost-per-click and the costs for the advertiser to remain competitive within the auction.

Quality Score

This plays a key role in determining in which position an Ad will appear within the auction and how much a user will need to pay for the click. Quality Score can be seen on a keyword level, and when it improves the cost-per-click will decrease and the average position within the results will increase.

There are 3 considerations related to Quality Score:

- **Expected click-through-rate:** This is reflective of the likelihood that the user will click upon an Ad
- **Relevancy:** The Ad copy used should be relevant and clearly relate to the searcher's search query; if it isn't, this will result in a lower Quality Score.
- **Landing Page:** The landing page that users are driven to needs to provide a positive user experience and be reflective of the intent of the search query.

It is estimated that each of these is given the following weighting:

- **Landing Page Experience –** 39%
- **Expected Click-Through-Rate –** 39%
- **Ad Relevancy –** 22%

Ad Rank

Ad Rank = Quality Score x Max. CPC Bid

Ad Rank considers the advertiser's maximum bid for the click, Quality Score and the estimated click-through-rate by a user, which includes how Ad extensions may assist in the likelihood of the CTR increasing. The Ad Rank of the Ad below is a key factor in the actual CPC that the advertiser pays if someone clicks on their Ad.

The Calculation of CPC: Example

Position in the Auction	Max. Bid	Quality Score	Ad. Rank	Position	CPC Calculation	Actual CPC
Advertiser 1	8	9	72	1	=42/9+0.01	€4.68
Advertiser 2	6	7	42	2	=32/7+0.01	€4.58
Advertiser 3	8	4	32	3	=28/4+0.01	€7.01
Advertiser 4	9	2	28	4		

The calculation of CPC is:

Ad. Rank of the competitor below in the auction / by your quality score + €0.01

MEF

FUTURE OF MESSAGING PROGRAMME

MOBILEECOSYSTEMFORUM.COM

Disclaimer

Mobile Ecosystem Forum makes no representation, warranty or undertaking 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 these guidelines. The document was developed by MEF's Future of Messaging Working Group in 2019 and in full compliance with the programme's antitrust compliance policy. The information contained in this document may be subject to change. Please check for latest versions online.