RCS Business Messaging: Recommended Good Practices

October 2018

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

About the Future Networks Programme

The GSMA's Future Networks Programme guides the mobile industry on how to use Internet Protocols (IP) to reduce the cost of transferring data, while meeting customers' expectations around reliability, security and interoperability.

The Programme is making it easier for operators to deploy Rich Communications Services (RCS); an evolution in mobile messaging, and is working closely with operators, aggregators, brands and technology providers to ensure that RCS is the future of brand communications.

The GSMA's holistic approach to 5G will ensure that vertical markets and consumers benefit from the opportunities created within the 5G Era. To meet user data demand and vertical capabilities, Future Networks will encourage innovative ways to reduce the capital intensity of the next generational step.

For more information, please visit the Future Networks website at: www.gsma.com/futurenetworks

Copyright Notice

Disclaimer

Antitrust Notice

1 Introduction

1.1 Overview

RCS (Rich Communication Services) Business Messaging is the evolution of mobile messaging, increasing and improving the ways in which people and businesses communicate. It provides brands with the opportunity to increase their engagement with customers, by making use of business messaging using chatbots, plug-ins and artificial intelligence (AI). End users benefit from no longer needing to download multiple apps to communicate with businesses; instead they can engage with businesses from within the messaging app itself.

The GSMA estimates that by 2021 the RCS Business Messaging market will be worth an estimated USD$74 billion, representing a key revenue opportunity for MNOs (Mobile Network Operators). However, in order to retain and build upon the trust and confidence end users currently have in MNO messaging services, MNOs need to ensure that RCS Business Messaging provides an experience consistent in quality with SMS business messaging.

This RCS Business Messaging: Recommended Good Practices document is designed to identify the areas in which all ecosystem participants can improve and enhance end users' experience of RCS Business Messaging. These good practices will continue to support the growth of the industry by improving the quality of services and customer satisfaction and facilitating the implementation of trusted service partnerships.

1.2 Scope

This document is targeted towards promoting the adoption of consistent RCS and RCS Business Messaging practices by all ecosystem participants including brands, messaging technology providers, aggregators, RCS Business Messaging platform providers and mobile network operators.

The GSMA encourages all RCS ecosystem players to adopt these good practices. However, this list is not exhaustive; it can be complimented by additional measures by ecosystem players.

The nature of this document is voluntary and non-binding. Ecosystem players who adopt these good practices should inform the GSMA and communicate it to their partners. The GSMA will retain a list of companies who adopt these principles.

In any instances, where the RCS Business Messaging: Recommended Good Practices may conflict with local legislation or regulation, local laws and regulation will always supersede the RCS Business Messaging: Recommended Good Practices.

1.3 Main Roles

It is essential for the understanding of the RCS Business Messaging: Recommended Good Practices to highlight the four key actors in the value chain, for messages sent from a business to end users (Mobile Terminated):

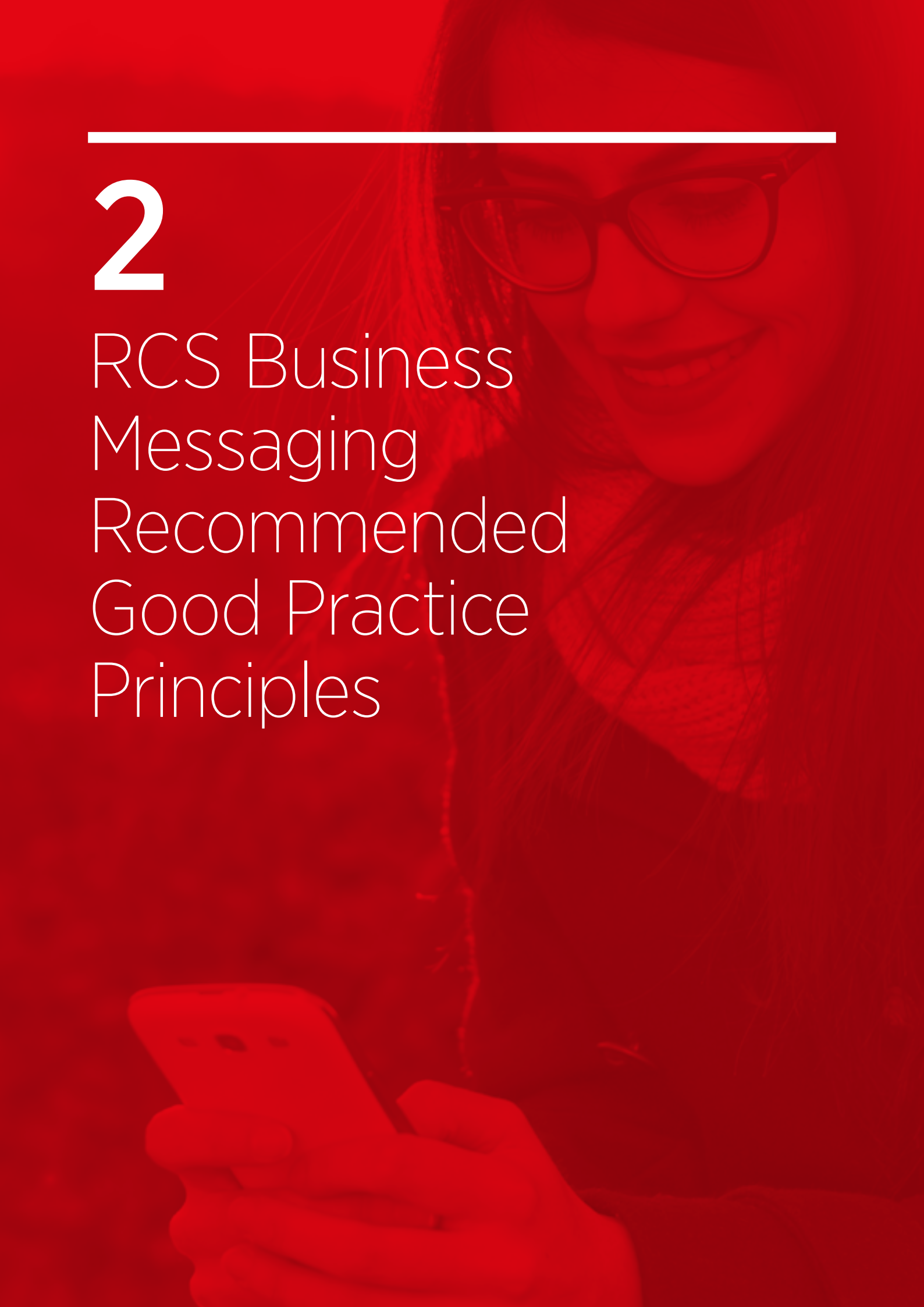
- The Message Generator: The company who is sending the message, or for whom the message is being sent e.g. bank, airline, government department.
- The Message Processor: Any company in the ecosystem that is involved in the processing, routing, or carrying the message en-route to its final destination.
- The Message Terminator: Any company (or companies) in the ecosystem that is responsible for delivering the message to the consumer handset – usually a Mobile Network Operator (MNO).
- The Message Recipient: Typically the end user, a person that the Message Generator has a legal right to send a message to.

For Mobile Originated (MO) messages where the message is sent from a customer or employee to a business then the Message Generator and Message Recipient roles above are reversed. For ease of reading, this document assumes that all messages are Mobile Terminated (MT) and therefore the definitions above apply.

1.4 Definitions and Abbreviations

For the purposes of this document the following definitions apply:

Term	Description
A2P	Application to Person messaging is communication initiated by an application, which may or may not result in a reply from the end user. A2P messaging includes but is not limited to marketing messages, appointment reminders, notifications and pin codes and can be provided by a mixture of providers, including chatbots, aggregators etc.
A2P Messaging Technology Provider	A company that provides the RCS A2P Messaging Platform used by service aggregators and brands. They may do so as a vendor or a partner of the Service Provider.
AI	Artificial Intelligence
API	Application Programming Interface
Brand / Enterprise	A business or entity that uses messaging to communicate with consumers. Examples include social networks, large and small businesses, financial institutions, schools, medical practices and non-profits.
Business Messaging Platform Providers	Companies that offer off-the-shelf or customisable platform solutions for launching RCS Business Messaging. This may be the MNOs and/or messaging technology providers.
Chatbot	An RCS-based 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 APIs	A standardised list of a limited set of APIs to facilitate developers and brands in consuming RCS services
Customer	Subscriber to MNO services
End user	Individual person who subscribes to messaging and RCS services
MaaP	RCS Business Messaging-Enabler layer to enrich communication between businesses (brand and enterprise) and MNO messaging users
MNO	Mobile Network Operator
MSISDN	Often referred to as the mobile contact number
NNI	Network to Network Interface – The interface that specifies signalling and management functions between two networks or a network and a hub
P2A	Person to Application – Communication initiated by the end user
P2P	Person to Person – Messaging between end users only
Plug-in	A mini application that appears within messaging or voice/video calling applications to aesthetically and functionally enrich the content of the conversation
RCS	Rich Communication Services
RCS Business Messaging	RCS Business Messaging is the evolution of SMS business messaging, increasing and improving the ways in which people and businesses communicate. It provides brands with the ability to make use of chatbots, plug-ins, and artificial intelligence (AI). Also see A2P.
Service Aggregator	Companies that offer a variety of value-added services to enterprises – not the least is messaging connectivity into multiple wireless providers
Service Providers	Any company or organisation which allows its subscribers access to the provided services
SMS	Short Message Service
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 Authority	Verification Authority is responsible for verifying and validating brands and chatbots against specific criteria. This is expected to be performed by the business messaging platforms but may be provided by any third-party.



2

RCS Business Messaging Recommended Good Practice Principles

The RCS Business Messaging Recommended Good Practices will be supported by the GSMA using a self-enrolment scheme. The RCS Business Messaging Recommended Good Practices will be added to the GSMA website as a reference for all players in the ecosystem.

Members participating in the MaaP ecosystem should follow these principles:

1 Principle 1: Do not create, carry or deliver unsolicited A2P RCS messages

1.1 All companies involved in the A2P RCS creation, routing and delivery, but in particular, Message Generators, should recognise that RCS is a powerful channel for businesses to interact with their consumers, as long as consumers have consciously and explicitly authorised that interaction.

1.2 Accept that consumers should be able to revoke their consent to be contacted and as a result interaction with them should cease as soon as technically possible.

2 Principle 2: Message Terminators have in place, mechanisms to prevent, detect, and report the misuse of services for the purpose of spam and fraud control

2.1 Effective policies and procedures:

2.1.1 Message Terminators should develop effective policies and procedures for fraud prevention and combating spam.

2.1.2 These policies and procedures should be reviewed regularly, or as and when the need arises to reflect any updates or changes.

2.2 Spam reporting:

2.2.1 When spam is reported the details should be shared amongst the MNOs and Business Messaging providers to the extent allowed by privacy good practise and technically possible.

2.2.2 The GSMA will maintain a list of Verification Authorities. When spam or fraud is detected, Verification Authorities may wish to inform other ecosystem players. NOTE: The GSMA accepts no liability in relation to the provision of the services provided by Verification Authorities, or any of the details reported. Each recipient of the report should undertake their own due diligence regarding the report.

2.2.3 MaaP Ecosystem participants should demonstrate their commitment to fraud prevention and combatting spam through proportionate measures.

2.3 Fraud control:

2.3.1 Identify and remove fraudsters from the A2P RCS value chain.

2.3.2 As reasonably as possible, block and report any suspected fraudulent activities in line with industry practice.

2.4 Software to monitor messages:

2.4.1 Message Terminators should create a system to monitor messages for Fraud / Spam purposes.

2.4.2 Chatbot verification (where implemented) should be used to provide additional assurance for verification and validation.

3 Principle 3: All companies have well-developed policies and processes and sufficient network and system capacity designed to provide reliable service provision

4 Principle 4: Service providers take robust steps designed to provide the RCS Business Messaging in a secure manner

4.1 Security governance:

4.1.1 All companies should develop, implement and regularly review a formal security policy.

4.1.2 Message Terminators should identify and assess security risks prior to offering RCS Business Messaging services and should continue to monitor such risks on an ongoing basis. e.g. abnormal message volumes, formats or patterns.

4.1.3 Modification of message content:

i) Message Processors and Terminators should not modify message content or metadata, unless legitimately required to do so for message delivery.

5 Principle 5: All companies communicate clear, sufficient and timely information to empower customers to make informed decisions

5.1 Effective disclosure and transparency:

5.1.1 All companies should ensure that Message Recipients are provided with clear, prominent and timely information regarding usage and terms and conditions.

6 Principle 6: Care should be observed regarding the timing and frequency of the interaction with customers

6.1 All companies, and Message Generators in particular, should seek to respect their consumers' preferences regarding the timing and frequency of the messages to be sent, particularly where explicitly indicated. When preferences are unknown, common sense and best judgement should be observed (e.g. all promotional messages should be sent during waking hours, 8am to 8pm of the Message Recipient), with the exemption of P2A initiated communication.

7 Principle 7: All companies have in place mechanisms designed to ensure that complaints are effectively addressed and problems are resolved in a timely manner

7.1 All companies should develop customer complaint policies and procedures.

8 Principle 8: All companies follow good data privacy practices when collecting, processing, and/or transmitting customers' personal data

8.1 Governance:

8.1.1 All companies should comply with good practices and relevant regulations governing customer data privacy in their relevant jurisdiction. In observing applicable regulations regarding storage, manipulation and transport of personal data, all companies should seek to deploy reasonable practices and appropriate technology, designed to protect consumers' personal data securely.

8.2 Transparency and Notice:

8.2.1 All companies should endeavour to ensure that Message Recipients are provided with clear information regarding their data privacy practices.

8.2.2 Message Terminators may need to consider updating consumer/retail service agreement terms and conditions as appropriate. All companies should respect agreed data handling in their agreements. In addition, all companies should honour the terms and conditions agreed with the consumer.

8.3 User Choice and Control:

8.3.1 All companies should endeavour to ensure that customers are informed of their rights and have opportunities to exercise meaningful choice and control over their personal information.

8.3.2 All companies should notify customers of any changes that materially affect the privacy of their personal information.

9 Principle 9: All companies should assist regulators, law enforcement bodies and other members of the ecosystem in investigating fraud incidents and identifying fraudulent actors within the ecosystem

9.1 Given the global and complex nature of the A2P RCS delivery chain, fraud may assume many different formats and hit different technical infrastructures, often in different countries. Therefore, quick and open communication amongst all industry peers is fundamental to limit the scope of fraud incidents, allowing the industry to stop them, once detected, as quickly as possible. Mitigating against fraud is likely the most powerful deterrent for potential fraudsters.

9.2 Companies should provide information required by regulators, law enforcement bodies or any other members of the ecosystem, which may help to stop a fraud incident or identify a fraudulent actor in a timely manner. This may include, for example, providing evidence of consumers' opt-in and opt-out preferences.

9.3 Information may be provided to the target Message Terminator, whom all companies are required to assist to their capability, to facilitate blocking of rogue activities.

9.4 In any instances where the RCS Business Messaging: Recommended Good Practices principles may conflict with local legislation or regulation, local laws will always supersede the RCS Business Messaging: Recommended Good Practices.

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