



**joyn Crane Product Definition Document**  
**Version 1.0**  
**15 May 2015**

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

---

**Security Classification: Non-confidential**

Access to and distribution of this document is restricted to the persons permitted by the security classification. This document is confidential to the Association and is subject to copyright protection. This document is to be used only for the purposes for which it has been supplied and information contained in it must not be disclosed or in any other way made available, in whole or in part, to persons other than those permitted under the security classification without the prior written approval of the Association.

**Copyright Notice**

Copyright © 2015 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 contain herein is in full compliance with the GSM Association's antitrust compliance policy.

## Contents

<b>1</b>	<b>Introduction</b>	<b>6</b>
1.1	Purpose of the document	6
1.1.1	Structure of the document	6
1.1.2	Crane client scope	6
1.2	Table of references	6
1.3	Conventions	8
1.4	Requirement and Technical Realisation Classification	8
1.5	Terms and Abbreviations	9
<b>2</b>	<b>Device Provisioning</b>	<b>11</b>
2.1	Description	11
2.2	User Stories and Feature Requirements	12
2.2.1	Configuration of the user's primary device by requesting user identity	12
2.2.2	Downloadable RCS applications / Multiple RCS instances	14
2.2.3	User consent	18
2.2.4	Service Introduction	20
2.2.5	Error Management	20
2.2.6	Provisioning push	21
2.3	Technical Information	21
2.3.1	Management of active IMS stack	21
2.3.2	Technical Implementation of User Stories and Service requirements	24
<b>3</b>	<b>Capability Discovery and Service Availability</b>	<b>27</b>
3.1	Description	27
3.2	User Stories and Feature Requirements	27
3.3	Technical Information of User Stories and Service requirements	32
3.3.1	Overview	32
3.3.2	Backward Compatibility	36
3.3.3	Configuration Parameters	37
<b>4</b>	<b>Operator Messaging</b>	<b>38</b>
4.1	Description	38
4.2	User Stories and Feature Requirements	38
4.2.1	Operator customisation for representation of Operator Messaging on the device.	42
4.2.2	Client Logic to propose the desired Messaging and File Transfer Service Capability Agnostic Messaging experience (send RCS to all contacts)	44
4.2.3	Client Logic to propose the desired Messaging Service – Integrated Messaging 'Online experience) (IM_CAP_ALWAYS_ON = 0 / SMS as default)	45
4.2.4	Integrated Messaging 'Offline experience'– (IM_CAP_ALWAYS_ON = 1 / RCS Chat as default between RCS users)	51
4.2.5	Integrated Messaging – File Transfer 1 (FT_HTTP_CAP_ALWAYS_ON=0 / online Experience only)	52
4.2.6	Integrated Messaging – File Transfer (FT_HTTP_CAP_ALWAYS_ON=1 / Offline experience)	54

4.3	Technical Information	55
4.3.1	Overview	55
4.3.2	Configuration Parameters	56
4.3.3	Capability Discovery	73
4.4	Technical Implementation of User Stories & Feature requirements	73
4.4.1	Backward Compatibility	74
4.4.2	Configuration Parameters	75
<b>5</b>	<b>1-to-1 Chat</b>	<b>76</b>
5.1	Description	76
5.2	User Stories and Feature Requirements	76
5.3	Technical Information	82
5.3.1	Overview	82
5.3.2	Technical Implementation of User Stories and Service requirements	82
5.3.3	Backward Compatibility	84
5.3.4	Configuration Parameters	84
<b>6</b>	<b>Group Chat</b>	<b>85</b>
6.1	Description	85
6.2	User Stories and Feature Requirements	86
6.3	Technical Information	94
6.3.1	Overview	94
6.3.2	Technical Implementation of User Stories and Service requirements	95
6.3.3	Backward Compatibility	98
6.3.4	Configuration Parameters	98
<b>7</b>	<b>File Transfer incl. Geolocation Push</b>	<b>99</b>
7.1	Description	99
7.2	User Stories and Feature Requirements	99
7.3	Technical Information	108
7.3.1	Overview	108
7.3.2	Technical Implementation of User Stories and Service requirements	108
7.3.3	Configuration Parameters	111
<b>8</b>	<b>Audio Messaging</b>	<b>111</b>
8.1	Description	111
8.2	User Stories and Feature Requirements	112
8.2.1	Sending Audio Messages	112
8.2.2	Notification on Receiving Audio Messages	114
8.2.3	Receiving Audio Messages	114
8.2.4	Implementation Examples	115
8.3	Technical Information of User Stories and Service requirements	115
8.3.1	Overview	115
8.3.2	Requirements matching	116
8.3.3	Backward compatibility	118
8.3.4	Configuration Parameters	119
<b>9</b>	<b>Backup &amp; Restore</b>	<b>119</b>
9.1	Description	119

9.2	User Stories and Feature Requirements	119
9.3	Technical Information	119
9.3.1	Overview	119
9.3.2	Technical Implementation of User Stories and Service requirements	120
9.3.3	Backward compatibility	120
9.3.4	Configuration Parameters	120
<b>10</b>	<b>Green Button Promise for Voice</b>	<b>120</b>
10.1	Description	120
10.2	User Stories and Feature Requirements	120
10.3	Technical Information	124
10.3.1	Overview	124
10.3.2	IP Voice and IP Video Call related Configuration Parameters	124
10.3.3	Technical Implementation of User Stories and Service requirements	131
10.3.4	Backward Compatibility	132
10.3.5	Configuration Parameters	132
<b>11</b>	<b>Green Button Promise for Video</b>	<b>132</b>
11.1	Description	132
11.2	User Stories and Feature Requirements	133
11.3	Technical Information	137
11.3.1	Overview	137
11.3.2	Technical Implementation of User Stories and Service Requirements	137
11.3.3	Backward compatibility	139
11.3.4	Configuration Parameters	139
<b>12</b>	<b>In-call Services</b>	<b>140</b>
12.1	Description	140
12.2	User Stories and Feature Requirements	140
12.2.1	In-call Services: General	140
12.2.2	In-call Services: "Live Video"	141
12.2.3	In-call Services: Image Share	144
12.2.4	In-call Services: Share any file during call	145
12.3	Technical Information	147
12.3.1	Overview	147
12.3.2	Technical Implementation of User Stories and Service Requirements	147
12.3.3	Backward Compatibility	150
12.3.4	Configuration Parameters	150
<b>13</b>	<b>API Extensions</b>	<b>151</b>
13.1	Description	151
13.2	User Stories and Feature Requirements	151
13.3	Technical Information	154
13.3.1	Overview	154
13.3.2	Requirements matching	155
<b>14</b>	<b>Security against Malware</b>	<b>157</b>
14.1	Description	157
14.2	User Stories and Feature Requirements	157

14.3	Technical Information	158
14.3.1	User Authentication	158
14.3.2	Encryption	159
14.3.3	Storage of Authentication and Identification Data	159
14.3.4	Applicability of Authentication Methods	162
<b>15</b>	<b>Data Off</b>	<b>164</b>
15.1	User Stories and Feature Requirements	165
15.2	Technical Information	168
<b>16</b>	<b>RCS Settings</b>	<b>170</b>
16.1	Description	170
16.2	User Stories and Feature Requirements	170
16.3	Technical Information	174
16.3.1	Technical Implementation of User Stories and Service requirements	174
<b>Annex A</b>		<b>178</b>
A.1	Personal Card format	178
A.2	Emoticon conversion table	180
A.3	Unicode Standard “Emoji” Emoticons	181
<b>Annex B</b>	<b>Document Management</b>	<b>182</b>
B.1	Document History	182
B.2	Other Information	182

## 1 Introduction

### 1.1 Purpose of the document

This document provides guidance to OEMs and Application Developers on the implementation of the Crane profile. Crane is backward compatible with Blackbird.

The Crane profile as detailed in this document has been developed by the following Operators (in alphabetical order):

- Deutsche Telekom
- KPN
- Orange
- Telefonica
- Vodafone

#### 1.1.1 Structure of the document

The Crane Product Description Document (PDD) details how the features are to be implemented in regards to the Functional Requirements and includes technical specification references and details that may influence how certain functions behave, creating an overall guide for OEMs and application developers.

- Chapter 2 covers discovery and activation.
- Chapter 3 covers capability discovery and service availability.
- Chapters 4 to 13 detail the 10 major Crane services.
- Chapters 14 to 16 address Security, Data Off and RCS Settings.

Each feature is structured into three parts: a user story that shall explain the user's view of the feature, the context and the benefit or the rationale why the feature makes sense. The second part lists the requirement(s), which describe how the user story shall be delivered to match the expectations. The final part is the technical implementation which maps to or explains how to use the supporting technical specification.

#### 1.1.2 Crane client scope

The Crane profile can be delivered in two ways for users:

1. Implemented natively within the device by the Original Equipment Manufacturer (OEM), tightly integrating the capabilities and services within the address book and many other native touch points across the device.
2. Implemented as a downloadable application that can be downloaded from Application stores and accessible as a separate application on the user's device, usually within the device's application folder or it's desktop.

In most cases implementation of features is identical for both native and downloadable clients and this document for the most part will not differentiate between the two. In those cases where implementation of a feature in a downloadable client differs from the native experience, this may be described separately within the relevant section.

## 1.2 Table of references

Ref	Doc Number	Title
[1]	[3GPP TS 22.140]	3GPP TS 22.140, release 10, Multimedia Messaging Service (MMS); Stage 1

Ref	Doc Number	Title
		<a href="http://www.3gpp.org/DynaReport/22140.htm">http://www.3gpp.org/DynaReport/22140.htm</a>
[2]	[3GPP TS 23.040]	3GPP TS 23.040, release 10, Technical realization of the Short Message Service (SMS) <a href="http://www.3gpp.org/DynaReport/23040.htm">http://www.3gpp.org/DynaReport/23040.htm</a>
[3]	[3GPP TS 24.167]	3GPP TS 24.167, release 10, 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; 3GPP IMS Management Object (MO) <a href="http://www.3gpp.org/DynaReport/24167.htm">http://www.3gpp.org/DynaReport/24167.htm</a>
[4]	[CAB_TS]	OMA Converged Address Book (CAB) Specification, Approved Version 1.0, 13 November 2012 <a href="http://www.openmobilealliance.org">http://www.openmobilealliance.org</a>
[5]	[NG.102]	IMS Profile for Converged IP Communications Version 1.0 15 May 2015 <a href="http://www.gsma.com/">http://www.gsma.com/</a>
[6]	[PRD-IR.51]	IMS Profile for Voice, Video and SMS over Wi-Fi Version 1.0 05 February 2015 <a href="http://www.gsma.com/">http://www.gsma.com/</a>
[7]	[PRD-IR.58]	IMS Profile for Voice over HSPA Version 7.0 11 March 2015 <a href="http://www.gsma.com/">http://www.gsma.com/</a>
[8]	[PRD-IR.92]	GSMA PRD IR.92 - "IMS Profile for Voice and SMS" Version 7.1 18 September 2013 <a href="http://www.gsma.com/">http://www.gsma.com/</a>
[9]	[PRD-IR.94]	GSMA PRD IR.94 - "IMS Profile for Conversational Video Service" Version 6.1 23 September 2013 <a href="http://www.gsma.com/">http://www.gsma.com/</a>
[10]	[RCC.07]	GSMA PRD RCC.07 version 6.0- "Rich Communication Suite 5.3 Advanced Communications Services and Client Specification" 28 February 2015 <a href="http://www.gsma.com/">http://www.gsma.com/</a>
[11]	[RCC.09]	GSMA PRD RCC.09 RCS 5.3 Endorsement of OMA CPM 2.0 Message Storage, Version 5.0 28 February 2015 <a href="http://www.gsma.com/">http://www.gsma.com/</a>
[12]	[RCC.10]	GSMA PRD RCC.10 Rich Communication Suite 5.3 Endorsement of OMA CPM 2.0 Interworking Version 4.0 <a href="http://www.gsma.com/">http://www.gsma.com/</a>
[13]	[RCC.11]	GSMA PRD RCC.11 Rich Communication Suite 5.3 Endorsement of OMA CPM 2.0 Conversation Functions Version 4.0 28 February 2015 <a href="http://www.gsma.com/">http://www.gsma.com/</a>
[14]	[RCC.14]	GSMA PRD RCC.14 Service Provider Device Configuration Version 1.0 16 February 2015 <a href="http://www.gsma.com/">http://www.gsma.com/</a>
[15]	[RCC.15]	GSMA PRD RCC.15 IMS Device Configuration and Supporting Services Version 1.0 16 February 2015 <a href="http://www.gsma.com/">http://www.gsma.com/</a>
[16]	[RCC.53]	GSMA PRD RCC.53 joyn Device API Specification

Ref	Doc Number	Title
		Version 2.0 16 October 2014 <a href="http://www.gsma.com/">http://www.gsma.com/</a>
[17]	[RCC.55]	GSMA PRD RCC.55 [TAPI-Security]: RCS Extensibility: Terminal API Security Version 1.0 15 October 2014 <a href="http://www.gsma.com/">http://www.gsma.com/</a>
[18]	[RCC.60]	Blackbird Product Definition Document, Version 4.0, 06 October 2014 <a href="http://www.gsma.com">www.gsma.com</a>
[19]	[RCC.61]	GSMA PRD RCC.61 RCS Common Core 1.1 Service Description Document Version 2.0 04 March 2015 <a href="http://www.gsma.com/">http://www.gsma.com/</a>
[20]	[RFC2425]	A MIME Content-Type for Directory Information IETF RFC <a href="http://tools.ietf.org/html/rfc2425">http://tools.ietf.org/html/rfc2425</a>
[21]	[RFC2426]	vCard MIME Directory Profile IETF RFC <a href="http://tools.ietf.org/html/rfc2426">http://tools.ietf.org/html/rfc2426</a>
[22]	[RFC5547]	A Session Description Protocol (SDP) Offer/Answer Mechanism to Enable File Transfer IETF RFC <a href="http://tools.ietf.org/html/rfc5547">http://tools.ietf.org/html/rfc5547</a>
[23]	[vCard21]	vCard, The Electronic Business Card, A versit Consortium Specification, 18 Sep 1996 <a href="http://www.imc.org/pdi/vcard-21.doc">http://www.imc.org/pdi/vcard-21.doc</a>

### 1.3 Conventions

It is a shared understanding by the standardising RCS Operators that any service described in the RCS standard may or may not be offered by any given Operator; however, it is agreed that if a feature is supported by an Operator, the Feature Requirements shall be supported as described by the Crane PDD.

NOTE: For device manufacturers and client developers requirements are classified based on the conventions defined in section 1.5 of this document.

Some additional information to clarify the requirement or User Story is presented as NOTES. Individual NOTES are not numbered. Content in NOTES shall not be considered as compulsory requirements as described in chapter 1.5 of this document.

### 1.4 Requirement and Technical Realisation Classification

Term	Description
<i>Shall/ Shall Not, Must/ Must Not</i>	These terms dictate that a functionality and/or process is <b>Mandatory</b>
<i>Required</i>	These terms dictate that a functionality and/or process is <b>Mandatory</b>
<i>Should/Should Not</i>	This term dictates that the functionality and or/process is <b>Highly Recommended</b>
<i>Recommended</i>	This term dictates that the functionality and or/process is <b>Highly Recommended</b>
<i>May</i>	This term dictates that the functionality and or/process is <b>Nice to Have</b>
<i>Optional</i>	This term dictates that the functionality and or/process is <b>Nice to Have</b>

**Table 1: Requirements Classification**



## 1.5 Terms and Abbreviations

Term	Description (contains technical and functional terms)
Aggregation of device capabilities	All of a user's capabilities for their RCS services on all of their RCS-enabled devices will be combined into a single set of capabilities which is shared with other users. Other users will not be able to determine on exactly which device another user has a specific capability, nor will other users know whether the user has multiple RCS devices available to them at all (using this capability information shared).
A-Party	The party that initiates a communication event e.g. creates and sends a chat message or File Transfer or initiates a call.
App	Smartphone application.
App ID	Unique identifier for an application.
Auto-Accept	A function on the device that shortcuts the user manual acceptance of the incoming communication event (such as chat, files etc.).
B-Party	The party that receives or is intended to receive a communication event e.g. Chat Message or File Transfer from A-Party.
Capability / Availability	A contact has a device registered for an RCS service that can initiate or respond to a requested RCS service.
CFB	Call Forward Busy.
Chat Message	A single text message that was conveyed from one user to another using the RCS Chat service.
CLIP	Calling Line Identification Presentation.
Common Message Store (CMS)	A network storage that enables Multi-Device and Backup and Restore use cases.
Contact	A contact is a communication partner either selected from the device contact list or typed into the dialler as a phone number.
Contact Card	The details of a single contact which are displayed whenever a contact is selected from the contact list.
Conversation History	A list of all the content exchanged between parties of a conversation.
CS	Circuit Switch.
CW	Call Waiting.
Default Messaging Client	In the case of multiple messaging clients on a device, the client chosen by the user to act as the default messaging client for messaging notification and message composing purposes.
Delivery Notification	Indication that a message was successfully received by the B-Party device.
DELIVERY TIMEOUT	A duration parameter set by the operator which triggers the RCS application to perform an action if the Delivery Notification of the receiving device has not been confirmed within the set time.
Developer	Application owner.
Developer ID	ID assigned to application owner. It is not the same as the App ID.
Device Wiping	Removing user specific data from the device.
Display Notification	Indication to the A-Party that the B-Party's device has displayed the message.
DTMF	Dual Tone Multi-Frequency.
Emoji	Emoji are "picture characters", that is, characters presented as pictographs —images of things such as faces, weather, vehicles and buildings, food and drink, animals and plants—or icons that represent emotions, feelings, or activities.
Emoticon	A graphical 'mood' element that technically is corresponding with a text string. The text string is conveyed by the standard, and interpreted on UI level and replaced with the corresponding graphical element.
EPC	Evolved Packet Core
External Loudspeaker	Speaker on the device which amplifies the audio of the call when activated.
Feature Tag	An IARI Tag assigned to a RCS functionality allowing to identify and route the RCS traffic invoked by those apps through APIs.

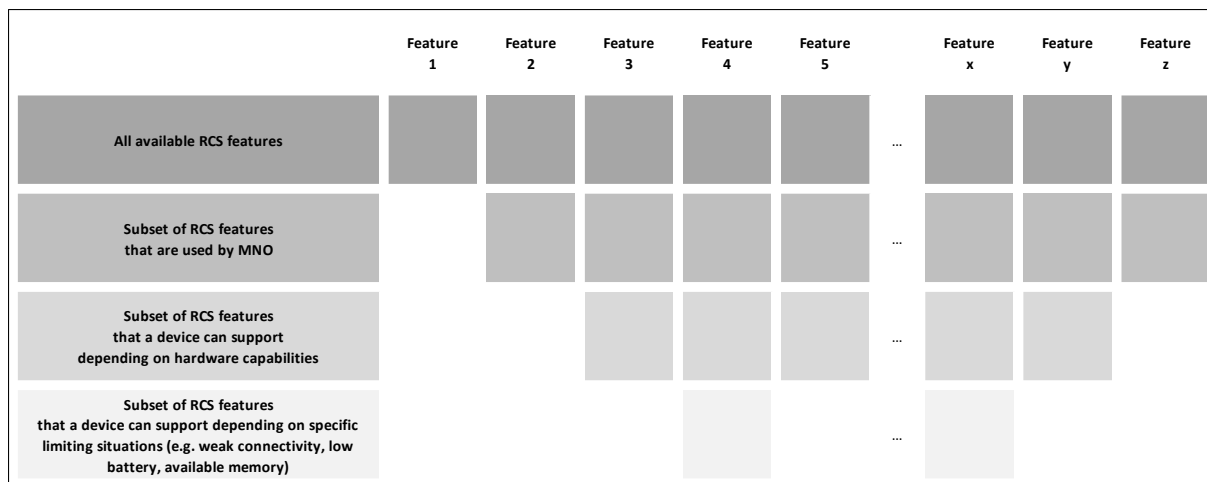
Term	Description (contains technical and functional terms)
Front Camera	Camera placed on the display side of a communication device.
GBA	Generic Bootstrap Architecture
Inactive device or Interface	A device or interface not currently active for a given session in a multi-device scenario.
Interconnected RCS Service	An RCS Service that can be accessed between users of network Operators supporting the same RCS Service capabilities.
Interface	Any entity that provides RCS Service capabilities to a user, e.g. browser-based, app-based, natively implemented.
IMSI	International Mobile Subscriber Identification.
Integrated Messaging	An Operator messaging service whereby the different message types are proposed to the end user, threaded together in a conversation and can be changed by the user. In this experience the message type used to deliver a message is indicated to the user
Messaging event	Includes all types of messages, files, content, new message notifications, previews, icons and message status notifications (sent and received).
MNO	Mobile Network Operator.
Multi-Device Support	RCS Service that enables a user to register more than one device under a single identity.
MSISDN	Mobile Subscriber Integrated Services Digital Number, i.e. mobile phone number.
OEM	Original Equipment Manufacturer.
"offline" user	A user who is known to be RCS enabled and not currently registered to the RCS service.
On-Net	Communication or signalling that does not go across the interworking interface (NNI) between networks or networks Operators.
"online" user	A user who is known to be RCS enabled and is currently registered to the RCS service.
Operator Messaging	Integration of all Operator Messaging Services into one single application. There are two options for Operator Messaging: "Integrated Messaging" and "Seamless Messaging".
Operator Messaging Services	One or more services from traditional messaging services (SMS, MMS) or RCS services (Chat, File Transfer, Audio Messaging, vCard Push, Geolocation Push).
Operator RCS Substitution Client (ORSC)	A downloadable RCS messaging client that is developed and/or approved by an MNO. An ORSC may or may not bring its own stack. An ORSC can be configured as the default messaging client.
PDD	Product Description Document
Primary Device or Primary Interface	Device which contains the SIM that matches the identity which the client uses to register to the IMS.
RCS activated	The RCS service has been successfully set-up by the network and the user (e.g. T&C) and is exposing its services to the user.
RCS Alias name	A name that is defined by the A-Party user that represents the A-Party user as a Chat participant on B-Party devices, if no Contact exists in the contact list.
RCS Client	A native or downloaded piece of software running on a device which provides the user with all features of a certain RCS/joyn release (as far as a platform permits) and which has been accredited by the GSMA.
RCS deactivated	The RCS service has been deactivated by the user via the Master Switch. In this state some or all of the RCS enablers are disabled.
RCS device enablers	RCS device enablers are functions/routines that are essential to the operation of RCS services but which are not transparent to the user. RCS enablers are: <ul style="list-style-type: none"> <li>• Provisioning request</li> </ul>

Term	Description (contains technical and functional terms)
	<ul style="list-style-type: none"> <li>• Registration</li> <li>• Capability discovery</li> <li>• IMS stack</li> <li>• Terminal APIs</li> </ul>
RCS-enabled	Capable of the RCS service, activated and ready to operate when the network conditions allow.
Rear Camera	Opposite to the front camera- positioned on the back of the device.
Seamless Messaging	An Operator messaging service whereby the user is not aware of the messaging technology used but the device / network determines which messaging technology is used.
Service availability	Service availability is a state of a specific user that is determined using Capability Discovery processes.
SDD	Service Definition Document – a document that describes the User Stories, Requirements and Technical Implementation Details of specific RCS services.
Smileys	Smileys are small graphical elements that can express mood, fun or icons to explain a thing or a status in a graphical, easy to use and understand manner. Example for smileys are 😊, 📞, 🌟 and 🌑.
Third Party RCS Client (3RC)	A client that provides RCS messaging and that is developed and/or approved by a third party using RCS APIs. A 3RC can be configured as the default messaging client. A 3RC cannot bring its own stack.
Thread (or messaging thread)	A thread (or “messaging thread”) is the history of all messages or files exchanged in past between two users, including message exchanged in past which are not part of the current conversation. This notion can be extended to Group, and then represents exchanges between all participants of the group.
UI	User Interface.
Value Added RCS Application (VARA)	An application that uses RCS services for exchange of information but provides a different service to the user (e.g. game, Field sales support etc.). A VARA cannot be configured as the default messaging client.
VoLTE	Voice over Long Term Evolution.
ViLTE	Video over Long Term Evolution.
xMS	The traditional Operator messaging services known as Short Message Service (SMS) and Multimedia Messaging Service (MMS).

## 2 Device Provisioning

### 2.1 Description

An Operator may provision different services for different users and/or devices based on internal policies (e.g. having an active subscription to one service). In the device provisioning phase, the services that are allowed for that user are configured on the device.



**Figure 1: RCS features and their availability depending on Operator choice, device capability, and specific limiting situations.**

Native RCS implementation shall start the activation process automatically when one of the triggers listed below occurs, unless certain conditions are fulfilled that prohibit activation depending of the trigger that occurred.

The triggers for the activation of RCS are:

1. First start
2. Factory reset
3. SIM swap
4. Firmware update (FOTA)
5. Re-activation of RCS via the Master switch
6. Reception of a provisioning request pushed by the network
7. Provisioning response sent by the network that revokes a former service suspension.

The conditions that prohibit the activation process if certain of the triggers above occur are:

1. RCS was deactivated by the user via the Master switch in order to suspend the service or to use another RCS app.
2. The service has been disabled by the network, e.g. if the user had not accepted terms and conditions.
3. The device has been automatically disabled after the user denied acceptance of terms and conditions via the provisioning mechanism.

Major changes of the Crane PDD compared to the Blackbird PDD are:

- Section 17 of Blackbird PDD ('joyn states' flow diagram) is now part of this section.
- Request of additional information for security purposes has been added.
- Welcome messages and End User Confirmation to be accessible at any time after the activation.
- Clarified behaviour of the RCS instance switch (Master Switch) for the native client.

## 2.2 User Stories and Feature Requirements

### 2.2.1 Configuration of the user's primary device by requesting user identity

**US2-1 As an Operator, I want my RCS customers to verify their identity before they use the RCS service**

- R2-1-1* When automatic identification of the user is not possible, the user shall be prompted to provide (manually type in) the MSISDN. To do so, a User Message (e.g. pop-up) shall be displayed.
- NOTE: Automatic authentication method should always prevail when available, therefore, even if manual identification method has been triggered (but not completed) because on non-cellular coverage (Wi-Fi), when moving to cellular data coverage the set-up process should be re-triggered.
- R2-1-1-1* Before the user is prompted to enter their MSISDN, they shall be informed why they are being asked to do so (e.g. Explain that the messaging app will include the Chat and File transfer).
- R2-1-2* To ensure validity of the provided MSISDN, a verification process shall take place:
- R2-1-2-1* A silent SMS with a password is sent to the device.
- R2-1-2-2* This SMS shall be intercepted by the RCS provisioning process and verified.
- R2-1-3* When the verification process has been completed successfully, the provisioning process shall be completed without any further user interaction.
- R2-1-4* If the SMS takes too long or is never received (e.g. because the network does not deliver the SMS properly or the user provided a wrong MSISDN), the user shall be presented with a screen informing them that the process cannot be completed at this stage.
- R2-1-5* In this case, the user shall be informed about the previously given MSISDN (so that the user can amend it if necessary) and shall be provided with the means to retry.
- NOTE: This procedure can be attempted a maximum of ten times after which manual Wi-Fi provisioning is stopped but automatic provisioning is still possible.
- R2-1-6* If the maximum number of attempts for manual identification is exceeded, the user should be presented with a screen informing them that the process cannot be completed over non-cellular data coverage and suggesting to connect to the cellular data network to complete the set-up process.

**US2-2 As a user, I want to seamlessly use RCS services after I bought a new RCS enabled smartphone.**

**As a user, I want to start using my RCS services independently of the connectivity status (Wi-Fi or cellular coverage) of my device while setting up the (new) device or downloading an RCS client.**

- NOTE: It is an accepted restriction that device provisioning does not happen if there is no data connectivity).

- R2-2-1* When the user activates RCS over a network that allows automatic authentication, then provisioning of the service and configuration of the device shall be done without any user interaction. However, there are three exceptions, covered in R2-4-1 and R2-5-1.
- R2-2-2* In any case, where the network hasn't been able to identify the user automatically, the device will enter into the process which describes the

configuration of the user's device by requesting the identity of the user via manual submission of the MSISDN.

## 2.2.2 Downloadable RCS applications / Multiple RCS instances

### **US2-3 As a user, I want and use as many RCS clients (native, ORSCs, 3RCs) and applications (VARAs) as I choose.**

- R2-3-1* It shall be possible for multiple RCS clients and Value Added RCS Applications (VARAs) to be active and working at the same time on a device.
- R2-3-1-1* Only one RCS client shall manage the user notifications of incoming xMS and RCS messages at a time and act as the default client for composing messages. This shall be known as the default messaging client.
- R2-3-1-2* If more than one RCS client is active and working at the same time, the user shall be able to choose which one of these RCS clients will act as the default messaging client.
- R2-3-1-2-1* A "Default Messaging Client" setting (e.g. toggle list) shall be made available in the device (see R16-18-2).

NOTE: Legacy messaging clients not supporting RCS shall not be able to operate as the default messaging client.

- R2-3-1-3* When an RCS client is set up and/or activated, the user may be asked whether they would like to set that RCS client as the default messaging client. This could be done via direction to the "default messaging client" setting (e.g. toggle list). If a user is not asked, the existing RCS client managing the user notifications and acting as the default messaging client shall continue to operate as such.
- R2-3-1-4* RCS and xMS messages and content may be displayed and made available from some or all of the active RCS clients and applications on a device.
- R2-3-1-5* User notifications of app to app traffic shall continue to be managed only by the app responsible for that particular app to app traffic, whichever client is chosen as the default messaging client.
- R2-3-2* The native RCS client's stack shall provide access to RCS Terminal APIs (T-API) to any authorised application wishing to use RCS services on behalf of the user.
- R2-3-3* In certain circumstances, an ORSC may install and use its own RCS stack on the device instead of the native RCS stack (e.g. this could be because there is no native stack present on the device, or the stack on the device is not suitable or needs to be upgraded to provide new functionality). In this case:
- R2-3-3-1* The ORSC shall be able to detect whether a native RCS stack exists already and if so whether RCS T-APIs are exposed by this native implementation and which T-API version.

If it is deemed appropriate to enable the ORSC's RCS stack, then:

- R2-3-3-2* The newly installed RCS stack brought by the downloaded app shall disable the operation of the existing active stack or prompt the user to confirm this action if it is not possible to do this automatically.
- R2-3-3-3* When the native RCS stack is disabled, the Master Switch shall be switched off. The user shall be able to enable it again by switching the Master Switch position to "ON".
- R2-3-3-4* The newly installed RCS stack included in the downloaded app may expose standard APIs to any other application already using or authorised to use the RCS APIs on that device.
- R2-3-3-4-1* Access to the new RCS stack's APIs shall be managed by the same mechanism in place for native API access.
- R2-3-3-4-2* Any application using the previously active RCS stack's APIs shall continue to use the new stack's API in a seamless way, i.e. without disrupting the user experience.
- R2-3-3-5* If an ORSC has included and activated its own RCS stack on the device, upon removal or disabling of the ORSC, any previously native RCS stack that was disabled by the ORSC shall be enabled again, or the user shall be prompted and guided on how to do so if automatic enabling is not possible.
- R2-3-3-6* The user prompt to reset the Master Switch (to "ON") shall include a 'don't show again' function to give the user the ability to limit the number of prompts presented.
- NOTE1: The use of RCS T-APIs is controlled by a security framework based on certificates issued by MNOs and OEMs. This framework must not be implemented by a 3RC or a VARA, it can only be provided by the native client/stack or an ORSC.
- NOTE2: Any ORSC, 3RC or VARA downloaded to the device should use the APIs provided by the native stack.

An RCS native implementation may enter into the following states depending on certain conditions:

- R2-3-4* Factory state: Native RCS on a device has not been provisioned yet or factory reset has been applied by the user. This is the out-of-the-factory status of RCS before any connection to the network has occurred. Once connectivity is established, the device enters the set-up process.
- R2-3-5* RCS on set-up process: The RCS service activation process is in progress. It is not yet visible on the device but HTTP requests are active.
- R2-3-6* RCS disabled: Native RCS on a device has not been successfully provisioned or has been deactivated by the Operator. This state is entered after provisioning failed deliberately, e.g. when an Operator denied provisioning of a RCS device since its user is not entitled to use the service, or due to technical failure. This state is also entered when an Operator decides to deactivate RCS on a device, e.g. if a customer is no longer entitled to use the service.  
In this state RCS services are not visible on the UI (respective entry points and message history are not presented) and the RCS enablers; IMS stack, register and capability discovery are disabled. The handling of auto provisioning depends on the exact reason for moving into this state which

leads to more sub states (for more details please refer to the RCS specification). However, one or more of the mentioned RCS enablers might be active if utilised by other services (e.g. VoLTE, which uses the same IMS stack, is active).

- R2-3-7* In the event of a SIM swap, if a valid configuration associated to the SIM is available in the device then it shall be used; otherwise the device enters the RCS on set-up process. Independent of the outcome, user data (e.g. configuration, messages, contacts etc.) shall not be deleted from the device in the event of a SIM swap (see 'SIM swap' in ).
- R2-3-8* RCS in launcher mode: This state applies only for those networks that require the user to accept the Terms & Conditions. It is considered highly likely that a user that rejected those Terms & Conditions on the first device start-up, learns later about RCS and wants to activate it. The RCS Master Switch shall be visible in this state, and if switched to "ON", will trigger the RCS set-up process.
- R2-3-9* RCS active: RCS is configured and active on the device. Capabilities are exchanged, all entry points enabled and all available RCS services active.
- R2-3-10* RCS deactivated: This state is entered if the user has deactivated RCS via putting the Master switch to "OFF". In this state the native RCS services are inactive, all its entry points with the exception of the Master switch are disabled (inactive or not shown) and all its user related content is available (Chat history, files, etc.). However, one or more of the mentioned RCS enablers might be active if utilised by other services (e.g. VoLTE, which uses the same IMS stack, is active). By clicking on the Master switch and switching it to "ON", the native device's RCS functionality can be re-activated.
- R2-3-11* In all case in which the service shall be activated it must be assured that no conflict will arise with an active RCS app the user has installed (please refer to 2.2.2 Downloadable RCS application/ Multiple RCS instances).

The following table depicts the relationship between triggers and the conditions that rule automatic activation of RCS.

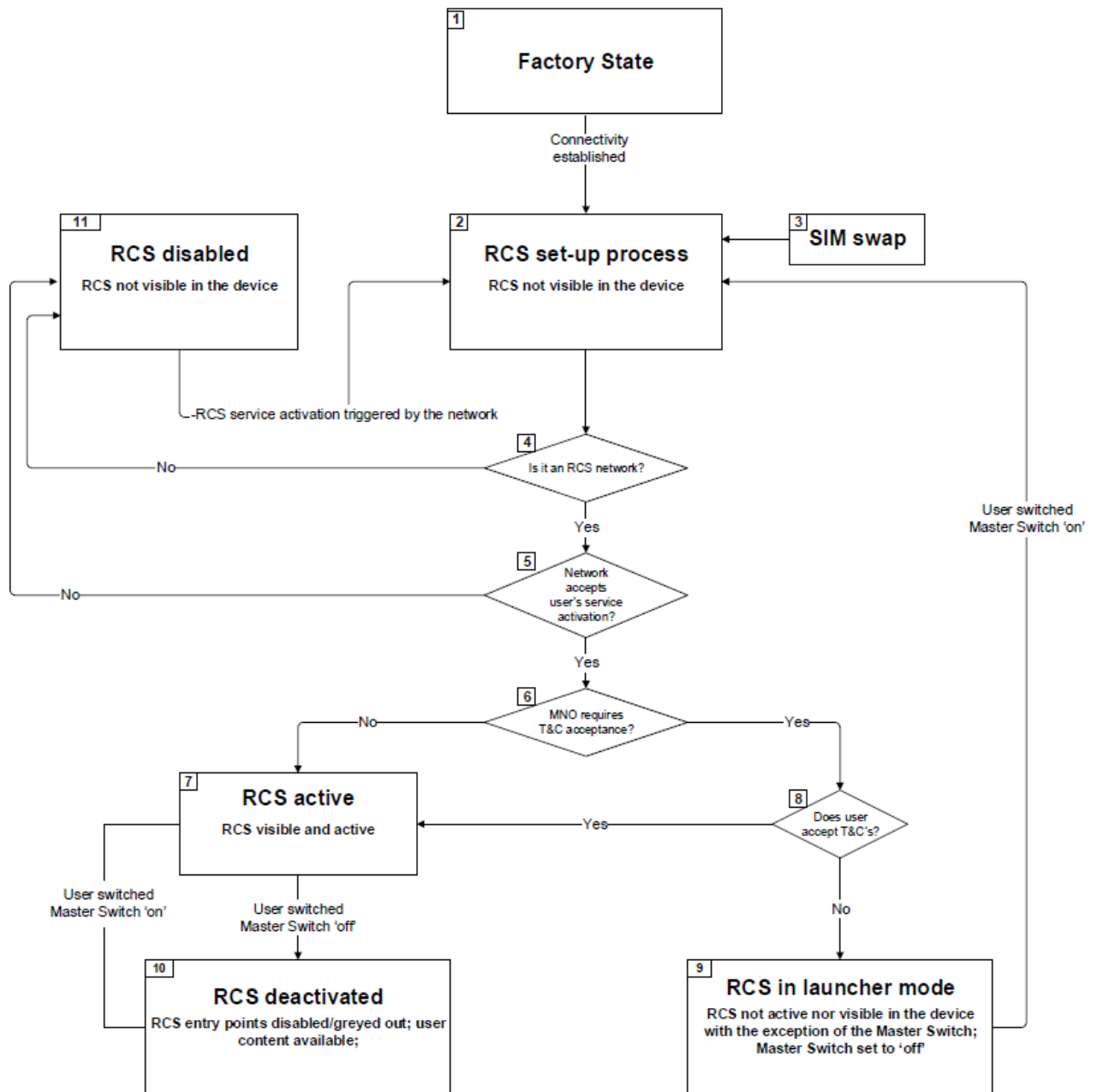


Triggers	Conditions		
	1. Deactivated by Master switch	2.Disabled by network	3.Disabled automatically
First start	N/A	N/A	N/A
Factory reset	Activate RCS and reset Master switch (to “ON”)	Activate	Activate RCS and reset Master switch (to “ON”)
SIM swap	<ul style="list-style-type: none"> <li>• Case 1: if a valid configuration associated to the inserted SIM is available ignore the trigger</li> <li>• Case 2: if not trigger RCS activation process and reset Master switch (to “ON”).</li> </ul>	<ul style="list-style-type: none"> <li>• Case 1: if a valid configuration associated to the inserted SIM is available ignore the trigger</li> <li>• Case 2: if not trigger RCS activation process.</li> </ul>	<ul style="list-style-type: none"> <li>• Case 1: if a valid configuration associated to the inserted SIM is available ignore the trigger</li> <li>• Case 2: if not trigger RCS activation process and reset Master switch (to “ON”).</li> </ul>
Firmware update	Ignore trigger	Ignore trigger	Ignore trigger
Reactivation via the Master Switch	Activate	Activate (Device in launcher mode)	Activate (Device in launcher mode)
Provisioning push	Ignore trigger	Activate	Activate
Network reactivation trigger	N/A	Activate	Activate

**Table 2: Triggers and conditions that rule automatic activation of RCS**

In cases, in which the service shall be activated but a downloadable RCS client was active before the trigger, the downloadable RCS client shall remain active. There are two exceptions:

1. the factory reset trigger and
2. the reactivation via Master Switch trigger.



**Figure 2: Status logic flow**

Figure 2 is an illustrative overview of the key device states and not an exhaustive depiction of all possible states. For details see R2-3-4 to R2-3-11.

### 2.2.3 User consent

An Operator may require that the user confirms their terms and conditions before the RCS service is made available to that user. If the Operator chooses to enforce this step, then the Operator will choose whether to prompt the user for confirmation using two buttons (e.g. "Accept"/"Reject"), or one button (e.g. "OK").

At any point after the service has been activated on the device, an Operator may require that further information be presented to the user. In this case, the Operator will choose whether the user will be asked to confirm the display of this information using either the one or two button method.

## User Message

### **US2-4 As an Operator, I want to be able to provide information and require consent BEFORE my customers use the RCS service.**

**R2-4-1** Upon Operator discretion a User Message (e.g. popup or toast) showing EITHER Terms & Conditions OR a Welcome Message (OR no User Message is shown) shall be displayed to the user during first-time configuration.

**NOTE:** Display of Terms & Conditions requires two buttons (e.g. “accept” & “decline”) for user action while display of Welcome Message requires only one button (e.g. “Ok”).

**R2-4-2** The presentation of the messages must be clear to the user and not hidden within the notification tray for action, but be presented ‘on top’ of the screen (see figure below).



**Figure 3: Example Terms & Conditions pop-up**

**R2-4-3** As soon as the user accepts the User Message, the RCS service shall be active on the device.

**R2-4-4** If the user declines the Terms & Conditions, RCS services shall not be available on the device, the RCS client shall become inactive (RCS Master switch set to ‘disabled’) and not visible on the device with the exception of the Master Switch that allows to re-enter the process (for details see R2-3-8).

**R2-4-5** If the user declines, a retry algorithm shall be able to retrigger the service activation and the Terms & Conditions acceptance process (on RCS capable networks). The retry algorithm shall be a retry after one day, then after one week, then after one month, then end.

## End User Confirmation Request

### **US2-5 As an Operator, I want to be able to provide information and require consent from my customers AFTER the RCS service has been activated**

- R2-5-1 Upon Operator discretion a popup showing a message (e.g. Terms & Conditions OR a Welcome message) shall be displayed to the user at any time after successful first-time registration.
- R2-5-2 The display of that message shall be able to come with EITHER one OR two buttons for the user to respond.
- R2-5-3 The Operator shall be able to determine the button texts (e.g. 'accept') of that popup.
- R2-5-4 The responses to the message shall be relayed back to the network.
- R2-5-5 The presentation of the message shall be clear to the user and not hidden within the notification tray for action, but be presented 'on top' of the screen.
- R2-5-6 Depending on the response by the user, the network can send a trigger to deactivate the RCS services on the device, i.e. RCS services shall not be available on the device, the RCS client will become inactive and not visible on the device or to put the device into the launcher mode in which the RCS Master Switch shall remain visible in the device (e.g. settings) to be able to re-enter the process of RCS activation.
- R2-5-7 Upon Operator policies, additional messages may be displayed to the user.

### **US2-6 As an Operator I want to request additional information from my customers during first-time registration in order to fulfil specific security purposes.**

- R2-6-1 Upon operator discretion, users can be requested to enter additional information during first-time registration in order to fulfil specific security requirements set by the Operator.

NOTE: Details are covered in 'Security against Malware', page 157.

### **US2-7 As a user, I want to have access to the text displayed as User Message and / or End User Confirmation Request at any time after being provisioned to the service.**

- R2-7-1 The text displayed as User Message and / or End User Confirmation Request shall be accessible for the user after the user has started using the service (e.g. in Messaging Settings).

## 2.2.4 Service Introduction

### **US2-8 As a user, I want the device to make me aware of new main functionalities added to my messaging app.**

- R2-8-1 The user shall get an introduction to new features, e.g. chat and SMS integrated, Delivery and Read notifications, RCS File transfer through the chat service and Group chat.

NOTE: This information shall be OEM specific.

## 2.2.5 Error Management

### **US2-9 As an Operator, I want technical errors to be handled with minimal user interaction.**

**The user may get any of the following errors:**

*R2-9-1* Reception of SMS (see R2-1-2-1) takes too long or is never received.  
NOTE: There are two possible causes:

1. The network does not deliver the SMS for whatever reason.
2. The user made a mistake when typing the MSISDN and the SMS is sent to a different device. In either case, the user shall be presented a screen informing them that the process is taking longer than expected. This screen shall contain a text box with the previously given MSISDN (so that the user can amend it if necessary) and a 'retry' button (final UI and text label is up to Operator discretion).

*R2-9-2* The procedure in R2-9-1 can be attempted a maximum number of times according to the Operator's definition. It is recommended to set the maximum number to 10 to be consistent with R2-1-5.

*R2-9-3* Temporarily unavailable: Applies to internal errors during configuration/provisioning or configuration server unreachable, as specified in section 2.3.3.2.4 of [RCC.07]. The device shall reattempt provisioning at a later stage (i.e. at the next device start-up)

*R2-9-4* Permanently unavailable: In case the Operator does not want to provide RCS services to a particular subscription an Operator defined error message shall be displayed and the provisioning process is stopped.

*R2-9-5* The user closes the MSISDN input field (e.g. by mistake) without providing any input: The user shall be presented the MSISDN input field a maximum number of three times while being not provisioned under non cellular connection. Further configuration attempts shall automatically start once the user connects to a cellular network.

## 2.2.6 Provisioning push

**US2-10 As an Operator, I want to be able to push configuration settings in special cases.**

Network initiated configuration request: Provisioning push will allow an Operator to force the reconfiguration of each user's device if needed:

*R2-10-1* The Operator shall be able to push configuration settings to new or existing RCS users (e.g. in the case of changing parameters).

*R2-10-2* The Operator shall be able to push configuration settings in case the network is upgraded to a new RCS release.

*R2-10-3* The Operator shall be able to push configuration settings when the device is permanently disabled but the user likes to start using RCS.

## 2.3 Technical Information

### 2.3.1 Management of active IMS stack

The requirements in section 2.2 require a mechanism to control which IMS stack is active (native or ORSC). Being device local the mechanism to support this will be OS specific. On Android™ it will be based on the following concepts:

- Identifying Android™ applications as RCS clients using a Manifest.xml meta-data property
- Identifying if a RCS client is enabled by accessing its Shared Preferences and reading a property from it.

- Accessing a RCS client settings screen by sending an intent using the action defined as a Manifest.xml meta-data property.

NOTE: In order to prevent having two RCS clients on the same device and, therefore, negative consequences in the user experience, the following mechanism shall be implemented by both native and ORSC client implementations. This mechanism is based on the following principles:

### 2.3.1.1 Client requirements

Android™ RCS clients shall define the following meta-data properties in their *Manifest.xml* file<sup>1</sup>.

Name	Value	Description
gsma.joyn.client	true	Used to identify the application as an RCS client
gsma.joyn.settings.activity	<String>	Equals to the intent action that be used to start the RCS client settings screen

**Table 1: Android RCS client Manifest meta-data properties**

Android RCS clients shall define a settings screen activity that can be opened by third party applications by using a simple intent which action string is equal to the value of the "gsma.joyn.settings.activity" meta-data property. Sending that intent to open the settings screen shall require no permission. Thus, the user decides (or not) to deactivate the third party application.

The following example illustrates the meta-data that shall be added to the *Manifest.xml* file, as well as a sample settings screen activity.

```

<application
    android:icon="@drawable/icon"
    android:label="@string/app_name">

    <!-- the following meta-data is used to identify the application as an RCS client -->
    <meta-data android:name="gsma.joyn.client" android:value="true" />

    <!-- the following meta-data is used to provide the value of the intent action that can be
    used by other applications to start the RCS client settings screen -->
    <meta-data
        android:name="gsma.joyn.settings.activity"
        android:value="com.vendor.product.MyRCSSettingsActivity" />

    <!-- RCS client shall define a settings property such that it can be open by third party
    applications using an intent which action string corresponds to the meta-data value
    defined above -->
    <activity android:name=".MyRCSSettingsActivity">
        <intent-filter>
            <action android:name="com.vendor.product.MyRCSSettingsActivity" />
            <category android:name="android.intent.category.DEFAULT" />
        </intent-filter>
    </activity>
    
```

**Table 2: Android meta-data usage**

<sup>1</sup> The naming of the parameters includes "joyn" for historic reasons to ensure compatibility with legacy joyn clients implementing the same mechanism for similar purposes. It is required to be provided regardless of whether the client implements a joyn profile.

Every RCS client shall define a publicly readable Shared Preferences using the name "*pckgname.gsma.joyn.preferences*", where '*pckgname*' parameter shall be replaced with the client's unique package name of the application (no two applications can have the same package name on the Android market). Client shall add this to the manifest as a meta data:

```
<meta-data android:name="gsma.joyn.preferences"  
android:value="pckgname.gsma.joyn.preferences" />
```

The shared preferences shall be created using the RCS client application context, using the mode `MODE_WORLD_READABLE`.

The shared preferences shall contain a Boolean property named "*gsma.joyn.enabled*". This property can have two values:

3. True: It will mean that the RCS client is enabled (user switch in settings set to "ON") and the application has been provisioned successfully.
4. False (default value): It will mean that the RCS client is disabled (user switch in settings set to "OFF") or the RCS client has never been provisioned yet.

The RCS client will modify the value of these properties according to the rules defined in the following section.

### 2.3.1.2 Client start-up behaviour

An RCS client which is started for the first time on a device shall:

- Retrieve the list of installed applications from the Package Manager, and identify existing RCS clients by looking for the Boolean meta-data property named "*gsma.joyn.client*", as defined in the previous section.
- For every RCS client that is found, the client shall open their shared preferences named "*pckgname.gsma.joyn.preferences*" and retrieve the Boolean property "*gsma.joyn.enabled*", as defined in the previous section.
- If an existing RCS client is found with the Boolean property "*gsma.joyn.enabled*" set to "*True*", it means that client is already active on the device. The new client shall inform to the user that there is another RCS client already configured in the device and that as a pre-requisite to use this one, it is necessary to disable it. In the same pop-up the possibility to access the RCS settings of the active RCS application (via intent mechanism) shall be offered. The intent action used to open the active RCS client settings screen shall be retrieved by reading its Manifest meta-data property named "*gsma.joyn.settings.activity*".
- After disabling the active client, its settings screen shall be closed and the new client shall be given control again. The new client shall then perform these first time start checks again which would lead to the conclusion that there is no active client and that therefore the new client shall become the active client (see NOTE below).
- If there is no existing RCS client, or that none of them are enabled, the new RCS client may proceed with provisioning and registration. Once the client is successfully provisioned and registered to the network it shall open its own "*pckgname.gsma.joyn.preferences*" shared preferences and set its own "*gsma.joyn.enabled*" property to "*True*".

If the RCS client is disabled (e.g. user switch in settings set to "OFF") it shall open its own "*pckgname.gsma.joyn.preferences*" shared preferences and set its own "*gsma.joyn.enabled*" property to "*False*".

This start-up behaviour shall also apply when there is an attempt to re-activate the disabled client; and when the disabled client is re-started.

### 2.3.2 Technical Implementation of User Stories and Service requirements

- R2-11-1* Provisioning on networks with automatic identification (see requirement R2-2-1) shall be done as described in [RCC.07] section 2.3.3.1 and 2.3.3.2 with only the Hyper Text Transfer Protocol (HTTP) solution being in scope as it is also needed when configuring over networks where identification is not possible (see R2-11-2). For the HTTP based mechanism, section 2.3.3.2 of [RCC.07] and its subsections shall apply in their entirety. If the network cannot authorise the user (as described in requirement R2-2-2) an HTTP 511 Response shall be returned as indicated in section 2.2.4 of [RCC.14], which shall (as indicated in [RCC.14]) result in the use of the procedures in section 2.3 of [RCC.14]. In that case if the IMSI is available, a device shall not ask the user for the MSISDN, and shall instead attempt the configuration providing only the IMSI in the HTTP request
- R2-11-2* Configuration over networks where automatic authentication is not possible (e.g. non-cellular networks) shall be realised using the HTTP mechanism as described in section 2.3. of [RCC.14] and its subsections providing the procedure required in requirements R2-1-1, R2-1-2, R2-1-2-1, R2-1-2-2, R2-1-3 and R2-9-1, with the error handling described in section 2.3.3.4 covering the behaviour required in R2-1-4 and R2-1-5. Requirement R2-1-1-1 shall be implemented locally on the device. The device shall assume that RCS is available on the user's network if DNS resolution of the HTTP configuration URL is possible using the MCC and MNC obtained from the SIM card. As described in section 2.3.2, if the IMSI is available, a device shall not ask the user for the MSISDN, and shall instead attempt the configuration providing only the IMSI. The Operator limitation required in R2-9-2 is covered by the NOTE in section 2.3.2 of [RCC.14].
- R2-11-3* Requirement R2-1-6 shall be implemented locally on the device
- R2-11-4* The rcs\_profile parameter shall be included in the HTTP GET requests and set to "joyn\_crane".
- R2-11-5* To ensure that multiple active RCS clients can work on a device at the same time and to ensure that only one client is the default messaging client active on a particular device (as required in R2-3-1 to R2-3-10) a device-local solution is required which will therefore be OS specific.
- For the Android™ OS this shall be implemented locally on the device and 3RCs and VARAs clients shall use the exposed APIs of the active and default messaging client, following RCS Device API.
- R2-11-6* For requirement R2-3-1-1 the client shall follow the mechanism described in R2-11-1.
- R2-11-7* Requirement R2-3-1-2 and the sub requirements shall be implemented locally on the device.
- R2-11-8* During the set up process or immediately after the RCS client is activated, a message shall be displayed to the user requesting if the client should be the default messaging client. If no information is provided by the user the active RCS client as described in R2-3-1-3 shall continue to operate as the default messaging client.
- R2-11-9* Requirement R2-3-1-4 shall be implemented locally on the device.



- R2-11-10* Requirement R2-3-1-5 shall be implemented locally on the device using IARIs to identify the application traffic as defined in section 3.12.4.2.2 of [RCC.07].
- R2-11-11* Requirement R2-3-2 shall be implemented based on section 13 'API Extensions'.
- R2-11-12* Requirement R2-3-3 and the sub requirements shall be implemented locally on the device.
- R2-11-12-1* For requirement R2-3-3-1, the client shall follow the mechanism described in section 2.3.1 of this document.
- R2-11-12-2* To disable the existing active stack as indicated in requirement R2-3-3-2, the client shall follow the mechanism described in section 2.3.1 of this document
- R2-11-12-3* Requirement R2-3-3-3 shall be implemented locally on the device.
- R2-11-12-4* Requirements R2-3-3-4, R2-3-3-4-1 and R2-3-3-4-2 shall be implemented locally on the device following section 4 of [RCC.55].
- R2-11-12-5* For requirement R2-3-3-5, when the user re-enables an RCS client, a HTTP configuration request shall be done to verify whether the available version of the RCS configuration parameters are still valid.
- R2-11-12-6* Requirement R2-3-3-6 shall be implemented locally on the device.
- R2-11-13* Requirements R2-3-4 to R2-3-10 shall be implemented locally on the device with the Operator having the possibility to disable the RCS client as indicated in requirement R2-3-10 by setting the RCS DISABLED STATE configuration parameter in a provided configuration document to -1 as described in section 2.3.3.2 of [RCC.07].
- R2-11-14* To avoid conflict with the active RCS client on the device, an ORCS shall follow requirement R2-11-5. If the ORCS activates its own stack, section 2.3.1 of this document applies
- R2-11-15* The user consent before use of the service described in user story US2-4 shall be realised through the mechanism for providing User Messages in the HTTP configuration described in section 2.2.3 of [RCC.14]. This mechanism shall be supported by the RCS clients and may be used upon the service provider's discretion.
- R2-11-16* As described in section 2.2.3 of [RCC.14] the User Message mechanism supports requirements R2-4-1 and R2-4-4.
- R2-11-17* Requirements R2-4-2 and R2-4-5 shall be implemented locally on the device.
- NOTE:** The retry algorithm described is to be realised in the device. An Operator can opt for more retries through the Provisioning Push mechanism described in US2-10.
- R2-11-18* For requirement R2-4-3 as defined the configuration shall be applied and the service shall be activated when the user presses the "Accept" button, moving to another screen shall be considered equivalent with this "accept" button action.
- R2-11-19* The user consent after activation of the service described in user story US2-6 shall be realised through the mechanism End User Confirmation Request mechanism described in section 3.1 of [RCC.15]. This mechanism shall be supported. This mechanism shall be supported by the RCS clients

and may be used upon service provider discretion. No specific handling apart from the normal processing of End User Confirmation Requests is thus assumed to be provided on the device.

- R2-11-20* As described in section 3.1 of [RCC.15] the End User Confirmation Request mechanism supports requirements R2-5-1, R2-5-2, R2-5-3 and R2-5-4. For requirement R2-5-2, in the case when one button is required, the End User Notification Request described in section 3.1.3 of [RCC.15] shall be used. For a message requiring two buttons, the End User Confirmation Request and Response described in section 3.1.1 and 3.1.2 of [RCC.15] respectively shall be used.
- R2-11-21* Requirement R2-5-5 shall be implemented locally on the device
- R2-11-22* For requirements R2-5-6 the network shall disable the RCS client by triggering a client reconfiguration using the procedure defined in R2-11-30 returning a HTTP configuration response with the RCS DISABLED STATE configuration parameter set to '-2' ensuring that the RCS touch points remain available as described in section 2.3.3.2 of [RCC.07].
- R2-11-23* For requirement R2-5-7, [RCC.07] does not impose restrictions on the use of the End User Confirmation request mechanism. Further messages can thus be sent at any point in time, including immediately after a message has been sent.
- R2-11-24* As described in section 2.2.5 of [RCC.14] an Operator can choose to fall back to the SMS-based authentication mechanism used on networks where automatic identification is not possible. This allows in combination with the mechanism described in section 2.3.2 and 2.3.5 of [RCC.14] to handle that SMS in a manner that is not transparent to the user thereby supporting the requirement R2-6-1. This same non-transparent handling of the SMS can be used to realise this requirement on networks where automatic identification is not possible.
- R2-11-25* Requirement R2-7-1 shall be implemented locally on the device by making the contents of any received User Message and non-volatile End User Confirmation Request available for consultation by the user at a later time. This consultation shall not require the user to provide a response to the request.
- R2-11-26* Requirement R2-8-1 shall be implemented locally on the device and the information shall be OEM specific
- R2-11-27* If the subscriber cannot be provisioned due to Operator policy (i.e. a permanent unavailability as described in requirement R2-9-4), the Service Provider can include a message as described in section 2.2.3 of [RCC.14] in a response disabling the RCS client (i.e. RCS DISABLED STATE set to -1).
- R2-11-28* As described in section 2.2.4 of [RCC.14], a number of consecutive internal errors (each resulting in a temporary unavailability as described in requirement R2-9-1) shall lead to a permanent unavailability. As described in section 2.3.4 [RCC.14], for non-cellular networks, this situation shall be applicable only to that particular network however.
- R2-11-29* A SMS shall be sent to the device with a specific format defined in section 3.1 and 3.2 of [RCC.14] respectively for the push request for initial configuration of a device on which RCS was permanently disabled (i.e. as a consequence of R2-11-29 and R2-11-30 required in R2-10-1 and R2-10-3), and a reconfiguration of an active RCS device (required in R2-10-1 and

R2-10-2), shall be enough to trigger a new configuration of a primary device.

*R2-11-30* For the reconfiguration of primary and additional devices on which RCS is already active (required in R2-10-1 and R2-10-2), it shall be possible to trigger a reconfiguration by sending an End User Confirmation Request to the device as specified in section 2.1.3.1 of [RCC.15].

### 3 Capability Discovery and Service Availability

#### 3.1 Description

The capability discovery is a process which enables RCS users to understand the set or subset of RCS services their contacts use, at certain points in time. Capability discovery can also be used by RCS entities to detect service awareness of other RCS users on behalf of an RCS service or user.

The availability of a RCS service is influenced by three categories of conditions:

1. Provisioning status
2. Device capability and status
3. Network conditions

Major changes of the Crane PDD compared to the Blackbird PDD are:

- References to 'joyn' in the User Interface have been removed.
- Behaviour of entry points to the different RCS services has been added.
- Interaction with ViLTE has been included.
- Any available RCS service deems a contact as RCS enabled, Chat service is no longer the minimum required.
- Polling of RCS contacts (after the initial one) are restricted to the device being plugged to a battery charger.
- RCS applications are limited to use cached capability information.
- Introduction of "last seen online" functionality

#### 3.2 User Stories and Feature Requirements

**US3-1 As a user, I want to be aware of the ways I can communicate with contacts stored in my contact list, regardless of their service provider or country where they reside.**

*R3-1-1* The device shall make the detected RCS capabilities visible to the user for contacts following a contact list scan or an individual contact capability check.

*R3-1-2* For a non RCS contact, the device shall only make services visible that are known to be compatible with defined RCS services.

*R3-1-3* For integrated messaging (as defined in Operator Messaging, page 38), there shall not be any RCS service entry points when the recipient is known to be a non RCS user.

*R3-1-4* The device shall make visible (based on the Operator configuration using the branded/unbranded parameter) whether a contact is RCS-enabled at least in the following touch points:

- Contact list

- Contact card
- Call log detailed view
- Activity log

NOTE: Appearance and visibility of RCS enabled contacts in these service entry points shall be left to OEM implementation. “joyn” iconography is no longer required.

**US3-2 As a user, I do not want to be disappointed by selecting a communication option that appears to be available but is not.**

- R3-2-1* RCS service entry points which represent an available service at a given point in time shall be selectable by the user.
- R3-2-2* Selecting an available RCS service shall initiate the device dialogue for that service.
- R3-2-3* In the case when the recipient (B-Party) has multiple devices, RCS service entry points which represent an available service at a given point in time shall be selectable on the A-Party device if at least one of the recipient’s devices is capable for this service.

**US3-3 As a user, I want to be sure that the information I have about my contacts RCS service capabilities is up to date and if they are available to communicate using those capabilities.**

- R3-3-1* Based on a capability discovery or service availability poll performed by the device, the user shall be able to see which contacts are available for certain RCS services.
- R3-3-2* Any capability discovery or service availability check of contacts shall happen in the background without any user notice.
- R3-3-3* Operators can configure how service entry points shall be presented at key touch points on the device where RCS communications can occur, specifically:
- R3-3-3-1* Service entry points for voice call shall always be visible and selectable at any given point in time.
  - R3-3-3-2* Service entry points for messaging shall always be visible and selectable at any given point in time. This requirement shall be applicable for Group Chat as well.
  - R3-3-3-3* Service entry points for File Transfer shall always be visible and selectable at any given point in time. This requirement shall be applicable for all services that use File Transfer as an enabler: Audio Messaging, vCard sharing and Geolocation Push.
  - R3-3-3-4* The IP Video Call service entry point shall be visible and selectable by the user if there is a high likelihood that the IP Video Call attempt will be successful at that time. If an IP Video Call is unlikely to be successful, the IP Video Call service entry point shall be greyed out and not selectable. This variant applies for any phone number including RCS and non RCS contacts.
  - R3-3-3-5* The In-Call-Service service entry point(s) shall be visible and selectable by the user if there is a high likelihood the respective In-Call-Service attempt will be successful at that time. If this attempt is unlikely to be successful, the service entry point for In-Call-Services shall be greyed out and not selectable.

NOTE 1: In the case the B-Party is a non RCS user with ViLTE, during call setup ViLTE capability is to be considered there is a high likelihood for a successful video call upgrade.

NOTE 2: "Likely to succeed" means capability or service availability exchange is indicating end-to-end support. "Likely to fail" means capability or service availability exchange is indicating "not available at this time".

*R3-3-4* A contact is deemed to be a RCS user when at least one RCS service capability is discovered and/or available for that contact.

*R3-3-5* On first RCS device boot up, after installation and/or set up of the RCS application, and after each re-configuration of the RCS service, the device shall perform an initial setup scan of the contact list and find out which of the contacts are enabled for RCS services.

*R3-3-6* Under certain circumstances after the initial setup scan, the device shall scan for RCS service capabilities of all contacts or defined subset(s) of contacts in the contact list in order to promote real time awareness and use of services. Any subsequent capability discovery and/or service availability checks shall only be made by the device based on the following:

*R3-3-6-1* The Operator shall be able to define a minimum time span between two full contact list scans (this includes the option to select 'no subsequent full contact list scans').

*R3-3-6-2* Scheduled scans of RCS enabled contacts shall only occur when the RCS capability information for the contact is older than the Operator configured value.

*R3-3-6-3* The device shall only perform capability scans of the entire contact list when connected to a charger. The device may split very long contact lists into chunks and perform the regular contact list updates on subsequent charging cycles.

*R3-3-6-4* A new "scan" of the contact list or set of contacts shall not commence until the previous one was completed.

*R3-3-6-5* The device shall request an RCS capability discovery and/or service availability check/update of an individual contact when capability information is invalid or expired AND one of the following applies:

*R3-3-6-5-1* When a new contact is added to the address book.

NOTE: If this contact is RCS enabled, their current capability is displayed.

*R3-3-6-5-2* When opening the contact from the contact list.

*R3-3-6-5-3* When starting a new conversation with the contact (e.g. when adding the contact to the "To:" field of a new message).

*R3-3-6-5-4* When opening or returning to a conversation or thread with the contact (including unlocking the screen for an open conversation).

*R3-3-6-5-5* When the A-Party has just come online during an ongoing conversation and the current messaging service is xMS (for Integrated Messaging option 1 and File Transfer option 1 scenario).

*R3-3-6-5-6* When initiating a voice or video call with a known RCS contact.

*R3-3-6-5-7* During a voice or video call with a known RCS contact.

- R3-3-6-6* The CAPABILITY VALIDITY timer shall be reset every time a Chat message or File transfer event is received and when a Delivery Notification for a sent message is received.
- R3-3-6-7* The Operator shall have the ability to limit the impact of capability and availability checks based on the following:

  - R3-3-6-7-1* An Operator defined minimum interval duration shall exist between two queries sent to the same RCS contact (CAPABILITY VALIDITY).
  - R3-3-6-7-2* An operator defined minimum interval duration shall exist between two queries sent to the same non-RCS contact.
  - R3-3-6-7-3* An operator defined telephone number prefix setting.
  - R3-3-6-7-4* RCS applications shall use known and valid contact capability or service availability information which is stored locally on the device (i.e. cached) when attempting to establish a connection with a contact.
  - R3-3-6-7-5* For In-Call services, a capability check shall always be made when the call has been set up and irrespective of whether the interval of capability checks has expired or not.
- R3-3-6-8* Each response to a capability/service availability request/update shall include the current or most recently available capability/availability information.
- R3-3-6-9* A sender of a capability / service availability request shall include the sender's own latest capability and availability information in that request.
- R3-3-7* The Operator shall be able to limit the impact of capability and availability checks (network load, device battery drain) by implementation of a capability and availability network element which caches online and / or offline capabilities and availability of RCS users and answers capability and availability checks.

  - R3-3-7-1* The Operator may respond to capability requests with current user capabilities or service availabilities which are stored on the capability or service availability server.
- R3-3-8* The RCS capability of a contact shall be removed when in the process of capability discovery and service availability exchange the network returns an error that indicates the user is not a provisioned RCS user.
- R3-3-9* When a client is permanently removed from a device or otherwise permanently deactivated, it shall attempt to inform the service provider.
- R3-3-10* A "triggered removal" shall be applied, when all of the following conditions apply:

  - R3-3-10-1* A RCS contact is manipulated by the user in such a way to trigger a capability and availability check (e.g. in a group chat picker) and its RCS capabilities are older than an Operator set parameter and the Operator does not request a periodic polling of the capabilities of contacts with obsolete capability information.
  - R3-3-10-2* The response to the capability exchange is inconclusive.
- R3-3-11* When the RCS application on the device is disabled by the Operator, the contacts RCS capability and availability indications associated with the

RCS application shall be removed from all associated device UI(s) on the user's device.

- R3-3-12* When the RCS application on the device is uninstalled by the user, the contacts RCS capability and availability indications associated with the RCS application shall be removed from all associated device UI(s) on the user's device.

**US3-4 As a user, I want to see when a contact was last active with messages in the contact specific conversation view so that I get a better indication about the likelihood that the contact actually receives and reads the chat message near time.**

- R3-4-1* In case capability detection indicates a contact is available for RCS chat and/or RCS file transfer, a time stamp is presented to the user when that contact was last active on RCS chat / file transfer.

- R3-4-2* The time stamp indicates a general activity of that contact based on:
- Sent RCS chat message or SMS from primary device to any other contact
  - Sent RCS File Transfer or MMS from primary device to any other contact
  - Actively accessed the messaging application to view or read messages.

- R3-4-3* Activity indication for a contact is presented within the conversation view with that contact.

- R3-4-4* The activity indication should be presented for only a few seconds (e.g. a toast) when entering a conversation or unlocking the device in an open conversation.

- R3-4-5* The format of the last seen active timestamp shall follow the following smart timestamp rules unless the device already uses smart timestamp:

*R3-4-5-1* If the last seen active information is equal to 59 minutes or less, then present "x minutes ago".

*R3-4-5-2* If the last seen active information is equal to 60 minutes but less than 5 hours, then present "x hours y minutes ago".

*R3-4-5-3* If last seen active information is equal to or greater than 5 hours, then present the true timestamp of the last activity.

*R3-4-5-4* If that timestamp refers to the day before, the present "yesterday" plus timestamp.

*R3-4-5-4-1* If that timestamp refers to any day before "yesterday" then present the date plus timestamp.

- R3-4-6* The device shall present the following status:

*R3-4-6-1* Updating: this state shall be shown once a contact has been selected and while its capabilities are verified. This state does not need to be displayed for non RCS capable contacts.

*R3-4-6-2* Last active at <time and date>: this state shall be shown for other RCS capable users after the result of the capability exchange has provided information on when the user was last active.

*R3-4-6-3* Active now: this state shall be shown for RCS users who are online and currently using the messaging app.

*R3-4-6-4* Ready to chat: this state shall be shown for users who are online but the last seen active information is not provided by the B-Party Operator.

*R3-4-6-5* SMS: this state shall be shown for RCS Capable users who are offline (only when IM CAP ALWAYS ON=0 in other configurations nothing is shown).

*R3-4-6-6* SMS only: this state shall be shown for non-chat-enabled contacts (only when IM CAP ALWAYS ON=0, in other configurations nothing is shown).

**US3-5 As a user, I want to configure whether other users can see the time stamp of my last activity in their conversation view. If I disable the feature I will not be able to see last activity time stamp of other users.**

*R3-5-1* The user shall be able to set whether other contacts can see their last activity.

*R3-5-2* If a user does not allow others to see their activity then the user shall not see any activity indication for their contacts.

**US3-6 As an Operator I want to decide whether I offer the 'last seen active' service to my users or not.**

*R3-6-1* The Operator shall be able to configure the service so that the function "last seen active" is available to users or not.

### 3.3 Technical Information of User Stories and Service requirements

#### 3.3.1 Overview

For joyn Crane, the Capability Discovery and Service Availability shall be realised based the SIP Options Exchange as specified in sections 2.6, 2.6.1.1, 2.7, 2.7.1.1 of [RCC.07].

*R3-7-1* Requirements R3-1-1 and R3-1-2 shall be implemented using SIP OPTIONS. The rest of the requirements under R3-1-3 and R3-1-4 shall be implemented locally on the device. The available services for requirement R3-1-3 are voice calling, Operator messaging with RCS messaging being available if configured through corresponding configuration parameters.

*R3-7-2* User Story US3-2 requirements are implemented locally on the device. In order to realise R3-2-3 requires the service provider to deploy an OPTIONS AS as specified in 2.6.1.1.5 of [RCC.07].

*R3-7-3* Requirement R3-3-1 shall follow SIP OPTIONS. Requirement R3-3-2 requirement shall be implemented locally on the device.

*R3-7-4* The requirements under R3-3-3 shall be implemented locally on the device.

*R3-7-5* Requirements under R3-3-4 are implemented locally on the device and is supported when any RCS service tag is exposed/discovered.

*R3-7-6* Requirements under R3-3-5 shall follow section 2.6.2 of [RCC.07].

*R3-7-7* Requirement R3-3-6-1 shall use POLLING PERIOD in A.10 [RCC.07]. Requirement R3-3-6-2 shall use CAPABILITY INFO EXPIRY in A.10 [RCC.07]. Requirements R3-3-6-3 and R3-3-6-4 requirements are implemented locally on the device.

*R3-7-8* Requirements under R3-3-6-5 requirements shall follow 2.6.2.1, 2.6.3.1, 3.3.6.3, and 3.3.4.1.3 of [RCC.07].

*R3-7-9* Requirement R3-3-6-5-5 shall be implemented locally on the device.

*R3-7-10* Requirement R3-3-6-5-6 shall be implemented locally on the device.



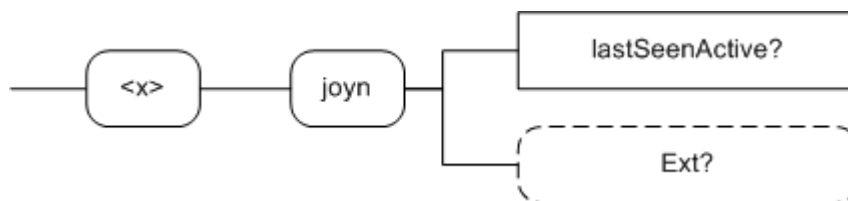
- R3-7-11* Requirement R3-3-6-5-7 follows 2.6.3.1 of [RCC.07] after a voice call is established.
- R3-7-12* Requirement R3-3-6-6 shall be implemented locally on the device.
- R3-7-13* Requirements under R3-3-6-7 shall follow the capability discovery optimizations defined in 2.6.3, 2.6.4, and A.10 [RCC.07]. Requirement R3-3-6-7-3 shall follow 2.6.4.1 of [RCC.07].
- R3-7-14* Requirement R3-3-6-8 shall be realised using the response of each SIP OPTIONS as described in section 2.6.1.1.2 of [RCC.07].
- R3-7-15* Requirement R3-3-6-9 shall be realised using SIP OPTIONS following section 2.6.1.1.2 of [RCC.07].
- R3-7-16* Requirement R3-3-7-1 may be realised in the Network using a SIP OPTIONS AS.
- R3-7-17* Requirement R3-3-8 is implemented locally on the device following error codes handling defined in 2.6.1.1. and 2.6.2.1 of [RCC.07].
- R3-7-18* Requirement R3-3-9 shall set the version set to -1 in the configuration request and follow client codes 2.3.3.2.1 and procedures defined in [RCC.07].
- R3-7-19* Requirement R3-3-10 is implemented locally on the device following 2.6.3 of [RCC.07] and POLLING PERIOD set to 0 as per A.1.10 of [RCC.07] or following 2.6.2.1 of [RCC.07] for inconclusive results.
- R3-7-20* Requirements R3-3-11 and R3-3-12 shall be implemented locally on the device.
- R3-7-21* To support requirement R3-4-1 and when enabled according to US3-5 and US3-6 and the associated technical realisation, a client shall include following tag in each SIP OPTIONS request that it sends in addition to the applicable tags as defined in section 2.6.1.1.2 of [RCC.07]:  
`+g.3gpp.iari-ref="urn%3Aurn-7%3A3gpp-application.ims.iari.rcs.lastseenactive"`  
When this tag was received in the SIP OPTIONS request and when enabled according to US3-5 and US3-6 and the associated technical realisation, the terminating client shall include following tag in the SIP OPTIONS response:  
`+g.3gpp.iari-ref="urn%3Aurn-7%3A3gpp-application.ims.iari.rcs.lastseenactive.<nn>"`, where <nn> is replaced with the time in minutes since the last activity of the user on that client according to requirement R3-4-2.
- R3-7-22* The maximum value included shall be 43200 (i.e. 30 days) which shall be used even if the last activity was older than that.
- R3-7-23* In multi-device situations, the received response to a capability request may include multiple lastseenactive tags. In this case, the client shall ignore all but the one with the smallest value for <nn>.
- R3-7-24* Requirement R3-4-2 shall be implemented locally on the device.
- R3-7-25* Requirements R3-4-3, R3-4-4, R3-4-5 and their sub requirements shall be implemented locally on the device with the information being displayed being based on the activity information received in the response to the capability exchange.

- R3-7-26** For the requirements under R3-4-6, The different status that shall be present are:
- Updating: When the client has sent a SIP OPTIONS request and no response was received yet
  - Last active at <time and date>: When a valid response with the 'lastseenactive' tag included was received and the value for <nn> was smaller than 43200. The information shall be presented as described in R3-4-5.
  - Active now: When the value of the response received is 0.
  - Ready to chat: When a valid response that does not include the 'lastseenactive' tag or a response including the 'lastseenactive' tag with the value for <nn> being 43200 or greater is received and the response indicates that the user is online (i.e. not including the automata tag).
  - SMS: When the contact is a known RCS user and an inconclusive response or a response indicating that the user is offline (i.e. including the automata tag) is received.
  - SMS only: when the Contact is marked as a non RCS user and no new capability exchange is being done.
- R3-7-27** Requirement R3-5-1 shall be implemented locally on the device as part of the Rich Communications settings.
- R3-7-28** For requirement R3-5-2, as mentioned in R3-7-21, a client where the feature is disabled shall not include the additional tags described in R3-7-21 in the SIP OPTIONS request and response.
- R3-7-29** For R3-6-1 a new joyn parameter shall be included in the RCS Configuration:

Configuration parameter	Description	RCS usage
LAST SEEN ACTIVE	This parameter defines whether the last seen active feature is enabled by the Operator. It can have following values: 0, default value: The additional tags defined in R3-7-21 are not included in the SIP OPTIONS requests and responses and the setting to enable/disable the feature is not shown to the user. 1: if enabled by the user according to US3-5 and the associated technical requirements, the additional tag defined in R3-7-21 is included in the SIP OPTIONS request as well as in the SIP OPTIONS response provided that it was included in the request.	Optional parameter

**Table 3: Last Seen Active parameter**

- R3-7-30** The parameter defined in R3-7-28 is provided as part of a joyn extension tree to the capability discovery management object defined in section A.2.8 of [RCC.07] with the tree and the parameter being formally defined as follows:



**Figure 4: joyn Capability Extension MO sub tree**

Where <x> is the Ext node of the CapDiscovery MO subtree defined in section a.2.8 of [RCC.07].

The associated HTTP configuration XML structure is presented in the table below:

```

<characteristic type="CAPDISCOVERY">
  <parm name="pollingPeriod" value="X"/>
  <parm name="pollingRate" value="X"/>
  <parm name="pollingRatePeriod" value="X"/>
  <parm name="capInfoExpiry" value="X"/>
  <parm name="nonRCScapInfoExpiry" value="X"/>
  <parm name="defaultDisc" value="X"/>
  <parm name="capDiscCommonStack" value="X"/>
  <characteristic type="CapDiscoveryWhitelist">
    <characteristic type="CapDiscoveryAllowedPrefixes">
      <parm name="Prefix1" value="X"/>
      <parm name="Prefix2" value="X"/>
      <parm name="Prefix3" value="X"/>
      ...
    </characteristic>
  </characteristic>
  <characteristic type="Ext"/>
    <characteristic type="joyn">
      <parm name="lastSeenActive" value="X"/>
      <characteristic type="Ext"/>
    </characteristic>
  </characteristic>
</characteristic>
    
```

**Table 4: Capability sub tree associated HTTP configuration XML structure including joyn Capability Discovery extension**

Node: <x>/joyn

Under this interior node Common Core related parameters are placed being used to control the UX of the client.

Status	Occurrence	Format	Min. Access Types
Required	One	node	Get

**Table 5: joyn Capability Discovery MO sub tree addition node**

- Values: N/A
- Type property of the node is: urn:gsma:mo:rsc-icapdis:5.2:Ext:joyn:Crane
- Associated HTTP XML characteristic type: "joyn"

Node: <x>/joyn/lastSeenActive

Leaf node that describes whether the last seen active feature described in US3-4 and US3-5 is enabled.

If not instantiated, the feature shall be disabled.

Status	Occurrence	Format	Min. Access Types
Required	ZeroOrOne	Bool	Get, Replace

**Table 6: joyn Capability Discovery MO sub tree addition parameters (lastSeenActive)**

- Values:
  - 0, default value: The additional tags defined in R3-7-21 are not included in the SIP OPTIONS requests and responses and the setting to enable/disable the feature is not shown to the user.
  - 1: if enabled by the user according to US3-5 and the associated technical requirements, the additional tag defined in R3-7-21 is included in the SIP OPTIONS request as well as in the SIP OPTIONS response provided that it was included in the request.
- Post-reconfiguration actions: As the client remains unregistered during configuration, there are no additional actions apart from de-registering using the old configuration and registering back using the new parameter.
- Associated HTTP XML characteristic type: "lastSeenActive".

Node: /<x>/Ext

An extension node for Service Provider specific parameters. Clients that are not aware of any extensions in this subtree (e.g. because they are not Service Provider specific) should not instantiate this tree.

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	Node	Get

**Table 7: joyn Capability Discovery MO sub tree addition Service Provider Extension Node**

- Values: N/A
- Type property of the node is: urn:gsma:mo:rcs-icapdis:5.2:Ext:joyn:Crane:Ext
- Post-reconfiguration actions: The client should be reset and should perform the complete first-time registration procedure following a reconfiguration (e.g. OMA-DM/HTTP).
- Associated HTTP XML characteristic type: "Ext".

### 3.3.2 Backward Compatibility

The only feature potentially affecting backwards compatibility is the Last Seen Active functionality introduced through US3-4 to US3-6.

### 3.3.2.1 joyn Crane Client to joyn Blackbird Network

When connecting to a joyn Blackbird network the joyn Crane Client will not receive the LAST SEEN ACTIVE configuration parameter defined in R3-7-29. As a consequence of its default handling the feature will be disabled.

### 3.3.2.2 Joyn Blackbird Client on a joyn Crane network

When a joyn Blackbird client connects to a joyn Crane network, it will indicate that it supports joyn Blackbird and should therefore receive a joyn Blackbird compatible configuration document. If the network provides a joyn Crane document, the joyn Blackbird client is expected to ignore the configuration parameter defined in R3-7-29.

### 3.3.2.3 joyn Crane Client to joyn Blackbird client

A joyn Crane client where the feature is enabled will include the feature tag defined in R3-7-21 in the SIP OPTIONS requests sent towards a joyn Blackbird client. The joyn Blackbird client will ignore these additional capabilities and not include the feature tag defined R3-7-21 in into its SIP OPTIONS response, leading to the joyn Crane client indicating the last activity state as Ready to Chat as defined in R3-7-28.

**NOTE:** If the user receiving the capability query has joyn Crane clients on which the feature enabled and joyn Blackbird clients, the information shown to their contacts will be based only on the activity of the joyn Crane clients. Therefore it is not recommended to enable the feature for users in such a multi-device environment.

A joyn Blackbird client will not include the feature tag defined in 0 in its SIP OPTIONS requests. As a consequence, a joyn Blackbird client will not include the feature tag in the responses that it sends on requests from a joyn Blackbird client.

**NOTE:** Interaction of a joyn Crane client where the feature is disabled with a joyn Crane client where the feature is enabled will follow this same pattern.

### 3.3.2.4 joyn Crane network to joyn Blackbird Network

According to [PRD-IR.90] the feature tags defined in R3-7-21 should be filtered out at the NNI. Even when this is not the case their inclusion will cause no issues as described in section 3.3.2.3 of this document.

## 3.3.3 Configuration Parameters

For joyn Crane networks the following Capability Discovery configuration parameter values apply.

Configuration Parameter	Crane Value
POLLING PERIOD	Service Provider Configurable
POLLING RATE	Service Provider Configurable
POLLING RATE PERIOD	Service Provider Configurable
CAPABILITY INFO EXPIRY	Service Provider Configurable
CAPABILITY DISCOVERY MECHANISM	Fixed Value: 0 (SIP OPTIONS) SIP OPTIONS shall be used for capability discovery

CAPABILITY DISCOVERY VIA COMMON STACK	Not applicable
CAPABILITY DISCOVERY ALLOWED PREFIXES	Service Provider Configurable
RCS CAPABILITY INFO EXPIRY	Service Provider Configurable
NON RCS CAPABILITY INFO EXPIRY	Service Provider Configurable

**Table 8: Capability Discovery configuration parameter values**

## 4 Operator Messaging

### 4.1 Description

Operator Messaging integrates various Messaging Services (SMS, MMS, 1-to-1 Chat, Group Chat, File Transfer, Geolocation Push, and Audio Messaging) to one single conversational view for the end consumer. This chapter is structured into two main parts: the representation of Operator Messaging on the device, and the client logic that proposes / decides the Messaging Service, based on availability of services and bearers on both sides of the conversation to convey the message or file. The proposed Messaging Service can be overridden at any time by the end consumer.

A device can be configured with one of the following options to determine the client logic used to propose the appropriate Messaging service at any given time:

EITHER

- Offline experience for messaging (IM\_CAP\_ALWAYS\_ON=0),OR
- Online experience for messaging (IM\_CAP\_ALWAYS\_ON=1),

AND

- Offline experience for sending files (FT\_HTTP\_CAP\_ALWAYS\_ON=0), OR
- Online experience for sending files (FT\_HTTP\_CAP\_ALWAYS\_ON=1),

OR

- Capability Agnostic experience for messaging and sending files.

During the Device Provisioning Process, the Operator sets parameters to configure the service in the way they want to offer the service.

Major changes of the Crane PDD compared to the Blackbird PDD are:

- Update of client logic for preferred Messaging Service.
- Inclusion of data flows summarising preferred Messaging Service selection logic.
- Inclusion of UI requirements and screen examples for Delivery Timeout behaviour.
- Inclusion of Capability Agnostic Messaging as an additional experience of Integrated Messaging

### 4.2 User Stories and Feature Requirements

**US4-1 As a user, I want to see all messages and files exchanged with a contact in a single threaded view.  
 As a user, I want a single environment for creating and viewing my**

**messages, covering a multitude of different services. By having this convenience, I don't have to change apps to carry out similar messaging tasks.**

*R4-1-1* In Operator Messaging, the user shall see any Messages and File Transfer events exchanged with a single contact grouped into one Conversation thread.

*R4-1-2* All Messages and File Transfer events shall appear in order of the time that they have been sent and received on the device. Details for message order are defined in '1-to-1 Chat', page 76 and 'File Transfer incl. Geolocation Push', page 99.

*R4-1-3* The Operator Messaging application shall combine the composing of RCS Messaging and File Transfer with xMS messaging.

*R4-1-4* Operator Messaging shall have no impact on the RCS Group Chat experience of the user.

NOTE: RCS Group Chat is the only Operator service today that delivers a full group chat experience, hence, there is no integration necessary).

*R4-1-5* All messaging entry points on a device shall ensure access to full the Operator Messaging experience.

NOTE: For native implementations.

**US4-2 As a user, I want full visibility about the Messaging Service that is used for sending a message or a file.**

*R4-2-1* Before sending a message, the sending button shall use appropriate means to indicate whether a message or file will be sent using xMS or RCS Chat / File Transfer.

*R4-2-2* The user shall be able to change the preferred messaging service on a, per message / file basis and on a general basis.

*R4-2-3* The user shall have full visibility of the service that is used during and after the creation of a new message / file transfer.

**US4-3 As a user, I want to know the status of any messages or files I have sent**

*R4-3-1* States for sent RCS messages and files as described in '1-to-1 Chat', page 76, 'Group Chat', page 85, and 'File Transfer incl. Geolocation Push', page 99, shall be supported in Operator Messaging.

*R4-3-2* For legacy xMS messages sent from a device, Delivery Notifications may be supported upon user choice or network default configuration.

*R4-3-3* For legacy xMS messages sent from a device, Display Notifications will not be available.

*R4-3-4* For legacy xMS messages sent from a device, the message status "pending" shall be provided (e.g. for messages queuing on the device).

*R4-3-5* For legacy xMS messages sent from a device, the status "Message failed" shall be supported in case the message could not be sent. (Re-sending the message may be triggered manually by the user).

*R4-3-6* Aggregation of Display notifications may be done: if it was confirmed the last message has been displayed, then all previously confirmed 'delivered' messages and files can be assumed displayed as well and the status may be aggregated in the last known 'displayed' status notification.

*R4-3-7* The 'failed' status notification shall never be aggregated but presented separately to the user.

**US4-4 As a user, I want to ensure that my messages are received in a user-friendly way.**

*R4-4-1* The A-Party Operator shall be able to request to revoke a message that has been sent to the B-Party (e.g. but not limited to, the case that a Delivery notification has not been received and the Operator intends to try a second delivery using a different Messaging Service).

NOTE: The Operator of the B-Party may not be able to revoke a message.

*R4-4-2* The A-Party Operator shall ensure that duplication of messages within the Operator Messaging application is avoided within their network control.

**US4-5 As a user, I want to ensure that my messages reach their destination as reliably and quickly as possible.**

*R4-5-1* To avoid a cluttered experience between Operator Messaging users and non-Integrated / non-Seamless Messaging RCS users, the user equipment shall be aware of the Integrated / Seamless Messaging capability of any of the RCS enabled contacts in order to adjust behaviour accordingly.

*R4-5-1-1* For devices configured with the Capability Agnostic Messaging experience only, obtaining the capability of RCS contacts is not necessary and therefore capability information shall not be requested.

*R4-5-2* The Operator shall ensure all messages and related messaging services originating from a device shall be conveyed in a manner that will ensure the quickest delivery to the recipient.

NOTE: This may involve the network conveying the message or file on a different Messaging Service or File Transfer service.

*R4-5-3* Store and Forward shall be available and provided by every RCS service provider to host messages and file transfer requests for its RCS users on the terminating leg when these users are offline.

*R4-5-4* For xMS messages sent from the device, Store and Forward function shall be available and provided by the Operator network.

NOTE: Details outside of this RCS specification.

*R4-5-5* For MMS files sent from the device, the user shall not be given the option of selecting files that are not compatible with the MMS technology.

*R4-5-6* For files sent from the device using MMS, the restrictions of the MMS service on file type and size will apply.

*R4-5-7* For MMS files sent from the device, the user shall be notified of file format changes based on the MMS service parameters.

*R4-5-8* For 1-to-1 Chat messages, the full RCS chat experience applies, e.g. but not limited to, emoticons and Emoji (guaranteed correct display), and Delivery and Display Notifications shall be available).

NOTE: Details of "the full RCS chat experience" are described in 1-to-1 Chat, page 76.

*R4-5-9* SMS messages shall support emoticons according to the RCS standard.

NOTE: It is an accepted compromise that some emoticons may not be correctly converted to graphics by legacy receiving devices.



*R4-5-10* SMS messages shall support Emoji according to the RCS standard, if UNICODE messaging encoding is available (either via automatic or manual selection). Whenever UNICODE encoding is not available, it shall not be possible to send Emoji.

NOTE: It is an accepted compromise that some Emoji may not be correctly converted to graphics by legacy receiving devices.

**US4-6 As an Operator, I want to make sure that any application taking on default management of xMS messaging on a device of an RCS-enabled user shall also display and take on management of RCS messages and ensure that the Operator promise of Operator Messaging is guaranteed.**

*R4-6-1* Any application allowed to manage (read, write, view) xMS on a device shall also be allowed to manage (read, write, view) RCS chat messages. Any application allowed to manage (read, write, view) RCS chat on a device shall also be allowed to manage (read, write, view) xMS messages.

*R4-6-2* Any application selected by the user as the default messaging application shall manage xMS and RCS messages (incl. File Transfer) as defined by the Operator Messaging rules detailed in this PDD.

*R4-6-3* Notifications for new incoming (RCS or xMS) messages shall be handled according to the specifications in 1-to-1 Chat, page 76, Group Chat, page 85, and 'File Transfer incl. Geolocation Push', page 99, and shall not be replicated across multiple apps on a device.

NOTE: This shall be to avoid a situation where a 'read' message is still seen as 'unread' in another application.

*R4-6-4* Notifications for new incoming (RCS or xMS) messages in case the user has multiple RCS devices shall be handled in line with the requirements of 'Backup & Restore', page 119.

NOTE: This shall be to avoid a situation where a 'read' message is still seen as 'unread' from another device when connected.

*R4-6-5* Any application managing xMS and RCS chat messages on a device shall follow the rules prescribed in this Operator Messaging section.

*R4-6-6* The Operator Messaging conversations shall be visible from the native messaging icon and/or the icon of the application which has taken on message management.

*R4-6-7* The Operator Messaging application must conform to the Messaging Service requirements when sending xMS messages from the device.

**US4-7 As a user, I want to use the various Operator Messaging services independently of the bearer that is available.**

*R4-7-1* SMS (delivery and reception) shall be available whenever connected to cellular coverage or EPC integrated Wi-Fi.

*R4-7-2* MMS (delivery and reception) shall be available whenever connected to cellular data, cellular (but no cellular data) plus Wi-Fi and EPC integrated Wi-Fi.

*R4-7-3* RCS services (delivery and reception) shall be available whenever connected to cellular data, Wi-Fi or EPC integrated Wi-Fi (this requirement shall be valid for users who are already provisioned).

## **4.2.1 Operator customisation for representation of Operator Messaging on the device.**

### **4.2.1.1 “Integrated Messaging” User Stories / Requirements**

**US4-8** As a user, I want a service logic to propose the Messaging Service to be used.

**US4-9** As a user, I want to be able to override the proposed Messaging Service during the message composing and file selection processes.

**US4-10** As a user, I always want to know what type of message I am sending, before submitting it and I want this information to be clearly represented on my screen.

**US4-11** As a user, I always want to know the type of message or file I have sent, and I want this information to be clearly represented on my screen.

*R4-11-1* When opening the conversation or entering the message composer on the device, the client logic shall propose the Messaging Service (either xMS based or RCS based) to be used for that message.

*R4-11-2* The device UI shall indicate to the user before a message / file is sent what the currently selected Messaging or File Transfer Service is.

*R4-11-3* The user shall have, the opportunity to change the Messaging or File Transfer Service override the proposed setting.

NOTE: This shall be a “one click experience” on UI level.

*R4-11-4* The user should have, at any time during the Message Composing or File Selection process, the opportunity to change the Messaging or File Transfer Service and override the proposed setting.

NOTE: This shall be a “one click experience” on UI level.

*R4-11-5* A warning may be shown to the user when the composer changes the sending Messaging Service whilst the user is typing a message, informing them that xMS or chat services are charged as per their tariff. If the warning is shown, the user shall have the possibility to dismiss such a notice permanently.

*R4-11-6* A manual user selection of a Messaging or File Transfer Service during an active conversation shall be persistent until either manually changed again by the user or until the user navigates out of the conversation thread.

*R4-11-7* The creation of a new conversation shall trigger the automatic selection of the proposed Messaging Service.

*R4-11-8* Any time during the process of selecting and sending a message or a file, the client logic shall propose a Messaging or File Transfer Service (either xMS based or RCS based) to be used for that message.

*R4-11-9* If the available technology changes while the user is in the process of composing a message or selecting a file, any impact of the technology change on the available message content must be made clear to the user, and they shall be able to reject or delay the automatic technology change if required.

*R4-11-10* After sending a message or file, the device UI shall differentiate the Messaging or File Transfer Service that was used.

**NOTE:** Differentiation shall allow the user to know which Messaging (i.e. chat / SMS) or File Transfer (i.e. File Transfer, MMS) Service was used to convey the message. Further detail on this requirement is provided in the joyn branding guidelines.

*R4-11-11* The RCS File Transfer service shall be clearly differentiated from MMS.

*R4-11-11-1* All RCS terminology and visual indicators should be used consistently across all RCS messaging clients and interfaces.

*R4-11-11-2* Where appropriate, text labels should be displayed to identify the different message statuses. Visual indicators may also be employed to identify the different message statuses.

*R4-11-11-3* The RCS File Transfer service should be clearly differentiated from MMS, for example through the use of appropriate text labels and visual indicators.

*R4-11-12* Where appropriate, the user should be made aware of any additional or enhanced File Transfer functionality available via RCS (vs. MMS), for example - but not limited to - the transfer of HD video.

*R4-11-13* When receiving a message or file, the device UI shall differentiate the Messaging or File Transfer Service that was used.

**NOTE:** Differentiation shall allow the user to know which Messaging (i.e. chat / SMS) or File Transfer (i.e. RCS File Transfer/ MMS) Service was used to convey the message.

*R4-11-13-1* The text labels 'Chat', 'SMS' and 'MMS' should be used where appropriate to identify the different Messaging Services for both sent and received messages.

*R4-11-13-2* Colour coding may also be used to differentiate message types, but should not be the only type of differentiation used.

*R4-11-14* If the Operator has changed the Messaging or File Transfer Service on the terminating leg to ensure delivery, the A-Party UI shall not change the Messaging or File Transfer Service indication (e.g. A-Party creates an RCS Chat Message, the Operator terminates this message as xMS if the B-Party has cellular connectivity but is not registered to RCS).

**NOTE:** In this case, a message is indicated as RCS Chat on the sending device and may be shown as SMS on the receiving device.

*R4-11-15* The device shall provide the user with an option to resend pending or failed RCS messages or files by another Messaging or File Transfer Service, e.g., but not limited to, cases where the A-Party loses connectivity due to changing radio conditions. If, in this case, the initial message was pending and has not yet been sent, the device shall not make further attempts to send the message using the attempted Messaging Service but shall propose the alternative Messaging Service to be used instead. If there are also further, more recent, undelivered RCS messages sent by the A-Party in that active conversation then the user is asked whether they would like to resend just the single message (for which the timer has expired) or all of the undelivered messages.

**US4-12 As a user, I want to be in control of the default messaging service in Operator Messaging.**

*R4-12-1* A setting shall allow the user to select the default sending method to be used:

- 'Proposed Messaging Service' (follow Integrated Messaging behaviour as defined in Integrated Messaging requirements), or
- 'Always RCS chat for RCS enabled contacts and SMS for non-RCS enabled contacts or
- 'Always SMS' (for RCS enabled contacts and non-RCS enabled contacts).

*R4-12-2* The default setting shall be "Proposed Messaging Service".

*R4-12-3* It shall always be visible to the user which Messaging Service is used, and the user shall have the option to change the chosen Messaging Service irrespectively of the setting in R4-12-1 upon user interaction (as a case by case decision taken in the messaging composer).

#### **4.2.2 Client Logic to propose the desired Messaging and File Transfer Service Capability Agnostic Messaging experience (send RCS to all contacts)**

**US4-13 As a user, I want to fully rely on my Operator to convey the Messaging Service to ensure quickest and most reliable message delivery.**

*R4-13-1* The Integrated Messaging composer shall select RCS as the Messaging and File Transfer Service when no network connection is available. These messages shall be queued for delivery when the device is reconnected. The user shall be notified that these messages are queued for delivery.

*R4-13-2* When the device is connected to cellular coverage without data coverage (not registered to the RCS platform), the default delivery mechanism for messaging and File Transfer proposed from the Integrated Messaging Application shall be xMS (functional restrictions for MMS apply).

NOTE: In case cellular is available but no data connection, all other RCS services (except Chat) will not be available.

*R4-13-2-1* If the user selects other RCS services (non text messaging) when in this mode these messages will be queued for delivery when the device is reconnected. The user shall be notified that these messages are queued for delivery.

*R4-13-3* When the device is connected to cellular coverage with data but not registered to the RCS platform, the default service from the Integrated Messaging Application shall be xMS.

NOTE: Restrictions in file size and -type for MMS apply.

*R4-13-4* When the device is registered to the RCS service, the default messaging service proposed by the Integrated Messaging Application shall be RCS.

NOTE: This shall also be valid for RCS messages/service to non-RCS enabled contacts.

*R4-13-5* When the device is registered to the RCS service and the sent RCS message times out due to a loss of IP connectivity, the RCS client/application may attempt to resend the RCS message in SMS mode without notifying the user or the RCS client/application may visually display a message sent error to the user.

**R4-13-6** When the device is registered for RCS service and the DELIVERY TIMEOUT parameter is enabled, the RCS client/application may attempt to resend a RCS message in xMS mode when the DELIVERY TIMEOUT timer expires before receiving a confirmation of a message delivered state.

**R4-13-7** At any time before or during message composing, the user shall be able to override the default messaging service proposed by the Integrated Messaging client to convey the message. If a messaging service type is selected by the user but cannot be used at the moment of sending, the message shall be cached on the device and sent as soon as the necessary connection is available.

**R4-13-8** The A-Party network is responsible for ensuring that the messages sent from the A-Party's device are delivered to the B-Party's network in the most appropriate and timely way.

**R4-13-8-1** The A-Party's network must ensure that the message service type of any message sent to the B-Party will be able to be handled by and delivered correctly to the recipient.

Capability Agnostic Messaging experience					
User A (Sender)	Connected to Cellular network	Yes	Yes	No	No
	Connected to RCS	Yes	No	Yes	No
User B (Receiver)	Connected to Cellular network	N/A			
	Connected to RCS				
Selected Service		RCS	xMS*	RCS	RCS*
*on-device caching of unsent messages is required and user shall be informed					

**Table 9: Table to explain and summarise static conditions for Capability Agnostic Messaging**

**4.2.3 Client Logic to propose the desired Messaging Service – Integrated Messaging ‘Online experience) (IM\_CAP\_ALWAYS\_ON = 0 / SMS as default)**

**US4-14 As a user, I want the best Messaging Service to be proposed to me to convey my messages.**

**R4-14-1** The preferred messaging service for composing and sending messages shall be determined by a number of factors, including but not limited to, the RCS Online/Offline status of the sender (A-Party) and the receiver (B-Party).

**NOTE:** See requirement R3-3-6-5 for Capability Validity and checking requirements. Neither user's cellular connectivity is relevant for determining the preferred messaging service.

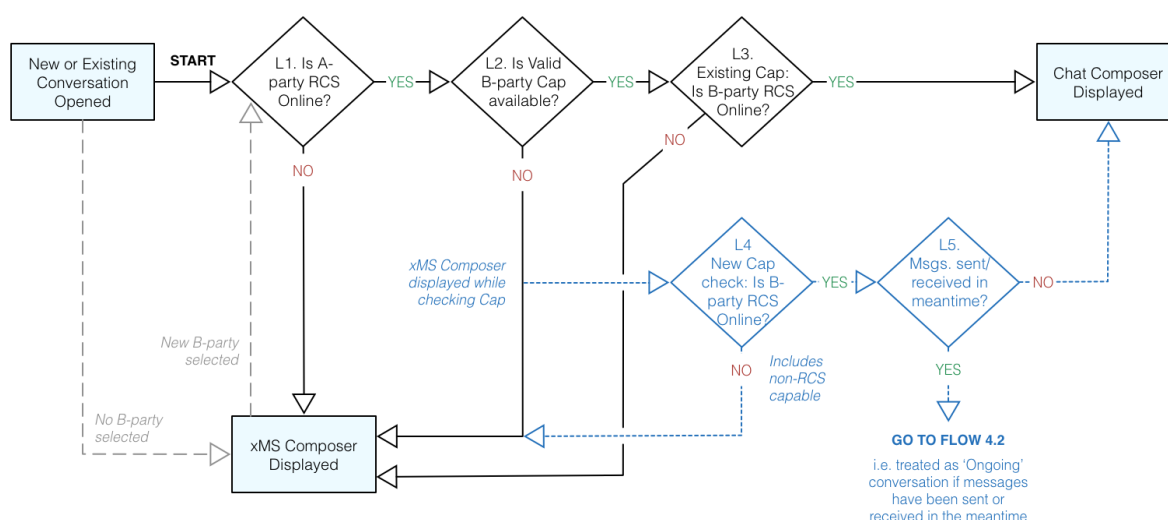
### 4.2.3.1 Entering a new or existing conversation

The preferred messaging service is automatically determined according to rules described below:

**R4-14-1-1** Preferred Messaging Service when entering a new or existing conversation (including, but not limited to, opening a conversation, returning to a conversation and unlocking the screen on an open conversation):

**R4-14-1-1-1** If a valid capability check is available when opening the conversation, then the preferred service is set accordingly.

**R4-14-1-1-2** If a new capability check is required, then xMS is the preferred service until the result of this new capability check is available. If the result of this new capability check is that the B-Party is RCS online, then the preferred service changes to Chat.



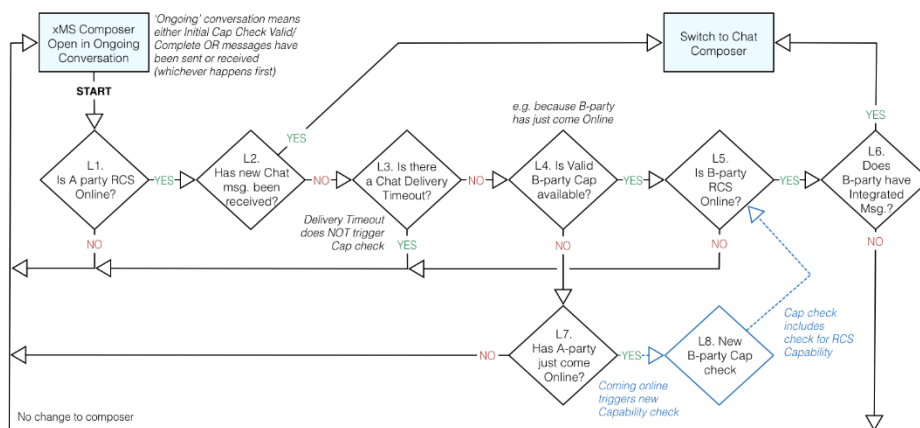
**Figure 5: Initial Technology Selection Logic When Entering a Conversation [IM\_CAP\_ALWAYS\_ON=0]**

### 4.2.3.2 During an ongoing xMS conversation

**R4-14-1-2** During an ‘on-going’ xMS conversation the proposed Messaging Service shall change according to Figure 8, including (but not limited to) the following cases:

**R4-14-1-3** When a chat message or RCS File is received from the B-Party.

**R4-14-1-4** When the B-Party, with Integrated (or Seamless) messaging, is discovered as RCS online.



**Figure 6: Technology Selection Logic During an ongoing Conversation (when current composer is xMS) [IM\_CAP\_ALWAYS\_ON=0]**

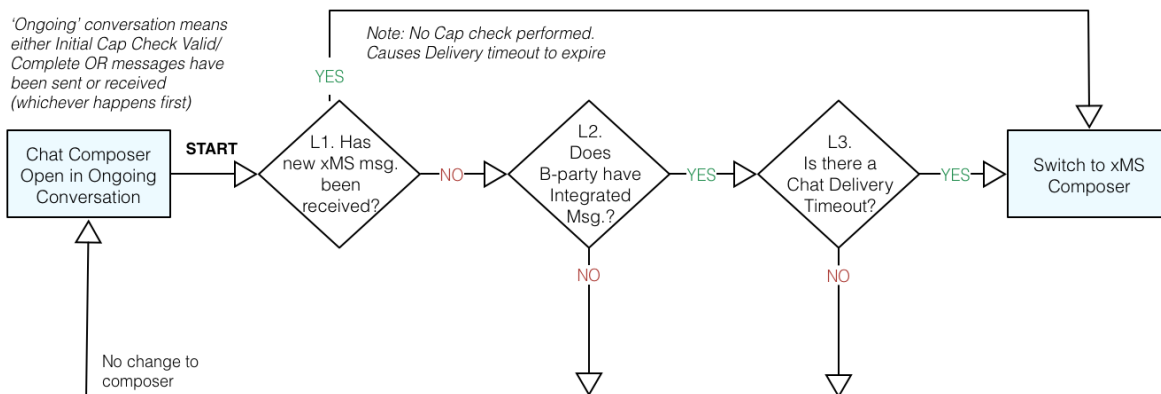
**4.2.3.3 During an on-going RCS conversation:**

*R4-14-1-5* During an ‘on-going’ RCS conversation the proposed Messaging Service shall change according to Figure 6, including, but not limited to, the following cases:

*R4-14-1-6* When an xMS message is received from the B-Party. This will cause the DELIVERY TIMEOUT timer to expire.

*R4-14-1-7* When the B-Party is an Integrated (or Seamless) Messaging user and expiry of the Delivery Timeout timer occurs.

**NOTE:** There is no immediate change to the Messaging Service if the A-Party loses data connectivity. The device waits for the expiry of Delivery Timeout before changing to xMS.



**Figure 7: Technology Selection Logic During an Ongoing Conversation (when current composer is Chat) [IM\_CAP\_ALWAYS\_ON=0]**

For details of the technology selection logic if the end user manually changes the flow Manual service change:

#### 4.2.3.4 “DELIVERY TIMEOUT”:

The DELIVERY TIMEOUT timer defines the timeout for reception of delivery reports for RCS messages and files sent to the B-Party. There is one DELIVERY TIMEOUT timer used per conversation.

*R4-14-1-8* This timer is armed/started during an RCS conversation, in any of the following situations:

- When sending an RCS chat message or file while there is no other message or file undelivered or unsent.
- When the A-Party loses IP connectivity, and there are undelivered or pending chat messages or files.

*R4-14-1-9* The DELIVERY TIMEOUT will be stopped when receiving a message or file delivery notification, but immediately restarted (“rearmed”) if there are still undelivered or pending RCS message(s).

*R4-14-1-10* When the DELIVERY TIMEOUT expires any undelivered messages shall have their status changed to “undelivered” and any pending messages shall have their status changed to “failed”.

*R4-14-1-11* DELIVERY TIMEOUT is only calculated for the first undelivered chat message or file transfer after a delivered one. Example:

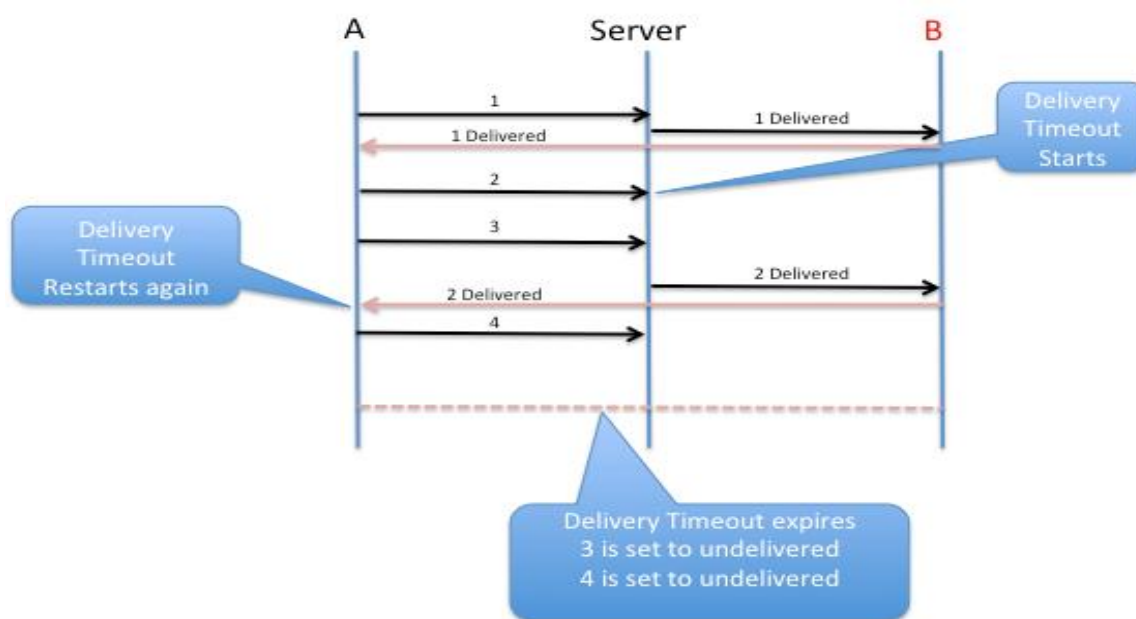


Figure 8: “DELIVERY TIMEOUT” flow diagram



Integrated Messaging 'Online experience' (IM_CAP_ALWAYS_ON=0) Selected Messaging Service								
User A (Sender)	Connected to cellular network	Yes	Yes	Yes	Yes	Yes	No	No
	Connected to RCS	Yes	Yes	Yes	Yes	No	Yes	No
User B (Receiver)	Connected to cellular network	Yes	Yes	No	No	N/A	Yes	N/A
	Connected to RCS	Yes	No	Yes	No		Yes	
Selected Service	Default	SMS	SMS	SMS	SMS	SMS	SMS*	SMS*
	Change after capability confirmation	RCS	SMS	RCS	SMS	SMS	RCS	SMS*
	Possible User Choice	SMS	RCS	SMS	RCS	RCS*	SMS*	RCS*
*on device caching of unsent messages is required and user shall be informed								

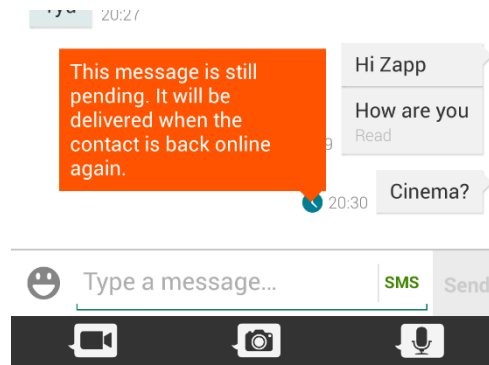
**Table 10: Table to explain and summarise static conditions and proposed Messaging Service by the device logic**

**R4-14-2 Undelivered chat messages (sent but not delivered)**

**R4-14-2-1** When A-Party is RCS online and a DELIVERY TIMEOUT expires, sent but not yet delivered chat messages shall be considered as “undelivered”. The user shall be able to send manually by SMS any “undelivered” chat messages by xMS.

**R4-14-2-2** The user shall be notified about undelivered chat messages:

- Inside the message thread: through an indication in the thread (message status indication). The first time this indication is shown, a contextual indication (e.g. tool tip) shall explain to the user what it means and what options the user has (e.g. resending via SMS).



**Figure 9: Example of a tool tip indication to notify the user of undelivered chat messages**

*R4-14-3* In the messaging inbox:

*R4-14-3-1* The user shall be informed through a system notification that:

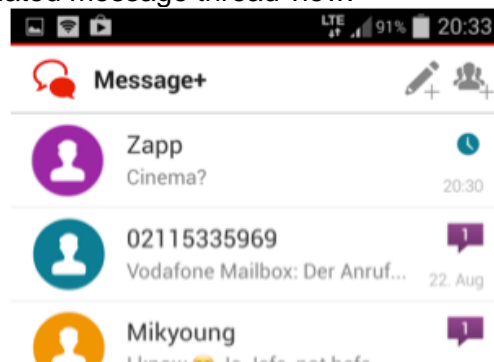
*R4-14-3-1-1* Some messages have not yet been delivered.

*R4-14-3-1-2* Those messages will be delivered when the receiver is back online.

*R4-14-3-1-3* The user shall be able to resend one or all of the undelivered messages by SMS.

*R4-14-3-2* Opening the notification shall forward the user to the associated message thread.

*R4-14-3-3* The same indication should be displayed in both the inbox view and the associated message thread view.



**Figure 10: Example of indication in Inbox of a thread containing undelivered messages**

*R4-14-4* When outside the message thread or inbox the user shall be informed through a system notification that:

*R4-14-4-1* Some messages have not yet been delivered:

*R4-14-4-1-1* These messages will be delivered when the receiver is back online again.

*R4-14-4-1-2* The user is able to resend these messages by xMS.

*R4-14-4-2* Opening the notification shall forward the user to the associated message thread.

#### 4.2.3.5 Unsent Chat Messages (pending)

*R4-14-4-3* When the A-Party goes offline during an ongoing chat conversation, pending chat messages (i.e. those the user has attempted to send but have not yet become “sent”) shall be queued and marked as “pending”. The user shall be able to retry manually the sending of one or all of these messages by xMS.

*R4-14-4-4* When a DELIVERY TIMEOUT expires for these pending chat messages, they shall be considered as “failed”. The user shall be able to retry manually the sending of one or all of these messages by xMS, or via chat if it becomes available again.

*R4-14-4-5* The user shall be notified about “pending” chat messages:

- Inside the message thread: through an indication in the thread (message status indication).
- In the messaging inbox: the visual indication should be used in both the message inbox view and the message thread view.
- Outside the message thread or inbox: notification shall not be displayed to the user.

*R4-14-4-6* The user shall be notified about “failed” chat messages:

- Inside the message thread: through indication in the thread (message status indication).
- In the messaging inbox: the same visual indication should be used in both the message inbox view and the message thread view.
- Outside the message thread or inbox: through a system notification. The notification shall inform the user that some messages are filed and will not be sent.
- Opening the notification shall forward the user to the associated message thread.

#### 4.2.4 Integrated Messaging ‘Offline experience’– (IM\_CAP\_ALWAYS\_ON = 1 / RCS Chat as default between RCS users)

**US4-15** As a user, I want the best Messaging Service to be proposed to me to convey my messages.

*R4-15-1* The messaging service to be proposed for sending messages to RCS capable users *shall* be determined by the connectivity status to the RCS platform of the sender (A-Party).

*R4-15-1-1* RCS Chat shall be the default Messaging Service for outbound messages proposed by the device for recipients (B-Party) being known as RCS capable contacts, irrespective of their connectivity status.

*R4-15-2* If the A-Party has lost IP connectivity to the RCS service, messages to B-Party being an RCS user shall be 1-to-1 Chat locally queued and sent once the IP connectivity is restored. In this case, the A-Party shall be informed about the loss of the connectivity status by the device appropriately.

*R4-15-2-1* If the A-Party is not registered to the RCS service (e.g. the user has chosen to switch their mobile data setting to “OFF”), the proposed Messaging Service shall be SMS.

**R4-15-3** SMS shall be the default messaging service for outbound messages proposed by the device logic for recipients (B-Party) being known or detected as not RCS capable. In case the device has no cellular connectivity, SMS messages shall be queued locally on the device and be sent once the connection to cellular is restored.

**NOTE:** In case cellular is not available, the SMS shall be locally queued on the device.

Integrated Messaging 'Offline experience' (IM CAP ALWAYS ON=1)- Selected Messaging Service					
User A (Sender)	Connected to Cellular Network	Yes	Yes	N/A	Yes
	Connected to RCS	No <sup>2</sup>	No <sup>3</sup>	Yes	Yes
User B (Receiver)	Connected to Cellular Network	N/A			
	Connected to RCS				
Selected Service	<b>Default</b>	RCS*	SMS	RCS	SMS**
	<b>User Choice</b>	SMS	RCS*	SMS***	N/A
*On-device caching of messages is required and user shall be informed ** If B-Party is known to be a non RCS user ***If cellular network connection is not available, on-device caching of messages is required and user shall be informed					

**Table 11: Table to explain and summarise static conditions and proposed Messaging Service by the device logic**

#### 4.2.5 Integrated Messaging – File Transfer 1 (FT\_HTTP\_CAP\_ALWAYS\_ON=0 / online Experience only)

**US4-16** As a user, I want the best File Transfer Service to be proposed to me to convey my files.

**R4-16-1** The File Transfer Service to be proposed for sending files shall be determined by the registration status to RCS platform of the sender (A-Party) and receiver (B-Party). When to refresh capabilities is described in section R3-3-6-5. The proposed File Transfer Service shall be adjusted according to the rules defined in R4-13-1 as the behaviour expected for File Transfer 1 is the same than the behaviour described in Integrated Messaging 1 section.

**R4-16-2** If the A-Party is not registered to RCS ('offline'), MMS shall be considered the default File Transfer Service proposed by the device logic.

**NOTE:** In this case, RCS File Transfer shall not be sent.

<sup>2</sup> Cellular data is switched on

<sup>3</sup> Cellular data is switched off

*R4-16-2-1* If MMS messages cannot be sent immediately, MMS shall be composed and queued locally on the device until data connection is restored.

*R4-16-3* If the A-Party is registered to RCS (“online”) and in cellular coverage, the current capabilities of B-Party determine the proposed messaging service. The proposed File Transfer Service shall be adjusted according to the rules defined in R4-13-1.

*R4-16-4* If A-Party is registered to RCS (“online”) but outside of cellular coverage, the current capabilities of the B-Party shall determine the proposed File Transfer Service.

*R4-16-4-1* If the B-Party is registered to RCS (“online”), then RCS File Transfer service shall be proposed.

*R4-16-4-2* If B-Party is not registered to RCS (“offline”) or if the A-Party has not yet determined B-Party’s capabilities, the proposed File Transfer Service shall be MMS and messages are queued locally on the device and delivered as soon as cellular connectivity is restored.

NOTE: This shall be the case even if B-Party is a known RCS user.

<b>File Transfer ‘Online experience’ (FT_HTTP_CAP_ALWAS_ON=0) - Selected File Transfer Service</b>				
User A	Connect to Cellular network	n/a	n/a	n/a
Sender	Connect to RCS	No	Yes	Yes
User B	Connect to Cellular network	n/a	n/a	n/a
Receiver (RCS user)	Connect to RCS	n/a	Yes	No
	<b>Default FT service</b>	<b>MMS*</b>	<b>RCS FT</b>	<b>MMS*</b>
<b>Proposed Service</b>	<b>User Choice</b>	<b>RCS FT</b>	<b>MMS</b>	<b>RCS FT</b>
*On-device caching of unsent files required and user shall be informed				

**Table 12: Table to explain and summarise static conditions and proposed Messaging Service by the device logic.**

#### 4.2.6 Integrated Messaging – File Transfer (FT\_HTTP\_CAP\_ALWAYS\_ON=1 / Offline experience)

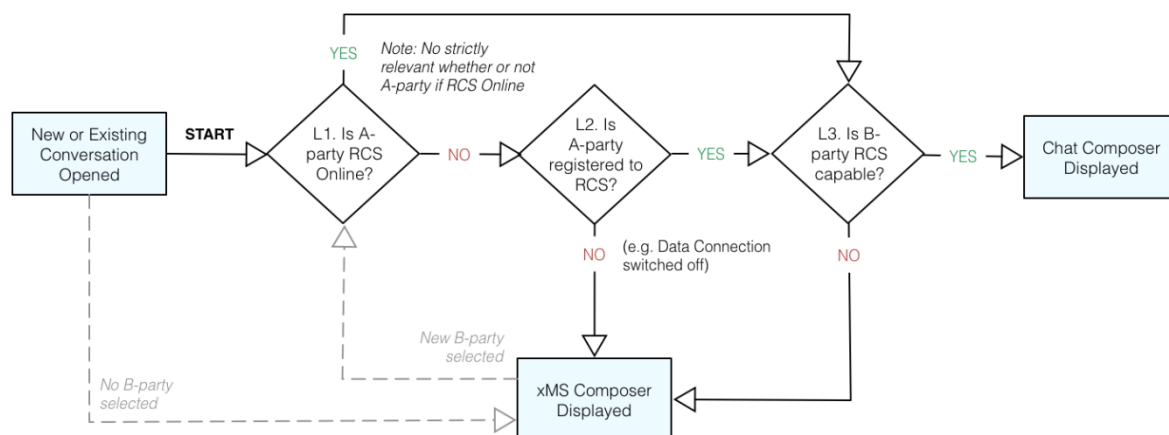


Figure 11: FT HTTP CAP ALWAYS ON=1 Flow diagram

**US4-17 As a user, I want the best File Transfer Service to be proposed to me to convey my files.**

- R4-17-1 The proposed File Transfer Service to be used for sending files shall be determined by the registration status to RCS platform of the sender (A-Party) and if the B-Party is a known RCS user .
- R4-17-2 If the A-Party is registered to RCS (“online”),
  - R4-17-2-1 RCS File Transfer shall be the default service for outbound files proposed by the device logic for recipients that are known RCS capable contacts, irrespective of their connectivity status.
  - R4-17-2-2 MMS shall be the default File Transfer Service for outbound messages proposed by the device logic for recipients that are known or detected to be not RCS capable.
  - R4-17-2-3 If an Operator has disabled the MMS service, the RCS File Transfer service shall be used to deliver files to non RCS users irrespective of the connection status of the sender.
- R4-17-3 If the A-Party is not registered to RCS (“offline”),
  - R4-17-3-1 Any files sent to a B-Party who is known as an RCS user shall be RCS File Transfer queued locally on the device and sent once the RCS connectivity is restored. In this case, the A-Party shall be informed about the “offline” status by the device appropriately.
  - R4-17-3-2 Any Files sent to a B-Party who is not known as an RCS user shall be sent as MMS. If no data connection is available, MMS shall be queued locally on the device, the A-Party shall be informed about the “offline” status by the device appropriately and the file will be sent once mobile data is available.

<b>File Transfer 'Offline experience' (FT_HTTP_CAP_ALWAS_ON=1) - Selected File Transfer Service</b>				
User A	Connect to Cellular network	n/a	n/a	n/a
Sender	Connect to RCS	Yes	No	n/a
User B	Connect to Cellular network	n/a	n/a	n/a
Receiver (RCS user)	Connect to RCS	n/a	n/a	n/a
	<b>Default FT service</b>	<b>RCS FT</b>	<b>RCS FT*</b>	<b>MMS**</b>
<b>Proposed Service</b>	<b>User Choice</b>	<b>MMS</b>	<b>MMS*</b>	n/a
*On-device caching of unsent files required and user shall be informed				
** If B-Party is known to be a non RCS user				

**Table 13: Table to explain and summarise static conditions and proposed Messaging Service by the device logic**

#### 4.2.7 Multimedia Message Service Selection

The sections above (sections 4.2.3 to 4.2.6) describe the logic for selecting the preferred messaging service for individual messages and File Transfers in a conversation. As described, the preferred messaging service is influenced by the IM\_CAP\_ALWAYS\_ON and FT\_HTTP\_CAP\_ALWAYS\_ON configuration parameters.

A client configuration where these two parameters are set to different values (e.g. where IM\_CAP is set to "0", and FT\_HTTP\_CAP is set to "1") can result in two different messaging services being selected for different messages in the same conversation. For example, SMS being selected for text messages and RCS File transfer for files. (This would be the case with a client configuration of IM\_CAP\_ALWAYS\_ON=0 and FT\_HTTP\_CAP\_ALWAYS\_ON=1, in a conversation where the A-Party is online and the B-Party is offline).

Some devices, however, allow users to enter both text and files while composing a single message.

*R4-17-4* When a single message includes both text and file components, the entire 'multimedia' message must be conveyed using the same messaging service to preserve the consistency of the message:

*R4-17-4-1* The MMS service must be used if xMS has been selected by the client logic for either the text and/or the file components of the multimedia message.

*R4-17-4-2* RCS chat and RCS File Transfer must be used only when RCS has been selected by the client logic for both the text and the file components of the multimedia message.

### 4.3 Technical Information

#### 4.3.1 Overview

Operator Messaging is a client functionality to provide the user with a common messaging service behaviour using multiple services and technologies. This section covers functional requirements for the client to select and apply the specified service behaviour for a number of messaging service. Whilst the Operator Messaging Service User Stories and Feature

Requirements deal with the co-existence of the services in the client, the technical implementation of the referred individual services shall be based on the following:

- The RCS 1-to-1 Chat service refers to the service defined in '1-to-1 Chat, page 76.
- The RCS File Transfer Service refers to the service defined in 'File Transfer incl. Geolocation Push', page 99.
- The Short Messaging Service (SMS) is provided by the client as follows:
- If the Short Messaging Service is selected by the client based on the User Stories of this section and the standalone messaging service is enabled by the service provider via the configuration parameter STANDALONE MSG AUTH as defined in sections A.1.3.3 and A.2.1 of [RCC.07] and the client is registered in IMS, then Standalone Messaging as defined in section 3.2 of [RCC.07] shall be used.
- Otherwise, the client shall use the Short Messaging Service as defined in [3GPP TS 23.040] or the Short Messaging Service over IP as defined in IR.92.
- The Multimedia Messaging Service (MMS) is provided by the client as follows:
- If the Multimedia Messaging Service is selected by the client based on the User Stories in this section and the standalone messaging service is enabled by the service provider via the configuration parameter STANDALONE MSG AUTH as defined in sections A.1.3.3 and A.2.1 of [RCC.07] and the client is registered in IMS, then Standalone Messaging as defined in section 3.2 of [RCC.07] shall be used.
- Otherwise, if enabled by the service provider via the configuration parameter MO MMS AUTH (see section 4.3.2.1.2) the client shall use the Multimedia Messaging Service as defined in 3GPP TS 22.140 and 3GPP TS 23.140.

For the application of standalone messaging in joyn Crane the following additional requirements apply:

- A client using standalone messaging as a technology to provide the SMS and MMS service as defined in this section shall not apply the capability discovery for standalone messaging as defined in section 2.6.1.1.2 of [RCC.07].
- A client shall regard a message on Ux level as a SMS or MMS according to the SMS/MMS technology selection rules regardless whether the message will be sent via CPM Pager Mode or CPM Large Message Mode. For User Stories for message transfer of SMS and MMS to multiple recipients in cases where Group Chat not applicable (e.g. US7-8) the client shall make use of the procedures for sending standalone messages to a CPM adhoc group. In accordance with section A.1.4.2 of [RCC.07] the OMA SIMPLE IM configuration parameters apply for the client.

### **4.3.2 Configuration Parameters**

The User Stories and Feature Requirements in the previous sections refer to a number of configuration parameters influencing the client behaviour for integrated and seamless messaging. Apart from the parameters defined in this section these are defined in sections A.1.3.3.3 and A.1.4 of [RCC.07].

#### **4.3.2.1 IM related Configuration Parameters**

The joyn client is configured to provide the Capability Agnostic experience as defined in section 4.2.2 by means of the following configuration parameter.



Configuration parameter	Description	Parameter usage
CAP AGNOSTIC MSG	<p>This parameter controls the Capability Agnostic messaging experience defined in section 4.2.2. The parameter can take the following values:</p> <ul style="list-style-type: none"> <li>0 the capability agnostic experience is not active for the user (default value).</li> <li>1 the capability agnostic experience is active for the user.</li> </ul> <p>If the value of the configuration parameter is set to "0" the client shall apply capability aware user experience as defined by the configuration parameters IM CAP ALWAYS ON defined in Table 77 in section A.1.4 of [RCC.07] and FT HTTP CAP ALWAYS ON defined in Table 21 of [RCC.61]</p> <p>If the value of the configuration parameter is set to "1" shall sent mobile originated messages always via the Chat or File Transfer service if it is registered for RCS. Thus the messaging capability as well as the values of IM CAP ALWAYS ON and FT HTTP CAP ALWAYS ON are not relvant for the client.</p> <p>The ability of the client to receive messages via other messaging services is not influenced by this parameter.</p>	Optional Parameter

**Table 14: joyn Chat related Configuration Parameters**

#### 4.3.2.2 MMS Control related Configurable Parameters

The service provider shall be able to control the MMS service configuration on the device. This requires the following configuration parameters.

Configuration parameter	Description	Parameter usage
MO MMS AUTH	<p>This parameter controls whether the mobile originated MMS service is enabled or disabled.</p> <p>If the parameter value is set to "0", then the mobile originated MMS service is disabled. The client shall not offer the user to send messages via MMS, i.e. the device shall never submit a message via MMS send transaction to the network, even if a MMS client configuration is available. In this case the ServiceProvider also takes control of the MMS client configuration via the Service Provider Client Configuration as defined in section 4.3.2.1.2</p> <p>If the parameter is set to "1", then the mobile originated MMS service is enabled. In this case the client shall offer the user to send messages via MMS as defined for operator messaging.. In this case the ServiceProvider also takes control of the MMS client configuration via the Service Provider Client Configuration as defined in section 4.3.2.1.2</p> <p>If the parameter is not present, then the mobile originated MMS service is enabled. In this case the client shall offer the user to send messages via MMS as defined for operator messaging, provided a MMS client configuration is available. If the parameter is not present Service Provider is not able to take control of the MMS client configuration as defined in section 4.3.2.1.2, i.e the device must retrieve the MMS configuration object by other means.</p> <p>The availability of mobile terminated MMS is not influenced by this configuration parameter.</p>	Optional Parameter

**Table 15: joyn MMS Configuration Parameters**

**4.3.2.3 Connectivity Management related Configuration Parameters**

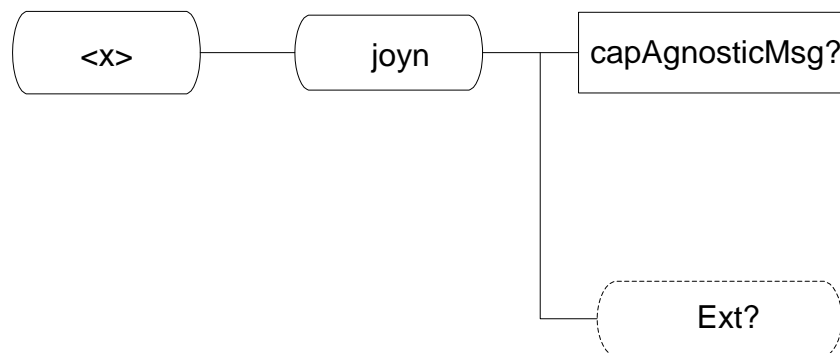
The service provider shall be able to manage the 3GPP Connectivity Management Objects on the device. This requires the following configuration parameters.

Configuration parameter	Description	Parameter usage
CONN MO CONTROL	<p>This parameter controls whether the configuration server takes control of the 3GPP Connectivity Management Objects on the device. The parameter can take the following values:</p> <ul style="list-style-type: none"> <li>0 The configuration server does not control 3GPP connectivity object on the device (default value). The configuration server shall not supply connectivity management object related data in the configuration xml.</li> <li>1 The configuration server does control the 3GPP connectivity object on the device. The configuration server will supply connectivity management object related data in the configuration xml.</li> </ul>	Optional Parameter

**Table 16: joyn Connectivity Control Configuration Parameters**

**4.3.2.4 Services sub tree extensions**

The additional chat control parameters are provided in a dedicated joyn sub tree provided as a Service Provider extension to the IM tree defined in [RCC.07] section A.2.6 (i.e. the <x> node is the Ext node of the IM tree):



**Figure 12: joyn Services sub tree**

The associated HTTP configuration XML structure and its integration into the IM MO is presented in the table below:

```

<characteristic type="IM">
  <parm name="imMsgTech" value="X"/>
  <parm name="imCapAlwaysON" value="X"/>
  <parm name="imWarnSF" value="X"/>
  <parm name="SmsFallBackAuth" value="X"/>
  <parm name="imCapNonRCS" value="X"/>
  <parm name="imWarnIW" value="X"/>
  <characteristic type="GroupChatNonRCSWhitelist" value="X"/>
    <parm name="imCapNonRCSGroupChat" value="X"/>
    <parm name="imCapNonRCSLimitGroupChat" value="X"/>
    <characteristic type="GroupChatAllowedPrefixes">
      <parm name=" Prefix1" value="X"/>
      <parm name=" Prefix2" value="X"/>
      <parm name=" Prefix3" value="X"/>
      ...
    </characteristic>
  </characteristic>
  <parm name="AutAccept" value="X"/>
  <parm name="AutAcceptGroupChat" value="X"/>
  <parm name="imSessionStart" value="X"/>
  <parm name="firstMessageInvite" value="X"/>
  <parm name="TimerIdle" value="X"/>
  <parm name="MaxConcurrentSession" value="X"/>
  <parm name="MaxSize1to1" value="X"/>
  <parm name="MaxSize1toM" value="X"/>
  <parm name="ChatRevokeTimer" value="X"/>
  <parm name="ftWarnSize" value="X"/>
  <parm name="MaxSizeFileTr" value="X"/>
  <parm name="MaxSizeFileTrIncoming" value="X"/>
  <parm name="ftThumb" value="X"/>
  <parm name="ftStAndFwEnabled" value="X"/>
  <parm name="ftCapAlwaysON" value="X"/>
  <parm name="ftAutAccept" value="X"/>
  <parm name="ftHTTPCSURI" value="X"/>
  <parm name="ftHTTPCSUser" value="X"/>
  <parm name="ftHTTPCSPwd" value="X"/>
  <parm name="ftDefaultMech" value="X"/>
  <characteristic type="Ext">
    <characteristic type="joyn">
      <parm name="capAgnosticMsg" value="X"
      <characteristic type="Ext">
    </characteristic>
  </characteristic>
  <parm name="pres-srv-cap" value="X"/>
  <parm name="deferred-msg-func-uri" value="X"/>
  <parm name="max_adhoc_group_size" value="X"/>
  <parm name="conf-fcty-uri" value="X"/>
  <parm name="exploder-uri" value="X"/>
</characteristic>

```

**Table 17: Services sub tree associated HTTP configuration XML structure**

This sub tree is formally defined as follows:

Node: <x>/joyn

The joyn specific parameters are are placed under this interior node.

Status	Occurrence	Format	Min. Access Types
Required	ZeroOrOne	Node	Get

**Table 18: joyn IM Extension MO sub tree addition node**

- Values: N/A
- Type property of the node is: urn:gsma:mo:rcc-im:5.3:Ext:joyn
- Associated HTTP XML characteristic type: "joyn"

Node: <x>/joyn/capAgnosticMsg

Controls the capability agnostic messaging behaviour of the client.

Status	Occurrence	Format	Min. Access Types
Required	ZeroOrOne	Bool	Get

**Table 19: Capability Agnostic Messaging IM MO sub tree addition parameters (capAgnosticMsg)**

- The parameter represents the configuration parameter CAP AGNOSTIC MSG defined in Table 15.
- Values:
  - 0: the capability agnostic experience is not active (default)
  - 1: the capability agnostic experience is active
- Post-reconfiguration actions:
  - If the re-configuration transits from "capability agnostic experience is not active" to "capability agnostic experience is active", then the client shall apply the capability agnostic experience
  - If the re-configuration transits from "capability agnostic experience is active" to "capability agnostic experience is not active", then the client shall apply the online or offline experience. Associated HTTP XML characteristic type: "capAgnosticMsg"

Node: <x>/joyn/Ext

An extension node for Service Provider specific parameters. Clients that are not aware of any extensions in this sub tree (e.g. because they are not Service Provider specific) *Should Not* instantiate this tree.

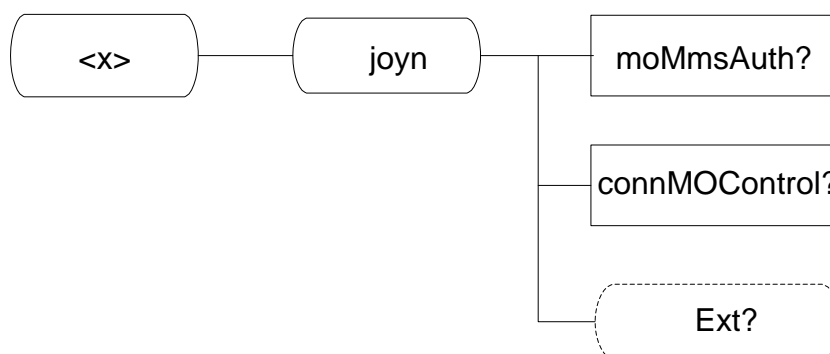
Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	Node	Get

**Table 20: joyn IM Extension MO sub tree addition Service Provider Extension Node**

- Values: N/A
- Type property of the node is: urn:gsma:mo:rcc-im:5.3:Ext:joyn:Ext
- Associated HTTP XML characteristic type: "Ext"

### 4.3.2.5 Services sub tree extensions

The MMS and connectivity management control parameters are provided in a dedicated joyn sub tree provided as a Service Provider extension to the Services tree defined in [RCC.07] section A.2.1 (i.e. the <x> node is the Ext node of the Services tree):



**Figure 13: joyn MO Services sub tree**

The associated HTTP configuration XML structure and its integration into the Services MO is presented in the table below:

```

<characteristic type="SERVICES">
  <parm name="presencePrfl" value="X"/>
  <parm name="ChatAuth" value="X"/>
  <parm name="GroupChatAuth" value="X"/>
  <parm name="ftAuth" value="X"/>
  <parm name="standaloneMsgAuth" value="X"/>
  <parm name="geolocPullAuth" value="X"/>
  <parm name="geolocPushAuth" value="X"/>
  <parm name="vsAuth" value="X"/>
  <parm name="isAuth" value="X"/>
  <parm name="rcsIPVoiceCallAuth" value="X"/>
  <parm name="rcsIPVideoCallAuth" value="X"/>
  <parm name="IR94VideoAuth" value="X"/>
  <parm name="allowRCSExtensions" value="X"/>
  <characteristic type="Ext">
    <characteristic type="joyn">
      <parm name="moMmsAuth" value="X"/>
      <parm name="connMOControl" value="X"/>
      <characteristic type="Ext"/>
    </characteristic>
  </characteristic>
</characteristic>
  
```

**Table 21: Services sub tree associated HTTP configuration XML structure**

This sub tree is formally defined as follows:

**Node:** <x>/joyn

Under this interior node where the joyn specific parameters are placed.

Status	Occurrence	Format	Min. Access Types
Required	One	Node	Get

**Table 22: joynServices Extension MO sub tree addition node**

- Values: N/A
- Type property of the node is: urn:gsma:mo:rcc-services:5.3:Ext:joyn
- Associated HTTP XML characteristic type: “joyn”

Node: <x>/joyn/moMmsAuth

Controls the MMS service behaviour of the client.

Status	Occurrence	Format	Min. Access Types
Required	ZeroOrOne	Bool	Get

**Table 23: MO MMS Services Extension MO sub tree addition parameters (moMmsAuth)**

- The parameter represents the configuration parameter MO MMS AUTH defined in Table 15.
- Values:  
 0: the mobile originated MMS service is disabled  
 1: the mobile originated MMS service is enabled
- Post reconfiguration actions: There are no additional actions apart from using the new parameter values.

Associated HTTP XML characteristic type: “moMmsAuth”

Node: <x>/joyn/connMOControl

Controls the connectivity management on the device.

Status	Occurrence	Format	Min. Access Types
Required	ZeroOrOne	Bool	Get

**Table 24: CONN MO CONTROL Services Extension MO sub tree addition parameters (connMOControl)**

- The parameter represents the configuration parameter CONN MO CONTROL defined in Table 16.
- Values:  
 0: the configuration server does not control the 3GPP Connectivity MO (default)  
 1: the configuration server does control the 3GPP Connectivity MO
- Post reconfiguration actions: There are no additional actions apart from considering the value of the configuration parameter for the management of the Connectivity Management Management Object related configuration parameters.

- Associated HTTP XML characteristic type: “connMOControl”

Node: <x>/joyn/Ext

An extension node for Service Provider specific parameters. Clients that are not aware of any extensions in this sub tree (e.g. because they are not Service Provider specific) *Should Not* instantiate this tree.

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	Node	Get

**Table 25: joyn Services Extension MO sub tree addition Service Provider Extension Node**

- Values: N/A
- Type property of the node is: urn:gsma:mo:rcs-services:5.3:Ext:joyn:Ext
- Post reconfiguration actions: There are no additional actions required.
- Associated HTTP XML characteristic type: “Ext”

#### 4.3.2.6 MMS Client Configuration related parameters

With the support of Operator Messaging the Service Provider Client Configuration Protocol can be used by the Service Provider to control the client settings for MMS.

The Service Provider Client Configuration protocol provides the configuration server with the ability to create, delete and replace MMS client configuration objects. The ability of the client to create, replace and delete an MMS configuration object on the Configuration Server (e.g. for multi device synchronisation) is subject to the Service Provider Client Configuration protocol evolution.

MMS client configuration via Service Provider Client Configuration is active for a device if the configuration parameter MO MMS AUTH is set to value "0" or "1", see table 15. If the parameter MO MMS AUTH is not present then MMS client configuration is not applicable, i.e. the MMS configuration object shall not be present in the configuration xml.

If the configuration xml received from the configuration server contains an MMS configuration object and there is no MMS configuration object available on the device, the client shall create one with the data received from the server. The data of the MMS configuration object shall be used for MMS.

If the configuration xml received from the configuration server contains the configuration parameter MO MMS AUTH with value "0" or "1" (see table 15) and an MMS configuration object and there is no MMS configuration objects available on the device, the client shall store the MMS object locally and apply it for MMS.

If the configuration xml received from the configuration server contains the configuration parameter MO MMS AUTH with value "0" or "1" (see table 15) and MMS configuration objects exist on the device, the client shall compare the value of the NAME parameter received in the xml with the ones stored on the device.

- If the NAME value in the xml does not match to an existing object, the client shall use the content of the xml object to create a new MMS configuration object. This MMS object shall be used for MMS.
- If the NAME value in the xml matches an existing MMS object, the client shall use the content of the xml object to replace the corresponding configuration object on the device. The replaced MMS object shall be used for MMS.



If the configuration xml received from the configuration server contains the configuration parameter MO MMS AUTH with value "0" or "1" (see table 15) and no MMS configuration object then the client shall delete all locally stored MMS configuration objects.

The following configuration parameter definitions apply for the application of the Service Provider Client Configuration Protocol.

Configuration parameter	Description	Parameter usage
NAME	This parameter provides the name of the MMS configuration data which may be displayed to the user. It also acts as the primary key for the addressing of MMS configuration objects via the Service Provider Device Configuration.	Optional Parameter
ADDRESS	This parameter provides the URI of the service provider's MMS Proxy Relay. The parameter shall be present if the NAME parameter is present.	Optional Parameter
CONNECTIVITY REFERENCE	This parameter provides the references to a proxy or NAP object. If a proxy is used as a target, it contains the value of the PROXY ID defined in Table 27. If a NAP is used as a target, it contains the ID defined in Table 26. The parameter may have multiple occurrences. At least one occurrence shall be present if the NAME parameter is present.	Optional Parameter
MMS MAX MESSAGE SIZE	This parameter provides the max authorized message size to be enforced by the client for mobile originated MMS messages. The parameter can take the values:  300    300 kByte 600    600 kByte  The parameters shall be present if the NAME parameter is present.	Optional Parameter

**Table 26: MMS client configuration parameters**

#### 4.3.2.6.1 Parameter Definition and Mapping

The following parameters of the OMA Management Object for MMS are applicable in the RCS client configuration. The parameters are mapped from [OMA-TS-MMS] as follows.

Joyn Configuration Parameter	Configuration parameter in [OMA-TS-MMS]	HTTP XML Characteristic type/parm name	HTTP XML element type
	/<X>	MMS	characteristic
NAME	/<X>/Name	Name	parm
ADDRESS	/<X>/Addr	Addr	parm
	/<X>/ToConRef/	ToConRef	characteristic
	/<X>/ToConRef/<X>	ConRef	characteristic

CONNECTIVITY REFERENCE	/<X>/ToConRef/<X>/ConRef	Conref<X> where <X> is a positive integer value determining the ordering	parm
MMS MAX MESSAGE SIZE	/<X>/MMSize	MMSize	Parm
	/<X>/Ext	Ext	characteristic

**Table 27: Mapping of MMS configuration elements**

#### 4.3.2.6.2 Summary Structure

The following provides the summary structure of the MMS application characteristic data in the HTTP configuration XML structure.

```
<characteristic type="MMS">
  <parm name="Name" value="X"/>
  <characteristic type="ToConRef">
    <characteristic type="ConRef">
      <parm name="ConRef1" value="X"/>
      <parm name="ConRef2" value="X"/>
    </characteristic>
  </characteristic>
  <parm name="Addr" value="X"/>
  <parm name="MMSize" value="X"/>
  <characteristic type="Ext"/>
</characteristic>
```

**Table 28: MMS sub tree associated HTTP configuration XML structure**

#### 4.3.2.6.3 Inclusion in the Service Provider Configuration Protocol XML Document

The following provides the summary structure of the MMS application characteristic data in the HTTP configuration XML structure.

```
<characteristic type="MMS">
  <parm name="Name" value="X"/>
  <characteristic type="ToConRef">
    <characteristic type="ConRef">
      <parm name="ConRef1" value="X"/>
      <parm name="ConRef2" value="X"/>
    </characteristic>
  </characteristic>
  <parm name="Addr" value="X"/>
  <parm name="MMSize" value="X"/>
  <characteristic type="Ext"/>
</characteristic>
```

**Table 29: MMS sub tree associated HTTP configuration XML structure**

#### 4.3.2.7 Connectivity Management Objects related configuration

The Service Provider Client Configuration protocol provides the configuration server with the ability to create, delete and replace connectivity client configuration objects as defined in [OMA-DDS-DM\_ConnMO].

The Service Provider Client Configuration shall support the management of both the Network Access Point (NAP) and Proxy objects. In this version of the specification the 3GPP NAP is supported.

The ability of the client to create, replace and delete connectivity configuration objects on the configuration server (e.g. for multi device synchronisation) is subject to the Service Provider Client Configuration protocol evolution.

Connectivity client configuration via Service Provider Client Configuration is active for a device if the configuration parameter CONN MO CONTROL value is set to "1", see Table 15.

If the parameter CONN MO CONTROL is not present then connectivity client configuration is not applicable, i.e. the connectivity configuration objects shall not be present in the configuration xml.

If the configuration xml received from the configuration server contains the configuration parameter CONN MO CONTROL with value "1" (see table 15) and an connectivity configuration objects and there is no connectivity configuration objects available on the device, the client shall store the connectivity configuration objects from the xml locally.

If the configuration xml received from the configuration server contains the configuration parameter CONN MO CONTROL with value "1" (see table 15) and connectivity configuration objects and there is connectivity objects already stored on the device, the client shall compare the value ID parameter of each object in the xml with the ID of each locally stored object:

- If the ID value of an object in the xml matches to an local object then the client shall replace the local object with the one received in the xml.
- If the ID value of the objects in the xml matches with no local object then the client shall create a new local object with the data received in the xml.

If the configuration xml received from the configuration server contains the configuration parameter CONN MO CONTROL with value "1" (see table 15) and no connectivity configuration object then the client shall delete all locally stored connectivity configuration objects.

The following NAP object parameter definitions apply for the application of the Service Provider Client Configuration Protocol.

Configuration parameter	Description	Parameter usage
ID	This parameter provides the identifier of the NAP object for cross reference.	Mandatory Parameter
NAME	This parameter provides the display name of the NAP configuration data object.	Optional Parameter
ADDRESS TYPE	This parameter provides the address type of the address in the network access profile.	Optional Parameter
ADDRESS	This parameter provides the address of the Network Access Point.	Mandatory Parameter
AUTH TYPE	This parameter provides the authentication protocol used by the NAP.	Manadatory Parameter
AUTH NAME	This parameter provides the user name for the authentication of the NAP.	Optional Parameter
AUTH SECRET	This parameter provides the password for the authentication of the NAP	Optional Parameter

PDP TYPE	This parameter provides 3GPP Packet Data PDP Type.	Optional Parameter
----------	--	--------------------

**Table 30: NAP object parameters**

The following PROXY object parameter definitions apply for the application of the Service Provider Client Configuration Protocol.

Configuration parameter	Description	Parameter usage
PROXY ID	This parameter provides the identifier of the proxy object for cross reference.	Mandatory Parameter
NAME	This parameter provides the display name of the connectivity configuration data object.	Optional Parameter
ADDRESS TYPE	This parameter provides the address type of the proxy address.	Optional Parameter
ADDRESS	This parameter provides the proxy address.	Mandatory Parameter
AUTH TYPE	This parameter provides the authentication protocol used by the proxy.	Manadatory Parameter
AUTH NAME	This parameter provides the user name for the authentication of the proxy.	Optional Parameter
AUTH SECRET	This parameter provides the password for the authentication of the proxy.	Optional Parameter
CONNECTIVITY REFERENCE	This parameter provides the references to the NAP objects. The parameter may have multiple occurrences. At least one occurrence shall be present if the ID parameter is present.	Optional Parameter
PORT NUMBER	This parameter provides the port number open by the proxy	Optional Parameter
SERVICES	This parameter provides the services supported by the proxy	Optional Parameter

**Table 31: Proxy object parameters**

#### 4.3.2.7.1 Parameter Definition and Mapping

The following parameters of the OMA Connectivity Management Object are applicable in the RCS client configuration. The parameters are mapped from [OMA-DDS-DM\_ConnMO] and [OMA-DDS-DM\_ConnMO\_3GPPPS] as follows.

Joyn Configuration Parameter	Configuration parameter in [OMA-DDS-DM_ConnMO]	HTTP XML Characteristic type/parm name	HTTP XML element type
	/<X>	NAP	characteristic
ID	/<X>/ID	id	parm
NAME	/<X>/Name	name	parm
ADDRESS TYPE	/<X>/AddrType	addrType	parm

ADDRESS	/<X>/Addr	addr	parm
	/<X>/AuthInfo	authInfo	characteristic
AUTH TYPE	/<X>/AuthInfo/AuthType	authType	parm
AUTH NAME	/<X>/ AuthInfo/AuthName	authName	parm
AUTH SECRET	/<X>/ AuthInfo/AuthSecret	authSecret	parm
	/<X>/BearerType	bearerType	parm
	/<X>/BearerParams	bearerParams	characteristic
	/<X>/BearerParams/3GPPPS	3GPPPS	characteristic
PDP TYPE	/<X>/BearerParams/3GPPPS/ PDPTType	PDPTType	parm
	/<X>/Ext	ext	characteristic

**Table 32: Mapping of NAP configuration elements**

Joyn Configuration Parameter	Configuration parameter in [OMA-DDS-DM_ConnMO]	HTTP XML Characteristic type/parm name	HTTP XML element type
	/<X>	PROXY	characteristic
PROXY ID	/<X>/ProxyId	proxyID	parm
NAME	/<X>/Name	name	parm
ADDRESS TYPE	/<X>/AddrType	addrType	parm
ADDRESS	/<X>/Addr	addr	parm
	/<X>/AuthInfo	authInfo	characteristic
AUTH TYPE	/<X>/AuthInfo/AuthType	authType	parm
AUTH NAME	/<X>/ AuthInfo/AuthName	authName	parm
AUTH SECRET	/<X>/ AuthInfo/AuthSecret	authSecret	parm
	/<X>/ToConRef/	ToConRef	characteristic
	/<X>/ToConRef/<X>	ConRef	characteristic
CONNECTIVITY REFERENCE	/<X>/ToConRef/<X>/ConRef	Conref<X> where <X> is a positive integer value determining the ordering	parm
	/<X>/Ports/	Ports	characteristic
	/<X>/Ports/<X>	Port<X> where <X> is a positive integer value determining the ordering	characteristic
PORT NUMBER	/<X>/Ports/<X>/PortNbr	PortNbr	parm
	/<X>/Ports/<X>/Services	Services	characteristic
	/<X>/Ports/<X>/Services/<X>	Serv	characteristic

SERVICES	/<X>/Ports/<X>/Services/<X>/ServiceName	ServiceName<X> where <X> is a positive integer value determining the ordering	parm
	/<X>/Ext	ext	characteristic

**Table 33: Mapping of Proxy configuration elements**

#### 4.3.2.7.2 Summary Structure

The following provides the summary structure of the NAP characteristic data in the HTTP configuration XML structure.

```

<characteristic type="NAP">
  <parm name="id" value="X"/>
  <parm name="Name" value="X"/>
  <parm name="AddrType" value="X"/>
  <parm name="Addr" value="X"/>
  <parm name="BearerType" value="X"/>
  <characteristic type="AuthInfo">
    <parm name="AuthType" value="X"/>
    <parm name="AuthName" value="X"/>
    <parm name="AuthSecret" value="X"/>
  </characteristic type/>
  <characteristic type="BearerParams">
    <characteristic type="3GPPPS">
      <parm name="PDPTType" value="X"/>
    </characteristic type/>
  </characteristic type/>
  <characteristic type="Ext"/>
</characteristic type/>

```

**Table 34: NAP sub tree associated HTTP configuration XML structure**

The following provides the summary structure of the Proxy characteristic data in the HTTP configuration XML structure.

```

<characteristic type="PROXY">
  <parm name="ProxyID" value="X"/>
  <parm name="Name" value="X"/>
  <parm name="AddrType" value="X"/>
  <parm name="Addr" value="X"/>
  <characteristic type="AuthInfo">
    <parm name="AuthType" value="X"/>
    <parm name="AuthName" value="X"/>
    <parm name="AuthSecret" value="X"/>
  </characteristic type/>
  <characteristic type="ToConRef">
    <characteristic type="ConRef">
      <parm name="ConRef1" value="X"/>
      <parm name="ConRef2" value="X"/>
    </characteristic type/>
  </characteristic type/>
  <characteristic type="Ports">
    <characteristic type="Port1">
      <parm name="PortNbr" value="X"/>
    </characteristic type/>
  </characteristic type/>

```

```

        <characteristic type="Services">
            <characteristic type="Serv">
                <parm name="ServiceName1" value="X"/>
                <parm name="ServiceName2" value="X"/>
            </characteristic>
        </characteristic>
    </characteristic>
</characteristic>
<characteristic type="Ports">
    <characteristic type="Port2">
        <parm name="PortNbr" value="X"/>
        <characteristic type="Services">
            <characteristic type="Serv">
                <parm name="ServiceName1" value="X"/>
                <parm name="ServiceName2" value="X"/>
            </characteristic>
        </characteristic>
    </characteristic>
</characteristic>
<characteristic type="Ext"/>
</characteristic>
    
```

**Table 35: Proxy sub tree associated HTTP configuration XML structure**

#### 4.3.2.7.3 Inclusion in the Service Provider Configuration Protocol xml Document

The NAP and Proxy client configuration is included in the configuration document as follows:

```

<?xml version="1.0"?>
<wap-provisioningdoc version="1.1">
    <characteristic type="VERS">
        <parm name="version" value="X"/>
        <parm name="validity" value="Y"/>
    </characteristic>
    <characteristic type="TOKEN">
        <parm name="token" value="U"/>
        <parm name="validity" value="V"/>
    </characteristic>
    <characteristic type="MSG">                                -- This section is OPTIONAL
        <parm name="title" value="R"/>
        <parm name="message" value="S"/>
        <parm name="Accept_btn" value="X"/>
        <parm name="Reject_btn" value="X"/>
    </characteristic>
    <characteristic type="PROXY">
        <parm name="ProxyID" value="X"/>
        <parm name="Name" value="X"/>
        <parm name="AddrType" value="X"/>
        <parm name="Addr" value="X"/>
        <characteristic type="AuthInfo">
            <parm name="AuthType" value="X"/>
            <parm name="AuthName" value="X"/>
            <parm name="AuthSecret" value="X"/>
        </characteristic type/>
        <characteristic type="ToConRef">
            <characteristic type="ConRef">
                <parm name="ConRef1" value="X"/>
                <parm name="ConRef2" value="X"/>
            </characteristic>
        </characteristic>
    </characteristic>
    
```

```

</characteristic>
<characteristic type="Ports">
  <characteristic type="Port1">
    <parm name="PortNbr" value="X"/>
    <characteristic type="Services">
      <characteristic type="Serv">
        <parm name="ServiceName1" value="X"/>
        <parm name="ServiceName2" value="X"/>
      </characteristic>
    </characteristic>
  </characteristic>
</characteristic>
</characteristic>
<characteristic type="Ports">
  <characteristic type="Port2">
    <parm name="PortNbr" value="X"/>
    <characteristic type="Services">
      <characteristic type="Serv">
        <parm name="ServiceName1" value="X"/>
        <parm name="ServiceName2" value="X"/>
      </characteristic>
    </characteristic>
  </characteristic>
</characteristic>
<characteristic type="Ext"/>
</characteristic>
<characteristic type="NAP">
  <parm name="id" value="X"/>
  <parm name="Name" value="X"/>
  <parm name="AddrType" value="X"/>
  <parm name="Addr" value="X"/>
  <parm name="BearerType" value="X"/>
  <characteristic type="AuthInfo">
    <parm name="AuthType" value="X"/>
    <parm name="AuthName" value="X"/>
    <parm name="AuthSecret" value="X"/>
  </characteristic type/>
  <characteristic type="BearerParams">
    <characteristic type="3GPPPS">
      <parm name="PDPTType" value="X"/>
    </characteristic>
  </characteristic>
  <characteristic type="Ext"/>
</characteristic>
<characteristic type="NAP">
  ...
</characteristic>
  ...
  <characteristic type="APPLICATION">
    ...
  </characteristic>
</wap-provisioningdoc>

```

**Table 36: Connectivity HTTP configuration XML structure**



Service providers need to be able to configure devices for the two Operator messaging integration modes defined in this Operator Messaging section. A new configuration parameter to control the Common Core messaging UX is defined as follows.

### 4.3.3 Capability Discovery

To realise the behaviour specified in this 'Operator Messaging' section, a client must be able to indicate whether a combined messaging UX is provided to the user. This is achieved by the use of the Combined Messaging UX SIP OPTIONS tag and Presence service-id as defined in section 4.3.3 of [RCC.61]. Clients configured for Capability Agnostic experience via the configuration parameter CAP AGNOSTIC MSG defined in section 4.3.2.1 of this document shall advertise in their capabilities support of integrated messaging to support interoperability with devices not applying the capability agnostic experience.

## 4.4 Technical Implementation of User Stories & Feature requirements

- R4-18-1* The requirements listed under user story US4-1 and US4-2 shall be implemented locally on the client.
- R4-18-2* The requirements listed under user story US4-3 shall be implemented locally on the client based on the submission, delivery and display status technology of the various messaging technologies.
- R4-18-3* For the requirements listed under user story US4-4 the Operator shall implement message revocation for 1-to-1 Chat as defined 3.3.4.1.10 of [RCC.07] For other messaging services and technologies than 1-to-1 chat revocation of messages is not supported.
- R4-18-4* The requirements listed under user story US4-5 shall be implemented locally on the device based on the capability discovery result. Requirement R4-5-1 shall be implemented as defined in section 4.3.3 of this document.
- R4-18-5* The requirements listed under user story US4-6 shall be implemented locally on the client.
- R4-18-6* The requirements listed under user story US4-7 shall be implemented as follows:
- R4-18-7* For requirement R4-7-1 the technology selection rule defined in section 4.3.1 of this document shall apply. Depending on the messaging technology the following access technologies are supported in the following priority order:
- R4-18-8* SMS provided by Standalone Messaging shall be supported in Legacy 3GPP access, LTE and EPC integrated Wifi as defined in [NG.102]. If no such access network is available it shall be provided by non intergrated Wifi access.
- R4-18-9* SMS provided by the Short Messaging Service over IP as defined in IR.92 shall be supported in LTE.
- R4-18-10* SMS provided by the Short Messaging Service as defined in [3GPP TS 23.040] shall be supported in Legacy 3GPP access and LTE.
- R4-18-11* MMS provided by Standalone Messaging shall be supported in Legacy 3GPP access, LTE and EPC integrated Wifi as defined in [NG.102]. If no such access network is available it shall be provided by non intergrated Wifi access.

- R4-18-12* MMS provided by the Multimedia Messaging Service as defined in 3GPP TS 22.140 and 3GPP TS 23.140 shall be supported in LTE and Legacy 3GPP access.
- R4-18-13* RCS messaging services (RCS 1-to-1 Chat, RCS File Transfer, RCS Group Chat) shall be supported in Legacy 3GPP access, LTE and EPC integrated Wifi as defined in [NG.102]. If no such access network is available it shall be provided by non intergrated Wifi access.
- R4-18-14* The requirements listed under user stories US4-8 through to US4-17 shall be implemented locally on the client. The following general procedural requirements shall be considered.

For requirements, related to the 'Online experience', where a client needs to determine the RCS registered status of the other party via capability discovery, the client implementation shall take the definitions of the automata tag in section 2.7.1.1 of [RCC.07] into account.

For the requirements, where a client needs to determine the messaging technology based on the network connection status and the device is in a situation where it attaches to the network anew (e.g. due to power-on or resume from airplane mode) it is recommended that the client awaits the completion of all network attach procedures first.

The determination of the integrated / seamless messaging capability of other RCS users is provided by the capability discovery of the Combined Messaging UX as defined in section 4.3.3 of this document.

If the DELIVERY TIMEOUT timer expires for a chat message or a File Transfer the client shall either initiate a capability discovery to determine whether messaging technology is to be switched or inform the user as defined in the Operator Messaging requirements.

If a joyn client is configured for the 'Capability Agnostic experience' by setting the configuration parameter CAP AGNOSTIC MSG to "1", (see section 4.3.2.1). it shall use for one to one communication only the RCS Chat and File Transfer Service and Geolocation Push unless the device is not registered in IMS.

#### **4.4.1 Backward Compatibility**

##### **4.4.1.1 Legacy Network**

Crane clients operated in legacy networks will not receive in the device configuration document parameters controlling the Operator Messaging UX as defined in section 4.3.2 of this document.

If the parameter MESSAGING UX is not provided by the network, the client will apply the default value defined in section 4.3.2 of [RCC.61], i.e. the Seamless Messaging functionality. A service provider with a blackbird network accepting Crane devices is advised to provide the MESSAGING UX parameter in the configuration document for Crane devices if no seamless messaging user experience shall be provided to subscribers.

If the parameter DELIVERY TIMEOUT is not provided by the network, the client shall apply the default value defined in section 4.3.2 of [RCC.61].

If the parameter FT HTTP CAP ALWAYS ON is not provided by the network, the client shall assume the value "1".

#### 4.4.2 Configuration Parameters

For joyn Crane networks the following Operator Messaging configuration parameter values apply.

Configuration Parameter	Crane Value
MESSAGING UX	"1"
DELIVERY TIMEOUT	Service Provider Configurable
FT HTTP CAP ALWAYS ON	Service Provider Configurable
IM CAP NON RCS	Service Provider Configurable
STANDALONE MGS AUTH	Service Provider Configurable
MAX SIZE STANDALONE	Service Provider Configurable
CAP AGNOSTIC MSG	Service Provider Configurable
MO MMS AUTH	Service Provider Configurable
NAME	Service Provider Configurable
ADDRESS	Service Provider Configurable
CONNECTIVITY REFERENCE	Service Provider Configurable
MMS MAX MESSAGE SIZE	Service Provider Configurable
ID	Service Provider Configurable
NAME	Service Provider Configurable
ADDRESS TYPE	Service Provider Configurable
ADDRESS	Service Provider Configurable
AUTH TYPE	Service Provider Configurable
AUTH NAME	Service Provider Configurable
AUTH SECRET	Service Provider Configurable
PDP TYPE	Service Provider Configurable
PROXY ID	Service Provider Configurable
NAME	Service Provider Configurable
ADDRESS TYPE	Service Provider Configurable
ADDRESS	Service Provider Configurable
AUTH TYPE	Service Provider Configurable
AUTH NAME	Service Provider Configurable
AUTH SECRET	Service Provider Configurable
CONNECTIVITY REFERENCE	Service Provider Configurable
PORT NUMBER	Service Provider Configurable
SERVICES	Service Provider Configurable
SMS_Over_IP_Networks_Indication	Service Provider Configurable

**Table 37: Operator Messaging Configuration Parameter Values**

## 5 1-to-1 Chat

### 5.1 Description

1-to-1 Chat enables customers to exchange chat messages with another party. This section describes the User Stories and Service Requirements for the core chat service and all features around the core.

Major changes of the Crane PDD compared to the Blackbird PDD are:

- The user shall be able to use standard text editing functions offered by the device (e.g. Copy & Paste) to create chat messages.
- Notifications for new incoming messages shall be intelligently aggregated
- Network initiated message recall
- Rules for message timestamps when displayed in the conversation
- Use of device LED to signal unread messages
- Order of conversations in the conversation overview (on new incoming messages)
- Representation of chat participants when contact is known in contact list or Alias name is available
- Introduction of a Common Message Store
- Introduction of a voice and video call service entry point from chat UI and requirements on how the device shall behave when the user uses it.

### 5.2 User Stories and Feature Requirements

#### **US5-1 As a user, I want to send Chat messages to my contacts.**

NOTE: This document describes the Chat service functionality for contacts on-net or on an Interconnected RCS service. Other contacts may have less functionality available. Please refer to Operator Messaging, page 38.

*R5-1-1* Any RCS user shall be able to send a Chat message to contacts in the contact list.

*R5-1-2* The user shall have the option to send a message at any time by entering an existing chat and continue.

NOTE: The 1-to-1 chat has no visible end. Despite the way it is technically realised, to the user it will always appear as a thread of messages to which they can reply at any time. The user may switch to other screens any time during or after a chat without affecting the chat history or the option to resume the chat at a later time.

#### **US5-2 As a user, I want to see the status of my sent Chat messages.**

*R5-2-1* For A-Party, the following message states shall be supported:

*R5-2-1-1* Message Pending: Transfer of the Chat message in progress (e.g. queuing on device).

*R5-2-1-2* Message Sent: Confirmation that the message has been correctly accepted by the A-Party's network.

*R5-2-1-3* Message Delivered: Confirmation that the message has been delivered to the B-Party device.

*R5-2-1-4* Message Displayed: Confirmation the message was displayed on the receiving device (technical confirmation that message was read by the recipient)

*R5-2-1-5* Message send failed: The expected outcome of the operation could not be confirmed by the network (in this case: Message Sent or Message Delivered status notification has not been received) and the device does not attempt to send the message again.

NOTE: Sending the message may be re-triggered manually by the user.

*R5-2-1-5-1* A Message send failed state shall be indicated to the user as well in case the Integrated Messaging implementation delivers a “DELIVERY TIMEOUT” error.

*R5-2-2* If the sending device is offline at the time a notification is received, notifications shall be stored on the network and forwarded once the sending device is online.

*R5-2-3* Aggregation of message status on UI level may be done in line with requirements R4-3-5 and R4-3-6.

**US5-3 As a user, I want to include smileys into my Chat messages.**

*R5-3-1* It shall be possible to add Emoji when creating a chat message by adding from a selection of graphical elements in the chat application.

NOTE: Standards for conversion of text strings to Emoji are described in Annex ‘Emoticon conversion table’, page 180.

*R5-3-2* It shall be possible to add the basic Emoticons when creating a chat message by typing in the respective text string, separated by blank spaces (e.g. “;-) “converts to☺) or typing in the respective text string without blank spaces if the string is the only characters of the message content.

NOTE: The basic set of Emoticons is listed in the Annex ‘Emoticon conversion table’, page 180.

*R5-3-3* Emoji shall be interpreted as detailed in the conversion table in the Annex of this document. The graphical elements that are used may vary from vendor to vendor, but the conveyed meaning must not be changed.

*R5-3-4* Emoticons from the basic set of Emoticons, which are received in Chat messages, shall be converted to graphics, if they were separated by blank spaces in messages (e.g. “;-)” converts to “☺”) or without the blank spaces if the emoticon string is the only characters of the message content.

**US5-4 As a user, I want to use the text editing tools of the device that are available on my device (e.g., but not limited to, copy paste, edit) for Chat messages.**

NOTE: In case of the user trying to paste an image into the text editor the device may ignore the user action.

*R5-4-1* The user shall have the option to select text (e.g. from a message, a website or any other text source) and use text editing tools such as copy & paste to create messages.

**US5-5 As a user, I want to see when the other party is currently writing a Chat message.**

*R5-5-1* The other party shall be able to see an “is typing” notification whenever a new Chat message is created.

**US5-6 As a user, I want to receive text Chat messages from my contacts.**

*R5-6-1* Any RCS user shall be able to receive Chat message(s) that are sent to them.

**US5-7 As a user, I can send a Chat message like a text and it is just delivered. B-Party does not need to accept the message.**

*R5-7-1* Chat messages shall be received directly in the inbox; no hand-shake acceptance shall be required.

**US5-8 As a user, I want to send text Chat messages to my contacts even when they're temporarily offline (e.g. device switched off). I expect them to receive these Chat messages when they come online again.**

*R5-8-1* If the B-Party is currently not connected to the RCS service (*"offline"*), the message(s) shall be delivered once the user is back registered on RCS.

NOTE1: If the B-Party receives the message using another service before reregistering to RCS, then the B-Party shall not be notified of the message. This prevents message duplication.

NOTE2: Details of alternative delivery methods from Operator Messaging page 38, may apply.

*R5-8-2* The Operator shall be able to set the storage duration for store & forward cases (deferred messaging) based on its own individual Operator parameters.

NOTE: The parameters may be aligned at a local level as the terminating network storage time has an impact on the sending network user's experience.

**US5-9 As a user, I want to be notified at any time my device receives a new Chat Message.**

*R5-9-1* On receiving a message, the user shall be notified with graphical and sound elements (similar as the device notifies of incoming SMS messages if not stated differently in this requirements document).

**US5-10 As a user, I want notifications of rapidly sequenced incoming Chat Messages intelligibly aggregated and counted.**

*R5-10-1* For audio notifications, device audio related settings shall prevail.

*R5-10-2* Rapid sequence of incoming Chat messages in one conversation shall be consolidated into one audible notification per conversation. Consolidation of visual notifications is not affected.

*R5-10-3* On selection of the visual notification for one or more new message(s) in a single Chat or Group Chat conversation, the user shall be forwarded to the respective Chat message and the visual notification shall be permanently removed from the notification centre or bar.

*R5-10-4* On selection of the visual notification for two or more new messages from different Chat or Group Chat notifications, the user shall be forwarded to the list of Chat or Group Chat conversations. In this case, the unread message visual identifier shall be removed once the last new message was read. Alternatively, the OEM may handle it differently on the device (e.g. the visual notification disappears already after selecting the notification and seeing the list of Chat or Group Chat conversations).

*R5-10-5* Any audible or visual notification shall be suppressed in case the reception is visible on the currently active screen of the device (e.g. if the user is

currently on the Chat screen with a person and a Chat Message is received).

**US5-11 As a user, I want to view my sent and received Chat messages in a time-based order.**

*R5-11-1* All messages exchanged with the same contact shall be threaded in the same chat thread.

NOTE: Where a contact has multiple phone numbers, then a thread should be created for each phone number. The thread name should clearly show which identity is in use (e.g. work, home and so on).

*R5-11-2* The order of messages shall be in line with the order messages have been sent and received on the device.

*R5-11-3* The originating network shall have the ability to recall RCS messages from the terminating store.

NOTE: This requirement does not affect any messages which have already been delivered to the terminating device.

*R5-11-4* Incoming and outgoing messages shall be displayed interlaced.

*R5-11-5* Sent messages shall be inserted into the conversation thread as they have been created.

**US5-12 As a user, I want to see the timestamp associated with each of my sent and received messages.**

*R5-12-1* The date and time associated with each chat message shall be displayed adjusted to the current device date and time.

*R5-12-1-1* This timestamp shall be generated for sent messages by the device in a consistent way as timestamps are generated for other device functions, e.g. SMS.

*R5-12-1-2* Timestamps for received messages shall be based on the UTC timestamp that comes with each message, aligned with the selected device time zone.

**US5-13 As a user, I want conversations which contain unread messages to be differentiated from conversations that contain messages I have seen.**

NOTE1: This requirement shall be valid for Messaging for Multi-Device as well.

NOTE2: Unseen files or file download notifications cover events that use File Transfer as an enabler e.g. but not limited to, Geolocation Push, Audio Messaging or vCard share.

*R5-13-1* Conversations with unread messages or unseen files or file download notifications shall be marked accordingly, e.g. by display of subject line in bold font and / or an unread message counter.

*R5-13-2* Conversations shall, elevate to the top of the Chat or Group Chat conversation list on reception of a new message.

*R5-13-3* If the device supports a notification LED (for screen-off notification) then this LED shall flash as long as there are unread RCS messages. The colour should differentiate from notifications of other applications, but may be identical for all Operator Messaging services.

**US5-14 As a user, I want the contact names of Chat conversations to be aligned with the according contact card (i.e. if a contact I am in a Chat conversation with is in my contact list, the identifying MSISDN shall be replaced with the name from the contact card).**

*R5-14-1* If the sender of a Chat message is in my contact list, the MSISDN shall be replaced with the sender's name on the contact list in any representations where the message sender is represented.

*R5-14-2* If the sender of a Chat message is not in my contact list, the MSISDN shall be replaced with the sender's RCS Alias name if available.

*R5-14-3* In case the Alias is being used to represent the sender's identity, the device UI shall use appropriate means to make it clear that the Alias name is unverified information.

NOTE: The Alias as specified in RCS is created by the message sender and could be set to any possible name, the real name of the person, or a nickname or in extreme cases – in an attempt of identity spoofing – the sender could try to pretend a false identity.

**US5-15 As a user, I don't want to feel restricted by Chat message size limits.**

*R5-15-1* Chat messages (incoming and outgoing) shall allow the user to send and receive messages with at least 999 characters.

NOTE: Operator defined parameter.

**US5-16 As a user, I want to exchange multi-media content in my Chat conversations (e.g. but not limited to, take an instant picture from camera and send from within the chat).**

NOTE: Details on multi-media content are covered in File Transfer incl. Geolocation Push, page 99.

*R5-16-1* The user shall be able to select and send Multi Media in Chat conversations.

*R5-16-2* The user shall be able to receive Multi Media in Chat conversations.

**US5-17 As a user, I want to maintain multiple conversations in parallel.**

NOTE: These conversations may be one-to-one or Group Chat conversations.

*R5-17-1* The device shall offer the option of multiple parallel Chat and Group Chat conversations at any given point in time.

**US5-18 As a user, I want to easily and quickly switch between multiple parallel Conversations.**

NOTE: These conversations may be One-to-One or Group Chat conversations.

*R5-18-1* The device shall offer the option to switch between conversations easily and quickly.

**US5-19 As a user, I want my messages backed up on Common Message Store which is trusted and safe.**

*R5-19-1* All Conversations shall be stored on the network.

NOTE: Details of that storage are at the individual Operator discretion.

*R5-19-2* The Operator shall be able to determine the storage duration for messages on the Common Message Store based on individual Operator parameters.



*R5-19-3* If the Operator deletes messages from the Common Message Store (e.g. for capacity limitation) these messages shall not be deleted from local consumer equipment.

**US5-20 As a user, I want to restore my conversations from the Common Message Store (e.g. but not limited to, after wiping a device or purchasing a new device).**

*R5-20-1* The user shall have the option to restore conversations from the Common Message Store (e.g.in case of handset replacement or automated local memory removal of messages on device to free up memory space).

**US5-21 As a user, I want to delete complete conversations.  
As a user, I want to select and delete single and multiple chat messages in a chat thread.**

*R5-21-1* The user shall have the option to delete a single Chat message from a conversation.

*R5-21-2* The user shall have the option to delete single and multiple Chat messages in a chat thread.

*R5-21-3* The user shall have the option to delete an entire conversation.

*R5-21-4* Any Chat messages or entire conversations that have been deleted by the user shall no longer be available on the Common Message Store.

**US5-22 As a user, I want to be able to forward a single sent or received chat message to one or more contacts.**

NOTE: This may be performed by the user by copying existing message text and pasting into a new Chat message.

*R5-22-1* The user shall have the option to forward a single sent or received Chat message to one or more contacts.

NOTE: This function may be executed using the copy and paste text editor function on the device.

**US5-23 As a user, I want to switch to a voice or video call with the B-Party during a conversation - and return to chat when the call is finished.**

*R5-23-1* The user shall have the option to easily access voice calls from the Chat UI with the contact in the conversation. After the call has ended, the user can return to the conversation.

*R5-23-2* The user shall be able to receive a voice call when actively engaged in a conversation and return to the chat when the voice call was ended.

*R5-23-3* The user shall have the option to easily access video calls from the Chat UI with the contact in the conversation. After the call has ended, the user can return to the conversation.

*R5-23-4* The user shall be able to receive a video call when actively engaged in a Chat or Group Chat conversation and return to the chat when the video call ends.

**US5-24 As a user, I want to block specific users so that I do not receive any kind of Chat Message from them anymore.**

*R5-24-1* If the sender of a Chat message is on my local device blacklist, the incoming message shall be ignored.

- R5-24-2* Messages from blocked contacts shall neither trigger visual nor audio notification.
- R5-24-3* For messages from blocked contacts, conversations shall not be created.
- R5-24-4* Incoming messages from blocked contacts shall not be displayed.
- R5-24-5* The recipient shall not have the option to see or respond to messages from a blocked contact.

## 5.3 Technical Information

### 5.3.1 Overview

The 1-to-1 Chat service is provided as defined in sections 2.7.1.1 and 3.3 of [RCC.07]. For the purpose of the following technical implementation of the user stories and service requirements the 1-to-1 Chat service is considered as a stand-alone end-to-end service. The technical implementation of the 1-to-1 Chat service in relation to the integrated messaging experience is provided in 'Operator Messaging', page 38.

[RCC.07] allows service providers to implement the one-to-one user experience based on SIMPLE IM or CPM. For joyn Crane, the 1-to-1 Chat shall be based on OMA SIMPLE IM. Section 3.3.4.3 of [RCC.07] is thus not applicable.

### 5.3.2 Technical Implementation of User Stories and Service requirements

#### US5-25

- R5-25-1* For user story US5-1 the following definitions apply:
- The 1-to-1 Chat service shall be offered to the user if the device configuration authorises the chat service via the CHAT AUTH parameter defined in section A.1.4.3 of [RCC.07].
  - The ability of the user to send chat messages to a contact depends on the result of the capability discovery and the service provider's capability to support store-and-forward as defined in section 2.7 of [RCC.07].
  - As defined by requirement R5-1-2 the chat transfer technology requires the client to create and manage a chat session without making it visible to the user. The chat session shall be managed by the client with regard to the session acceptance and time-out as defined by the configuration parameters IM SESSION START, IM SESSION AUTO ACCEPT and IM SESSION TIMER of [RCC.07].
- R5-25-2* For the message transfer states of requirement R5-2-2 the following technical implementation applies:
- **Pending:** When the user presses ENTER to send the message until the first success response is received from the network. The message may be in this state for some time when the user is NOT registered with the IMS core (e.g. offline or airplane mode).
  - **Sent:** a first SIP provisional response is received from the network if the message is sent as part of the INVITE or a MSRP 200 OK is received in case the message was sent over MSRP.
  - **Delivered:** When receiving the Delivery Notification with status set to "delivered".

- **Displayed:** When receiving the Displayed Notification with the status set to “displayed”.
- **Error:** When an error different from 486/487 is received.

NOTE 1: Receipt of a 486/487 doesn't change the status of the message

NOTE 2: In addition to the definitions, an error status is met if no Delivery notification has been received for a message after the time indicated by the DELIVERY TIMEOUT value, as defined in section 4.3.2 of this document.

- R5-25-3* Notifications on delivery status information as defined in R5-2-1-5-1 shall be stored and forwarded in the store & forward server as specified in section 3.3.4.1.5 of [RCC.07].
- R5-25-4* For the requirements in user story US5-3 the device shall support the encoding and display of the graphical elements as defined in the referred Annexes.
- R5-25-5* The requirements in user story US5-4 shall be implemented locally on the device.
- R5-25-6* The indication that the other party is typing in requirement R5-5-1 is derived from the reception of the "isComposing" indication as defined in section 3.3.4.1 of [RCC.07]. It should be noted that the "isComposing" indication can only be transferred if an active chat session exist. Clients should send the "isComposing" indication only if a chat session exists for the conversation the user is typing in.
- R5-25-7* The requirements of user story US5-6 shall be implemented as defined in section 3.3.4 of [RCC.07].
- R5-25-8* As a clarification of the user story US5-7 it shall be noted that the client shall not apply any procedures for the acceptance of the delivery of single messages. If the first message is carried in a SIP INVITE then the client should enforce the chat session auto accept policy of the service provider as defined via the configuration parameters IM SESSION START and SESSION AUTO ACCEPT defined in section A.1.3.3. of [RCC.07]. In all other cases the device shall rely on the value of the SESSION AUTO ACCEPT parameter which needs to be set by the service provider to 1 to enforce the client to accept the session immediately.
- R5-25-9* The store-and-forward functionality defined in user story US5-8 shall be implemented as defined in sections 3.3.4.1.4 and 3.3.4.1.5 of [RCC.07].
- R5-25-10* The requirements of user stories US5-9 and US5-10 shall be implemented locally on the device.
- R5-25-11* For the requirements in user story US5-11 the client shall support the following procedure:
- It is the responsibility of the Messaging Server to deliver messages in the correct order, so the Client can rely on it when sorting messages. The client shall interleave the sent and received messages in the chronological order.
  - After the client has synchronised with the Common Message Store successfully, then messages shall be sorted in accordance with the time indicated in the CPIM DateTime header value received with message from the Common Message Store.

- R5-25-12* The requirement R5-11-3 shall be implemented as defined in section 3.3.4.1.10 of [RCC.07].
- R5-25-13* The requirements of user story US5-12 shall be implemented locally on the device.
- R5-25-14* The requirements of user story US5-13 shall be implemented locally on the device.
- R5-25-15* The user alias defined in user story US5-14 for addresses which do not match a contact shall be implemented as defined in section 2.5.3.3 of [RCC.07].
- R5-25-16* For the realization of requirements of user story US5-15 the client shall enforce the max message size for sending messages as defined by the configuration parameter MAX SIZE 1-to-1 IM defined in section A.1.3.3. of [RCC.07]. It is required for service providers to set the value to "999" or more.
- R5-25-17* For the requirements of user story US5-16 File Transfer will be used as defined in 'File Transfer incl. Geolocation Push', page 99. For the interactions with the 1-to-1 Chat message service the requirements of section 3.5.2 of [RCC.07] apply.
- R5-25-18* The requirements of user stories US5-17 and US5-18 shall be implemented locally on the device.
- R5-25-19* The requirements of user stories US5-19 and US5-20 are implemented as defined in 'Backup & Restore', page 119.
- R5-25-20* The requirements of user stories US5-21 through to US5-23 shall be implemented locally on the device.
- R5-25-21* The requirements of user story US5-24 will be implemented as defined in section 3.3.4.1.1 or 3.3.4.1.2 of [RCC.07].

### 5.3.3 Backward Compatibility

Legacy networks will not provide the parameter REVOKE TIMER in the configuration document. If the parameter is not present then Message Revocation shall not be applied by the client.

### 5.3.4 Configuration Parameters

For joyn Crane networks the following 1-to-1 Chat configuration parameter values apply.

Configuration Parameter	Crane Value
PRES-SRV-CAP	"0"
CONV-HIST-FUNC-URI	See section A.1.3 of [RCC.07]
DEFERRED-MSG-FUNC-URI / MSG-STORE-URI	See section A.1.3 of [RCC.07]
CHAT AUTH	"1"
STANDALONE MGS AUTH	Service Provider Configurable
IM CAP ALWAYS ON	Service Provider Configurable
IM WARN SF	Service Provider Configurable
IM CAP NON RCS	"0"
IM WARN IW	n/a

IM SMS FALLBACK AUTH	"0"
IM SESSION AUTO ACCEPT	Service Provider Configurable
IM SESSION START	Service Provider Configurable
FIRST MSG IN INVITE	"1"
IM SESSION TIMER	Service Provider Configurable
MAX CONCURRENT SESSIONS	Service Provider Configurable
MULTIMEDIA IN CHAT	"0"
MAX SIZE 1-to-1 IM	Service Provider Configurable
MAX SIZE STANDALONE	Service Provider Configurable
CHAT MESSAGING TECHNOLOGY	"0"
CHAT REVOKE TIMER	Service Provider Configurable

**Table 38: One-to-One Chat configuration parameter values**

## 6 Group Chat

### 6.1 Description

Group Chat allows customers to exchange chat messages with a number of contacts at the same time. Specific Group Chat features ensure proper handling of Group Chat – opposed to multiple one-to-one chat message distribution. In this section, User Stories, Feature Requirements and the proposed Technical Implementation.

Major changes of the Crane PDD compared to the Blackbird PDD are:

- Participation in Closed Group Chat conversations (*Closed Group Chat is a variant of the Group Chat as specified in RCS which is implemented by some Mobile Network Operators which are not using the joyn Crane profile.*)
- Users shall only be able to add new participants to an open Group Chat if the Operator -set maximum number of participants has not been reached.
- Representation of chat participants when contact is known in contact list or Alias name is available
- Store & forward for message status notifications
- Introduction of a size limit to Group Chat message length
- Notifications for new incoming messages shall be intelligently aggregated
- Using device LED for new incoming Group Chat message indication
- Order of conversations in the conversation overview (on new incoming messages)
- Rules for message timestamps when displayed in the conversation
- Muting audible notifications for new incoming messages for selected Group Chat conversations
- Introduction of a voice and video call service entry point from chat UI and requirements on how the device shall behave when the user uses it
- Introduction of a Common Message Store
- Behaviour of the client for blacklisted contacts participating in a Group Chat
- Display Notification on the senders side as an additional message status

## 6.2 User Stories and Feature Requirements

### **US6-1 As a user, I want to create an open Group Chat Conversation with a selection of my contacts.**

- R6-1-1* Any RCS user shall be able to create an open Group Chat conversation by selecting capable (for this service) contacts from the contact list and invite them to an open Group Chat.
- R6-1-2* It shall be possible to create an open Group Chat conversation by adding a (for this service capable) participant to a 1-to-1 Chat conversation. The existing 1-to-1 Chat conversation remains in the Chat conversation list, and a new Group Chat is created.
- R6-1-3* Any (for this service capable) RCS user shall be able to participate in an open Group Chat conversation when invited.
- R6-1-4* Any (for this service capable) RCS user shall be able to participate in a closed Group Chat conversation when invited.
- R6-1-5* The Operator shall be able to set a maximum number of participants in a Group Chat conversation.

NOTE: It is beneficial for proper RCS Interworking that RCS Operators align on the maximum number of participants, at least at a local level.

- R6-1-6* It shall only be possible to set up a new Group Chat conversation if the initiating user is connected to the RCS platform.
- R6-1-7* It shall be configurable for the Operator to allow non-RCS contacts being invited to open Group Chats.
  - R6-1-7-1* It shall only be possible to invite non-RCS (legacy) users to the group chat when it is created.
  - R6-1-7-2* It shall be configurable for the Operator to limit the maximum number of SMS participants.
  - R6-1-7-3* RCS capable Group Chat participants should see legacy participants differentiated from RCS users (e.g. 'SMS-only' label).
  - R6-1-7-4* The Group Chat experience shall be the same as a normal group chat.
- R6-1-8* It shall not be possible for the user to create closed Group Chats.

### **US6-2 As a user, I want to add a subject title to any open Group Chat Conversation.**

- R6-2-1* When creating a Group Chat conversation it shall be possible for the initiator to define a subject title.
- R6-2-2* If no subject title has been defined, the application shall automatically generate a subject title (e.g. list of users on the Group Chat "Liz, Thomas plus 3 others").
- R6-2-3* It shall be possible to maintain more than one Group Chat with identical Group Chat subject titles.

### **US6-3 As a user, I want to add a contact from my contact list to an existing open Group Chat conversation.**

- R6-3-1* Participants in an open Group Chat conversation shall be able to add new participants from their contact list.
- R6-3-2* It shall be visible to the user what the maximum allowed number of participants in the Group Chat is.

*R6-3-3* It shall not be possible to add new Group Chat participants in an open Group Chat conversation once the maximum number of participants has been reached as configured by the Operator.

*R6-3-4* It shall be possible to add participants to a Group Chat if they are not registered to the RCS platform (“offline”) at the time where the addition takes place.

NOTE: These participants are known to be RCS enabled but not registered to RCS service at the time of addition.

*R6-3-4-1* It shall not be possible to add legacy non-RCS contacts to a Group Chat.

*R6-3-5* Other Group Chat participants shall see the new participant- irrespective of whether the new participant is registered to the RCS platform (“online”) or not (“offline”) from the time the new participant was invited.

**US6-4 As a user, I don’t want anybody to be able to add a participant to a closed Group Chat conversation after it has been created.**

*R6-4-1* Participants in a closed Group Chat conversation shall not be able to add any further participants to the Group Chat conversation once the Group Chat conversation invites have been sent.

**US6-5 As a user, I want to know who is participating in a Group Chat conversation at any point in time.  
As a user, I want the contact names of Group Chat participants to be aligned with the according contact card (i.e. if a contact I am in a Group Chat conversation with is in my contact list, the identifying MSISDN shall be replaced with the name from the contact card).**

*R6-5-1* Any participant in a Group Chat conversation shall be able to see a list of participants at any point in time.

*R6-5-2* If the sender of a Group Chat message is a stored contact in the recipient’s address book, the MSISDN shall be replaced with the sender’s name on the contact list in any representations where the message sender is represented.

*R6-5-3* If the sender of a Chat message is not a stored contact in the recipient’s address book, the MSISDN shall be replaced with the sender’s RCS Alias name if available.

*R6-5-4* If the Alias is being used to represent the sender’s identity, the device UI shall use appropriate means to indicate that the Alias name is unverified information.

NOTE: The Alias as specified in RCS is created by the message sender and could be set to any possible name, the real name of the person, or a nickname or in extreme cases – in an attempt of identity spoofing – the sender could try to pretend a false identity.

*R6-5-5* If neither the contact name nor the RCS Alias is available, a participating contact shall be represented with their MSISDN in the list of Group Chat participants.

*R6-5-6* If new Group Chat participants join the Group Chat, all other Group Chat participants shall be notified with graphical elements inside the Group Chat conversation only.

*R6-5-7* If Group Chat participants leave the conversation, all other Group Chat participants shall be notified with graphical elements inside the Group Chat conversation only.

**US6-6 As a user, I don't want to deal with Group Chat invites and acceptances, I want to join a Group Chat conversation whenever I am invited to participate.**

*R6-6-1* Any user who was invited to a (closed or open) Group Chat conversation shall automatically become a participant of that Group Chat conversation no invite / acceptance 'handshake process' required.

*R6-6-2* The user shall be able to see who originally set up the Group Chat.

**US6-7 As a user, I want to send text Group Chat messages to an existing Group Chat conversation.**

*R6-7-1* Any participant in a Group Chat conversation shall be able to send messages to all Group Chat participants.

*R6-7-2* If the originating user tries to send messages to other Group Chat participants while not connected to the RCS platform ("offline"), the messages shall be queued locally on the device and sent out once the device reconnects to RCS platform ("online") again.

**US6-8 As a user, I can send a Group Chat message to an existing Group Chat conversation like a text and it is just delivered. Recipients do not need to explicitly accept any single message.**

*R6-8-1* Any message exchanged in the Group Chat conversation shall be received on other participants' devices without any form of acceptance of the message.

**US6-9 As a user, I want to send text Chat messages to my Group Chat participants even when they're temporarily offline (e.g. device switched off). I expect them to receive these Chat messages when they come online again.**

*R6-9-1* If any participant in a Group Chat conversation is currently not registered on the RCS service ("offline"), any message(s) or update(s) to the list of Group Chat participants shall be delivered once the user is back registered on RCS ("online").

*R6-9-2* The Operator shall be able to set the storage duration for store & forward cases (deferred messaging) based on individual Operator parameters.

NOTE: The parameters may be aligned on local level as the terminating network storage time has an impact on the sending network user's experience.

**US6-10 As a user, I want to include smileys into my Chat messages.**

*R6-10-1* It shall be possible to add Emoji when creating a Chat message by adding from a selection of graphical elements in the chat application.

NOTE: Standards for conversion of text strings to Emoji are described in the Annex Emoticon conversion table page 180.

*R6-10-2* It shall be possible to add the basic Emoticons when creating a Chat message by typing in the respective text string, separated by blank spaces (e.g. ";-)" "converts to "☺") or typing in the respective text string without blank spaces if the string is the only characters of the message content.

NOTE: The basic set of Emoticons is listed in the Annex 'Emoticon conversion table', page 180.



- R6-10-3* Emoji shall be interpreted as detailed in the conversion table in the Annex of this document. The graphical elements that are used may vary from vendor to vendor, but the conveyed meaning must not be changed.
- R6-10-4* Emoticons from the basic set of Emoticons, which are received in Chat messages, shall be converted to graphics, if they were separated by blank spaces in messages (e.g. “;-)” converts to “☺”) or without the blank spaces if the emoticon string is the only characters of the message content.

**US6-11 As a user, I don’t want to feel restricted by Group Chat message size limits.**

- R6-11-1* Group Chat messages (incoming and outgoing) shall allow to send and receive messages with at least 999 characters.

NOTE: Operator defined parameter.

**US6-12 As a user, I want to see the status of my sent Group Chat messages.**

- R6-12-1* For A-Party, the following message states shall be indicated to the user:

*R6-12-1-1* Message Pending: Transfer of the Chat message in progress (e.g. queuing on device).

*R6-12-1-2* Message Sent: Confirmation that the message has been correctly accepted by the A-Party’s network.

*R6-12-1-3* Message Delivered: Receiving devices have noticed that a message has been received by the device.

*R6-12-1-4* Message send failed: The expected outcome of the operation could not be confirmed by the network (in this case: Message Sent or Message Delivered status notification has not been received) and the device does not attempt to send the message anymore).

NOTE: Sending the message may be re-triggered manually by the user.

- R6-12-2* If the sending device is offline at the time a notification is received, notifications shall be stored on the network and forwarded once the sending device is online.

**US6-13 As a user, I want to see when the other party is currently writing a Group Chat message.**

- R6-13-1* The other party shall be able to see an “[name from contact list or MSISDN] is typing” notification whenever a new Chat message is being created.

**US6-14 As a user, I want to be notified at any time my device receives a new Group Chat message.**

- R6-14-1* On receiving a Group Chat message, the user shall be notified with graphical and sound elements (similar as the device notifies incoming SMS messages if not stated differently in this document).

*R6-14-2* For audio notifications, device audio related settings shall prevail.

*R6-14-3* Any audible or visual notification shall be suppressed in case the reception is visible on the currently active screen of the device (e.g. if the user is currently on the chat screen with a person and a File Transfer is received).

*R6-14-4* If the device supports a notification LED (for screen-off notification) then this LED shall flash as long as there are unread RCS messages. The colour should differentiate from notifications of other applications, but may be identical for all Operator Messaging services.

**US6-15 As a user, I want notifications of rapidly sequenced incoming Group Chat messages intelligibly aggregated and counted.**

- R6-15-1* Rapid sequence of incoming Group Chat messages in one Group Chat conversation shall be consolidated into one audible notification per Group Chat conversation. Consolidation of visual notifications is not affected.
- R6-15-2* On selection of the visual notification for a single new message or multiple messages from one Group Chat conversation, the user shall be directed to the respective Group Chat message.
- R6-15-3* On selection of the visual notification for two or more new messages from different Group Chats, the user shall be forwarded to the list of (Group Chat) conversations. In this case, the unread message visual identifier shall be removed once the last new message was read. Alternatively, the OEM may handle it differently on the device (e.g. the visual notification disappears already after selecting the notification and seeing the list of Group Chat conversations).
- R6-15-4* The visual notification shall be permanently removed after the user has opened the message.

**US6-16 As a user, I want to be able to mute individual Group Chat conversations which results in silencing any audible notification or vibration on incoming new Group Chat messages or notifications on joining / leaving participants from that specific Group Chat conversation.**

- R6-16-1* The user shall be able to mute selected Group Chat conversations, i.e. no audio or vibrate notification shall be performed on incoming new messages within the selected Group Chat conversation.
- NOTE: This selection does not have any effect on notifications in any other than the selected Group Chat conversation.

**US6-17 As a user, I want to see the subject title and group picture as the identifier of a Group Chat conversation in the list of Chat and Group Chat conversations.**

- R6-17-1* Any Group Chat shall be represented with subject title and group picture (and possibly unread message identifier) in the list of Chat conversations.

**US6-18 As a user, I want conversations which contain unread messages to be differentiated from conversations that contain messages I have seen.**

NOTE: This requirement shall be valid for Messaging for Multi-Device as well.

- R6-18-1* Group Chat conversations shall elevate to the top of the conversation list on reception of a new message.
- R6-18-2* Group Chat conversations with unread messages shall be marked accordingly, e.g. by display of the subject line in bold font and / or an unread message counter.

**US6-19 As a user, I want to receive Group Chat messages from any of the contacts participating in a Group Chat conversation.**

- R6-19-1* Any RCS user shall be able to receive Chat messages that are sent to Group Chat conversations.
- NOTE: Group Chat participants who are blacklisted on the user's device are treated separately.
- R6-19-2* Group Chat messages shall be received straight in the inbox; no hand-shake acceptance shall be required.

*R6-19-3* Any participant of a Group Chat shall only be able to see messages that have been exchanged between the time they joined the Group Chat and when they choose to leave the Group Chat.

NOTE: Group Chat participants who are blacklisted on the user's device are treated separately.

*R6-19-4* It shall not be possible for any participant of a Group Chat conversation to see any messages that have been exchanged before the participant has joined the Group Chat.

**US6-20 As a user, I want to exchange multi-media content (e.g. but not limited to: take an instant picture from camera and send from within the chat) in my Group Chat conversations.**

NOTE: Details on multi-media content are covered by File Transfer incl. Geolocation Push, page 99.

*R6-20-1* The user shall be able to select and send multi-media elements in Group Chat conversations.

*R6-20-2* The user shall be able to receive multi-media elements in Group Chat conversations.

**US6-21 As a user, I want to view my sent and received Group Chat messages in a time-based order.**

*R6-21-1* All messages exchanged within the same Group Chat conversation shall be threaded in the same group chat thread in timely order.

*R6-21-2* The order of messages shall be in line with the order messages have been sent and received on the device.

*R6-21-3* Incoming and outgoing messages shall be displayed interlaced.

*R6-21-4* Outgoing messages shall be inserted into the Group Chat Conversation thread as they have been sent.

**US6-22 As a user, I want to see the timestamp associated with each of my sent and received messages.**

*R6-22-1* The date and time associated with each chat message shall be displayed adjusted to the current device date and time.

*R6-22-2* This timestamp shall be generated for sent messages by the device in a consistent way as timestamps are generated for other device functions, e.g. SMS.

*R6-22-3* Timestamps for received messages shall be based on the UTC timestamp that comes with each message, aligned with the selected device time zone.

**US6-23 As a user, I want all Group Chat conversations to permanently reside on my phone, and I can resume that group whenever I decide to do so.**

*R6-23-1* Any participant in a Group Chat conversation shall be able to send a Chat message to other participants in the Group Chat at any given point in time.

*R6-23-2* If the chat application is closed either by manual user interaction (e.g. by selection of another RCS function, pressing the 'home' key or switch to another application) or phone interaction (e.g. receiving call), the connection to the ongoing Group Chat shall be kept. In this case, the user shall stay in the group, continue to receive incoming new messages and

resume at any point in time. The other participants shall not receive any notification about this procedure.

**R6-23-3** A Group Chat expires in the network when there is no activity in it for a few minutes. However, when this happens, the device shall hide this network behaviour from the user and simulate the experience of a permanent Group Chat, showing the conversation in the Chat history and allowing any subsequent continuation. The following solution shall be implemented:

**R6-23-3-1** Session related information is not shown to the user, i.e. 'Chat closed' shall not be displayed at the UI level.

**R6-23-3-2** Sending a new message shall be enough to continue a Group Chat that has timed out at network level.

**R6-23-3-3** When the user hits 'Send' the Group Chat session is set up and the user's message is also sent.

**R6-23-3-4** When a Group Chat is restarted, no notifications of users joining shall be displayed for participants that were already part of the local participant list. The Group Chat header shall show if any participant is unavailable and shall give access to details of participants.

**R6-23-3-5** The Group Chat shall continue in the existing Chat window. The full history of the session shall be preserved.

**R6-23-3-6** While the Chat is closed at network level, the 'Participants list' should still be expandable in order for the user to be able to see the recipients of their new message.

**US6-24 As a user, I want to maintain multiple Chat and Group Chat conversations in parallel.**

**R6-24-1** The device shall display multiple parallel Chat and Group conversations at any given point in time.

**US6-25 As a user, I want to easily and quickly switch between parallel Chat conversations.**

**NOTE:** These Chat Conversations may be One-to-One or Group Chat Conversations.

**R6-25-1** The device shall allow the user to switch between parallel Chat and Group Chat conversations easily and quickly.

**US6-26 As a user, I want to be able to leave a Group Chat conversation at any point in time. After I left a Group Chat conversation, the conversation thread is still visible in the list of my conversations, but I am neither able to send any messages to that Group nor do I receive any kind of updates from that Group.**

**NOTE:** Re-joining Group Chat conversation once left is only possible if the user is re-invited to that (open) Group Chat. Re-joining a closed Group Chat conversation is not possible.

**R6-26-1** Any participant in a Group Chat conversation shall be able to leave at any point in time.

**R6-26-2** Any participant who has left a Group Chat conversation shall no longer receive any new messages or updates to the participants list.

**R6-26-3** After a Group Chat participant has left, the Group Chat conversation shall still be visible in the list of conversations (if not manually deleted),

containing any messages or participant list updates for the period of participation of the user.

*R6-26-4* It shall be possible for a user to re-join a Group Chat conversation which they explicitly left if they are re-invited by another participant who is still active in the Group Chat.

NOTE This requirement shall only apply to open Group Chats.

*R6-26-5* After leaving a Group Chat, the user shall be informed that they will no longer receive any messages from that Group Chat, and that they have to ask an active Group Chat participant to re-invite if they if the user wants to re-join that Group Chat.

NOTE: This information shall be presented in a non-intrusive way to the user, and the user shall be able to select a “never show again” function.

**US6-27 As a user, I want to use the text editing tools of the device that are available on my device (e.g. but not limited to, copy paste, edit) for Chat messages.**

NOTE: In case of the user trying to paste an image into the text editor the device may ignore the user action.

*R6-27-1* The user shall have the option to select text (e.g. from a message, a website or any other text source) and use text editing tools such as copy & paste to create messages.

**US6-28 As a user, I want to select and delete single and multiple chat messages in a Group Chat thread.**

*R6-28-1* The user shall have the option to delete a single Chat message from a Group Chat conversation.

*R6-28-2* The user should have the option to delete single and multiple Chat messages in from a Group Chat conversation.

**US6-29 As a user, I want to delete complete Group Chat conversations.**

*R6-29-1* The user shall have the option to delete an entire Group Chat conversation. Deleting an entire Group Chat conversation shall automatically trigger leaving the Group Chat.

**US6-30 As a user, I want to be able to forward a single sent or received chat message or multimedia content to one or more contacts.**

NOTE: This may be performed by the user by copying existing message text and pasting into a new Chat message.

*R6-30-1* The user shall have the option to forward a single sent or received Group Chat message or multimedia content to one or more contacts.

NOTE: This function may be executed using the copy and paste text editor function of the device.

**US6-31 As a user, I want to switch to a voice or video call with one of the Group Chat participants by selecting one person from the participants list and initiating the call.**

NOTE: During the voice or video call, the user may make use of the Group Chat application.

*R6-31-1* The user shall have the option to easily access and make a voice call to one of the Group Chat participants. After the call has ended, the user interface should return to the Group Chat conversation.

*R6-31-2* The user shall have the option to easily access and make a video call to one of the Group Chat participants. After the call has ended, the user interface should return to the Group Chat conversation.

**US6-32 As a user, I want to be able to answer any incoming voice or video call during a Group Chat conversation - and resume the Group Chat when the call is finished.**

NOTE: During the voice or video call, the user may make use of the Group Chat application.

*R6-32-1* The user shall be able to receive a voice call when actively engaged in a Group Chat conversation and when the voice call ends, the user interface should return to the Group Chat conversation.

*R6-32-2* The user shall be able to receive a video call when actively engaged in a Group Chat conversation and when the video call ends, the user interface should return to the Group Chat conversation.

**US6-33 As a user, I want my Group Chat messages backed up on the Common Message Store which is trusted and safe.**

*R6-33-1* All Group Chat conversations shall be stored on the Common Message Store.

NOTE: For a participant, only the part of the Group Chat conversation from the moment they are invited until the moment they leave the Group Chat will be stored.

**US6-34 As a user, I want to restore my Group Chat conversations from the Common Message Store (e.g. but not limited to, after wiping device or purchasing a new device).**

*R6-34-1* The user shall have the option to restore Group Chat conversations from the Common Message Store (*e.g. in case of handset replacement*).

**US6-35 As a user, I want to block specific users so that I do not receive any kind of Group Chat message from them anymore. However, I want to be aware that there was a message of a blocked contact to understand the context of the Group Chat. I want to see that even blocked contacts are participating in a Group Chat conversation.**

*R6-35-1* If one or more participants in a Group Chat conversation are on my local device blacklist, these contacts shall appear on the list of Group Chat participants.

*R6-35-2* If the sender of a Group Chat message is on my local device blacklist, the incoming message shall be shown as an anonymous empty placeholder message in the message thread. No visual or audio notification shall be performed for that message.

## 6.3 Technical Information

### 6.3.1 Overview

The group chat service is provided as defined in section 3.4 of [RCC.07].

For the purpose of the following technical implementation of the user stories and service requirements the group chat service is considered as a stand-alone end-to-end service.

[RCC.07] allows service providers to implement the group chat user experience based on SIMPLE IM or CPM. The service provider is able to select the technology via the CHAT

MESSAGING TECHNOLOGY configuration parameter defined in section A.1.3.3. of [RCC.07]. The joyn Crane Group Chat shall be based on OMA SIMPLE IM only. The related CHAT MESSAGING TECHNOLOGY configuration parameter defined in section A.1.4.3. of [RCC.07] has to be set accordingly by the service provider.

[RCC.07] allows service providers to implement the file transfer user experience based on File Transfer over MSRP or File Transfer over HTTP.

For Crane networks the support of Full Store and Forward for Group Chat as defined in section 3.4.4 of [RCC.07] is mandatory.

A more detailed overview of applicable sections of the baseline specification will be provided once the detailed use case analyses identifies the required feature set.

### 6.3.2 Technical Implementation of User Stories and Service requirements

*R6-36-1* For user story US6-1 the following definitions apply:

- The Group Chat service shall be offered to the user if the device configuration authorises the service via the CHAT AUTH, GROUP CHAT AUTH and CONF-FCTY-URI parameters defined in section A.1.3 of [RCC.07].
- The procedures for initiation of a group chat and the conditions for the client to select capable contacts are defined in section 3.4.4. of [RCC.07]. The service provider is able to determine for the client which contacts are capable for a group chat, i.e. chat contacts only, or any contact including non RCS contacts.
- The requirement R6-17-1 is implemented via the IM CAP NON RCS GROUP CHAT and GROUP CHAT BREAKOUT ALLOWED PREFIXES parameters defined in section A.1.3.3 of [RCC.07]. The following clarification of the parameter values of IM CAP NON RCS GROUP CHAT shall be taken into account.

(0): the device is neither allowed to initiate a Group Chat with non RCS users nor to add non RCS users to a Group Chat. (default value)

(2): the device is allowed to initiate a Group Chat with non RCS users but not allowed to add non RCS users to a Group Chat.

- The technical implementation of the closed Group Chat is defined in section 3.4.4.2 of [RCC.07]. To fulfil the requirements in R6-1-8, a Crane RCS client shall prevent initiating a new closed Group chat towards the CONF-FCTY-URI. In addition, the controlling function of a Messaging Server of Crane service providers should block invitations to a closed Group Chat.
- If the client receives an invitation to a closed Group Chat it shall be accepted. The client shall enforce the close Group Chat policy, i.e. it shall not allow the user to add new participants to the group.
- To restart a closed Group Chat according to section 3.4.4.1.7 of [RCC.07], the client shall send an invitation to the stored focus Session Identity. The CONF-FCTY-URI shall not be used for the restarting a closed Group Chat. If the restart of the closed Group Chat fails with SIP 404, then the client should attempt to initiate the Group Chat as an open Group Chat with the stored participants list towards the CONF-FCTY-URI.

- R6-36-2* The subject of a Group Chat conversation as defined in user story US6-2 is implemented in accordance with sections 3.4.4.1.1. and 3.4.4.1.2 of [RCC.07].
- R6-36-3* The client shall allow members of an open Group Chat Conversation to add new participants as defined in section 3.4.4.1.2 of [RCC.07] to fulfil the requirements of user story US6-3.
- NOTE 1: To avoid sending notifications to participants twice in short succession, the conference focus shall briefly delay notifying the existing participants of the “pending” state of the newly added participant to allow for automatic acceptance of the Chat (e.g. because of Store and Forward). In that case the participant’s state will change to “active” almost immediately.
- NOTE 2: The client shall not allow the user to add participants if the maximum allowed number of participants is reached. The maximum allowed number of participants for a Group Chat is determined as defined in sections 3.4.4.1.2 and 3.4.4.1.7 of [RCC.07].
- NOTE 3: The client behaviour to not allow addition of non RCS users to a Group Chat shall be enforced by the service provider by setting of the value of the device configuration parameter IM CAP NON RCS GROUP CHAT.
- R6-36-4* The technical implementation of the clients and the messaging server to provide the Closed Group Chat as defined for user story US6-4 shall be based on section 3.4.4.2 of [RCC.07]. Please refer to the requirements on Closed Group Chat in Crane as defined for R6-1-8.
- R6-36-5* In order to be able to display the list and status of users in a group conversation as required in user story US6-5 each client shall subscribe to the conference event package as defined in section 3.4.4.1.1 of [RCC.07]. The client will be informed by the Messaging Server about the list of participants and their status based on this subscription.
- The user alias for Group Chat users described in requirements R6-5-3 and R6-5-4 is implemented as defined in section 2.5.3.3 of [RCC.07].
- R6-36-6* The client implementation shall ensure that the invitation to a Group Chat does not require explicit user input to accept it as required in user story US6-6. However the service provider is able to define the technical procedure of the client to accept an invitation to a Group Chat by use of the configuration parameters IM SESSION AUTO ACCEPT GROUP CHAT as defined in section A.1.3.3. of [RCC.07].
- R6-36-7* For the requirements of user story US6-7, in order to send text to a conversation while a Group Chat exists the client shall send the message using this session. If no session exists the client shall restart the Group Chat as defined in section 3.4.4.1.7. and send the message to it.
- R6-36-8* The client shall not implement client UI procedures to accept reception of messages or group chat invitations to fulfil the requirements of user story US6-8.
- R6-36-9* The requirements of user story US6-9 is fulfilled by means of the Group Chat Store and Forward functionality (section 3.4.4.3 of [RCC.07]).
- R6-36-10* The implementation of the smilies and emoji in the requirements of US6-10 shall be supported as defined in the documents in the Annex.



- R6-36-11* For the realization of the requirements in user story US6-11 the client shall enforce the max message size for sending messages as defined by the configuration parameter MAX SIZE GROUP IM defined in section A.1.4.3. of [RCC.07]. It is required for service providers to set the value to "999" or more.
- R6-36-12* The Status indication for chat messages and File Transfer sent in the group chat are the same as defined for '1-to-1 Chat', page 76 and 'File Transfer incl. Geolocation Push', page 99.
- R6-36-13* Notifications on delivery status information as defined in R6-12-2 shall be stored and forwarded in the Messaging Server as specified in section 3.4.4.3 of [RCC.07].
- R6-36-14* The requirements for US6-13 to display typing notifications is implemented same as for 1-to-1 Chat as defined in section 3.4.4. of [RCC.07].
- R6-36-15* The requirements for user stories US6-14 through to US6-16 are implemented locally on the device.
- R6-36-16* The subject of a Group Chat Conversation as required in requirement R6-17-1 is implemented as defined in user story US6-2. There is no technical implementation for the share of a group chat picture within the group. The client shall assign the picture locally
- R6-36-17* The requirement of user story US6-18 for Display Notifications is implemented as defined in section 3.4.4.1.5 of [RCC.07].
- R6-36-18* The requirements for user story US6-19, shall be implemented locally on the device. For acceptance of Group Chat sessions the client shall apply the behaviour as defined by the configuration parameters IM SESSION AUTO ACCEPT GROUP CHAT and IM SESSION START. The client shall not apply any UI procedures for the acceptance of the delivery of single messages.
- R6-36-19* For Crane networks multimedia in Group Chat is to be sent only via File Transfer. The Device shall be configured accordingly by the Service Provider.
- R6-36-20* For the requirements in user story US6-21 the client shall support the following procedures:
- It is the responsibility of the Messaging Server to deliver messages in the correct order, so the Client can rely on it when sorting messages. The client shall interleave the sent and received messages in the chronological order.
  - After the client has synchronised with the Common Message Store successfully, then messages shall be sorted in accordance with the time indicated in the CPIM DateTime header value received with message from the Common Message Store.
- R6-36-21* The requirements of user story US6-22 shall be implemented locally on the device.
- R6-36-22* The requirements of user story US6-23 shall be implemented locally on the device based on the Group Chat life cycle definitions in section 3.4.4 of [RCC.07].
- R6-36-23* The requirements of user stories US6-24 and US6-25 shall be implemented locally on the device.

*R6-36-24* The requirements of user story US6-26 shall be implemented as defined in section 3.4.4.1.3.1 of [RCC.07]. If the user wants to leave a group chat while it is inactive, the client shall restart the Group Chat first, as defined in section 3.4.4.1.7 of [RCC.07].

Subsequent invitations to a Group Chat the user has voluntarily left shall be accepted by the client.

*R6-36-25* The requirements of user stories US6-27 through to US6-32 shall be implemented locally on the device.

*R6-36-26* The requirements of user stories US6-33 through to US6-34 are implemented as defined in section 3.4.4.1.8 of [RCC.07] and 'Backup & Restore', page 119, and 'Operator Messaging', page 38.

*R6-36-27* The specific requirement for handling of locally blocked contacts in user story US6-35 appears to be only a UX function to be implemented locally on the device. However with regard to the interactions with Group Chat in the network, the client should treat the blocked contacts as regular contacts.

NOTE: Messages sent to the group will also be delivered to the blocked contact.

### **6.3.3 Backward Compatibility**

joyn Crane clients shall use File Transfer over HTTP for the transfer of a file to a Group if supported by the conference focus as defined in section 3.5.4.8.1 of RCC.07 RCS 5.2. If the conference focus does not support File Transfer over HTTP the client may apply the alternative procedure defined in section 3.4.2.3 of [RCC.07]. In this case the client shall transfer the file sequentially to the participants of the group chat via a single file transfer session.

If a HTTP File Transfer is initiated and one or more of the parties in the Group Chat do not support receiving it (i.e. did not provide the application/vnd.gsma.rcs-ft-http+xml MIME content type in the a=accept-wrapped-types attribute in the SDP that it provided during the Group Chat session set up), the conference focus shall compose a plain text message to those participants explaining that a file was sent to the participants in the chat that cannot be retrieved automatically by the client. That message shall also provide the link to the file to allow retrieving the file manually through the browser.

When receiving the MSRP 200 OK response on the MSRP SEND request used to relay this message, the Messaging Server shall send a positive Delivery Notification to the sender in case such a notification was requested.

Networks supporting earlier versions of joyn will not support Group Chat with non RCS users. Thus the device configuration document will not contain parameters to control Group Chat to non RCS users. The client shall apply the default value and not offer Group Chat to non RCS contacts to the user.

Networks supporting Group Chat to non RCS contacts are advised not to provide the corresponding configuration parameters to Blackbird clients.

If the conference focus of a Group Chat with non RCS users is moving from a supporting service provider to a non-supporting service provider the sending of messages to non RCS users will fail.

### **6.3.4 Configuration Parameters**

For joyn Crane networks the following Group Chat configuration parameter values apply.

Configuration Parameter	Crane Value
MAX_AD-HOC_GROUP_SIZE	Service Provider Configurable
CONF-FCTY-URI	Service Provider Configurable
GROUP CHAT AUTH	"1"
GROUP CHAT FULL STORE FORWARD	"1"
GROUP CHAT INVITE ONLY FULL STORE FORWARD	"0"
IM CAP NON RCS GROUP CHAT	Service Provider Configurable  If the parameter is present only values "0" and "2" are allowed.
GROUP CHAT BREAKOUT ALLOWED PREFIXES	Service Provider Configurable
IM SESSION AUTO ACCEPT GROUP CHAT	"1"
MAX SIZE GROUP IM	Service Provider Configurable

**Table 39: Group Chat configuration parameter values**

## 7 File Transfer incl. Geolocation Push

### 7.1 Description

File Transfer enables transferring files from one RCS device to one or more RCS devices. The main service entry points will be the Chat and Group Chat applications on the phone, but there shall be other service entry points as well. This Service Description Document describes the User Stories, Service Requirements and technical implementation details for the core File Transfer service and all features around the core.

Geolocation Push allows a user to share their current position or selected location with one or more RCS contacts.

Major changes of the Crane PDD compared to the Blackbird PDD are:

- Resizing of video files before sending
- Cancel sending of a file while the send process is still ongoing became a mandatory requirement
- Store & forward for message status notifications
- Notifications for new incoming messages shall be intelligently aggregated
- Use of device LED to signal new files
- Introduction of a Common Message Store
- Allow to share / save incoming File Transfer content

### 7.2 User Stories and Feature Requirements

**US7-1 As a user, I want to transfer files to contacts and receive files from other RCS users.**

**As a user, I want to transfer and receive a file of any file format.**

NOTE: Any file format can be selected and transferred, irrespective of the receiving device capabilities of representing the content in an appropriate way.

*R7-1-1* File Transfer shall allow the transfer of any file from a sending device to one or more recipients.

NOTE: This document describes the File Transfer functionality between RCS users. Other Contacts without RCS may have less functionality available. Please refer to Operator Messaging, page 38.

*R7-1-2* File Transfer shall be capable of transferring exactly one file at a time.

NOTE: The user interface of a device may want to allow multiple selection of files for File Transfer and then process these files as separate File Transfer jobs.

**US7-2 As a user, I want to transfer a file from multiple service entry points on my device.**

*R7-2-1* There shall be a number of service entry points to File Transfer, including, but not limited to, 1-to-1 Chat, Group Chat, Contact Card, and Gallery.

**US7-3 As a user, I want to see the status of any file I sent (including those which have not been delivered (yet)).**

*R7-3-1* File Transfer shall support delivery status notifications per individual file (sender device):

*R7-3-1-1* File Transfer Pending: Waiting to transfer the file to the network (e.g. queuing on device).

*R7-3-1-2* File Transfer in progress: Progress bar that indicates the transfer progress of the file transmission (from sending device to the network).

*R7-3-1-3* Cancelled: The sender shall have the option to cancel the File Transfer during the File Transfer process.

*R7-3-1-4* File delivered: Transmission of the File Transfer request has been successfully completed to the receiving network.

*R7-3-1-5* File downloaded: Automatic or user initiated download of file is complete.

*R7-3-1-6* File Transfer failed: The expected outcome of the operation could not be confirmed by the network.

NOTE: In this case, File Sent or File Delivered status notification has not been received and the device does not attempt to transfer the file anymore. The failed File Transfer event may be re-triggered manually by the sender.

*R7-3-2* If the sending device is offline at the time a notification is received, notifications shall be stored on the network and forwarded once the sending device is online

**US7-4 As a user, I want the option to resize pictures before transferring the file, in order to limit transfer volume, memory need and transfer time.**

NOTE: "resize" means changing the picture size to either a high, medium and low size of the picture.

*R7-4-1* Selecting a picture file format that can be rendered by the sending device shall offer the option to resize the picture to smaller file size in order to

save memory, network load and transfer time. “Resize” means changing the picture resolution.

NOTE: In most cases, users are aware of the use of the picture on receiver side, for instance whether it shall be displayed on small screens only, or whether it may be printed on large scale. This feature provides the user with an option to adopt to these cases.

**US7-5 As a user, I want the option to resize videos before transferring the file, in order to limit the transfer volume, the size of storage needed and the time to transfer the file.**

NOTE: “resize” means changing the resolution to either a high, medium and low format

*R7-5-1* The default resizing option proposed shall be 480p at 1200kbps.

*R7-5-2* Selecting a video file which is of a resolution higher than the default resizing option shall offer the option to resize the video file (Video Resolution) to a smaller file size in order to save memory, network load and transfer time. For each resizing option, the user shall see what the file size would be after that resizing option is applied.

*R7-5-3* When a video is recorded with the specific purpose of sending using File Transfer, the video shall be recorded in 480p at 1200 kbps resolution.

**US7-6 As a user, I don't want to perceive a restriction in file sizes that I want to transfer.**

*R7-6-1* The Service Provider shall be able to configure the File Transfer service to set a maximum file size to be accepted by the File Transfer service.

NOTE: It is recommended that RCS Operators agree on a common file size limit to ensure interoperability at least on a local level.

*R7-6-2* The Service Provider shall be able to configure a warning threshold value. When a user attempts to transfer a file larger than this value, auto-acceptance is not possible.

**US7-7 As a user, I want to transfer a file to multiple users at a time within a Group Chat.**

*R7-7-1* File Transfer within a Group Chat shall transfer the file to all participants of the Group Chat.

*R7-7-2* The ability to send files shall be available independent of whether the Operator supports legacy Group Chat or not.

NOTE 1: Any adaption from standard Group Chat File Transfer for legacy (non-RCS) contacts is done on network level).

NOTE 2: The sender side shall only send the file once over the network in this case.

**US7-8 As a user, I want to transfer a file to multiple users at a time from the gallery or a file browser.**

*R7-8-1* The Operator Messaging service selection shall be made based on capabilities of the participants and cannot be determined before the participants are selected.

*R7-8-2* The Operator Messaging service that is selected shall be identical for all targets of this file transfer.

NOTE: The sender side shall only send the file once over the network in this case

R7-8-3 The file shall be transferred using MMS if all of the following requirements are met:

R7-8-3-1 The selected content is compatible with MMS requirements and

R7-8-3-2 one or more selected recipients are not RCS capable, and

R7-8-3-3 the Operator does not support RCS Group Chat legacy support.

NOTE 1: Sending a file to multiple recipients using MMS shall be possible on the handset in the event that the customer is not provisioned as an RCS user.

NOTE 2: If the selected content is not compatible with MMS service (and cannot be scaled down), the operation shall be interrupted and the user shall be informed that the selected content cannot be sent using MMS.

R7-8-4 The file shall be transferred as RCS File Transfer in Group Chat, if:

R7-8-4-1 All of the selected contacts are RCS capable; a Group Chat shall be created (or, if there is an existing Group Chat with the selected participants, this shall be used) and the file shall be transferred in that Group Chat.

NOTE: This case is independent of whether the Operator supports legacy support for Group Chat or not.

R7-8-4-2 The Operator supports legacy support for Group Chat; a Group Chat shall be created (or, if there is an existing Group Chat with the selected participants, this shall be used) and the file shall be transferred in that Group Chat, irrespective of whether the selected recipients are RCS Group Chat capable or not.

R7-8-5 If the user is an Integrated Messaging user, both RCS Group Chat and MMS are threaded in the same conversation with that group of recipients.

R7-8-6 If the user is not an Integrated Messaging user, RCS Group Chat conversations and MMS conversations are threaded separately on the device.

**US7-9 As a user, I want to be able to cancel files while the sending process has not been completed yet.**

R7-9-1 The device shall provide the user with the option to cancel a File Transfer while the file is still in the process of being sent on the originating leg.

NOTE: Once the File Transfer on the originating leg is completed, there is no way for the sender to stop the process of File Transfer.

**US7-10 As a user, I want to transfer a file with my contacts even when they're temporarily offline (e.g. device switched off). I expect them to receive the file when they come online again.**

R7-10-1 In case the B-Party is currently not registered on the RCS service ("offline"), the request to deliver the file shall be delivered to the B-Party device once the user is registered again on RCS ("online").

NOTE: This requirement refers to the store & forward feature.

R7-10-2 If a user attempts to download a file that has expired from the network storage, they shall be informed that the file is no longer available.

NOTE: This requirement relates to the store & forward feature.

**US7-11 As a service provider, I want to limit how long a file is available on the network for offline users.**

R7-11-1 The Operator shall be able to define the network storage time for File Transfers that have not been downloaded yet.

NOTE: This requirements relates to the store & forward feature.

**US7-12 As a user, I want the device to notify me about new incoming files in a similar way to new incoming messages.**

**As a user, I want to be notified in case of incoming positions / locations.**

R7-12-1 On receiving a file or preview thumbnail, the user shall be notified with graphical and sound elements (in a similar way to how the device notifies about incoming messages).

NOTE: The standard customisation options of the device for incoming notifications shall be available.

R7-12-2 For audio notifications of a new File Transfer request, device settings shall prevail.

R7-12-3 Rapid sequence of incoming File Transfer requests and Chat messages in one Chat conversation shall be consolidated into one audible notification per Chat conversation. Visual notifications are not affected.

R7-12-4 On selection of the visual notification for a File Transfer, the user shall be directed to the respective thumbnail preview (in case of auto-accept is off) or file (in case File Transfer auto-accept is on) within the Chat or Group Chat conversation.

R7-12-5 The visual notification for an incoming File Transfer shall be permanently removed from the notification centre bar, once the thread with the file or thumbnail preview has been opened.

NOTE: Independently of whether the user has clicked the notification or has accessed the thread from the messaging application.

R7-12-6 Any audible or visual notification shall be suppressed in case the reception is visible on the currently active screen of the device (e.g. if the user is currently on the chat screen with a person and a File Transfer is received).

R7-12-7 For notification of a new incoming location or position, the above mentioned requirements shall be valid accordingly.

NOTE: Geolocation Push feature is technically using File Transfer mechanisms.

R7-12-8 If the device supports a notification LED (for screen-off notification) then this LED shall flash as long as there are un-opened RCS File Transfers. The colour should differentiate from notifications from other applications, but may be identical for all Operator Messaging services.

**US7-13 As a user, I want to receive incoming files within a new or existing Chat or Group Chat conversation.**

**As a user, I want sent and received files to be part of the Chat or Group Chat conversation thread in similar order and appearance of chat messages, but representing the transferred content.**

R7-13-1 Incoming files shall be displayed within a new or existing Chat Conversation.

- R7-13-2* Files shall be threaded in the conversation as an event similar to chat messages. The same ruling for order of messages as specified in '1-to-1 Chat', page 76 and 'Group Chat', page 85, shall be applied to files.
- R7-13-3* Chat of Group Chat conversations shall be sorted descending according to the time stamp of the last action (e.g. but not limited to, a received File Transfer, Audio Message or Geolocation Push) within the conversation (i.e. the conversation with the latest event timestamp shall be on top of the list).
- R7-13-4* Chat or Group Chat conversations with unread events (any event that is received within the Chat conversation, including, but not limited to, Chat messages, received files, received Geolocation Push, received Audio Messages) shall be marked accordingly, e.g. by display of subject line in bold font and / or a unread message counter.
- R7-13-5* The user shall have the option to select a file and forward / share the file with contacts from the contact list.
- R7-13-5-1* On the UX level, sharing received content from the chat conversation shall be a straightforward experience.
- R7-13-5-2* Sharing files from the RCS implementation shall not be restricted to RCS services but support all applications with sharing capability that the device OS is aware of.
- R7-13-6* If a shared file is a picture of supported picture format, the user shall have the option to select the file and display in full screen mode.
- R7-13-7* If a shared file is a picture of supported picture format, the user shall have the option to select the file and display in full screen mode.

**US7-14 As a user, I want to see incoming files as a thumbnail preview (or generic icon if content cannot be rendered on receiving device) including file size indication.**

**As a user, I want to trigger file download to my device by selecting the thumbnail preview.**

**As a user, I want to be in control of the acceptance of the File Transfer (individually or for all File Transfer events).**

- R7-14-1* In case "File Transfer Auto-Accept" is set to "OFF":
- R7-14-1-1* The incoming File Transfer presents a thumbnail preview of the file, including file size, on the receiving device first.
- R7-14-1-2* The thumbnail preview shall be a preview of the actual picture (if the file type is a picture in a format that can be rendered by the receiving device), a file type specific icon.
- NOTE: There shall be file type specific icons at minimum for standard RCS content types for Contact Card, Audio Messaging and Geolocation Push or a generic icon.
- R7-14-1-3* Selection of the preview icon on the receiving device shall trigger the download of the full file to the user's device.
- R7-14-1-4* The user shall have the option to delete the thumbnail preview without downloading the content.
- R7-14-2* In case Auto-accept for File Transfer is set to "ON":
- R7-14-2-1* The user shall not have to accept the download for each received File Transfer.



*R7-14-2-2* The file shall be automatically downloaded and shall be accessed in the Chat conversation.

*R7-14-3* The Operator shall have the option to set the default value for “File Transfer Auto Accept” via the device provisioning process.

*R7-14-4* The user shall have the option to select or deselect “File Transfer Auto-Accept”.

**US7-15 As a user, I want to have a visible notification about the status of received files.**

*R7-15-1* File Transfer shall support status notifications per individual file (receiver device):

*R7-15-1-1* In case of auto accept off: Thumbnail preview received – indication that file is waiting for download trigger on receiving network.

*R7-15-1-2* File Transfer in progress on receiving device – progress bar that indicates the transfer of the file (from network store to receiving device) after download was triggered.

*R7-15-1-3* Cancelled – the receiver shall have the option to cancel the File Transfer during the File Transfer process.

*R7-15-1-4* File downloaded.

*R7-15-1-5* File Transfer failed – File Transfer could not be confirmed successfully completed by the network and client does not attempt to retrieve the file any further. (In case of File Transfer store & forward function is available, the user may be able to manually re-trigger File Transfer and resume from where the File Transfer failed. In case of no File Transfer store & forward, the user has to option to ask the sender to re-send the file).

**US7-16 As a user, I want to transfer a contact information from the contact list to other RCS users.**

*R7-16-1* Selecting “Send Contact” from a Contact Card shall send the Contact details in vcf-format to a recipient that shall be selected.

NOTE: vCard as the default format, details in the Annex A1 Personal Card format, page 178.

*R7-16-2* Devices shall be capable to render vCard files in .vcf format according to RCS standard (see Annex A1 ‘Personal Card format’, page 178) and offer to store received Contacts in the device contact list.

**US7-17 As a user, I want to be able to resume interrupted File Transfers.**

NOTE: On sending and receiving side.

*R7-17-1* If a File Transfer has been interrupted on the sending or receiving side (e.g. in case of, but not limited to, if device lost radio coverage), the File Transfer shall resume automatically from the point of interruption once the required conditions have been restored (e.g. device is back in radio coverage).

*R7-17-2* If the receiver’s device does not have enough storage space to download the full file:

*R7-17-2-1* A notification shall be provided to the receiver before downloading the full file.

*R7-17-2-2* Storage space shall be freed up manually by the receiver before download attempt shall be possible.

*R7-17-2-3* The user shall have the option to re-start the file download as long as the Operator storage time (as in R7-11-1) has not expired.

**US7-18 As a service provider, I want to be able to limit the size of the files that are transferred.**

*R7-18-1* If the sending device attempts to send a file larger than the limit for File Transfer, the A-Party shall be notified that the file exceeds the size limit supported by the service.

NOTE: In order to avoid user disappointment caused by different maximum allowed file sizes on different networks, it is recommended to align maximum file size at least on national level across Operators.

**US7-19 As a user, I want to block specific users so that I do not receive any kind of files from them anymore.**

*R7-19-1* Incoming File Transfers from contacts on the local device blacklist

*R7-19-1-1* Shall be ignored by the device.

*R7-19-1-2* The user shall not be made aware of any File Transfer attempts from blacklisted contacts.

*R7-19-1-3* No notifications or thumbnail previews shall be displayed.

*R7-19-1-4* In case the user has selected "File Transfer Auto-Accept" as a setting on their device, any incoming File Transfer attempts from blacklisted contacts shall not be auto-accepted.

**US7-20 As a user, I want to administrate File Transfers in Chat and Group Chat conversations intuitively.**

*R7-20-1* The user shall have the option to delete File Transfer events (outgoing or incoming) from a Chat or Group Chat conversation:

*R7-20-1-1* Deleting a single File Transfer directly from the chat conversation.

*R7-20-1-2* Delete multiple File Transfer events (with or without other associated events in the conversation such as Chat messages).

*R7-20-1-3* Deleting a File Transfer from the Chat or Group Chat conversation shall delete the entry in the conversation thread and the Operator Store (e.g. Common Message Store).

*R7-20-2* If received or sent files are automatically stored on a device or online repository (e.g. an RCS gallery on the device picture gallery), then deleting the File Transfer events from the conversation thread does not automatically delete any files from this repository. In case the user permanently wants to delete this content, separate user action is required (as per individual device operation).

**US7-21 As a user, I want my Operator to store my sent and received files safely and securely.**

*R7-21-1* Any successfully sent and received files shall be stored on the network.

NOTE: This is Common Message Store feature.

*R7-21-2* Details of the network storage shall be controlled by the individual Operator, including, but not limited to:

R7-21-2-1 Total volume of storage capacity per user.

R7-21-2-2 Maximum storage time of conversations, messages, files etc.

**US7-22 As a user, I want to restore my sent and received files from the network Operator storage**

NOTE: Central File Storage, e.g. in case of handset replacement.

R7-22-1 The user shall have the option to restore transferred files from the network storage (e.g. in case of handset replacement).

**US7-23 As a user, I want the ability to share my current position or a selected location with any of my contacts (RCS contacts or legacy non-RCS contacts).**

NOTE 1: Pre-requisite: The Geolocation Push Service relies on a map function on the sending device that supports the RCS functionalities.

NOTE 2: Pre-requisite: There is no intention to build positioning or map functions within the RCS standard.

R7-23-1 Chat, Group Chat and In-Call sharing shall be service entry points to initiate a Geolocation Push.

R7-23-2 There may be other service entry points available on the device to initiate a Geolocation Push (e.g. Contact Card, call log).

R7-23-3 The Geolocation Push Service should offer a 'legacy mode' to send positions or locations to non-RCS recipients or recipients with RCS versions that do not support Geolocation Push.

NOTE: Legacy mode may be provided by a link to online map display or a 'screenshot' with map picture.

**US7-24 As a user, I want to preview an automatically detected position on map and have the ability to change this manually before sending.**

R7-24-1 If the current position shall be sent, the location shall be automatically detected and suggested to the end user.

R7-24-2 The user shall have the option to preview and correct the automatically detected position on a map view before sending.

R7-24-3 The Geolocation Push service shall support sending of a location that was picked from the map.

**US7-25 As a user, I want to tag positions or locations with a text field.**

R7-25-1 The user shall have the option to tag a position or location with a free text field before sending.

**US7-26 As a user, I want to receive positions / locations in a map view. As a user, I want to use standard map functions e.g. "guide me to..." feature.**

NOTE: These functions are not provided by the RCS implementation.

R7-26-1 When receiving a position or location, the RCS Geolocation Push user shall have the ability to see the position / location on a map.

R7-26-2 When receiving a position or location, the RCS Geolocation Push user shall be able to see any tags that were added by the sender.

*R7-26-3* When receiving a position or location, the RCS Geolocation Push user shall be able to use map and navigation tool functions such as 'guide me to...' feature.

NOTE: The compliance with this feature may depend on the capabilities of the receiving handset.

*R7-26-4* When receiving a position or location, the legacy (non-RCS or RCS without Geolocation Push Service) user should receive either a link that opens a map application on the web, or a map image.

## 7.3 Technical Information

### 7.3.1 Overview

The File Transfer service is provided as defined in section 3.5 of [RCC.07]. There are a number of technologies to provide the File Transfer user experience. It is a service provider option which File Transfer technology is deployed.

The selection of the transfer technology for files is derived by the client as result of the capability discovery as defined in sections 2.6.1.1.2, 2.6.1.2.3 and 3.5.4.8.1 of [RCC.07].

For Crane networks file transfer technology shall be File Transfer via HTTP. File Transfer via MSRP will be supported for backward compatibility reasons with no support of File Transfer Resume, Store and Forward and Thumbnails. Therefore only the capabilities for File Transfer and File Transfer via HTTP of section 2.6.1.1.2 of [RCC.07] will be used.

### 7.3.2 Technical Implementation of User Stories and Service requirements

*R7-27-1* For the requirements of user story US7-1 the following definitions apply:

- The File Transfer service shall be offered to the user if the device configuration authorises the service via the PROVIDE FT parameter defined in section A.1.5 of [RCC.07].
- The ability of the user to send files to a contact depends on the result of the capability discovery as defined in section 2.7 of [RCC.07].

*R7-27-2* The requirements of user story US7-2 shall be implemented locally on the device.

*R7-27-3* The requirements of user story US7-3 shall be implemented as follows. The implementation depends on the file transport technology used:

- **Pending:**

For File Transfer over MSRP; when the user presses ENTER to send the message until the first SIP success response is received from the network.

For File Transfer over HTTP; when the user presses ENTER to send the message until the first HTTP POST success response is received from the network.

The File Transfer may be in this state for some time when the user is NOT registered with the IMS core (e.g. offline or airplane mode).

- **Progress:**

For File Transfer over MSRP; from the reception of the first SIP Response is received from the network until the final MSRP 200 OK is received.

For File Transfer over HTTP; from the reception of the first success HTTP response from the network until a provisional response is received from the network for the SIP INVITE or a MSRP 200 OK is received from the network for the chat message carrying the File Transfer via HTTP message body content.

- **Cancelled:** If the user has cancelled the File Transfer and the client did invoke the user story US7-9.
- **Sent:**  
For File Transfer over MSRP; when receiving the final MSRP 200 OK.

For File Transfer over HTTP; when receiving the provisional response for the SIP INVITE or a MSRP 200 OK for the chat message transferring the File Transfer via HTTP message body.

- **Delivered:**  
For File Transfer over MSRP without store and forward; same as sent.

For File Transfer over MSRP with store and forward, when receiving the Delivery Notification

For File Transfer over HTTP, when receiving the Display Notification

- **Failed:**  
When a notification that the file has been sent is not received and the device does not attempt to transfer the file anymore.

NOTE: The A-Party Operator shall ensure that duplication of messages within the Operator Messaging application is avoided within their network control.

*R7-27-4* Notifications on delivery status information as defined in R7-3-2 shall be stored and forwarded in the store & forward server as specified in section 3.3.4.1.5 of [RCC.07].

*R7-27-5* The requirement R7-4-1 shall be implemented locally on the device. When transferring a large image using File Transfer (regardless of whether it is HTTP or MSRP based), as described in R7-5-1 a client shall check whether it is possible to reduce the size of the image. It may use following mechanism for this:

- The default scale factor F for the image shall be,  $F = \min(1280/w, 1280/h, 1.0)$ .

NOTE: The w (width) and the h (height) shall be used in pixels for the calculation.

- If the factor (F) is 1, the original image shall be transferred.
- Otherwise, the size of the image shall be reduced using following algorithm:
- Scale both dimensions by the same factor F (same for width and height so the aspect ratio is maintained).
- Compress as JPG with q=75%
- Compare the new image size with the original, and only offer the possibility to send a resized image if the resulting file is smaller than the original one

*R7-27-6* The requirement of user story US7-5 shall be implemented locally on the device.

- R7-27-7* The file size limits required in the user story US7-6 are configured via the FT MAX SIZE, FT WARN SIZE and optionally FT MAX SIZE INCOMING parameters defined in section A.1.5 of [RCC.07].
- R7-27-8* For the technical implementation of user story US7-7 the following applies. For File Transfer in a Group Chat session only the File Transfer over HTTP technology will be used in Crane networks. Thus the conference focus located in Crane networks will indicate support of File Transfer over HTTP as defined in section 3.5.4.8.3 of [RCC.07].
- R7-27-9* The requirements in use case US7-8 shall be implemented locally on the device based on the following mechanisms:
- For the requirement R7-8-3-1 the client shall check whether the selected media content consists or can be locally transcoded to formats and codecs defined in [OMA-MMS-CONF].
- For the requirements R7-8-3-2 and R7-8-4-1 the RCS capability shall be discovered based on the RCS capability discovery defined in section 3.3.1. The "online status" of the recipients shall not be taken into account in this context
- For the requirement in R7-8-3-3, R7-8-4-2 the client shall check the value of the configuration parameter IM CAP NON RCS GROUP CHAT to determine whether the service provider supports Group Chat for legacy recipients. It is supported by the service provider if the value is set to "1" or "2".
- If the Service Provider supports Group Chat for legacy recipients then each address of non RCS contacts shall be matched against the list in GROUP CHAT BREAKOUT ALLOWED PREFIXES. If all recipient addresses match the list, then the file can be transferred via Group Chat.
- R7-27-10* The technical implementation of the cancelation of the File Transfer via MSRP as required in user story US7-9 is defined in section 3.5.4.3 of [RCC.07]. A File Transfer via HTTP shall be cancelled by interruption of the ongoing HTTP transfer flow at the time of user input.
- R7-27-11* The technical implementation of File Transfer store and forward of user story US7-10 is defined in sections 3.5.4.7 and 3.5.4.8 of [RCC.07]. The file will remain stored for a period determined based on service provider policy fulfilling the requirement in R7-11-1.
- R7-27-12* The requirement of user story R7-11-1 is provided by a service provider policy on the messaging server or the HTTP content server.
- R7-27-13* The requirements of user stories US7-12 and US7-13 shall be implemented locally on the device.
- R7-27-14* The client's File Transfer auto accept behaviour defined in requirements of user story US7-14 are controlled via the FT AUT ACCEPT parameter defined in section A.1.5 of [RCC.07].
- The requirements of the user story US7-14 related to thumbnail preview are implemented for File Transfer over MSRP as defined in section 3.5.4 of [RCC.07] and for File Transfer over HTTP as defined in section 3.5.4.8 of [RCC.07]. For File Transfer over MSRP to offline users (store and forward) thumbnails are not supported as defined in section 3.5.4.7.2 of [RCC.07].
- R7-27-15* The requirements of user story US7-15 shall be implemented locally on the device.

- R7-27-16* The transfer format for personal cards of user story US7-16 is defined in section 3.5.4.9.1 of [RCC.07].
- R7-27-17* The requirement to resume interrupted File Transfers of user story US7-17 shall only be supported if File Transfer over HTTP is used as defined in section 3.5.4.8 of [RCC.07].
- R7-27-18* The file size limits defined in the user story US7-18 are configured via the FT MAX SIZE parameter defined in section A.1.5 of [RCC.07].
- R7-27-19* The user story US7-19 will be implemented as defined in section 3.5.4.1 of [RCC.07].
- R7-27-20* The administration of File Transfers defined in user story US7-20, US7-21 and US7-22 in conjunction with the Common Message store is defined in section 3.5.4.8.6 of [RCC.07] for File Transfer over HTTP and [RCC.09] for File Transfer over MSRP.
- R7-27-21* The requirements of the user stories from US7-23 to US7-26 are implemented via the Geolocation PUSH feature defined in section 3.10 of [RCC.07].

### 7.3.3 Configuration Parameters

For joyn Crane networks the following File Transfer configuration parameter values apply.

Configuration Parameter	Crane Value
PROVIDE FT	"1"
FT MAX SIZE	Service Provider Configurable
FT WARN SIZE	Service Provider Configurable
FT THUMB	"0"
FT STANDFWD ENABLED	"0"
FT CAP ALWAYS ON	"0"
FT AUT ACCEPT	Service Provider Configurable
FT HTTP CS URI	Service Provider Configurable
FT HTTP CS USER	Service Provider Configurable
FT HTTP CS PWD	Service Provider Configurable
FT DEFAULT MECH	"HTTP"

**Table 40: File Transfer configuration parameter values**

## 8 Audio Messaging

### 8.1 Description

The Audio Messaging feature allows RCS users to send Audio Messages to one or more RCS users at a time. Audio Messaging provides a new dimension of communication using the spoken voice to convey a message, allowing the recipient to listen to the message within their RCS interface. The handling of Audio Messaging files follows the rules of File Transfer as described in File Transfer incl. Geolocation Push with the following refinements detailed below.

The Audio Messaging feature is new to Crane, and did not exist in Blackbird.

## 8.2 User Stories and Feature Requirements

### **US8-1 As a user, I want to record and send an Audio Message to one or more of my RCS contacts at a time.**

*R8-1-1* An RCS user with the Audio Messaging feature will be able to see which of their contacts can receive Audio Message files.

NOTE: This is not based on a specific Audio Messaging capability, but the ability of the user to support RCS File Transfer as per 'Capability Discovery and Service Availability'.

*R8-1-2* It shall be possible to create and send an Audio Message in Chat and Group Chat conversations.

*R8-1-3* Audio Messaging shall use File Transfer Store & Forward as defined in the File Transfer section.

*R8-1-4* Audio Messaging service shall be capable of sharing exactly one Audio Message at a time.

*R8-1-5* The Audio Message shall stay within limits of the File Transfer maximum size limits as defined in the File Transfer section.

*R8-1-6* Interruptions in transfer of Audio Messages shall be handled as defined in the File Transfer section.

### 8.2.1 Sending Audio Messages

*R8-1-7* Audio Messaging shall be available from the following service entry points:

*R8-1-7-1* It shall be possible to create and send an Audio Message to an RCS contact from an existing 1-to-1 Chat or Group Chat session.

*R8-1-7-2* A UI entry point of the contact card of an RCS contact shall allow the possibility of creating and sending of an Audio Message.

*R8-1-7-3* A UI entry point of the messaging application shall allow the possibility of creating and sending of an Audio Message.

*R8-1-7-4* A UI entry point from the call log or call history for RCS contacts shall allow the possibility of creating and sending of an Audio Message.

*R8-1-8* Audio Messaging within a Group Chat shall transfer the Audio Message to all participants in the Group Chat.

NOTE: The sender side shall only send the file once over the network in this case.

*R8-1-9* Audio Messages are created by a simple user interaction e.g. pressing or holding down a soft key or button to record the message. Once the soft key or button is pressed again or released, the message recording is terminated and the Audio Message may be presented to the sender for playback and/or sending.

*R8-1-10* Audio Messaging shall support status notification per individual Audio Message as described in requirement R7-15-1.

*R8-1-10-1* Audio Message transfer pending: Waiting to transfer the Audio Message to the network (e.g. queuing on device).

*R8-1-10-2* Audio Message transfer in progress: Progress indicator that displays the transfer progress of the Audio Message transmission (from sending device to the network).



- R8-1-10-3* Cancelled: Presented when the sender has chosen to cancel the Audio Message sending during the transfer process.
- R8-1-10-4* Audio Message delivered: Transmission of the underlying File Transfer request has been successfully completed to the receiving network.
- NOTE: On receiving side, the Audio Message is either ready for download or has been downloaded.
- R8-1-10-5* Audio Message downloaded: Either an automatic or user-initiated download of the Audio Message is complete.
- R8-1-10-6* Audio Message transfer failed: The sending device does not attempt to send the file to the network anymore (however sending may be re-triggered manually by the user).
- R8-1-11* If the sending device is offline at the time a notification is delivered, notifications shall be stored on the network and forwarded once the sending device is online again.
- R8-1-12* The sender shall be able to cancel the sending of an Audio Message before transfer is complete in accordance with requirements in the 'File Transfer incl. Geolocation Push' section.
- R8-1-13* If a sender is interrupted when they are recording an Audio Message, e.g. by an incoming call, then the recording shall stop, and the recording that was made shall be held in the device for later use.
- R8-1-14* Sent Audio Messages shall be displayed and available for playback from a Chat conversation which is associated with the participant(s) concerned.
- R8-1-14-1* Audio Message recording shall be limited to a maximum length of ten minutes.
- NOTE: Operators should consider this maximum length when setting the maximum file size supported by a File Transfer.
- R8-1-15* During Audio Message recording, a progress bar or countdown timer may be shown to indicate how long the user is able to record for before recording is stopped automatically and the next step in the Audio Message sending process is followed.
- R8-1-16* The limit shall be based on the maximum Audio Message recording duration which shall be either ten minutes or a duration based on the maximum file size supported by the Operator, whichever is smaller).
- R8-1-17* Once the maximum Audio Message duration or File Transfer maximum size limit has been reached during a recording, the recording shall stop and the user shall be informed that the message has reached its limit. The Audio Message sharing process shall then continue as if the user had chosen to stop recording manually.
- R8-1-18* The limits imposed by the maximum duration and maximum file size of the Audio Message recording shall not affect the quality of the audio recording. I.e. if the maximum file size does not accommodate a duration of ten minutes in the handset's standard recording format, the recording shall not be carried out at a lower quality to guarantee a ten minute length, but a shorter duration limit shall apply.

## 8.2.2 Notification on Receiving Audio Messages

**US8-2 As a user, I want to be able to receive and listen to Audio Messages that are shared with me as part of a 1-to-1 Chat or Group Chat session.**

- R8-2-1* Notifications on reception of an Audio Message or preview icon shall be in line with the according requirement/s in the File Transfer section.
- R8-2-2* A new Audio Message notification may look different from a new Chat message or File Transfer notification in order to indicate it as being an Audio Message.
- R8-2-3* Sorting of Chat and Group Chat conversations on new incoming Audio Messages shall be in line with the according requirement/s in the File Transfer section.
- R8-2-4* Selecting a visual notification shall trigger the appropriate action according to requirements in the File Transfer section.

## 8.2.3 Receiving Audio Messages

- R8-2-5* For Audio Messaging, the rules of File Transfer Auto-Accept shall be in line with the according requirement/s in the File Transfer section.
- R8-2-6* A user will be notified of Audio Messages sent to them whilst they were offline as soon as they are online again.
- R8-2-7* Incoming Audio Messages from contacts on the local device blacklist shall follow requirement R7-19-1.
- R8-2-8* If the receiving device does not have enough space to store the incoming Audio Message, the regulations in requirement R7-17-2 shall apply.
- R8-2-9* When a customer plays back an Audio Message, it shall be played through the handset's internal earpiece (telephone speaker) or through any other currently active audio output.
- R8-2-10* There shall be an option for the user to switch the Audio Message playback to the handset's loudspeaker during playback of the message.

**US8-3 As a user, I want to find my Audio Messages as part of the Chat conversation with a specific contact or Group Chat.**

- R8-3-1* It shall be possible to delete Audio Messages from a conversation thread according to requirements defined for files in the File Transfer section.
- R8-3-2* Audio Messages shall be stored on a central Operator storage in accordance with requirements defined in the File Transfer section.
- R8-3-3* Audio Messages shall display an Audio Messaging specific icon in the Chat or Group Chat conversation. The Audio Message icon shall provide a clear visual association with the Audio Message file type, so that a user shall easily identify it as a sound file and shall understand that clicking on it will lead to download and/or playback of an Audio Message.
  - R8-3-3-1* This icon shall be visually distinguishable from a music file icon.
- R8-3-4* Audio Messages shall be available for playback from the Chat or Group Chat conversation by sending and receiving parties.
- R8-3-5* Audio Messages shall be saved in the conversation history along with Chat messages and files in a chronological order (as per ordering requirements specified in Chat and Group Chat sections).

- R8-3-6 Audio Messages shall be displayed with information on the message's time and date and duration.
- R8-3-7 In the case of Multi-Device, requirements in the File Transfer section, shall apply.
- R8-3-8 Incoming Audio Messages shall be represented in Chat conversations in accordance with requirements in the File Transfer section.
- R8-3-9 Status notifications for incoming Audio Messages shall be supported in accordance with requirements in the File Transfer section.

### 8.2.4 Implementation Examples

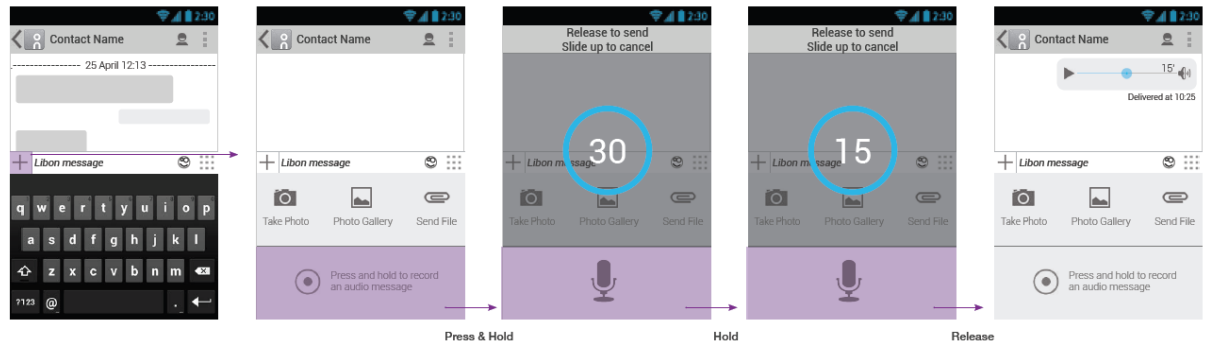


Figure 14: Sending an Audio Message

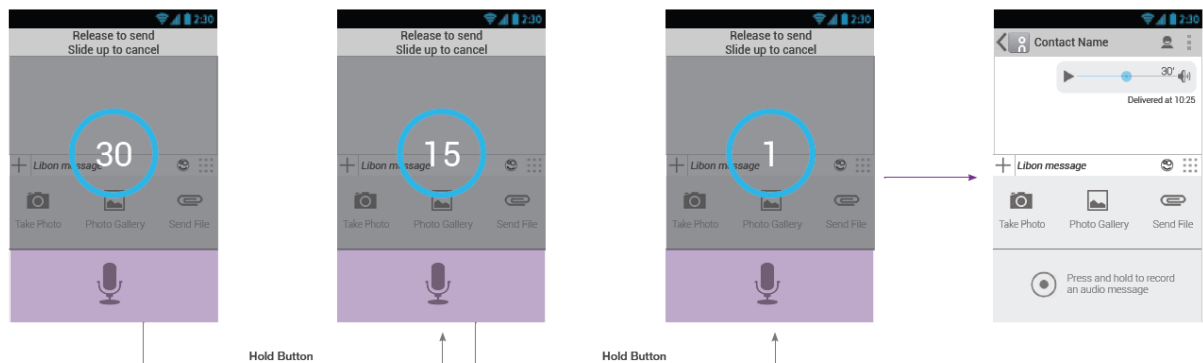


Figure 15: Stopping recording of an Audio Message when maximum duration is reached

## 8.3 Technical Information of User Stories and Service requirements

### 8.3.1 Overview

An Audio Message is a specifically formatted file as per section 3.11.4.1 of [RCC.07] that is recorded on the sender's device using the Adaptive Multi-Rate (AMR) codec and exchanged with contacts via the File Transfer feature.

Audio Message is a File Transfer specific content type as specified in sections 3.5.1.1.2 & 3.5.4.9.2 of [RCC.07].

As such, Audio Messaging uses the procedure defined for File Transfer, as per [RCC.07] section 3.5, to exchange Audio Messages such as:

- Procedures for handling File Transfer interruptions and failures,
  - Use of Delivery Notifications
  - Rules for Auto-Accept
  - Use of a local device blacklist
- Rules for managing shortage of space for local storage

Any contact having the File Transfer capability is seen as being compatible with Audio Messaging.

An Audio Message is identified via its format (section 3.11.4.1 of [RCC.07]) and shall be displayed accordingly by the UI. A specific icon, pre-embedded in the device, shall be associated to the Audio Message.

The content of the Audio Message can be played directly from the Chat application upon user action as indicated by the File Disposition being set to 'render' (see section 3.11.4.2.2. of [RCC.07]).

The maximum length of an Audio Message is controlled by the Service Provider via the MAX RRAM DURATION parameter defined in section A.1.16 of [RCC.07]. The default value of this parameter is 600 seconds (10 minutes).

### 8.3.2 Requirements matching

- R8-4-1* Audio Messaging shall be done as described in section 3.11 of [RCC.07].
- R8-4-2* Requirement R8-1-1 relies on the RCS Capability Discovery feature as per Capability Discovery and Service Availability page 27. No specific "Audio Messaging" capability (tag or service) is added for this feature. As Audio Messaging relies on the File Transfer mechanism, support of Audio Messaging is derived from the support of the File Transfer capability (refer to Table 33 of [RCC.07]).
- R8-4-3* As a file can be sent to one or more contacts, requirement R8-1-2 is covered.
- R8-4-4* As Audio Messaging is based on the File Transfer mechanism as per [RCC.07] section 3.5, it inherits from the File Transfer features:
- Store and forward is one of these features, hence, requirement R8-1-3 is covered.
  - Interruptions in transfer of Audio Messages, hence, requirement R8-1-6 is covered.
- R8-4-5* Requirement R8-1-4 shall be implemented locally on the device.
- R8-4-6* To stay within limits of the File Transfer maximum size, as required in R8-1-5, the service provider shall configure the MAX RRAM DURATION parameter defined in section A.1.16 of [RCC.07] to an adequate value (i.e. a file encoded with the highest encoding quality for the maximum duration gives a lower resulting file size in Kilobyte than the FT MAX SIZE parameter value).

#### 8.3.2.1 Sending Audio Messages

- R8-4-7* Requirement R8-1-7 and its sub requirements are UI related and shall be implemented locally on the device.

- R8-4-8* To fulfil requirement R8-1-8, Audio Messaging uses the procedure defined for File Transfer, as per 'File Transfer incl. Geolocation Push' to exchange Audio Messages to a group of contacts.
- R8-4-9* Requirement R8-1-9 shall be implemented locally on the device.
- R8-4-10* Requirement R8-1-10 and its sub requirements are covered via the File Transfer corresponding requirements (see 'File Transfer incl. Geolocation Push').
- R8-4-11* Notifications on delivery status information as defined in R8-1-11 shall be stored and forwarded in the store & forward server as specified in section 3.3.4.1.5 of [RCC.07].
- R8-4-12* Requirement R8-1-12 is covered by the ability to cancel a File Transfer (see 'File Transfer incl. Geolocation Push').
- R8-4-13* Requirement R8-1-13 shall be implemented locally on the device.
- R8-4-14* As an Audio Message is a file, it shall be part of a Chat conversation as required by requirement R8-1-14. The content of the Audio Message can be played directly from the Chat application upon user action. This is indicated by the File Disposition being set to 'render' (see section 3.11.4.2.2. of [RCC.07]):
- For FToHTTP, the File Disposition is located in the *file-disposition* attribute of the file-info element of the main file.
  - For FToMSRP, the File Disposition is the File-Disposition SDP attribute as described in [RFC5547].
- R8-4-15* Requirement R8-1-14-1 sets a limit of ten minutes for a recorded Audio Message. This is achieved by setting the MAX RRAM DURATION parameter defined in section A.1.17 of [RCC.07] to 600 (seconds).
- R8-4-16* Requirements R8-1-15, R8-1-16, R8-1-17 and R8-1-18 shall be implemented locally on the device, taking into account the MAX RRAM DURATION parameter defined in section A.1.16 of [RCC.07].

### 8.3.2.2 Notification on Receiving Audio Messages

- R8-4-17* As an Audio Message is a file (see 'File Transfer incl. Geolocation Push', page 99):
- Notifications shall be triggered, hence, requirement R8-2-1 is covered.
  - Sorting as per requirement R8-2-3 is covered.
  - Action resulting to the selection of a visual notification as per requirement R8-2-4 is covered.

*R8-4-18* Requirement R8-2-2 shall be implemented locally on the device.

### 8.3.2.3 Receiving Audio Messages

- R8-4-19* As an Audio Message is a file:
- It shall comply with the rules of File Transfer Auto-Accept as described in 'File Transfer incl. Geolocation Push', fulfilling R8-2-5.
  - The Store and forward mechanism as defined in 'File Transfer incl. Geolocation Push', will take care of requirement R8-2-6.
  - The local blacklist mechanism as defined in 'File Transfer incl. Geolocation Push', will take care of requirement R8-2-7.

- Management of local storage space as required in 'File Transfer incl. Geolocation Push', will take care of requirement R8-2-8.

*R8-4-20* Requirement R8-2-9 shall be implemented locally on the device.

*R8-4-21* Requirement R8-2-10 shall be implemented locally on the device.

#### **8.3.2.4 Audio Messages are part of the Chat Conversation with a specific contact or Group Chat**

*R8-4-22* As an Audio Message is a file:

- Deletion as required in File Transfer incl. Geolocation Push, is supported, fulfilling requirement R8-3-1.
- Storage in the Common Message store as defined in 'File Transfer incl. Geolocation Push', is supported, fulfilling requirement R8-3-2, R8-3-5 and R8-3-7.
- Availability of Audio Messages from the Chat and Group Chat conversation follows the one defined for File Transfer as required in 'File Transfer incl. Geolocation Push', fulfilling requirement R8-3-4.
- Audio Messages are represented in Chat Conversations, fulfilling requirement R8-3-8.
- Status notifications for incoming Audio Messages shall follow the status notification for incoming File Transfer request as required in 'File Transfer incl. Geolocation Push', page 99 and fulfilling requirement R8-3-9.

*R8-4-23* Requirement R8-3-3 shall be implemented locally on the device. The Audio Messaging icon has to be embedded in the device.

*R8-4-24* Regarding requirement R8-3-6, the message's time and date information are retrieved from the corresponding elements conveying the File Transfer request as per '1-to-1 Chat', 'Group Chat' and 'File Transfer incl. Geolocation Push'. When using the FToHTTP technology, the duration is retrieved from the <playing-length> element of the File Transfer via HTTP message body as defined in Table 76 of [RCC.07]. When using the FToMSRP technology, the duration may be derived by the Client via an extrapolation from the size of the AMR file.

*R8-4-25* A file being identified as an Audio Message, according to its format defined in section 8.3.1 (Overview) shall be associated with a specific icon embedded in the Client.

### **8.3.3 Backward compatibility**

#### **8.3.3.1 Legacy network**

A Crane device on a legacy network will not get the Crane specific configuration parameters. For Audio Messaging, MAX RRAM DURATION will not be set. A Crane device shall then take into account the default value (10 minutes).

The Audio Messaging being based on (legacy) File Transfer mechanism, a Crane device will be able to use this feature on a legacy network.

### 8.3.3.2 Legacy client

A legacy client is not able to send Audio Messages, however, it may receive Audio Messages via File Transfer request. Depending on its support of the file format and its support of AMR decoding, the legacy client may or may not be able to read the message.

### 8.3.4 Configuration Parameters

Configuration parameter	Description
MAX RRAM DURATION	Service Provider Configurable The resulting file size shall not exceed the maximum file size as defined in FT MAX SIZE

Audio Messaging is based on the File Transfer technology, parameters from section 7.3.3 are also applicable.

## 9 Backup & Restore

### 9.1 Description

Backup & Restore shall allow users to automatically store messages and message content stored on the network and restore those in case of e.g., but not limited to, handset exchange or reset to factory settings. It is expected that the infrastructure components that are used for this function will allow extension to multiple devices being used by the same user identity.

The whole section is a new addition in Crane.

### 9.2 User Stories and Feature Requirements

**US9-1 As an RCS user, I want to replace my handset with another RCS capable device or ‘factory reset’ my RCS device without losing all my messages and message content.**The operator shall be able to implement a network storage that allows to backup and restore messages and message content (including sent message status information and the message service indicator) seamlessly.

*R9-1-2* In the case the user changes their or resets their device to factory status, the device shall restore all messages and message content from the network storage.

*R9-1-3* The operator shall be able to configure devices to enable or disable the availability the option for backup and restore for their users.

NOTE: ‘Messaging for Multi-Device’ as defined in [RCC.61] is not supported in the scope of Crane and has been deferred to the next release.

### 9.3 Technical Information

#### 9.3.1 Overview

Backup and Restore requires the deployment of a Common Message store in the network and a dedicated Message Store client on the device as defined in [RCC.09] and [RCC.11].

Client interactions with the Common Message store shall follow the procedures described in sections 3.2.1.5, 3.2.4.7, 3.2.6.2, 3.2.6.3 and Annex B.4. of [RCC.07].

### 9.3.2 Technical Implementation of User Stories and Service requirements

- R9-2-1* Requirement R9-1-1 shall be fulfilled by the procedures described in section 9.3.1 of this document.
- R9-2-2* For requirement R9-1-2, the reset to factory status shall be implemented locally on the device. If backup and restore is enabled for the user, the client shall connect to the CMS and fetch all stored objects according to procedures described in section 9.3.1 of this document.
- R9-2-3* For requirement R9-1-3, the MESSAGE STORE URL parameter as defined in Annex A.1.4.3 of [RCC.07] shall be configured accordingly.

### 9.3.3 Backward compatibility

Not applicable.

### 9.3.4 Configuration Parameters

For Crane networks the following Backup& Restore configuration parameters values apply:

Configuration Parameter	Crane Value
MESSAGE STORE URL	Service Provider Configurable
MESSAGE STORE USER / PASSWORD	Service Provider Configurable
MESSAGE STORE AUTH	Service Provider Configurable
SMS MESSAGE STORE	Service Provider Configurable
MMS MESSAGE STORE	Service Provider Configurable
DISABLE DIRECTION HEADER	Service Provider Configurable

**Table 41: Back up and Restore configuration parameter values**

## 10 Green Button Promise for Voice

### 10.1 Description

The Green Button Promise for voice describes the behaviour of the voice calling function on RCS/VoLTE devices under various coverage conditions.

This section describes the User Stories and Service Requirements for the Green Button Promise for Voice Call services and all features around that core.

The whole section is a new addition in Crane.

### 10.2 User Stories and Feature Requirements

**US10-1 As a user, I want one single entry point to voice call independent of the enabling voice service.**

- R10-1-1* Any entry point to initiate a voice call from the device shall be a single button independent of the enabling voice service.
- R10-1-2* The entry point to initiate a voice call shall not indicate the enabling voice service.



**US10-2 As a user, I (i.e. user A) want to be able to make and receive voice calls with my mobile device while my device is registered on any cellular network bearer.**

- R10-2-1* The voice call from a primary device shall be successful and meet the operator specific voice call performance criteria (e.g. call drop rates, successful call setup rates).
- R10-2-2* Given the end-to-end support of high definition voice codecs, the voice call shall be delivered with high-quality audio.
- R10-2-3* In case of multiple technology options are available to deliver the call, the one that provides the higher voice quality (in terms of stability and audio quality) shall prevail.
- R10-2-4* If radio condition allows, the cellular data connection of the device shall not change nor be interrupted when having a voice call.

**US10-3 As a user, I (i.e. user A or B) want to be able to make and receive voice calls with my mobile device in areas without sufficient cellular reception.**

- R10-3-1* Voice calls shall be possible through a trusted (preferred) as well as untrusted Wi-Fi connection of the device.

NOTE: "Trusted Wi-Fi" refers to a Wi-Fi connection offered by the service provider or via a third party trusted by the service provider. "Untrusted Wi-Fi" refers to any other Wi-Fi connection.

- R10-3-2* Wi-Fi voice calls from primary devices shall be successful and meet operator specific Wi-Fi Calling performance criteria (e.g. call drop rates, successful call setup rates).
- R10-3-3* Given the end-to-end support of high-definition voice codecs, Wi-Fi voice calls shall be delivered with high-quality audio.

**US10-4 As a service provider, I want to configure WiFi Calling on my network.**

- R10-4-1* It shall be supported to enable or to not enable / disable the Wi-Fi Calling service per user via a network configuration.

**US10-5 As a service provider, I want the user to be able to manually enable or disable the Wi-Fi Calling service.**

- R10-5-1* If Wi-Fi Calling is supported on a network for that user, a Wi-Fi Calling switch in phone settings shall be visible to allow the user to enable or disable the Wi-Fi Calling service manually "ON / OFF".
- R10-5-2* The default position of the switch shall be based on operator configuration (ON or OFF).
- R10-5-3* If a network / Operator does not support Wi-Fi Calling at all, no such Wi-Fi Calling switch shall be shown to the user in the device.
- R10-5-4* In case the user is no longer entitled to use Wi-Fi Calling, any incoming or outgoing call while the device is connected to Wi-Fi shall be routed as

normal cellular voice service and the Wi-Fi Calling switch shall no longer be visible.

**US10-6 As a service provider, I want the Wi-Fi Calling service to be used by the mobile device in case voice calls are not available over other voice services (e.g. CS / VoLTE).**

*R10-6-1* The device should only use a Wi-Fi connection for voice calls if the cellular connection cannot be used for voice calls.

NOTE: It is our intention in the longer term to allow the operator to configure the exact behaviour of the Wi-Fi voice service. This can be either cellular preferred or Wi-Fi preferred, or customer choice with a configurable default preference. However in the Crane timeline, it is acceptable to satisfy the requirement as defined in R10-6-1.

**US10-7 As a user, I want to add another contact to an ongoing voice call.**

*R10-7-1* Adding an additional participant to an ongoing voice call shall be supported while the detailed experience might differ based on the actual underlying voice service (e.g. CS / VoLTE).

NOTE: Managing the participants of a group voice call or activity notifications (e.g. who is talking or who left / joined a group) are not in scope.

**US10-8 As a user, I want to use emergency call services even if Wi-Fi Calling is the last resort for voice call connectivity.**

*R10-8-1* Emergency call services shall always use a cellular voice call as long as available (including potential national roaming if required by local regulators).

**US10-9 As a service provider, I may want to allow supplementary services both for voice calls on cellular and over a Wi-Fi connection such as Calling Line Identification Presentation (CLIP), Call Waiting (CW), Call Hold, Call Forward Busy (CFB), Call Forward Unreachable, Call Forward No Reply and Conference Call.**

*R10-9-1* Supplementary Services such as Calling Line Identification Presentation (CLIP), Call Waiting (CW), Call Hold, Call Forward Busy (CFB), Call Forward Unreachable, Call Forward No Reply and Conference Call may be offered by a service provider during any voice call independent of the actual voice service.

**US10-10 As a user, I want to use Dual Tone Multi-Frequency (DTMF) tones during calls both on cellular and over a Wi-Fi connection.**

*R10-10-1* DTMF should be supported during a call over both on cellular and over the Wi-Fi bearer in both the sender's and receiver's experience.

**US10-11 As a user, I want to know which bearer (Cellular or Wi-Fi) is used for the voice call due to the potential less stability and limited mobility a call over Wi-Fi can provide.**

*R10-11-1* The device shall inform the user in a non-intrusive way (e.g. similar to the network indicator in the notification bar or in the in-call screen) that the Wi-Fi bearer is used or going to be used for any potential outgoing or incoming voice calls.

*R10-11-2* Default ringtone shall be the same for incoming voice calls independent of the enabling voice service.

*R10-11-3* During an on-going call over Wi-Fi an indication of the connection quality should be displayed to indicate any potential impact of a poor Wi-Fi connection causing a poor voice call quality.

**US10-12 As a user, I want my voice call to continue in case of connectivity change.**

*R10-12-1* The terminal shall support call continuity among cellular voice services. In this case and if radio condition allows, the cellular data connection of the device shall not change nor be interrupted.

*R10-12-2* The terminal shall support call continuity from Wi-Fi to LTE and vice versa where LTE coverage is available.

*R10-12-3* The terminal shall support call continuity from Wi-Fi to non-LTE connectivity situations and vice versa.

**US10-13 As a service provider, I want the user to have the same options to react to an incoming call independent of the enabling voice service used and whilst there is no other on-going call.**

*R10-13-1* It shall be possible for a user to be notified about an incoming voice call in the same way, independent of the actual voice service used. The user shall then be able to:

- a) Reject the incoming call.
- b) Accept the incoming call.

**US10-14 As a service provider, I want the user to have the same options to react to an incoming call independent of the enabling voice service used and whilst being engaged in another on-going call.**

*R10-14-1* It shall be possible for a user to be notified about an incoming voice call during another on-going voice call in the same way, independent of the actual voice service used. The user shall then be able to:

- a) Reject the incoming call.
- b) Accept the incoming call and put the on-going one on hold. Once the new call ends, the one on hold *shall* resume automatically.
- c) Accept the incoming call and terminate the on-going call.

**US10-15 As a user, I want to see voice calls independent of the actually used voice service in my on-device activity log / call log where voice calls are used to be listed.**

*R10-15-1* Calls over Wi-Fi shall be listed in the same way as CS / VoLTE calls in the same call log view, each visually differentiated whether it was an outgoing, incoming and answered, or incoming but missed call.

*R10-15-2* The visual indication in the call logs shall be the same independent of the enabling voice service.

**US10-16 As a user, I want any rule stored on my device to block contacts for incoming communication to apply independently of the voice service.**

*R10-16-1* Existing rules for blocking contacts on the local device shall be considered also when the device is connected for voice calls via Wi-Fi.

### 10.3 Technical Information

#### 10.3.1 Overview

Voice over LTE (IR.92 voice) is a technical enabler for delivering a voice call service when in LTE coverage as defined in [PRD-IR.92].[PRD-IR.92]

Voice over EPC-integrated Wi-Fi (IR.51 voice) is another technical enabler for delivering voice call service under Wi-Fi access as defined in [PRD-IR.51].

IR.92 and IR.51 voice are two fully compatible IMS services and the clients are expected to support the common set of procedures described in [NG.102].

Traditional Circuit Switched (CS) voice services are delivered on 2G/3G networks.

RCS IP Voice call is not supported for primary devices.

#### 10.3.2 IP Voice and IP Video Call related Configuration Parameters

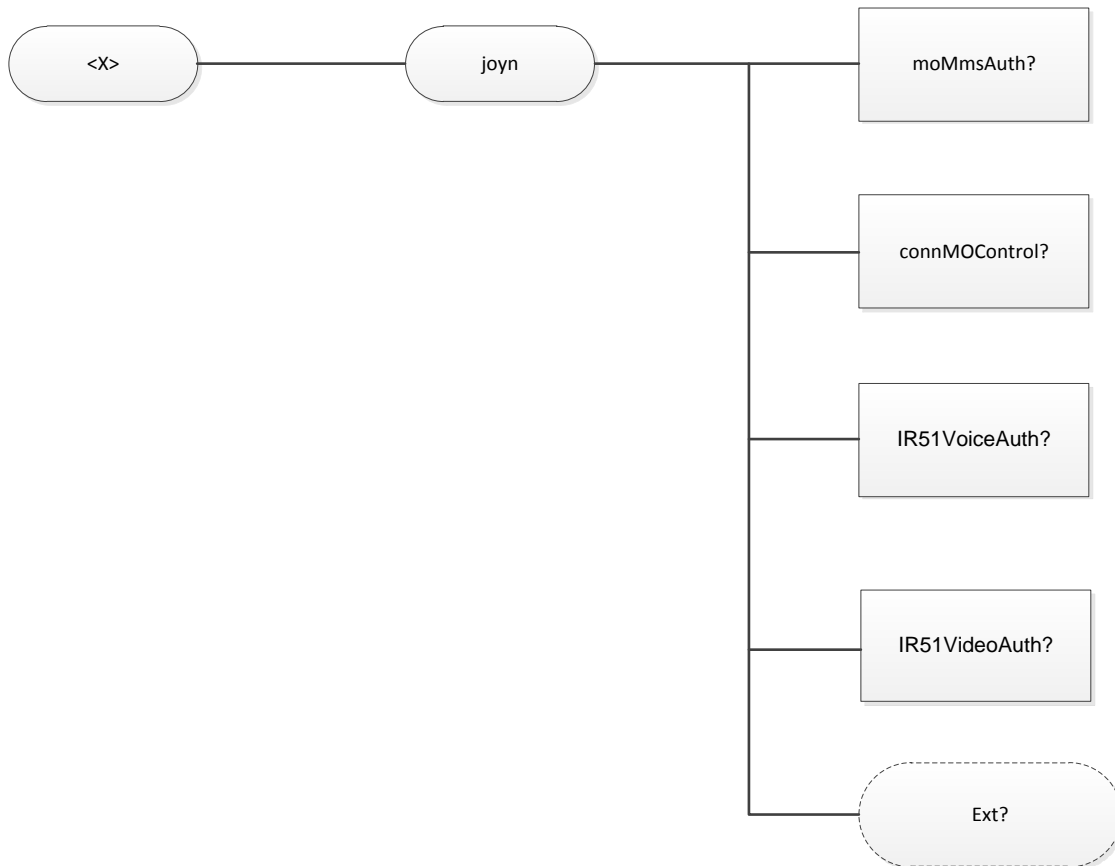
Based on sections 10.1, 10.2, 11.1 and 11.2 of this document, new configuration parameters are needed to be defined.

Configuration parameter	Description	RCS usage
PROVIDE IR51 VOICE	This parameter allows to enable (1) or disable IR.51 Voice Calling	Mandatory parameter
PROVIDE IR51 VIDEO	This parameter allows to enable (1) or disable IR.51 Video Calling	Mandatory parameter
IR51 PREVALENCE	This parameter indicates the IR.51 voice and conversational video service rules of dominance over coexisting technical enablers	Optional parameter It is mandatory and becomes relevant if PROVIDE IR51 VOICE or PROVIDE IR51 VIDEO is set to 1.

IR51 SWITCH UX	This parameter controls the display of the Wi-Fi switch for IR.51 voice and conversational video service and its default position (ON or OFF) when visible.	Optional Parameter  It is mandatory and becomes relevant if PROVIDE IR51 VOICE or PROVIDE IR51 VIDEO is set to 1.
----------------	---	---

**Table 42: joyn IR51 Voice and Video Configuration parameters**

The PROVIDE IR51 VOICE and PROVIDE IR51 VIDEO parameters are placed in a dedicated joyn subtree provided as a Service Provider extension to the Services tree defined in [RCC.07] section A.2.1. (i.e. the <x> node in the Ext node of the Services tree):



**Figure 16: joyn MO Services sub tree**

The associated HTTP configuration XML structure and its integration into the Services MO is presented in the table below:

```

<characteristic type="SERVICES">
<parm name="presencePrfl" value="X"/>
<parm name="ChatAuth" value="X"/>
<parm name="GroupChatAuth" value="X"/>
<parm name="ftAuth" value="X"/>
<parm name="standaloneMsgAuth" value="X"/>
<parm name="geolocPullAuth" value="X"/>
<parm name="geolocPushAuth" value="X"/>
<parm name="vsAuth" value="X"/>
<parm name="isAuth" value="X"/>
<parm name="rcsIPVoiceCallAuth" value="X"/>
<parm name="rcsIPVideoCallAuth" value="X"/>
<parm name="IR94VideoAuth" value="X"/>
<parm name="allowRCSExtensions" value="X"/>
<characteristic type="Ext">
    <characteristic type="joyn">
        <parm name="moMmsAuth" value="X"/>
        <parm name="connMOControl" value="X"/>
        <parm name="IR51VoiceAuth" value="X"/>
        <parm name="IR51VideoAuth" value="X"/>
        <characteristic type="Ext"/>
    </characteristic>
</characteristic>
</characteristic>
    
```

**Figure 17: Services sub tree associated HTTP configuration XML structure**

Node: <x>/joyn

Node: /<x>/joyn/IR51VoiceAuth

Leaf node that represents the authorization for user to use IR51 Voice Calling service  
 The node shall be instantiated if the rcsDisabledState node is not provided.

Status	Occurrence	Format	Min. Access Types
Required	ZeroOrOne	bool	Get, Replace

**Table 43: Services MO sub tree addition parameters (IR51VoiceAuth)**

- Values: 0,1
  - 0- Indicates that IR51 Voice Calling service is disabled
  - 1- Indicates that IR51 Voice Calling service is enabled

- Post-reconfiguration actions: The client should be reset and should perform the complete first-time registration procedure following a reconfiguration (e.g. OMA-DM/HTTP) as described in section 2.3.1.1 of this document.
- Associated HTTP XML parameter ID: "IR51VoiceAuth"

Node: /<x>/joyn/IR51VideoAuth

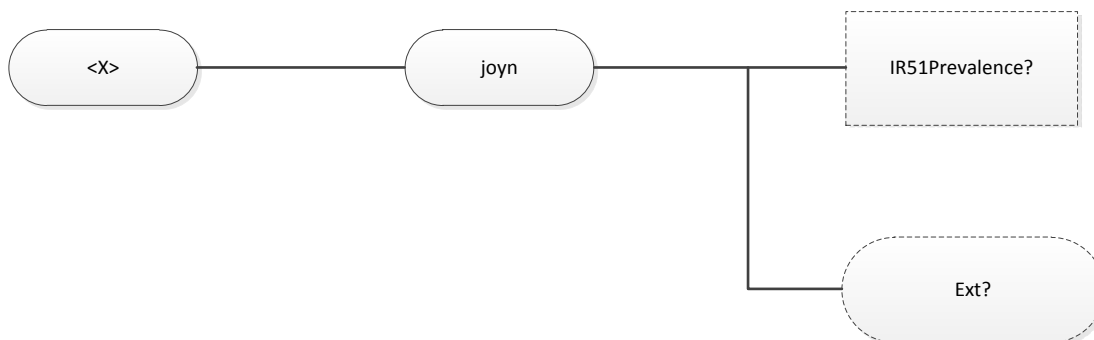
Leaf node that represents the authorization for user to use IR51 Video Calling service  
 The node shall be instantiated if the rcsDisabledState node is not provided.

Status	Occurrence	Format	Min. Access Types
Required	ZeroOrOne	bool	Get, Replace

**Table 44: Services MO sub tree addition parameters (IR51VideoAuth)**

- Values: 0,1
  - 0- Indicates that IR51 Video Calling service is disabled
  - 1- Indicates that IR51 Video Calling service is enabled
- Post-reconfiguration actions: The client should be reset and should perform the complete first-time registration procedure following a reconfiguration (e.g. OMA-DM/HTTP) as described in section 2.3.1.1 of this document.
- Associated HTTP XML parameter ID: "IR51VideoAuth"

The PROVIDE IR51 PREVALENCE parameter is placed in a dedicated joyn subtree provided as a Service Provider extension to the additions to the IMS MO sub tree defined in [RCC.15] section 2.2.2.2 (i.e. the <x> node in the Ext node of the additions to the IMS MO subtree):



**Figure 18: joyn MO IMS sub tree additions parameter**

The associated HTTP configuration XML structure and its integration into the additions to the IMS MO sub tree parameters is presented in the table below:

```

<characteristic type="APPLICATION">
  <parm name="AppID" value="X"/>
  <parm name="Name" value="X"/>
  <parm name="AppRef" value="IMS-Settings"/>
</characteristic type="ConRefs">
    
```

```
<characteristic type="Refs">
  <parm name="ConRef1" value="X"/>
  <parm name="ConRef2" value="X"/>
  ...
</characteristic>
</characteristic>
<parm name="PDP_ContextOperPref" value="X"/>
<parm name="Timer_T1" value="X"/>
<parm name="Timer_T2" value="X"/>
<parm name="Timer_T4" value="X"/>
<parm name="P-CSCF_Address" value="X"/>
<parm name="Private_User_Identity" value="X"/>
<characteristic type="Public_User_Identity_List">
  <characteristic type="Public_user_identities">
    <parm name="Public_User_Identity1" value="X"/>
    <parm name="Public_User_Identity2" value="X"/>
    ...
  </characteristic>
</characteristic>
<parm name="Home_network_domain_name" value="X"/>
<characteristic type="Ext">
  <parm name="endUserConfReqId" value="X"/>
  <characteristic type=" transportProto">
    <parm name="psSignalling" value="X"/>
    <parm name="psMedia" value="X"/>
    <parm name="psRTMedia" value="X"/>
    <parm name="psSignallingRoaming" value="X"/>
    <parm name="psMediaRoaming" value="X"/>
    <parm name="psRTMediaRoaming" value="X"/>
    <parm name="wifiSignalling" value="X"/>
    <parm name="wifiMedia" value="X"/>
    <parm name="wifiRTMedia" value="X"/>
  </characteristic>
  <parm name="uuid_Value" value="X"/>
  <characteristic type="Ext"/>

  <characteristic type="joyn">
    <parm name="IR51Prevalence="X"/>"
  </characteristic type="Ext"/>
</characteristic>
<characteristic type="ICSI_List">
  <characteristic type="ICSIs">
    <parm name="ICSI1" value="X"/>
    <parm name="ICSI_Resource_Allocation_Mode1" value="X"/>
    <parm name="ICSI2" value="X"/>
    <parm name="ICSI_Resource_Allocation_Mode2" value="X"/>
  </characteristic>
</characteristic>
<characteristic type="LBO_P-CSCF_Address">
  <characteristic type="LBO_P-CSCF_Addresses">
    <parm name="Address1" value="X"/>
    <parm name="AddressType1" value="X"/>
    <parm name="Address2" value="X"/>
    <parm name="AddressType2" value="X"/>
    ...
  </characteristic>
</characteristic>
```



```

    <parm name="Resource_Allocation_Mode" value="X"/>
    <parm name="Voice_Domain_Preference_E_UTRAN" value="X"/>
    <parm name="SMS_Over_IP_Networks_Indication" value="X"/>
    <parm name="Keep_Alive_Enabled" value="X"/>
    <parm name="Voice_Domain_Preference_UTRAN" value="X"/>
    <parm name="Mobility_Management_IMS_Voice_Termination" value="X"/>
    <parm name="RegRetryBaseTime" value="X"/>
    <parm name="RegRetryMaxTime" value="X"/>
    <characteristic type="PhoneContext_List">
        <characteristic type="PhoneContext_List">
            <parm name="PhoneContext1" value="X"/>
            <parm name="Public_User_Identity1" value="X"/>
            <parm name="PhoneContext2" value="X"/>
            <parm name="Public_User_Identity2" value="X"/>
            ...
        </characteristic>
    </characteristic>
    <parm name="SS_domain_setting" value="X"/>
    <parm name="PS_domain_IMS_SS_control_preference" value="X"/>
    <characteristic type="APPAUTH">
        <parm name="AuthType" value="X"/>
        <parm name="Realm" value="X"/>
        <parm name="UserName" value="X"/>
        <parm name="UserPwd" value="X"/>
    </characteristic>
    </characteristic>
    
```

**Figure 19: IMS sub tree associated HTTP configuration XML structure**

Node: <x>/joyn

Node: /<x>/joyn/IR51Prevalence

Leaf node that represents the rules of dominance of IR51 voice and conversational video services over coexisting technical enablers.

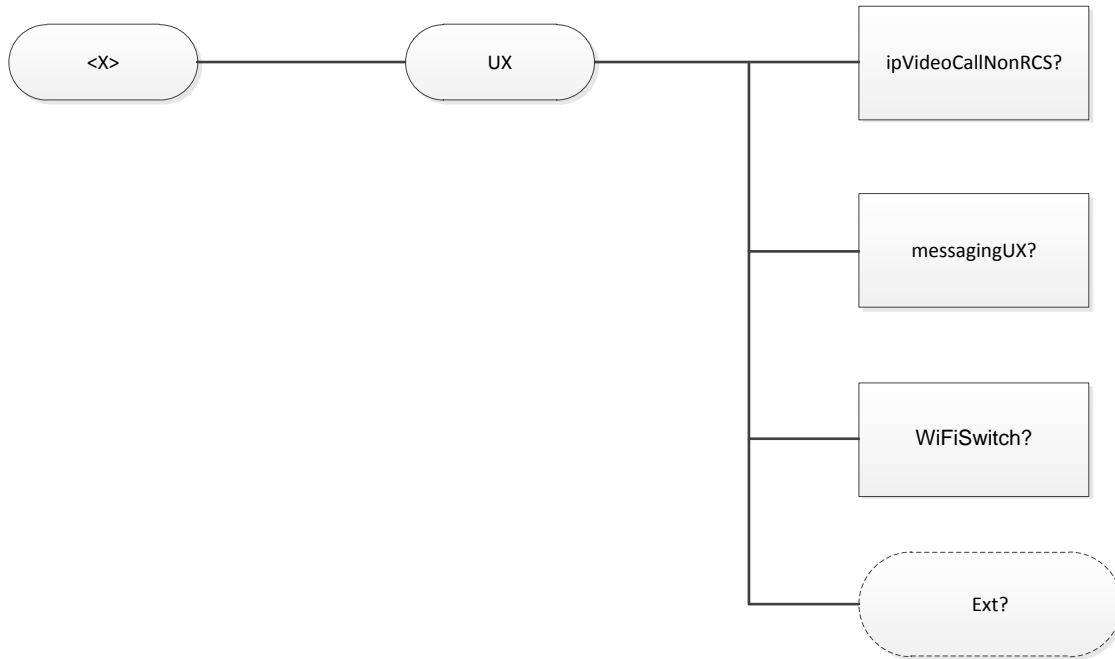
The node shall be instantiated if the rcsDisabledState node is not provided.

Status	Occurrence	Format	Min. Access Types
Optiona l	ZeroOrOne	bool	Get, Replace

**Table 45:IMS MO sub tree addition parameters (IR51Prevalence)**

- Values (0,1)
  - 0- Indicates that IR.51 voice and conversational video services are allowed (if available)if no cellular access and PS voice and video services are available
  - 1- Indicates that IR.51 voice and conversational video services are enabled based on mobility management rules described in section 5.8 of [PRD-IR.51]
- Post-reconfiguration actions: As the client remains unregistered during configuration, there are no additional actions apart from de-registering using the old configuration and registering back using the new parameter.
- Associated HTTP XML parameter ID: "IR51Prevalence"

The IR51 SWITCH UX parameter will be placed in the UX MO sub tree defined in [RCC.61].



**Figure 20: UX MO sub tree**

The associated HTTP configuration XML structure is presented in the table below:

```

<characteristic type="UX">
<parm name="ipVideoCallNonRCS" value="X"/>
<parm name="messagingUX" value="X"/>
<parm name="IR51SwitchUX" value="X"/>
<characteristic type="Ext"/>
</characteristic>
    
```

**Figure 21: UX subtree associated HTTP configuration XML structure**

Node: /<x>/UX

Node: /<x>/UX/IR51SwitchUX

Leaf node that describes whether the Wi-Fi switch for IR.51 voice and conversational video services is visible to the user and its default position (OFF or ON).

If not instantiated, the Wi-Fi switch for IR.51 voice and conversational video services shall not be displayed to the user.

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	Int	Get, Replace

**Table 46: UX MO sub tree addition parameters (WiFiSwitch)**

- Values:
  - 0 Wi-Fi switch for IR.51 voice and conversational video services is not visible to the user (default value)
  - 1 Wi-Fi switch for IR.51 voice and conversational video services is visible to the user with default position set to OFF

- 2 Wi-Fi switch for IR.51 voice and conversational video services is visible to the user with default position set to ON
- Post-reconfiguration actions: As the client remains unregistered during configuration, there are no additional actions apart from de-registering using the old configuration and registering back using the new parameter.
  - Type property of the node is: urn:gsma:mo:gcc-ux:1.0:IR51SwitchUX
  - Associated HTTP XML characteristic type: "IR51SwitchUX"

### 10.3.3 Technical Implementation of User Stories and Service requirements

- R10-17-1* Requirements R10-1-1 and R10-1-2 shall be implemented locally in the device.
- R10-17-2* Requirements R10-2-1,R10-2-3 and R10-2-4 shall be realised as described in [NG.102] for Multimedia Telephony over E-UTRAN and Legacy 3GPP access considerations.
- R10-17-3* Requirement R10-2-2 shall be fulfilled based on Real-time media negotiation, transport and codec procedures described in section 3 of [PRD-IR.92].
- R10-17-4* Requirements R10-3-1 and R10-3-2 shall be realised as described in [NG.102] for Multimedia Telephony over EPC integrated WI-Fi.
- R10-17-5* For requirement R10-3-3, section 4.12 of [PRD-IR.51] shall apply
- R10-17-6* Requirement R10-4-1 shall be fulfilled by configuring the PROVIDE IR51 VOICE parameter defined in section 10.3.2 of this document.
- R10-17-7* Requirements R10-5-1, R10-5-2 and R10-5-3 shall be fulfilled based on the PROVIDE IR51 VOICE and IR51 SWITCH UX parameters defined in section 10.3.2 of this document
- R10-17-8* For requirement R10-5-4, Wi-Fi service deactivation by the Service Provider shall result to user reprovisioning.
- R10-17-9* For requirements R10-6-1 the IR51 PREVALENCE parameter defined in section 10.3.2 of this document shall be configured and set to zero.
- R10-17-10* For requirement R10-7-1, procedures as defined in section 2.3.3 of [PRD-IR.92] shall apply. The actual implementations are based on Service Provider policies.
- R10-17-11* For requirement R10-8-1 section 3.3 of [NG.102] shall apply.
- R10-17-12* Requirement R10-9-1 shall be fulfilled based on the technical procedures described in section 2.12 of [NG.102].
- R10-17-13* Requirement R10-10-1 shall be fulfilled based on the technical procedures described in section 2.2 of [PRD-IR.92].
- R10-17-14* Requirements R10-11-1, R10-11-2 and R10-11-3 shall be implemented locally on the device.
- R10-17-15* For requirement R10-12-1 Annex A.3.2 of [NG.102] shall apply.
- R10-17-16* For requirement R10-12-2 section 2.18 of [NG.102] shall apply.
- R10-17-17* For requirement R10-12-3 Annex A.3.1 of [NG.102] shall apply.

*R10-17-18* Requirement R10-13-1 shall be implemented locally on the device. For the call establishment and termination, section 2.16 of [NG.102] shall apply

*R10-17-19* Requirement R10-14-1 shall be implemented locally on the device. For the call establishment and termination, section 2.16 of [NG.102] shall apply. For the Communication Hold service, section 2.12 of [NG.102] shall apply.

*R10-17-20* Requirements R10-15-1 and R10-15-2 shall be implemented locally on the device.

*R10-17-21* If the device offers the possibility to block incoming calls from contacts, requirement R10-16-1 shall be implemented locally on the device and shall be independent of the technology used for the call.

### 10.3.4 Backward Compatibility

Not applicable.

### 10.3.5 Configuration Parameters

For Crane networks the following IP Voice Call configuration parameters values apply:

Configuration Parameter	Crane Value
PROVIDE RCS IP VOICE CALL	"0" for primary devices
RCS IP VOICE CALL BREAK OUT	N/A
RCS VOLTE SINGLE REGISTRATION	Service Provider Configurable
NO MSRP SUPPORT	Service Provider Configurable
PROVIDE IR51 VOICE	Service Provider Configurable
IR51 PREVALENCE	Recommended Value: 0 NOTE: For future compatibility the value of this parameter is left to the Service Provider
IR51 SWITCH UX	Service Provider Configurable

**Table 47: IP Voice Call configuration parameter values**

## 11 Green Button Promise for Video

### 11.1 Description

Video calling is an important feature to evolve the Operator calling experience. Video calling will offer a sustainable and reliable video calling experience across multiple devices and different bearers triggered by a single video calling 'button'. Widespread reach across customer locations and use cases will be ensured. This section describes the User Stories and Service Requirements for Green Button Promise for Video service and all features around that core delivered through IP Video call enablers.

NOTE: This section focusses on general behaviour once a Video Call has been connected between users and in particular the behaviour of initiating a Video Call "from scratch", i.e. without being already in the context of an on-going voice call. The behaviour of upgrading an on-going voice call to a video call is described in section 12 (In-call Services).

The whole section is a new addition to Crane.

## 11.2 User Stories and Feature Requirements

**US11-1 As a user, I (i.e. user A) want to initiate from various call related entry points (e.g. contact card, call logs) a lip sync IP video call to a contact (i.e. user B).**

- R11-1-1* From any call related entry point on a device a user should be able to initiate an IP video call to a contact whenever it is possible.
- R11-1-2* The IP Video Call shall offer lip sync experience.
- R11-1-3* In the case there are multiple video call services available, the service that provides the higher voice quality (stability and audio quality) shall prevail.

**US11-2 As a user, I (i.e. user A) want to be able to initiate an IP Video Call using a single “start video call” button, irrespective of network bearer used.**

- R11-2-1* Any entry point to initiate an IP Video Call from the device shall be a single button independent of the enabling video call service.

NOTE: CS Video Call shall not be offered as part of this one-button experience.

- R11-2-2* The entry point to initiate an IP Video Call shall not indicate the enabling video call service.

**US11-3 As a service provider, I want to configure the availability of the IP Video Call service depending on the different cellular data bearer conditions.**

- R11-3-1* It shall be able to configure the availability of the IP Video Call service based on the different cellular data bearers.

**US11-4 As a user, I (i.e. user A or B) want to make and receive IP Video Calls with my mobile device in areas without sufficient cellular reception.**

- R11-4-1* IP Video Calls shall be possible ontrusted and untrusted Wi-Fi bearer.

NOTE: “Trusted Wi-Fi” refers to a Wi-Fi connection offered by the service provider or via a third party trusted by the service provider. “Untrusted Wi-Fi” refers to any other Wi-Fi connection.

**US11-5 As a service provider, I want the Wi-Fi Video Calling service to be used by the mobile device in case IP Video Calls are not available over cellular data bearers.**

- R11-5-1* The device should only use a Wi-Fi connection for vdeo calls if the cellular data connection cannot be used for IP Video Calls.

**US11-6 As a user, I (i.e. user A) want to know in advance whether I can have with a high likelihood a video call with the user B or not.**

- R11-6-1* The availability of the IP Video Call service shall be (re-)validated once a user accesses the screen view containing the IP Video Call service entry point.

- R11-6-2* The IP Video Call entry point shall clearly indicate whether there is a high likelihood that the IP Video Call attempt will be successful at that time or not (e.g. by using full vs greyed-out iconography).
- R11-6-3* In case the A-Party device does not provide a camera (hardware limitation), the IP Video Call capability is not given. There shall not be a service entry point for initiating an IP Video Call.
- R11-6-4* In case the B-Party device does not have a camera built in (neither front facing nor rear facing) but is able to display video in 352x288 pixel resolution @ 15 fps (or better), the A-Party shall be able to trigger a one-way IP Video Call to B-Party device. B-Party obviously shall have no option to activate the video channel back to A-Party.
- R11-6-5* In case the B-Party device does not have a camera built in (neither front facing nor rear facing) and is not able to display video in 352x288 pixel resolution @ 15 fps (or better), the A-Party shall not be able to trigger an IP Video Call to B-Party.

**US11-7 As a user receiving an incoming IP video call, I (i.e. user B) want to decide whether to:**

- a) Decline the call which leads to an “unanswered video call” indication to the calling party (i.e. user A),
- b) Accept the call without transmitting my camera view, or
- c) Accept the call with transmitting my camera view.

*R11-7-1* The receiver shall be able to accept or decline an incoming IP Video Call.

*R11-7-2* The receiver shall have the option to answer the incoming IP video call with or without transmitting the own camera view back to the sender.

**US11-8 As a user receiving an incoming IP Video Call, I (i.e. user B) want to have the incoming video call differentiated from an incoming voice call.**

*R11-8-1* The incoming call screen shall show to the user that the incoming call is a video call.

*R11-8-2* Default ringtone for incoming IP Video Calls shall be as same as for voice calls, but the user shall be allowed to differentiate the ringtone for an incoming IP Video Call from an incoming voice call.

**US11-9 As a user answering an incoming IP video call, I (i.e. user B) want the incoming voice automatically on a connected headset. If there is no headset connected, then play the voice on my external loudspeaker.**

*R11-9-1* When an IP video call is accepted, the audio part should be played either via a connected headset (if connected) or via the external loudspeaker (if no headset connected).

**US11-10 As users in an IP Video Call, we want to continue the transmission of the video as long as possible under changing connectivity situations delivering a high quality and lip sync experience.**

*R11-10-1* In case during an on-going IP video call one user moves out of LTE coverage, the transmission of the video media part of the IP Video Call should be maintained if network conditions allow.

**US11-11 As users in an IP Video Call, we want the best possible quality of video available to us throughout the IP Video Call for the radio bearer we use.**

*R11-11-1* An IP Video Call over LTE shall benefit from a higher video quality than available on 3G.

*R11-11-2* An IP Video Call over WiFi shall benefit from a higher video quality than available on 3G.

*R11-11-3* The quality of the IP Video Call shall be adapted to the currently available bandwidth (e.g. by changing radio conditions) and use bitrates lower than the maximum negotiated when the IP Video Call was initiated.

*R11-11-4* If technically possible, the quality of the IP Video Call shall be adapted to the currently available bandwidth and use bitrates higher than the rate negotiated when the IP Video Call was initiated.

**US11-12 As users in an IP video call with insufficient bandwidth, I want to be made aware of when the video stream is interrupted until bandwidth is improved and the video transmission is continued.**

*R11-12-1* When connectivity during an IP Video Call is insufficient to deliver a decent video stream, the video stream displayed to the user shall be interrupted and a visual indication shall be provided that connectivity is insufficient and the video continues when connectivity conditions are improved.

NOTE 1: Preferably a visual icon is used instead of an "error message".

NOTE 2: The criteria to decide whether the video quality is acceptable is left to the implementation.

**US11-13 As users in an IP video call, we want to continue the call as voice call only in case video cannot be maintained for any reason anymore, so that the call does not drop entirely.**

*R11-13-1* If, during an ongoing IP Video Call, one user loses the ability to transmit video completely (i.e. loss of data), the call should continue as voice call without video.

*R11-13-2* If it is not possible to continue the call as (a) best effort quality video call or as (b) voice call, a call may eventually drop.

**US11-14 As users in an IP video call, we want to stop (and restart) transmitting the own camera view at any point during the call without interrupting the call, i.e. audio is maintained during the call.**

*R11-14-1* Each user in an IP video call shall be able to stop (and restart) transmitting their own live video at any point during the call.

*R11-14-2* If a user stops sharing the own camera view, an in-call screen shall be displayed clearly indicating how the user can share their camera again.

*R11-14-3* Stopping the transfer of the camera view by one or even by both users shall not interrupt the transmission of audio, so that the call continues as voice call.

**US11-15 As users in an IP video call, we want to mute (and unmute) the own voice (i.e. mute microphone) at any point during the call without interrupting the call, i.e. video is maintained during the call.**

*R11-15-1* Each user in an IP Video Call shall be able to mute (and unmute) their own live audio at any point during the call.

**US11-16 As users in an IP video call, when we rotate (i.e. user A / B) our devices the correct video orientation is displayed based on the orientation of each device.**

*R11-16-1* The device shall handle the different orientation permutations depending on how the device is rotated during an IP Video Call.

**US11-17 As users in an IP video call, we (i.e. user A / B) want to toggle between front and rear camera without interruption when the device supports two cameras.**

*R11-17-1* The user shall be able to toggle the camera (i.e. front / back) which is recording the transmitted IP video signal if the phone supports two cameras.

*R11-17-2* If the phone supports two cameras, the front facing camera shall be activated by default when the video transmission is started.

**US11-18 As users in an IP video call, we (i.e. user A / B) want to see an indication of the connection quality on the in-call screen so that we know that compromises on the video quality might be due to limitations in the local data connectivity leg.**

*R11-18-1* During an on-going IP Video Call a “connection quality indicator” should be displayed on the in-call screen to indicate risk of video call switching to audio-only or dropping completely due to unsatisfactory coverage.

NOTE: The criteria to decide whether the video quality is acceptable is left to the implementation.

**US11-19 As a service provider, I may want to allow supplementary services during IP Video Calls when another (voice/video) call comes in such as Calling Line Identification Presentation (CLIP), Call Waiting (CW), Call Hold, Call Forward Busy (CFB), Call Forward Unreachable, and Call Forward No Reply.**

*R11-19-1* Supplementary Services such as Calling Line Identification Presentation (CLIP), Call Waiting (CW), Call Hold, Call Forward Busy (CFB), Call Forward Unreachable, and Call Forward No Reply may be offered by a service provider during an IP Video Call.



NOTE: Supplementary services shall be aligned across voice and video call types.

**US11-20 As a user, I want to see my (initiated and received) IP video calls in my call logs similar to any other voice call.**

*R11-20-1* The IP Video Call must be displayed in the single (voice AND video) call log interface (per contact or global call log).

*R11-20-2* In that single log of the user's device, an IP Video Call shall be differentiated with a specific visual reference from a standard voice call and/or from an enriched voice call (i.e. with content sharing that has taken place during the call).

*R11-20-3* Similar to voice call events, initial video call events (i.e. not added in-call) shall be differentiated between answered and unanswered video calls.

*R11-20-4* The B-Party shall be informed of any video calls they has missed. The notification shall clearly show that the missed call is an IP Video Call.

*R11-20-5* The visual indication of an IP Video Call in the call logs shall be the same for all IP Video Calls independently of the video call service that was used.

### 11.3 Technical Information

#### 11.3.1 Overview

The IP Video Call service shall be realised based on three main technical enablers:

- Video over LTE (IR.94 conversational video) technical enabler as defined in [PRD-IR.94],
- Video over EPC-integrated Wi-Fi (IR.51 conversational video) technical enabler as defined in [PRD-IR.51], and
- RCS IP Video Call service as described in sections 2.2.1, 2.7.1.2.2 and 3.9 of [RCC.07].

The three technical enablers shall co-exist based on procedures defined in [NG.102].

RCS IP Video Call service is used only when the establishment of end to end IR.94/IR.51 conversational video service is not possible.

Note the three implementations are fully compatible:

- Capability discovery: If the result of the exchange is that IR.94/IR.51 conversational video is supported in one end and only RCS IP Video Call is supported in the other, the IP video call is possible to establish.
- Service initiation and acceptance: A device that supports IR.94/IR.51 conversational video service shall accept an incoming SIP INVITE for RCS IP Video Call as a SIP INVITE for IR.94/IR.51 conversational video and vice-versa as the services are compatible.

#### 11.3.2 Technical Implementation of User Stories and Service Requirements

*R11-21-1* Requirement R11-1-1 shall be implemented locally on the device based on the technical enablers described in section 11.3.1 of this document.

*R11-21-2* Requirement R11-1-2 is fulfilled based on used technical enablers ( as per section 11.3.1 of this document).

- R11-21-3* Requirement R11-1-3 is fulfilled based on the used technical enablers for voice (as per section 11.3.1 of this document).
- R11-21-4* Requirements R11-2-1 and R11-2-2 shall be implemented locally on the device.
- R11-21-5* For requirement R11-3-1, IR.94 conversational video service is only available under LTE coverage where that service is deployed. IR.94 conversational video service is enabled/disabled by configuring the PROVIDE IR94 VIDEO parameter defined in Annex A.1.13 of [RCC.07]. For RCS IP Video call, the requirement is fulfilled by configuring the PROVIDE RCS IP VIDEO CALL parameter defined in Annex A.1.13 of [RCC.07].
- R11-21-6* The realisation for requirement R11-4-1 is covered in section 11.3.1 of this document.
- R11-21-7* Requirement R11-5-1 is fulfilled based on the IR51 PREVALENCE parameter defined in section 10.3.2 of this document. The parameter value shall be set to zero.
- R11-21-8* For requirement R11-6-1 section 2.9 of [NG.102] shall apply.
- R11-21-9* Requirement R11-6-2 shall be implemented locally on the device.
- R11-21-10* Requirement R11-6-3 shall be implemented locally on the device. The IR.94/IR.51 conversational video services and the RCS IP video call service shall not be advertised by the client through the SIP OPTIONS exchange mechanism.
- R11-21-11* Requirement R11-6-4 shall be implemented locally on the device. Section 2.2.2 of [PRD IR.94] shall apply. The capability of IR.94/IR.51 video or RCS IP Video call is included as part of the capability exchange mechanism.
- R11-21-12* Requirement R11-6-5 shall be implemented locally on the device. The client shall not advertise the capability of IR.94/IR.51 conversational video or RCS IP Video call service in the applied capability exchange mechanism.
- R11-21-13* Requirement R11-7-1 shall be implemented locally on the device. For IR.94/IR.51 conversational video service section 2.2.2 of [PRD-IR.94] shall be considered. For RCS IP Video call service section 3.9 of [RCC.07] shall apply.
- R11-21-14* Requirement R11-7-2 shall be implemented locally on the device. Section 2.2.2 of [PRD-IR.94] shall apply.
- R11-21-15* Requirements R11-8-1 and R11-8-2 shall be implemented locally on the device.
- R11-21-16* Requirement R11-9-1 shall be implemented locally on the device.
- R11-21-17* For requirement R11-10-1, different handover scenarios shall be considered:
- For LTE to EPC integrated Wi-Fi cases, procedures described in section 2.18 of [NG.102] shall apply.
  - For SR-VCC procedures to 2G/3G and as per section A.2. of [PRD-IR.94], the video media from the video call after the session transfer is discontinued.
  - For handover scenarios that result from using IR.94 conversational video to using RCS IP Video call, video session needs to be re-established.

- R11-21-18* Requirement R11-11-1 shall be fulfilled based on section 3 of [PRD-IR.94].
- R11-21-19* Requirement R11-11-2 shall be fulfilled based on sections 4.8.2 of [PRD-IR.51] and section 3 of [PRD-IR.94].
- R11-21-20* For requirements R11-11-3 and R11-11-4, the technical enabler shall be considered. For IR.94/IR.51 conversational video section 3.3 of [PRD-IR.94] shall apply. For RCS IP video call section 3.9 of [RCC.07] shall apply.
- R11-21-21* Requirement R11-12-1 shall be implemented locally on the device.
- R11-21-22* For requirement R11-13-1, used technology shall be taken into account. For IR.94/IR.51 conversational video call, section 2.4.1 of [PRD-IR.94] shall apply. RCS IP Video call downgrade on the primary device will result in an RCS IP Voice call that is a best effort service.
- R11-21-23* For requirement R11-13-2, IR.94/IR.51 conversational video service downgrade due to mid-session network failure will not result in the establishment of an RCS IP Video call. If failure is caused by handover use cases, IR.94/IR.51 conversational services are not supported.
- R11-21-24* Requirements R11-14-1 and R11-14-3 shall be implemented locally on the device. For IR.94 conversational video, it shall be fulfilled based on section 2.2.2 of [PRD-IR.94]. For IR.51 conversational video, proceed as described in section 4.5 of [PRD-IR.51]. For RCS IP Video call service, dropping the video media will result to RCS IP Voice call.
- R11-21-25* Requirement R11-14-2 shall be implemented locally on the device.
- R11-21-26* Requirement R11-15-1 shall be implemented locally on the device.
- R11-21-27* For requirement R11-16-1, for IR.94 conversational video and for RCS IP Video call service section 2.4.2 of [PRD-IR.94] shall apply. For IR.51 conversational video service, section 4.8.2 of [PRD-IR.51] shall apply.
- R11-21-28* Requirements R11-17-1 and R11-17-2 shall be implemented locally on the device.
- R11-21-29* Requirement R11-18-1 shall be implemented locally on the device.
- R11-21-30* For requirement R11-19-1 section 2.12 of [NG.102] shall be taken into consideration.
- R11-21-31* Requirements R11-20-1, R11-20-2, R11-20-3, R11-20-4 and R11-20-5 shall be implemented locally on the device.

### 11.3.3 Backward compatibility

Not applicable.

### 11.3.4 Configuration Parameters

The configuration parameters defined in Annex A.13 of [RCC.07] and section 10.3.2 of this document are specific to IP Video Call. For Crane they will be handled as follows:

Configuration parameter	Description
PROVIDE IR94 VIDEO	Service Provider Configurable
PROVIDE RCS IP VIDEO CALL	Service Provider Configurable

RCS IP VIDEO CALL UPGRADE FROM CS	Fixed Value: 0 Upgrade from CS not considered
RCS IP VIDEO CALL UPGRADE ATTEMPT EARLY	Fixed Value: 0 Upgrade from CS not considered
RCS IP VIDEO CALL UPGRADE ALLOWED ON CAPABILITY ERROR	Fixed Value: 0 Upgrade from CS not considered
IP VIDEO CALL DEFAULT MECH	N/A
VIDEO UX	Fixed Value: 0
PROVIDE IR51 VIDEO	Recommended Value: 0 NOTE: For future compatibility the value of this parameter is left to the Service Provider
IR51 PREVALENCE	Service Provider Configurable
IR51 SWITCH UX	Service Provider Configurable

**Table 48: Crane IP Video Call configuration parameters**

## 12 In-call Services

### 12.1 Description

In-call Services in Crane covers, similar to the Blackbird PDD, the ability to share video and images during an ongoing voice call. With the Crane release these features are further evolved to reflect additional voice call services like VoLTE and Wi-Fi Calling.

NOTE: In-call Services will evolve according to the work currently done in the Operator Interest Group for Enriched Calling. This will not change the current requirements.

Summary of Changes from Blackbird

- Addition of “Live” Video section to establish the framework for different video technologies that can be used within the context of a voice call.
- Removal of streaming of recorded video files via Video Share.
- Change of Image Share to an receiver’s experience only.

### 12.2 User Stories and Feature Requirements

#### 12.2.1 In-call Services: General

**US12-1** As a user during a voice call, I want to use enhanced functionality that allows me to have a more meaningful and engaging (i.e. “richer”) conversation with the person I am in the call with.

- R12-1-1* All In-Call Services shall be made accessible from the In-call screen which is by definition only shown during an on-going call.
- R12-1-2* All services shall only be delivered in a one-to-one call.
- R12-1-3* The user shall be able to recognise whether the individual In-call Services are available to use with the conversation partner.
- R12-1-4* Once a call is connected and a capability refresh has detected the end-to-end availability of In-call Services a non-intrusive (in volume and character of the sound) audio notification should be played to the user to indicate the availability of In-call Services. The audio notification shall be different in character of the sound compared to any audio notification indicating incoming requests for In-call Services events.
- R12-1-5* In addition, an informative dialogue should be presented to the user making aware of the availability of In-call Services. On this dialogue, the user shall be able to permanently disable the audio and visual information to be presented again (“do not notify again”). If the user opens the screen and looks at the notification, it shall be possible to close the notification.
- R12-1-6* When either participant of the call places the call “On Hold”, any entry point to the “live video” shall be disabled.

### **12.2.2 In-call Services: “Live Video”**

In addition to the “Video Share” feature of previous RCS versions, Crane introduces two video services: Video over LTE (ViLTE, IR.94) and RCS IP Video Call (ViIP) both captured under the term “IP Video Call”. From a user’s perspective, all three services shall be available as “Live Video”. Selection of the technical enabler is dependent on available network conditions in the end-to-end usage scenario. Each technology has its benefits and limitations and the individual use is based on each Operator’s configuration. The implementation of Crane does NOT require RCS IP Video (ViIP) but only RCS Video Share and ViLTE (if supported by the implementing device/network).

**US12-2 As a user in a voice call, I (i.e. user A) want to have the ability to share “live video” (i.e. the camera view) from my in-call screen with the other participant of the call (i.e. user B) whenever it is possible. While sharing, the video is delivered as a real-time stream to the receiver’s screen, the sound is still delivered via the ongoing Voice Call.**

- R12-2-1* During an ongoing voice call there shall be the option for both users to share “live video” with the other party if a “live video” share is supported end-to-end.
- R12-2-2* The entry point to add “live video” to an ongoing voice call shall be a single button independent of the enabling “live video” service.
- R12-2-3* In case a “live video” share is added during an ongoing voice call, the voice call shall continue with no degradation of the reliability of the voice call.
- R12-2-4* In case of multiple “live video” services being available, the one that provides a lip sync experience shall prevail.
- R12-2-5* Sending “live video” shall only be made available in case Wi-Fi, HSPA or higher data connectivity is given.

- R12-2-6* In case the user is connected for data only on 3G, “live video” shall only be made available for receiving.
- R12-2-7* If one user is not connected for data at least on 3G (or on Wi-Fi), “live video” shall not be made available to both users.
- R12-2-8* In case the underlying voice call is terminated, the “live video” share shall be terminated as well.
- R12-2-9* The user shall not be able to record the transmitted “live video” share (i.e. both receiving and sending “live video” share).
- R12-2-10* There shall be no option to stream a previously recorded video to the other conversation party.

**US12-3 As a user, I (i.e. user A) want to know in advance whether I can add “live video” with a high likelihood to the voice call in that moment or not.**

- R12-3-1* The ability to add “live video” shall be validated during the voice call.
- R12-3-2* Re-validation of the ability to add “live video” shall happen in case of connectivity changes on either side of the users.
- R12-3-3* In case the A-Party device does not provide a camera (hardware limitation), the ability to add a “live video” is not given. There shall not be any service entry point for adding “live video”.
- R12-3-4* In case the B-Party device does not have a camera built in (neither front facing nor rear facing) but is able to display video in 352x288 pixel resolution @ 15 fps (or better), the A-Party shall be able to trigger a 1-way “live video” to B-Party device. B-Party obviously shall have no option to activate the video channel back to A-Party.
- R12-3-5* In case the B-Party device does not have a camera built in (neither front facing nor rear facing) and is not able to display video in 352x288 pixel resolution @ 15 fps (or better), the A-Party shall not be able to trigger “live video” to B-Party.

**US12-4 As a user, when receiving a “share live video” request, I (i.e. user B) want to decide whether to:**

- a) Decline the incoming “live video” request and continue with a plain voice call,
  - b) Accept the incoming “live video” request without sending my camera view, or
  - c) Accept the incoming “live video” request and sending also my camera view.
- R12-4-1* The receiver (user B) shall be able to reject an incoming “live video” request and the voice call continues.
- R12-4-2* The receiver (user B) shall be able to accept an incoming “live video” request (i.e. no auto-accept) without initiating “live video” from their side.
- R12-4-3* The receiver (user B) shall be able to accept an incoming “live video” request (i.e. no auto-accept) with initiating “live video” from their side as well.

- R12-4-4* The receiver (user B) shall not be able to also add “live video” from their side in case any of the two parties (i.e. user A / B) is on 3G only.
- R12-4-5* The sender (user A) shall be notified accordingly about the selection of the receiver (user B) i.e. accepting or rejecting the “live video” service.
- R12-4-6* If the receiver (user B) decides to initiate “live video” back to the originator (user A), the originator shall not be prompted to accept or reject the “live video” request.
- R12-4-7* In case the receiver sends back a “live video” then the stream shall be shown directly on the originator’s device.
- R12-4-8* Upon acceptance of user A’s “live video” stream, the camera view shall be streamed to the receiver (user B) and displayed on the receiver’s screen.
- R12-4-9* An audio signal played on the recipient’s (i.e. user B) side should accompany any reception of an incoming “live video” request.

**US12-5 As a user accepting an incoming “live video” request, I (i.e. user B) want the incoming voice automatically on a connected headset. If there is no headset connected, then play the voice on my external loudspeaker.**

- R12-5-1* When an incoming “live video” is accepted, the audio part should be played either via a connected headset (if connected) or via the external loudspeaker (if no headset connected).

**US12-6 As a user sharing “live video”, when I rotate (i.e. user A / B) my device the correct video orientation is displayed on both ends.**

- R12-6-1* The device shall handle the different orientation permutations depending on how the device is rotated during a “live video” sharing to always show the incoming video in the right orientation (e.g. not upside down).

**US12-7 As a user sharing “live video” from my camera, I (i.e. user A / B) want to toggle between front and rear camera and upon selection video is changed without interruption (if the device supports two cameras).**

- R12-7-1* The user shall be able to toggle the camera (i.e. front / back) which is recording the transmitted live stream given the phone supports two cameras.
- R12-7-2* If the phone supports two cameras, the front camera shall be active by default for transmission of the “live video”.

**US12-8 As a user sharing “live video”, I (i.e. user A / B) want to stop sharing video at any point during the call without interrupting the underlying voice call.**

- R12-8-1* A user shall be able to terminate either its own and/or a received “live video” at any point during the call (i.e. three options (1) to stop own, (2) to stop received, and (3) to stop the complete “live video”) without degradation of the reliability of the underlying voice call.

NOTE: This is an explicit stop of the transmission not a “hiding” of video while the actual stream continues.

**US12-9 As users sharing "live video", we want to continue our call as "voice call only" if video support is lost during the call on either "live video" sharing leg.**

*R12-9-1* In case of loss of a "live video" share due to any reason the underlying voice call shall continue.

**US12-10 As users sharing "live video" (both one and two-way), we want the best possible quality of video available to us throughout the "live video" share for the bearer we use.**

*R12-10-1* A "live video" share over LTE shall benefit from a higher video quality than available on 3G.

*R12-10-2* A "live video" share over WiFi shall benefit from a higher video quality than available on 3G.

*R12-10-3* The quality of the "live video" stream shall be adapted to the currently available bandwidth (e.g. by changing radio conditions) and use bitrates lower than the maximum negotiated when the "live video" was initiated.

*R12-10-4* If technically possible, the quality of the "live video" stream shall be adapted to the currently available bandwidth and use bitrates higher than the rate negotiated when the "live video" was initiated.

**US12-11 As users sharing "live video" via ViLTE, we want to continue the transmission of the video as long as possible under changing connectivity situations delivering a high quality and lip sync experience.**

*R12-11-1* In case of changing connectivity conditions during an ongoing "live video" share, the transmission of the "live video" shall be maintained in a seamless manner if network conditions allow.

*R12-11-2* If "live video" cannot be continued seamlessly due to changing connectivity, an automatic establish of the "live video" share shall be attempted by the party changing its connectivity.

NOTE: Existing flows for initiating and accepting "live video" shall be followed as specified above.

**US12-12 As a user, I want to see (in my call logs) an indication if a "live video" share initiated by me or the other party during the call event.**

*R12-12-1* Both A-Party and B-Party call logs should identify that a "live video" share event occurred during the call.

*R12-12-2* Live video content shared during a call is not stored or accessible after the call for either party.

### 12.2.3 In-call Services: Image Share

Image Share is a service that allows sending a picture (either stored in a user's device or taken for the purpose) while in a voice call with a contact. The service differs from File Transfer only in terms of user experience and interface. In fact, sharing during a call, given the real time context, is an immediate task with minimal user interaction displaying the shared content within (or on top) of the calling screen. The Image Share functionality is



supported for Crane only for legacy reasons to support incoming Image Share requests. Crane does not support Image Share to “share a picture” from A-Party side, i.e. there shall be no entry point for sending Image Share.

**US12-13 As a user, when receiving an image share request, I (B-Party) want to decide whether to:**

- a) Decline the incoming image share request and continue with a plain voice call,
- b) Accept the incoming image share request.

*R12-13-1* The receiver shall be able to accept or reject an incoming image share (no auto-accept). The sender shall be notified accordingly about the selection of the receiver.

*R12-13-2* Upon acceptance the picture is transferred to the receiver.

*R12-13-3* Once the transfer of the image is completed the received picture shall be displayed with minimal user interaction on the receiver's screen.

*R12-13-4* When the underlying call is terminated for any reason, the image share shall stop and the receiver may no longer have access to the image.

*R12-13-5* While a received image share is displayed, the receiver should not be able to take a screenshot of the shared image.

*R12-13-6* An audio signal played on the recipients side should accompany any reception of an incoming image share request.

**US12-14 As a user accepting an incoming image share, I (B-Party) want the incoming audio automatically sent to a connected headset. If there is no headset connected, then I want the audio to be sent to my external loudspeaker.**

*R12-14-1* When an incoming image share is accepted, the audio call should be played either via a connected headset (if connected) or via the external loudspeaker (if no headset connected).

*R12-14-2* While the image is displayed it shall be made easy for the user to use the standard in-call features (i.e. toggle loudspeaker, mute, etc).

#### **12.2.4 In-call Services: Share any file during call**

The functionality to share any file during a call is basically based on File Transfer that happens usually within the context of messaging. Sharing during a call therefore happens within the context and user flows of the on-going voice call.

**US12-15 As a user while in a voice call, I (A-Party) want to share any file from my in-call screen with the other participant of the call (B-Party) whenever it is possible.**

*R12-15-1* File Transfer shall be possible during an on-going voice (e.g. CS/VoLTE/Wi-Fi Calling) call while the call shall continue seamlessly on the same bearer.

NOTE 1: This includes the case where other In-call Services are also in progress.

NOTE 2: The transmission of “live video” needs to be stopped by the user to initiate / accept an incoming file share.

*R12-15-2* During a voice call, the A-Party shall be able to send a file to the B-Party directly from the screen.

NOTE: This includes the case where other in call services are also in progress.

- R12-15-3* The support of file types and file sizes shall follow the behaviour described in R7-1-1.
- R12-15-4* Images and videos shall be able to be resized as described in R7-4-1 and R7-5-1 respectively.
- R12-15-5* An on-going File Transfer shall be completed even if the call was terminated. After completion a notification shall be displayed that the file is now accessible via the call logs.
- R12-15-6* Any file shared during a call shall be accessible from within the in-call screen for the duration of the on-going call. The file or a preview of the file shall be displayed on the in-call screen if the sending device supports the display of that file type. If display/preview of that specific file type is not supported a placeholder indicating the file name and type shall be displayed.
- R12-15-7* Most common file types for photos (e.g. jpeg, gif, png) shall be, at minimum, supported by the device to ensure display of the file.
- R12-15-8* While a shared file is displayed it shall be made easy for the user to use the standard in-call features (i.e. toggle loudspeaker, mute, etc.).
- R12-15-9* Browsing through the exchanged (sent AND received) files shall be possible during the whole duration of the call.

**US12-16 As a user while in a voice call when receiving a file share request, I (B-Party) want to decide whether to accept or reject the incoming invitation based on my Operator's configuration for File Transfer.**

- R12-16-1* Upon receiving an incoming file, the File Transfer shall follow the rules as described in US7-14 regarding automatic or manual download of the file.
- R12-16-2* Upon accepting the File Transfer (either automatically or manually) the file or a preview of the file shall be automatically displayed on the B-Party's In-call screen if the receiving device supports the display of that file type. If display/preview of the that specific file type is not supported the user shall be accordingly notified to ensure the simplest user experience how to access the file and a placeholder indicating the file name and type shall be displayed
- R12-16-3* Most common file types for photos (e.g. jpeg, gif, png) shall be, at a minimum, supported by the device to ensure display of the file.
- R12-16-4* Once the file transfer is started (either automatically or manually), the user shall be informed about the ongoing download process by visual (e.g. a progress bar) or text (e.g. 'loading').
- R12-16-5* Any file received during a call shall be accessible from within the in-call screen for the duration of the on-going call.
- R12-16-6* While a shared file is displayed it shall be made easy for the user to use the standard in-call features (i.e. toggle loudspeaker, mute, etc.).
- R12-16-7* Browsing through the exchanged (sent AND received) files shall be possible during the whole duration of the call.
- R12-16-8* An audio signal played on the recipients side should accompany any reception of an incoming file share / file share request.

- R12-16-9* It shall be possible to open a full file viewer application from the displayed file / preview of the file for further user interaction with the file (e.g. save, edit, share, etc.).

## 12.3 Technical Information

### 12.3.1 Overview

Based on the requirements, the in-call services are constituted of the following main services:

- “Live” Video: In line with the requirements in sections 10 and 11 of this document, in case the voice call is end to end IR.92/IR.51 voice call and the video service is available, “Live” Video shall be implemented as an end to end IR.94/IR.51 conversational video call based on procedures described in [NG.102]. In this case, the RCS Video Share service as described in section 2.7.1.2 and 3.6 of [RCC.07] Shall not be available to the user. In any other case, RCS Video Share service Shall be used. For the cases of IR.92/IR.51 voice interwork to legacy, RCS Video Share service is used. RCS Video Share service is possible to be established over LTE or EPC integrated WiFi access.
- Image share (share a picture during a call): Implemented via the RCS Image Share service as described in section 3.6 of [RCC.07].
- Sharing any file during a call: Implemented via the RCS File Transfer service as described in section 3.5 of [RCC.07].

The client shall indicate support for the listed services based on Capability Exchange mechanism described in section 2.9 of [NG.102].

NOTE: There is one exception to be considered; if the device is in a IR.92 / IR.51 voice call, the availability of the upgrade to video call (implemented through IR.94/IR.51 conversational video ) shall rely on the contact header negotiation during the call establishment (SIP INVITE and response).

RCS sharing services outside a voice call covered in sections 3.6.1.3, 3.6.1.4.4, 3.6.2.2, 3.6.2.4, 3.6.4.1.2 and 3.6.6.2 of [RCC.07] are outside the scope and thus not applicable.

### 12.3.2 Technical Implementation of User Stories and Service Requirements

*R12-17-1* Requirements R12-1-1 shall be implemented locally on the device.

*R12-17-2* For requirement R12-1-2, section 3.6.2.1.1 of [RCC.07] shall be taken into consideration. The client shall initiate in call services while being in a one to one call.

For requirement R12-1-3 section 12.3.1 of this document shall be taken into consideration.

*R12-17-3* Requirements R12-1-4, R12-1-5 and R12-1-6 shall be implemented locally on the device.

#### 12.3.2.1 Live Video

*R12-17-4* Requirement R12-2-1 shall be implemented locally on the device based on clarifications provided in section 12.3.1 of this document.

*R12-17-5* Requirement R12-2-2 shall be implemented locally on the device.

- R12-17-6* For requirement R12-2-3, in case IR.94/IR.51 conversational video is added, section 2.4 of [PRD-IR.94] shall apply.
- R12-17-7* Requirement R12-2-4 is in line with the service prioritisation described in section 12.3.1 of this document under the bullet of “Live” video.
- R12-17-8* For requirement R12-2-5, IR.94/IR.51 conversational video service is available only under E-UTRAN/EPC integrated Wi-Fi coverage. For the case of RCS Video Share, the PROVIDE VS parameter defined in Annex 1.6 of [RCC.07] shall be set accordingly.
- R12-17-9* Requirement R12-2-6 is related to RCS Video Share service. The RCS client shall not initiate an RCS Video Share session while being under 3G coverage. The PROVIDE VS parameter defined in Annex 1.6 of [RCC.07] shall be set accordingly so as not to allow video share service under 3G coverage.
- R12-17-10* For requirement R12-2-7, section 2.7 of [RCC.07] shall apply.
- R12-17-11* For requirement R12-2-8, in case IR.94/IR.51 conversational video service is used, IR.92/IR.51 voice call termination will result to video service termination . For the case that video share service is used, as per section 3.6 of [RCC.07] the requirement is aligned with the service description.
- R12-17-12* For requirements R12-2-9 and R12-2-10, for the RCS Video Share service and in order to prevent recording, the ALLOW VS SAVE parameter shall be set to zero.
- R12-17-13* For requirements R12-3-1 and R12-3-2, section 12.3.1 of this document shall apply.
- R12-17-14* Requirement R12-3-3 shall be implemented locally on the device. The RCS Video Share and IR.94/IR.51 conversational video services shall not be advertised by the client through the SIP OPTIONS exchange mechanism.
- R12-17-15* Requirement R12-3-4 shall be implemented locally on the device. For IR.94/IR.51 conversational video, section 2.2.2 of [PRD-IR.94] shall apply. For the RCS Video Share service, the client of user B shall not initiate an RCS Video Share session. The capability of IR.94/IR.51 conversational video or RCS Video Share is included as part of the capability exchange mechanism.
- R12-17-16* Requirement R12-3-5 shall be implemented locally on the device. For IR.94/51 conversational video, section 2.2.2 of [PRD IR.94] shall apply The client shall not advertise the capability of IR.94/IR.51 conversational video or RCS Video Share in the applied capability exchange mechanism.
- R12-17-17* For requirements R12-4-1, R12-4-2 and R12-4-3, for IR.94/IR.51 conversational video service section 2.2.2 of [PRD-IR.94] shall apply. For the RCS Video Share service section 3.6 of [RCC.07] shall apply.
- R12-17-18* Requirement R12-4-4 is only relevant for the RCS Video Share service. Similar to requirements R12-2-6 and R12-2-7, the PROVIDE VS parameter defined in Annex 1.6. of [RCC.07] shall apply.
- R12-17-19* Requirement R12-4-5 shall be implemented locally on the device based on the SIP INVITE response.

- R12-17-20* Requirements R12-4-6, R12-4-7, R12-4-8 and R12-4-9 shall be implemented locally on the device.
- R12-17-21* Requirement R12-5-1 shall be implemented locally on the device.
- R12-17-22* For requirement R12-6-1, for IR.94 conversational video service section 2.4.2 of [PRD-IR.94] shall apply. For IR.51 conversational video service, section 4.8.2 of [PRD-IR.51] shall apply. For RCS Video Share service, it shall be implemented following the image orientation extension described in 2.7.1.2.2 of [RCC.07].
- R12-17-23* Requirements R12-7-1 and R12-7-2 shall be implemented locally on the device.
- R12-17-24* For requirement R12-8-1, the video service used shall be taken into consideration. For IR.94/IR.51 conversational video, section 2.2.2 of [PRD-IR.94] shall apply.
- For RCS Video Share service, procedures as described in sections 3.6.4.3.4 and 3.6.4.3.5 of [RCC.07] shall apply.
- R12-17-25* For requirement R12-9-1, in case of IR.94/IR.51 conversational video service loss section 2.4 of [PRD-IR.94] shall apply.
- R12-17-26* For requirement R12-10-1, for IR.94 conversational video service section 3 and 4.2 of [PRD-IR.94] shall apply. For RCS Video Share service over LTE section 3.6.4.1.5 of [RCC.07] shall apply.
- R12-17-27* For requirement R12-10-2, for IR.51 conversational video service section 4.12 shall be considered.
- R12-17-28* For requirements R12-10-3 and R12-10-4 for RCS Video Share service section 3.6.4.1.4 of [RCC.07] shall apply.
- R12-17-29* For requirement R12-11-1, for IR.94/IR.51 conversational video service section 2.18 and Annex A of [NG.102] shall be taken into consideration. Change of connectivity conditions that result to service transition from IR.94/IR.51 conversational video service to RCS Video Share service or the opposite will result to service re-establishment. For change of connectivity conditions where RCS Video Share service remains the used service, sections 2.4.7 and 2.4.8 of [RCC.07] shall be taken into consideration.
- R12-17-30* Requirements R12-11-2 shall be implemented locally on the device.
- R12-17-31* Requirement R12-12-1 shall be implemented locally on the device.
- R12-17-32* For requirement R12-12-2, similar to R12-2-10, the ALLOW VS SAVE parameter defined in Annex A.1.6. of [RCC.07] shall be set to zero

### **12.3.2.2 Image Share**

In order to support image share requests coming from legacy clients, image share capability shall be included in the capability exchange during an ongoing call. However, the absence of entry point for outgoing image share requests shall be implemented locally on the device.

- R12-17-33* Requirements R12-13-1 and R12-13-2 are implemented as per section 12.3.1 of this document (image share bullet).
- R12-17-34* Requirement R12-13-3 shall be implemented locally on the device.
- R12-17-35* Requirement R12-13-4 for image access after the termination of the call, as per section 3.6.4.1.3 of [RCC.07], SDP attribute will not be

included due to legacy sender and consequently the shared image during the call will not be recorded by the receiver.

*R12-17-36* Requirement R12-13-5 and R12-13-6 shall be implemented locally on the device.

*R12-17-37* Requirement R12-14-1 and R12-14-2 shall be implemented locally on the device.

### 12.3.2.3 Share any file during call

*R12-17-38* The realisation of requirement R12-15-1 shall be implemented as defined in section 12.3.1 of this document (sharing any file during a call bullet).

*R12-17-39* Requirement R12-15-2 shall be implemented locally on the device. It is required for a client/device implementation to be able to identify whether a File Transfer is received from the other party in a call to, if so, present the File Transfer within the call window instead the messaging application.

*R12-17-40* Requirements R12-15-3 and R12-15-4 shall follow the procedures described in section 7.3 of this document.

*R12-17-41* Requirements R12-15-5, R12-15-6, R12-15-7, R12-15-8 and R12-15-9 shall be implemented locally on the device.

*R12-17-42* For requirement R12-16-1, section 7.3 of this document shall be considered.

*R12-17-43* For requirement R12-16-2, file display options are the same as described in section 7 of this document and are not different within an in-call context. The in-call screen display and the user notification for an unsupported file shall be implemented locally on the device.

*R12-17-44* Requirements R12-16-3, R12-16-4, R12-16-5, R12-16-6, R12-16-7, R12-16-8 and R12-16-9 shall be implemented locally on the device

### 12.3.3 Backward Compatibility

#### 12.3.3.1 Blackbird Clients

Blackbird clients shall be provisioned by crane networks without including the INCALL UX parameter defined in section 3 of [RCC.61] and ALLOW VS SAVE parameter defined in Annex 1.6. of [RCC.07]. The rest of the content sharing parameters remain the same.

#### 12.3.4 Configuration Parameters

The configuration parameters specific to in call services are defined in Annex A of [RCC.07] and [RCC.61]. For Crane they will be handled as follows:

Configuration parameter	Description
PROVIDE VS	Service Provider Configurable
PROVIDE IS	Service Provider Configurable
ALLOW VS SAVE	Fixed Value: 0
VS MAX DURATION	Service Provider Configurable
IS MAX SIZE	Service Provider Configurable

INCALL UX	Fixed Value: 0 NOTE: when receiving a provisioning document from a legacy network (blackbird), this parameter is not provided. A value of 0 shall be assumed in this case.
-----------	---

**Table 49: Crane Content Sharing configuration parameters**

## 13 API Extensions

### 13.1 Description

RCS APIs enable Operator developers (MNO Apps), OEM developers (OEM Apps) and developers from companies outside of the Operators (Third party apps) to integrate RCS features into their applications. APIs can be used by all these three different parties to enrich their applications with RCS functionalities, to build extra functionality on top of the native out of the box RCS experience.

MNOs leverage in-house developers, OEM developers and developers from companies outside of the Operator to propose innovative user experiences, which increase RCS use and data traffic and introduce new service extensions independent of OEM involvement.

This document covers requirements for all APIs available across any device and network.

NOTE1: The scope of API access is at first limited to MNO and OEM apps only. However the enablers put in place for this OEM/MNO API access shall be extensible to support Third party access in the future. This means that access to Third party apps running on an MNOs network can be opened by that MNO at their own discretion.

NOTE2: In this document “developer” means either OEM application developer, MNO application developer or Third party developer

The whole section is a new addition to Crane.

### 13.2 User Stories and Feature Requirements

**US13-1 As a user, I want to be able to install apps which use RCS APIs.**

**US13-2 As a user, I want to be reminded that my RCS APIs do not function on my device when I execute a RCS extension while I have deactivated my native RCS service.**

**US13-3 As a developer, I want to be able to add RCS communication features to my application using RCS functionality exposed through APIs.**

*R13-3-1* RCS APIs shall be provided via the terminal.

*R13-3-2* RCS APIs may be provided via the network in addition.

NOTE: The supported RCS APIs are listed in R13-7-3 below.

**US13-4 As a developer, I want to be able to integrate new RCS communication features into the native user interface using special APIs (UI hooks), at the following points:**

- Messaging Application,
- Call Application (s) (i.e. Dialler, Call Set-up Screen, In-call Screen, Incoming Screen),
- Contacts Application,

- Call Logs,
- “Sharing” Touch point.

NOTE: Details of UI Hooks and their actual availability are to be mutually agreed between interested Operators and implementing OEMs. These are explicitly not part of Crane.

**US13-5 As an Operator, I want the developer to insert an App ID, a Developer ID and the Feature Tags into the source code to be able to use RCS APIs.**

- R13-5-1* An App ID shall identify the app which generates the traffic through the RCS APIs.
- R13-5-2* A Developer ID shall identify the owner of the app.
- R13-5-3* App ID and Developer ID shall be are both unique.
- R13-5-4* An RCS enabled app installed on a device shall be able to offer one or more services that are each identified by a specific ID, a Feature Tag, that is considered as a capacity of the user / device.

**US13-6 As a developer, I want to be able to use a specific API called “Multimedia session” allowing two apps that have the same Feature Tag, to exchange specific data.**

- R13-6-1* A multimedia session shall be only established between two apps that support the same Feature Tag.
- R13-6-2* An interface shall check for a specific user the support of the same Feature Tag.
- R13-6-3* An RCS enabled app using “Multimedia session” shall provide a capability that follows the regular capability discovery mechanism.

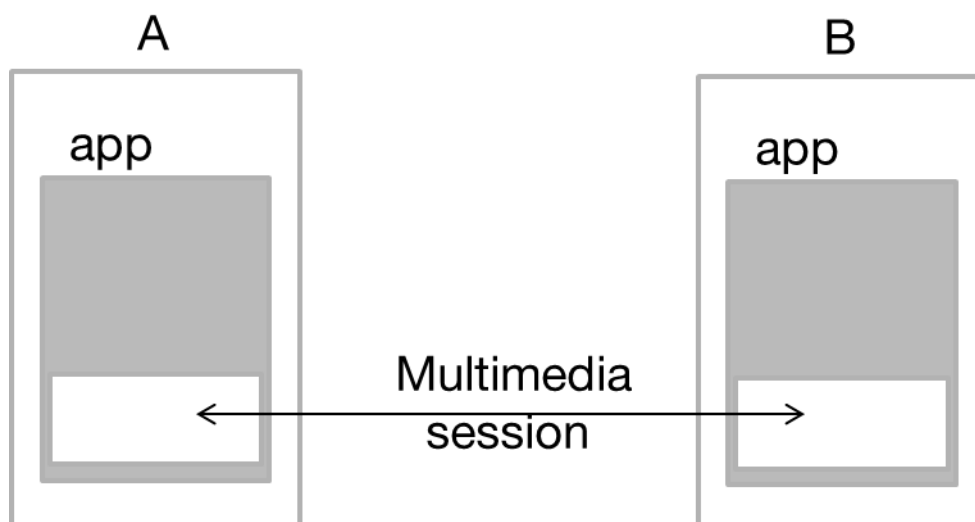


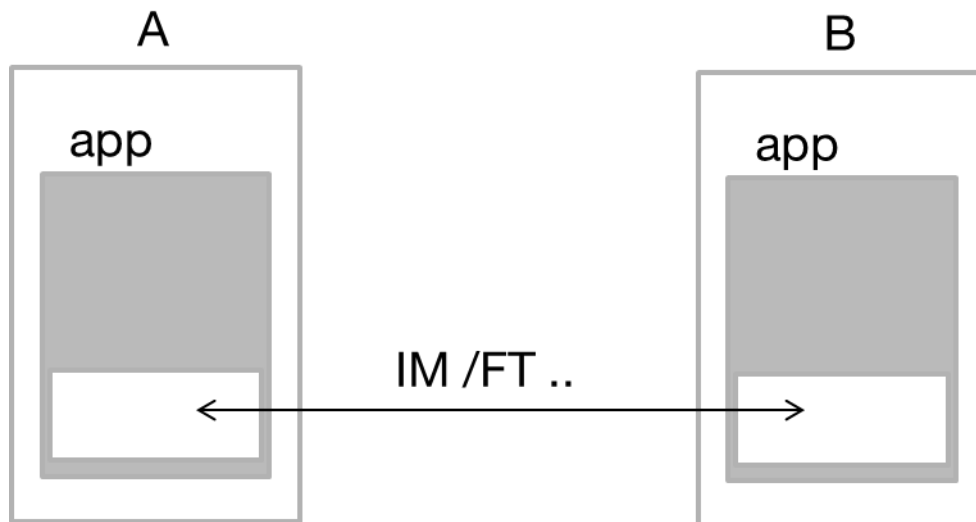
Figure 22: Multimedia session

**US13-7 As a developer, I want to be able to integrate RCS communications features within my apps through APIs so that end users are able to establish a communication from these apps. Two different scenarios shall be supported:**

- R13-7-1* The A-Party triggers an RCS communication between two apps using the APIs (App to App): In this mode, A-Party and B-Party shall both have the same Feature Tag. B-Party receives the RCS communication within this

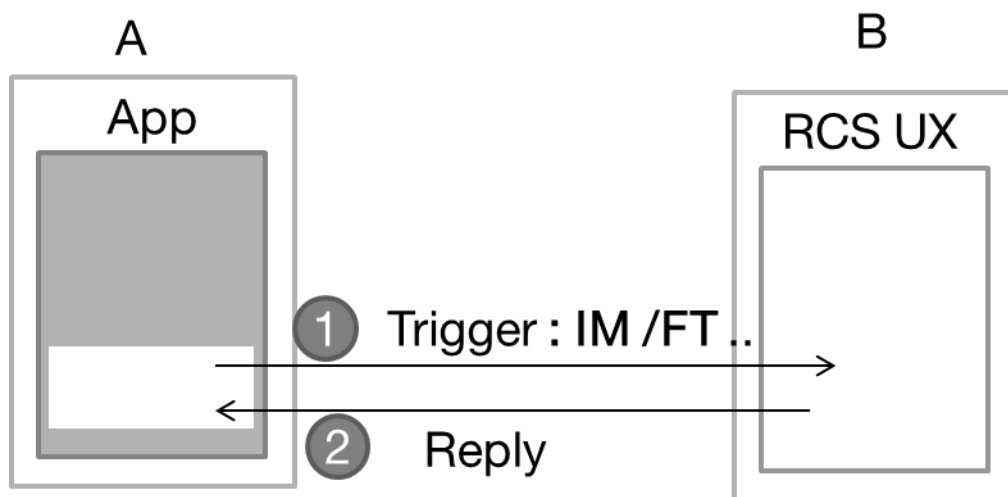


app (identified by the Feature Tag).



**Figure 23: App to App communication**

*R13-7-2* The A-Party triggers a standard RCS communication from an app using the APIs (App to RCS UX): In this second mode, B-Party is not required to have a specific app or service (identified by its Feature Tag) from where the communication has been generated. The B-Party receives the RCS communication in their native RCS app. The B-Party can reply to A from their native User Interface and the A-Party receives it on the app using the APIs and continues the conversation thread.



**Figure 24: App to RCS UX communication**

*R13-7-3* The RCS APIs shall support:

- Instant Messaging,
- File Transfer including geo-location,
- Audio Messaging,
- IP Video Call,
- Video share during a call

- Request for services configuration information relevant for the application (e.g. max number of participants in a Group Chat, max file size of a File Transfer, warning threshold for a File Transfer, IM CAP ALWAYS ON, and FT HTTP CAP ALWAYS ON).

**US13-8** As a user, I want to be able to see (via capability discovery) which of my contacts have installed the same RCS-enabled apps as I have installed.

**US13-9** As a user, when I install an RCS-enabled app, I want to be able to decide whether or not I want to make it discoverable to other users via capability discovery. If I opt not to make the app discoverable, my contacts will not see that I have installed the app. I cannot tailor the capability discovery response by contact.

**US13-10** As a user, I want to be able to change the discoverability setting for specific applications via RCS Settings. Apps may also provide this option within the application UI.

**US13-11** As a user, I want to be able to trigger interaction with a contact having the same enabled RCS app from the address book/contact card or from within the app.

**US13-12** As a user, when I uninstall an RCS-enabled app it is no longer notified to other RCS enabled app users in Capability exchange.

**US13-13** As an Operator, I want to be able to find out how many instances of each RCS-enabled app have registered their capability with my network, via the Feature tag.

**US13-14** As a user, when I install an app enabled by RCS, I want to be informed that this app will use the RCS services through the API.

**US13-15** As an Operator, I want to measure the data traffic triggered by each specific RCS-enabled app on my network, identified by the app's Feature Tag(s).

**US13-16** As an Operator, I can block traffic and withdraw access for a specific service or application making use of the RCS APIs, identified by the specific Feature Tags. Blocking an app which sends traffic (chat or File Transfers, etc.) to the native RCS UI (App-to-Native messaging) will not affect the user's ability to send such traffic from other apps or from their native RCS UI.

## 13.3 Technical Information

### 13.3.1 Overview

There are three different enablers that can expose different types of RCS API:

- Device or Terminal API
- Network API
- UI Hook.

This current version only covers Device API. Technical requirement matching for Network API and UI Hooks will be completed in a maintenance or future release of the Common Core.

The technical answers to above requirements may have technical requirements on several elements of the end to end RCS infrastructure:

- The terminal and associated RCS stack exposing Terminal API

- The UNI / NNI interface
- The application using the Terminal API
- The service provider RCS infrastructure

### 13.3.2 Requirements matching

*R13-17-1* For Terminal API, requirements of user stories US13-1 and US13-3 are covered by [RCC.53].

*R13-17-2* The requirements of user story US13-2 and US13-5 are left to device implementation.

*R13-17-3* Requirement R13-5-1 for identification of the services offered by the application is done through the IARI which uniquely identifies the service. This is ensured:

- At the UNI level, through the definition of the IARI and its usages in sections 2.6.1.1.3 and 2.6.1.2.6 of [RCC.07].

NOTE: The term application is equal to the term Extension as used in [RCC.07].

- At the terminal level, through the procedures defined in sections 4.4.4.5 of [RCC.53] and in section 8 of [RCC.55].

*R13-17-4* For requirement R13-5-1 and R13-5-2, identification of the developer for Second Party apps is covered by the security model defined in [RCC.55]. For Third Party apps, this is up to MNO implementation.

*R13-17-5* For requirement R13-5-3 the following applies:

- For the Feature Tag, uniqueness is ensured by the procedures described in section 5.3 for the second party app and in section 6.3 of [RCC.55].
- For Developer ID and App ID, this is dependent on MNO handling of those Identifiers.

*R13-17-6* Requirement R13-6-1 for multimedia sessions between the same application is covered:

- At UNI Level, using the multimedia session by the procedures defined in section 3.12.4.2.2 of [RCC.07].
- At the terminal level, through the procedures of section 4.4.12 of [RCC.53] for the Blackbird features.

*R13-17-7* Requirement R13-6-2 is ensured by procedures of capability discovery of [RCC.53].

*R13-17-8* Requirement R13-6-3 is ensured with the same procedures than requirement US13-8.

*R13-17-9* For requirement R13-7-1 and R13-7-3 the following applies:

- At the UNI level
  - If the communication is messaged based, using the MSRP protocol, the app shall follow the procedures defined in section 3.12.4.2.1.1 of [RCC.07].
  - If the communication is real time based, using the RTP protocol, the app shall follow the procedures defined in section 3.12.4.2.1.2 of [RCC.07].
- At the Terminal level through the procedures defined in [RCC.53].

*R13-17-10* For requirement R13-7-2 and R13-7-3 the following applies:

- At the UNI level, an app can set a communication with any other RCS entity which does not have specifically the same app using an RCS service by following the procedures defined in section 3.12.4.1 of [RCC.07].

*R13-17-11* Requirements of user story US13-8 is only applicable to applications that use features of requirements of user story US13-6 or requirement R13-7-1. The discovery is performed via the standard capability exchange mechanism (see 'Capability Discovery and Service Availability', page 27). Each app is uniquely identified by an IARI as defined in sections 2.6.1.1.3 and 2.6.1.2.6 of [RCC.07]. An app shall not be granted access to trigger a capability exchange itself. However the app may have access to the result of a prior capability exchange.

*R13-17-12* Requirement for user stories US13-9 and US13-10 are ensured at the application and stack level. These requirements are only applicable to applications that use features associated to requirement US13-6 or US13-7. When the user decides that a specific application shall not be discoverable by others contacts, this means that the application shall no longer apply the procedure described in sections 2.6.1.1.3 and 2.6.1.2.2.6 of [RCC.07] for that specific application. This requirement needs to be enforced on the client and is up to its implementation.

*R13-17-13* Requirements for user story US13-11 are ensured at the terminal level for the triggering from the address book and at the application level for the triggering within the application. At the address book level, this is ensured through the procedures defined in [RCC.53]. At the application level, it's up to the application to display this information provided through the API as per [RCC.53].

*R13-17-14* When an application is uninstalled, the requirements for user story US13-12 are covered at the stack level, by following the procedures defined in section 4.4.4.5 of [RCC.53].

*R13-17-15* The requirements of user story US13-13 are only applicable to applications that use features associated to user story US13-6 or requirement R13-7-2. It is ensured at the network level and is up to service provider policy. Identification of the app registering shall be done via the SIP REGISTER request that conveys the identity of the app through its IARI tag set in the Contact header as described in section 2.4.4.5 of [RCC.07].

*R13-17-16* Requirements for user story US13-14 is covered through procedures of section 4.4.2 of [RCC.53].

*R13-17-17* Requirements for user story US13-15 are applicable to all application using API (i.e. either derived from user story US13-6 or US13-7). They can be ensured at the network level and are up to service provider policy. Identification of the app generating a specific traffic may be done by linking the data plane with the SIP session that has allowed the data session establishment as the SIP INVITE request that was used to set the session shall convey the identity of the app through its IARI tag set in the Contact header as described in section 3.12.4.1 and 3.12.4.2 of [RCC.07].

NOTE: An application derived from user story US13-7 cannot be identified when using standalone messaging using SIP Message.

*R13-17-18* The requirements of user story US13-16 are covered:

- At the UNI level, a Service Provider can control dynamically the authorization of any app to access the RCS infrastructure, for any user, via the EUCR mechanism described in section 3.12.4.3 of [RCC.07]. These network initiated requests indicate to the device to block an app or a list of apps for a certain duration (the duration can be unlimited).
- At the network level, triggering of the revocation procedures in the network is dependent on individual Operator policy on revocation procedures.

#### *R13-17-19 Security model*

- Devices exposing API shall restrict applications from accessing the RCS infrastructure based on the security model defined in [RCC.55] and on the service provider's policy provided through provisioning (see Device Provisioning, page 11). The 'ALLOW RCS EXTENSIONS' parameter defined in Table 94 of [RCC.07] indicates at a general level whether apps are allowed or not.

## 14 Security against Malware

### 14.1 Description

Authentication in RCS services on an individual device is today done with a solution based on username / password combination. There is a risk that these credentials are hijacked by a malware application and used for spoofing identities. There is a need to offer an enhanced security function at least temporarily until a long term solution is available.

This entire section is to be considered a new section on top of Blackbird implementations.

### 14.2 User Stories and Feature Requirements

#### **US14-1 As a user, I want to use my Operator communication services safely and securely.**

- R14-1-1* RCS services shall use an authentication mechanism that is safe and secure, not allowing 3rd party applications to retrieve any user data including data that is relevant for authentication against networks.
- R14-1-2* Authentication mechanism(s) shall be defined for a user on devices with a SIM.
- R14-1-3* Authentication mechanism(s) shall be defined for a user on devices without a SIM.
- R14-1-4* Devices containing a SIM which is associated with the user's RCS identity shall use any available SIM-based authentication mechanism in preference of a non-SIM based authentication mechanism.
- R14-1-5* User interaction to ensure security solutions shall be minimised.
- R14-1-6* If manual user interaction is required, this interaction shall be limited to a single one time experience and not be repeated, in case – but not limited to – device re-provisioning.
- R14-1-7* If manual user interaction is required, for native implementations any user interaction shall be performed on one single screen (or an intuitive flow of screens).

#### **US14-2 As an Operator, I want to customise the enhanced security function.**

*R14-2-1* The security solution shall offer the option for the Operator to enable or disable the function with appropriate security control.

R14-2-1-1 Enable or disable over the air.

R14-2-1-2 Enable or disable for selected devices.

*R14-2-2* If user interaction is required, the user shall be guided to accomplish the interaction in a way that RCS use of the primary identity is enabled in a secure way after the set-up process.

**US14-3 As an Operator, I want to ensure that traffic and content generated by an RCS identity is generated by that identity's true user.**

*R14-3-1* Second Party and Third Party applications shall inherit the identity of the stack therefore whilst API access may be controlled (not addressed here) no additional RCS authentication shall be required from second and third party applications.

*R14-3-2* All traffic generated by an identity shall be identifiable as such.

### 14.3 Technical Information

The technical implementation of RCS involves a number of technologies on the user network interface. Encryption, user authentication and access authorization is applied by the client and the network on a per protocol basis (e.g. SIP, HTTP, IMAP). The level of security for the individual technologies depend on the selection of the mean of authentication applied in the technical specification.

#### 14.3.1 User Authentication

The following main user authentication and methods are used in RCS.

*R14-4-1* User Authentication via the UICC based Authentication and Key Agreement protocol (AKA). This authentication protocol comes with a high level of security based on shared secrets exchanged between the UICC and the network authentication centre. As a result of the initial authentication session keys are agreed which are used to secure the UNI signalling flow. As an extension to the UICC based authentication the key material received from the AKA authentication can be used by the client to create additional security associations with network services based on the Generic Bootstrap Architecture (GBA) as defined in [3GPP TS 33.220]

*R14-4-2* User Authentication via the basic or digest access authentication based on credentials (user name and password) exchanged between the application and the peer network application. Since the RCS user stories aim to prevent that the user is involved in the exchange of the access credentials an automatic provisioning of the credentials is applied via device provisioning. The digest procedure in itself is secure and robust against attacks. It is vulnerable to attacks to discover the credentials via access to the application's key store or spoofing attacks based on the credential management procedure (e.g. malware pretending to be an RCS application).

*R14-4-3* Network based user identification via "header enrichment" or "GPRS IMS Bundled Authentication" (GIBA) which is in fact a single-sign-on (SSO) prolonging the authentication of the user at the time of bearer set-up for the usage of services within the bearer session. The bearer set-up in a 3GPP network is typically based on the UICC based Authentication and Key

Agreement protocol. The IP address assigned at the time of bearer set-up is used as the “token” to identify the user within the existing bearer session. This identification mechanism is secure in itself, provided that the Service Provider takes precautions in securing the trusted and untrusted network access to prevent fraudulent IP address claims. However attackers will be able to gain unauthorised access to the network services using a bearer session on behalf of the user.

*R14-4-4* User based Authentication via one time password (OTP), whereby the user is authenticated for a signalling transaction by using a token transfer over a channel with a secure identification or authentication context, e.g. the short message service or a sign on to a web portal. Based on the one time authentication a long term authentication context can be generated (SSO) to prevent the need for subsequent authentication transactions. Depending on the usage scenario the OTP based authentication can be executed without user impact (e.g. primary devices in non 3GPP access) or with user impact (additional non SIM devices).

The single token exchange via OTP is secure in itself. However it is vulnerable to spoofing attacks to gain access to the token used to authenticate the access, e.g. via initiation of the authentication by malware on behalf of the user and eavesdropping of the OTP transfer.

### 14.3.2 Encryption

The User Network Interface transactions should be always encrypted to prevent eavesdropping of the user’s personal communication in the various access and transit networks. RCS makes use of the common encryption protocols, i.e. Transport Layer Security and IPsec.

### 14.3.3 Storage of Authentication and Identification Data

The RCS client need to store for active RCS users authentication and identification data (user identification data, password, token) used for network access. The client shall store this data in a secure manner to prevent access from users and invaders.

For the requirements in user story US14-1 the following applies.

*R14-4-5* RCS makes use of a number of authentication mechanisms with some of them being vulnerable to attacks as summarised on a high level in section 14.3.1. Thus the risk that 3rd party applications are able to retrieve user data or to make use of communication services on behalf of the user persists. The main RCS vulnerability comes from the fact that user identification and authentication data is made available to consumers via a device management technology with weak security measures.

The following authentication mechanisms and encryption methods are used on a UNI technology basis.

*R14-4-5-1* HTTP(s) based client configuration in 3GPP access makes use of either the Generic Bootstrapping Architecture (GBA) (see R14-4-1) or network based user identification via (see R14-4-3) as defined in section 2.4 and 2.2 of [RCC.14] respectively. The authentication mechanism is negotiated between client and server as defined in [RCC.14]. A client not being in SIM Ready State shall not invoke client configuration procedure.

As defined in section 2.2.5 the Service Provider may decide to further secure the network based authentication identification via invocation of the SMS based procedure which adds additional authentication (see R14-4-44). The SMS based procedure may be further secured by the service provider by enforcing user input of the OTP as defined in section 2.3.5 of [RCC.14].

Client configuration transactions carrying user data are encrypted via TLS/SSL as defined in sections 2.2.5 of [RCC.14].

Client configuration transactions carrying user data are encrypted via TLS/SSL as defined in sections 2.3.3.2.5 of [RCC.07].

*R14-4-5-2* HTTP(s) based client configuration on non 3GPP access for primary makes use of either AKA based on the GBA (see R14-4-1) or the authentication method (see R14-4-4) as defined in sections 2.3, 2.5 and 2.6 of [RCC.14]. The authentication mechanism is negotiated between client and server as defined in [RCC.14]. A client not being in SIM Ready State shall not invoke client configuration procedure

Client configuration transactions are encrypted via TLS/SSL as defined in 2.3.3.2.5 of [RCC.07].

*R14-4-5-3* The authentication method for IMS access depends on the IMS registration mode of the device, the type of access and the device configuration. The client shall apply the IMS authentication as defined in sections 2.5 and 2.6 of [NG.102]. As clarification to [NG.102] the following applies

Note 1 of section 2.5.3 of [NG.102]; the client shall not take any actions to enforce different private user ID for the two registrations.

A client not being in SIM Ready State shall not register in IMS.

The encryption of SIP signalling is determined by client configuration as defined in section 2.8 and A.2.10 of [RCC.07].

*R14-4-5-4* The authentication method for HTTP transaction of File Transfer over HTTP shall be based on either basic or digest authentication (see R14-4-2) based on the credentials received by the client via device configuration or via bootstrapped security association (see R14-4-1) as defined in section 3.5.4.8.3 and 3.5.4.8.6.4 of [RCC.07].

The authentication mechanism is negotiated as defined in section 3.5.4.8.3 and 3.5.4.8.6.4 of [RCC.07].

A client not being in SIM Ready State shall not invoke the file transfer transactions.

HTTP File Transfer transactions carrying user data are encrypted via TLS/SSL as defined in 3.5.4.8.5 of [RCC.07].

*R14-4-5-5* The authentication method for IMAP sessions for the Common Message Store is either based on an AKA based bootstrapped security association (see R14-4-1) or based on basic authentication (see R14-4-2) with the CMS credentials received by the client via device configuration as defined in section 2.13.1.5 of [RCC.07]. The authentication mechanism is negotiated as defined in section 3.2.4.7.7



of [RCC.07]. A client which is not in SIM Ready State shall not login to the Common Message Store.

IMAP sessions are encrypted by use of TLS as defined in section 2.6.2.1 of [RCC.07]. The definition of section 2.13.1.5 regarding the use of STARTTLS shall be ignored. Section 3.2.6.2.1 takes precedence

*R14-4-5-6* The authentication method for HTTP/XCAP transactions with the XDMS is either based either based on AKA based on the Generic Bootstrapping Architecture (GBA) (see R14-4-1) or digest authentication (see R14-4-2) with the IMS credentials received by the client via device configuration or network based user identification (see R14-4-3) as defined in section 2.13.1.4 of [RCC.07].

The encryption of HTTP/XCAP is based on TLS as defined in section 2.8 of [RCC.07].

*R14-4-5-7* For MSRP transaction no additional user identification is applied. The MRSP transactions rely on the user identity that has been authenticated in the related SIP registration of session.

The encryption of MSRP signalling is determined by client configuration as defined in section 2.8 of [RCC.07] and 2.2.2.2 of [RCC.15].

*R14-4-5-8* For RTP media streams no additional user identification is applied. The RTP transactions rely on the user identity that has been authenticated in the related SIP registration of session.

The encryption of RTP streams is determined by client configuration as defined in section 2.8 of [RCC.07] and 2.2.2.2 of [RCC.15].

*R14-4-6* For the requirements in user story US14-2 to minimise the user interaction for security solutions a case by case analyses of user interaction flows for device configuration and personalization is done below. User interactions can be characterised with regard to their user experience as “in-band” or “out-of-band”. In-band refers to user interactions that can be smoothly integrated in the user interface based on well-defined RCS signalling flows. Out-of-band refers to user interaction flows that come not with RCS signalling flows but with another media channel, most likely a user readable short message.

*R14-4-6-1* “HTTP(s) based client configuration mechanism over 3GPP access” as defined in section 2.2 of [RCC.14] is transparent for the user if the service provider supports with the network to supports network based user identification. If the Operator does not support network based user authentication, then it may invoke the procedures for the client configuration over non 3GPP access. The corresponding user interactions apply as defined below.

*R14-4-6-2* “HTTP(s) based client configuration mechanism over non 3GPP access” as defined in section 2.3 of [RCC.14] requires user prompt for MSISDN and OTP password which is “in-band”. The OTP password in itself is received in between the two prompts is “out-of-band”. The exact flow depends of the device capabilities to determine the user identity (IMSI) of the SIM or to receive short messages on UDH ports or the service provider policy to enforce user prompts for OTP as defined in section 2.3.2 of [RCC.14].

*R14-4-6-3* For the configuration of additional devices sharing an identity there are a number of user interactions involved.

The primary device holding the user's identity to be federated with the additional device may support a procedure to enable the user consent based on the external EUCR as defined in section 2.1.2 of [RCC.15]. The user dialogue associated with this action is "in-band".

The procedure to request the federation of the user identity of a primary device via the "HTTP(s) based client configuration mechanism for alternative devices sharing a user identify" as defined in section 2.3.5 of [RCC.14] requires user prompt for MSISDN and service provider indication on the additional device. In addition the user may need to enter an OTP or a PIN as defined in section 2.5.1 of [RCC.14] and 2.1.2.1 of [RCC.15]. This full user interaction flow is "in-band".

The reception of the OTP on the primary device via SMS as defined in section 2.5.1 of [RCC.14] is "out-of-band".

The user interaction for the federation consent on a primary device via the external EUCR as defined in section 2.1.2.1 of [RCC.15] is "in-band".

The user interaction for the input of a PIN on the primary device as defined in section 2.1.2.2 of [RCC.15] is "in-band".

*R14-4-7* For the requirements in user story US14-2 the following applies:

*R14-4-7-1* The enhanced security function can be enabled or disabled by the service provider as defined in section 2.3.3.2.5 and 2.3.3.3.4 of [RCC.07].

*R14-4-7-2* The enhanced security function makes use of general client procedures for the user identification and authorization. These procedures have only limited capabilities to convey Operator specific explanatory text. Only the out-of-band transaction provides the service provider with the capability to convey specific information. However this is outside of the scope of this specification.

*R14-4-8* For the requirements in user story US14-3 the following applies:

*R14-4-8-1* The RCS implementation assumes one common user identity managed across all involved technologies (e.g. SIM, Device Configuration, IMS, and Messaging Server, Common Message store, Voice and Video services). It is the service provider responsibility to maintain this user identity and the related authentication, permission and preference data in sync across all technologies and network services. The RCS client shall use for RCS access only the user data retrieved from the SIM or via the user profile received from Device Configuration. This allows the network to assign all traffic and service usage events to this single user identity.

#### **14.3.4 Applicability of Authentication Methods**

This section gives an overview of the applicability and support requirements of user authentication methods defined in section 14.3.1 of this document for the types of RCS clients defined in this specification and its interfaces to the network.

User Network Interface	Primary Device	
	Single Registration Configuration (see NOTE)	Dual Registration Configuration (see NOTE)
Service Provider Client Configuration Configuration Over Cellular Networks	Support of network based authentication is mandatory. Support of fall-back to OTP based authentication is mandatory. Support of security configuration mechanism over PS and support of SMS port zero policy is mandatory. Support of GBA authentication is mandatory.	
Service Provider Client Configuration Configuration Over non 3GPP networks	Support of OTP based authentication is mandatory. Support of GBA authentication is mandatory.	
IMS Access Authentication	Support AKA based authentication is mandatory in accordance with [NG.102]	Support of SIP digest with the credentials from client configuration is mandatory in accordance with [NG.102]
HTTP File Transfer Content Server Authentication	Support of HTTP digest and basic authentication with the credentials from client configuration is mandatory Support of GBA based authentication is mandatory.	
Message Store Server Authentication	Support of plain password authentication is mandatory. Support of GBA based authentication is mandatory.	
Authentication for HTTP/XCAP transactions with the XDMS	Support of HTTP digest and basic authentication with the credentials from client configuration is mandatory Support of network based authentication is mandatory. Support of GBA authentication is mandatory.	

**Table 50: Authentication Mechanisms for embedded clients on primary device**

NOTE: The configuration of whether to support a single registration or two separate registrations is dependent on the RCS VOLTE SINGLE REGISTRATION parameter in the IMS MO and the NO MSRP SUPPORT parameter in the APN Configuration MO of [RCC.07] (see Table 2 of [NG.102]).

User Network Interface	Primary Device		
	ORSC		3RC, VARA
	Using terminal API	Not using terminal API	
Service Provider Client Configuration Configuration Over Cellular Networks	Same as device that provides the terminal API	Support of network based authentication is mandatory. Support of fall-back to OTP based authentication is mandatory. Support of security configuration mechanism over PS and support of SMS port zero policy is mandatory. The authentication mechanism is negotiated between the client and server in accordance with [RCC.14]	Same as device that provides the terminal API
Service Provider Client Configuration Configuration Over non 3GPP networks	Same as device that provides the terminal API	Support of OTP based authentication is mandatory.	Same as device that provides the terminal API
IMS Access Authentication	Same as device that provides the terminal API	Support of SIP digest with the credentials from client configuration is mandatory	Same as device that provides the terminal API
HTTP File Transfer Content Server Authentication	Same as device that provides the terminal API	Support of HTTP digest and basic authentication with the credentials from client configuration is mandatory	Same as device that provides the terminal API
Message Store Server Authentication	Same as device that provides the terminal API	Support of plain password authentication is mandatory.	Same as device that provides the terminal API

**Table 51: Authentication Mechanisms for non embedded clients on primary device**

NOTE: At the time of writing there is no definition of a terminal API to joyn Crane. It is assumed that support of new technologies of the User-Network Interface and their authentication methods are transparent to the API.

## 15 Data Off

Customers in many cases switch cellular data usage off locally on their device, mainly driven by the experience of commercial conditions in situations such as data roaming. To allow the Operator to offer IR 92 / IR 94 and RCS services to their customers even in these use cases, the data off switch shall have an Operator configurable impact on the device connectivity. It shall be up to the individual Operator to ensure a good Operator service experience by the

end user in cases that allow IP service usage even if the data switch was set to “OFF” by the end user.

This entire section is to be considered a new section on top of Blackbird implementations.

## 15.1 User Stories and Feature Requirements

### **US15-1 As a user, I want to use Operator voice and video calling irrespective of my chosen connectivity conditions.**

*R15-1-1* Voice and video services shall be available whenever the device is registered to a cellular network or a Wi-Fi connection is available.

NOTE: The availability of voice and video services offer over Wi-Fi is at the discretion of the Operator.

*R15-1-2* The Operator shall be able to zero rate data traffic which is induced by voice and video calling and meter minutes instead.

NOTE: Signalling that is used for production of Operator voice and video services shall be in the background and hidden from the user, i.e. also not metered.

*R15-1-3* Operator voice services shall be available over the cellular network irrespective of the setting of the cellular data switch.

*R15-1-4* Operator video services shall be based on Operator configuration (see R15-4-2) be available over the cellular network when the cellular data switch is switched off.

*R15-1-5* In domestic case and roaming, the Operator tariff scheme for voice and video services applies.

*R15-1-6* Operator voice and video services over cellular shall be disabled by the device in-flight mode. Voice and video calls over Wi-Fi may be possible (if offered by the Operator and allowed by the airline, see note to 15.1.1).

*R15-1-7* Wi-Fi based Operator voice, as described in RCS, shall only be available (if offered by the Operator) if Wi-Fi capability is enabled on the device, the device is attached to a (public or private) Wi-Fi access point and the Wi-Fi access point has connection to the Operator voice service.

### **US15-2 As a user, I want to use Operator Messaging Services irrespective of my chosen connectivity conditions.**

*R15-2-1* The Operator shall be able to zero rate data traffic which is induced by Operator Messaging and meter events instead.

NOTE: Signalling that is used for production of Operator Messaging shall be in the background and hidden from the user, i.e. also not metered.

*R15-2-2* Operator Messaging over cellular shall be disabled by the device in-flight mode. Usage over Wi-Fi may be possible (if offered by the operator and allowed by the airline).

*R15-2-3* RCS Messaging as part of Operator Messaging shall be based on operator configuration (see R15-4-2) be available over the cellular network when the cellular data switch is switched off.

*R15-2-4* The SMS service shall be available whenever the device is registered to a cellular network.

*R15-2-5* In domestic case and in roaming, the Operator tariff scheme for Operator Messaging services applies.

- R15-2-6* The Operator MMS service shall be available whenever the device is registered to a cellular network.
- R15-2-7* The various device settings for MMS (e.g. but not limited to, MMS auto-acceptance, MMS auto-acceptance in roaming, etc.) shall apply.
- R15-2-8* The Operator RCS Messaging Services shall be available whenever the device is connected to a cellular network or a Wi-Fi connection is available.
- NOTE: Wi-Fi service offer is at the discretion of the Operator.
- R15-2-9* The Operator may apply as part of the terms and conditions a “Fair Use Policy for Data Consumption of RCS Services on Home Network” which shall not apply for usage on visited networks (e.g. in case of national or international roaming).
- R15-2-10* In case there is only a reduced Operator Messaging function available due to connectivity restrictions caused by the data switch set to “OFF”, the user should be informed by the device about the restricted functionality and offered a shortcut UI function to the data switch to select “ON” for full functionality.

**US15-3 As a user, I want to use 3rd party services on my (smartphone) device or browse the Internet or an Intranet.**

- R15-3-1* The Operator Internet Access service shall be available whenever the device is registered to a cellular network and the user is enabled by the Operator to use cellular data services.
- R15-3-2* The device may offer internet access services using a Wi-Fi connection as well. The user shall be free to select which access service shall be used for connection to Internet services at any point in time.
- R15-3-3* Signalling that is required for the production of internet-based 3rd party services is not separated from any user data and counted as such as user data.
- R15-3-4* Internet-based 3rd party services are not available over cellular access when the cellular data switch is switched off.
- R15-3-5* Internet-based 3rd party services can be accessed over Wi-Fi (if offered by the 3rd party) if Wi-Fi capability is enabled on the device, the device is attached to a (public or private) Wi-Fi access point and the Wi-Fi access point has connection to the internet.

**US15-4 As an Operator, I want to use various technologies for the production of Operator communication services.**

- R15-4-1* For production of Operator voice, video and messaging services, the following technologies / bearers shall be considered in scope:
- R15-4-1-1* CS call over 2G network,
  - R15-4-1-2* CS call over 3G network,
  - R15-4-1-3* VoLTE call over 4G network,
  - R15-4-1-4* RCS IP call over Wi-Fi bearer,
  - R15-4-1-5* SMS over 2G and 3G network,
  - R15-4-1-6* IR.92 SMS over 4G network,
  - R15-4-1-7* MMS over 2G and 3G network,
  - R15-4-1-8* MMS over 4G network,

- R15-4-1-9* RCS Chat over 2G, 3G, 4G network or Wi-Fi bearer,
  - R15-4-1-10* RCS File Transfer over 2G, 3G, 4G network or Wi-Fi bearer,
  - R15-4-1-11* RCS In-Call services over 3G, 4G networks or Wi-Fi bearer,
  - R15-4-1-12* RCS IP Video Call over 3G, 4G network or Wi-Fi bearer,
  - R15-4-1-13* IR.94 ViLTE over 4G network,
  - R15-4-1-14* Operator Provisioning over 2G, 3G, 4G networks or Wi-Fi bearer.
- R15-4-2* The availability of the services listed in requirement R15-4-1 shall be configurable on a per- Operator basis as per the table below.

	<b>Proposal to satisfy implementation scenarios</b>	<b>Example: Implementation Scenario 1</b>
CS Voice (as in 15.4.1.1 to 15.4.1.2)	<b>Always on</b>	Always on
SMS (as in 15.4.1.5)	<b>Always on</b>	Always on
IP Voice (as in 15.4.1.3 to 15.4.1.4)	<b>Configurable</b>	Always on
PS xMS (as in 15.4.1.6 to 15.4.1.8)	<b>Configurable</b>	Always on
RCS Chat (as in 15.4.1.9)	<b>Configurable</b>	Always on
RCS File Transfer (as in 15-4-1-10)	<b>Configurable</b>	Always on
RCS In-Call Services (as in 15-4-1-11)	<b>Configurable</b>	Always on
RCS IP Video (as in 15-4-1-12)	<b>Configurable</b>	Always on
ViLTE (IR.94) (as in 15.4.1.13)	<b>Configurable</b>	Always on
Provisioning (as in 15.4.1.14)	<b>Configurable</b>	Always on
PS data/Internet Access	<b>Always off</b>	Always off
<b>NOTE</b>	<b>Any configuration affects device and network</b>	

**Table 52: Summary of proposed implementation and desired behaviour of services when DATA is OFF**

## 15.2 Technical Information

*R15-5-1* The technical realisation of data off behaviour is applicable to devices in the following way:

*R15-5-1-1* TE1: For primary devices that use the IMS or HOS APN for RCS (see ALWAYS USE IMS APN in section A.1.12 of [RCC.07] and RCS VOLTE SINGLE REGISTRATION in 'Green Button Promise for Voice' section, page 120) the complete behaviour is applicable.

*R15-5-1-2* TE2: For primary devices that use the internet APN for RCS (see ALWAYS USE IMS APN in section A.1.12 of [RCC.07] and RCS VOLTE SINGLE REGISTRATION in 'Green Button Promise for Voice' section, page 120), the connectivity when data is switched off would be handled based on the provided value of the RCSE ONLY APN as described in section 2.9.1.4 of [RCC.07]. The data off behaviour is applicable only when an RCSE ONLY APN is configured.

*R15-5-2* For requirement R15-1-1, PS voice services shall be available if allowed by configuration (see "Green Button Promise for Voice" section, page 120), supported by the current network coverage and allowed based on the current data off setting (see R15-5-21). If PS voice services are not allowed, a CS voice call shall be possible when the device is connected to a cellular 2G/3G network. When connected to an LTE network calls can in that case be provided through Circuit Switched Fall-Back. A CS voice call is not possible for a device that only has Wi-Fi coverage.

*R15-5-3* For requirement R15-1-2, such zero rating is possible for the Home Public Landline Mobile Network (HPLMN) Operator as well as for the Visited Public Landline Mobile Network (VPLMN) Operator for the voice service itself. For the configuration of supplementary service by a VoLTE subscriber, the HPLMN Operator can zero rate based on the specific destination of the traffic. Given that a home routed APN is used for XCAP, such differentiation of traffic may not be possible for the VPLMN Operator.

NOTE: Rating in the VPLMN is only relevant for inter- Operator charging and thus not directly for the end user. The inter- Operator charging model should be such so that the end user model makes sense from a business perspective.

*R15-5-4* For requirement R15-1-3, see R15-5-2.

*R15-5-5* Requirement R15-1-4 shall be implemented locally on the device taking into account the behaviour of RCS services in relation to the current data off setting configured as per R15-5-21.

*R15-5-6* For requirement R15-1-5, see R15-5-3.

*R15-5-7* Requirement R15-1-6 shall be implemented locally on the device when the Operator has configured RCS IP Voice to be available over Wi-Fi. Since the device has no defined way to find out automatically, compliancy to the airline policy for enabling Wi-Fi is up to the end user.

*R15-5-8* Requirement R15-1-7 is fulfilled through the RCS IP voice service as described in 'Green Button Promise for Voice' section, page 120.

*R15-5-9* For requirement R15-2-1, such zero rating is possible for the HPLMN Operator for all services because messages and signalling always pass through the home network and target well defined addresses. That allows to differentiation from other traffic.



- R15-5-10* For the VPLMN for requirement R15-2-1, zero rating would always be possible for SMS whereas MMS and File Transfer via HTTP use a home routed APN which will prevent the VPLMN from applying such differentiated charging in an easy way allowing only for generic volume based charging without differentiation between signalling and media. For the enablers for the other Operator messaging services (RCS Chat, Standalone Messaging and File Transfer via MSRP) the situation for the VPLMN Operator depends on whether or not IMS roaming is in place for RCS. Without IMS roaming or if RCS is not using IMS roaming (i.e. TE2), zero rating will not be possible allowing only for generic volume based charging without differentiation between signalling and media. If IMS roaming is in place, the VPLMN can differentiate between the signalling to establish the session and the media streams, but for the media stream itself only volume based charging can be applied without further differentiation.
- R15-5-11* Requirement R15-2-2 shall be implemented locally on the device. Since the device has no defined way to find out automatically, compliancy to the airline policy for enabling Wi-Fi is up to the end user.
- R15-5-12* Requirement R15-2-3 shall be implemented locally on the device taking into account the behaviour of RCS services in relation to the current data off setting configured as per R15-5-21.
- R15-5-13* Requirement R15-2-4 is fulfilled for SMS over CS. When using SMS over SGs (Signalling Gateways) in LTE coverage, the device shall establish a data connection even when data is turned off in which case the device shall not allow any data over that connection (unless allowed as per R15-5-21). SMS over IP shall only be possible when Data is switched on or when SMS over IP is allowed when Data is off as per R15-5-21.
- R15-5-14* For requirement R15-2-5, the HPLMN Operator can apply any tariff scheme for any Operator messaging service. For the VPLMN Operator tariffs the restrictions in R15-5-10 should be taken into account.
- R15-5-15* For requirement R15-2-6 MMS shall be available when data is off if allowed as per R15-5-21. This shall be implemented locally on the device.
- R15-5-16* Requirement R15-2-7 shall be implemented locally on the device.
- R15-5-17* Requirement R15-2-8 shall be implemented locally on the device when connected on Wi-Fi. When connected on cellular and when using the IMS APN, RCS messaging shall be available as per SMSOIP DATA OFF described in R15-5-21. When RCS is using the internet APN (TE2), RCS messaging shall be available as per section 2.9.1.4 of [RCC.07]: if data is on, RCS messaging shall be available. If data is off and RCS is using the internet APN, the RCSE-ONLY APN shall be used if configured and RCS Messaging shall be available on cellular networks if allowed as per R15-5-21. If no value is configured for the RCSE ONLY APN configuration parameter, RCS Messaging shall not be available on cellular networks in those circumstances.
- R15-5-18* For requirement R15-2-9, a Fair Use Policy in the home network shall be possible as a consequence of R15-5-9 The Operator can differentiate on whether the user is in the home or visited network based on the P-Access-Network-Info header field in the SIP signalling.
- R15-5-19* Requirements R15-3-1, R15-3-2, R15-3-4 and R15-3-5 shall be implemented locally on the device.

*R15-5-20* For requirement R15-4-1, signalling generated by a 3rd party service cannot be differentiated from user traffic of that 3rd party service because the signalling is defined in a proprietary way by the 3rd party without involvement of the Operator. As a consequence such signalling shall be considered as regular data traffic.

*R15-5-21* Requirements R15-4-1 and R15-4-2 shall be realised according to section 2.9.1.5 and 2.9.1.6 of [RCC.07].

## 16 RCS Settings

### 16.1 Description

RCS is a Service Platform for Operators to develop and implement new communication services. To allow users to manage their RCS services appropriately, a “Settings” function needs to be implemented into devices / clients.

Major changes of the Crane PDD compared to the Blackbird PDD are:

- RCS Master Switch placement
- Refined Image and newly introduced Video resizing options
- joyn Wi-Fi Voice call settings replaced with IP Voice call settings
- Show us on a map aggregation settings have been deleted (function removed from specifications)
- Conditions when Cellular Data Switch is set to “OFF” and the Operator allows RCS usage in that case.

### 16.2 User Stories and Feature Requirements

**US16-1 As a user, I want to switch between RCS instances on one device to ensure smooth operation.**

NOTE: Details of the behaviour of this switch are described in Device Provisioning.

*R16-1-1* An RCS “Master Switch” shall be available to activate / deactivate the native RCS service on the device. If the Master Switch is set to “OFF”, non-RCS IMS services (e.g. VoLTE) shall not be affected.

*R16-1-1-1* If the Master Switch is set to “OFF”, VARAs relying on RCS APIs shall not be able to use RCS functionality on that device unless provided by an active ORSC.

*R16-1-2* There shall be various entry points on the device for the Master Switch, for example:

*R16-1-2-1* Wireless and Networks settings on the device (if available)

*R16-1-2-2* “Messaging” -> “Settings”

*R16-1-2-3* “Other relevant entry points (e.g. call settings if rich call services are implemented).

*R16-1-3* If the Master Switch is visible from more than one location on the device, then the implementation shall be consistent (i.e. if the Master Switch is changed in one location, the change shall be consistent for all locations).

*R16-1-4* Any downloaded applications that have been installed on a device shall have an own switch to activate / deactivate themselves (this may be provided by the application or the operating system of the device).

*R16-1-5* The Master Switch shall be labelled “Rich Communications”.

*R16-1-5-1* If the user switches the Master Switch to “OFF”, a User Message (e.g. pop up or toast) shall be presented to the user to inform them what the consequences are and the user shall have to confirm the action.

*R16-1-6* In this state, the deactivated native RCS client is in status “Deactivated”. Consequently, no messages can be sent nor capability requests are answered through this RCS client.

*R16-1-7* After reactivation of the native RCS client, all its entry points shall be activated again.

**US16-2 As a user, I want to set an RCS Chat Alias.**

*R16-2-1* The user shall have the option to customise the name label which is presented during RCS Communications to participants for whom the user is not in the contact list.

**US16-3 As a user, I want to enable or disable IP Voice Calls.**

NOTE: Towards the user, the RCS IP Call is delivered as “Wi-Fi Voice Call”.

*R16-3-1* Customers shall be allowed to activate/deactivate the RCS IP Voice Call using an appropriate switch.

*R16-3-2* Default position shall be ‘Activated’.

*R16-3-3* This user setting shall be visible only when RCS IP Voice Call is activated by the MNO.

**US16-4 As a user, I want to switch “ON/OFF” SMS Delivery Notification.**

*R16-4-1* The user shall have the option to select or deselect automatically sending a Delivery Notification for SMS they receive in an Integrated Messaging scenario.

*R16-4-2* The default setting shall be based on individual Operator configuration.

**US16-5 As a user, I want to enable or disable automatic MMS download in Integrated Messaging.**

*R16-5-1* The user shall have the option to enable or disable automatic MMS download in Integrated Messaging.

*R16-5-2* The default setting shall be “enabled”.

**US16-6 As a user, I want to enable or disable MMS download in roaming case in Integrated Messaging.**

*R16-6-1* The user shall have the option to enable or disable the automatic download of MMS whilst they are roaming.

*R16-6-2* The default setting shall be “disabled”.

**US16-7 As a user, I want to personalise my device and need access to settings that allow me to do so.**

*R16-7-1* The user should have the option to personalise the native or downloadable RCS client. The following features should be covered:

- Notification sounds for incoming RCS events (e.g. One-to-One Messages, Group Messages, File Transfers),

- Notification preferences,
- Customised ringtones (for voice calls (same ringtone will apply to Circuit-switched, VoLTE) or Video over IP),
- Visual customization for chat (for example fonts, bubble styles, backgrounds etc.),
- LED settings.

**US16-8 As a user, I want to enable or disable the sending of the notification that tells the sender the message was displayed.**

*R16-8-1* The user shall have the option to enable or disable the sending of a notification to the sender that tells the sender the message was displayed.

*R16-8-2* The default for this setting shall be “enabled”.

**US16-9 As a user, I want to enable or disable automatic acceptance for File Transfer.**

*R16-9-1* The user shall have the option to enable or disable auto-acceptance for incoming File Transfer:

*R16-9-1-1* FT Auto Accept: I/O (default value set to I).

*R16-9-1-2* FT Auto Accept while roaming: I/O (default value set to O).

**US16-10 As a user, I want to be able to control the image resizing options in RCS File Transfer.**

*R16-10-1* The user shall have the option to set one of the following selections:

*R16-10-1-1* Always resize a selected option which is then stored as default value

*R16-10-1-2* Always ask

*R16-10-1-3* Never resize

*R16-10-2* The default setting shall be “always ask”.

*R16-10-3* For downscaling pictures, the following requirements shall apply:

*R16-10-3-1*The size of the image shall be reduced using following algorithm: Scale both dimensions by the same factor F (same for width and height so the aspect ratio is maintained). Compress as JPG with q=75%. Compare the new image size with the original, and only offer the possibility to resize if the resulting file is smaller than the original one.

*R16-10-3-2*The default scale factor F for the image shall be,  $F = \min(1280/w, 1280/h, 1.0)$ . It shall be noted the w (width) and the h (height) shall be used in pixels for the calculation.

*R16-10-3-3*If the factor (F) is 1, the original image shall be transferred.

**US16-11 As a user, I want to be able to control the video resizing options in RCS File Transfer.**

*R16-11-1* The user shall have to option to set one of the following selections:

*R16-11-1-1* Always resize to a selected option which is then stored as default value

*R16-11-1-2* Always ask

*R16-11-1-3* Never resize

*R16-11-2* The default setting shall be “always ask”.

*R16-11-3* The resizing options shall be based on OEM / developer choices including the default value of 480p @ 1200kbps.

*R16-11-4* When the set of resizing options are presented to the user, the default one highlighted or selected shall be 480p encoded at a rate of 1200 kbps.

*R16-11-5* The video resizing shall be accomplished in the background and the user shall be able to take control of the phone instantly (to e.g., but not limited to, answer incoming calls, make a call, etc.).

**US16-12 As a user, I want to enable or disable the LED notification (if such function is supported by my device).**

*R16-12-1* The user shall have the option to enable or disable the device LED for incoming message or File Transfer notification.

*R16-12-2* The default setting shall be “enabled”.

**US16-13 As a user, I want to enable or disable vibration notification for new incoming RCS messages or File Transfers.**

*R16-13-1* The user shall have the option to enable or disable the device vibration for incoming message or File Transfer notification.

*R16-13-2* The default setting shall be “enabled”.

**US16-14 As a software developer, I want to display on request an ‘about’ page that explains details of the RCS client.**

*R16-14-1* The device shall provide the user with an ‘about’ page that indicated the version of the device and the RCS implementation to allow efficient identification of the client / device details.

**US16-15 As a user, I want to be able to change my preference for whether undelivered RCS messages are automatically sent again by SMS or not.**

*R16-15-1* The user shall be able to set one of the following options:

*R16-15-1-1* Always resend undelivered RCS messages as SMS,

*R16-15-1-2* Always ask,

*R16-15-1-3* Never resend undelivered RCS messages as SMS.

*R16-15-2* The default setting shall be “always ask”.

**US16-16 As a user, I want to see the connectivity status of my RCS application.**

*R16-16-1* The RCS implementation shall inform the user about the connected / disconnected status of the client as a visual indication in the settings menu, adjacent to the other RCS settings.

*R16-16-2* If the connectivity status changes, the user shall not be presented with any audible or visible notification other than specified in R16-16-1.

**US16-17 As a user, I want to see the battery consumption of the basic functions of the device, including RCS, consolidated into one single statistics.**

*R16-17-1* The native battery statistics function of the device shall inform the user about the total battery consumption of native functions, including RCS features, in one consolidated value.

**US16-18 As a user, I want to set the default messaging client to be used for sending messages and handling RCS notifications.**

- R16-18-1* The user shall have the option to choose from a list of available RCS clients (native client, ORSCs and 3RCs) which one to be used as the default messaging client.
- R16-18-2* A “default messaging client” toggle list shall be made available in the device to achieve this.
  - R16-18-2-1* This toggle list shall only be displayed when there is more than one client able to access and manage RCS messaging services.
  - R16-18-2-2* All native clients, ORSCs and 3RCs that are able to access and manage RCS messaging services shall appear in the list.
  - R16-18-2-3* Only one client can be selected as the default messaging client at a time.
  - R16-18-2-4* Only native RCS clients, ORSCs and 3RCs that are able to access and use RCS services shall appear on the list.

### 16.3 Technical Information

A number of requirements for service configuration parameters on the client are provided.

#### 16.3.1 Technical Implementation of User Stories and Service requirements

- R16-19-1* The technical implementation of the requirements for user story US16-1 to switch between multiple RCS instances on a device are provided in Device Provisioning, page 11.
- R16-19-2* The technical implementation of the requirements of US16-1 regarding Master Switch shall be provided by means of the RCS switch defined in section 2.9.1.4 of [RCC.07] with the following additions:
  - The availability of the RCS switch on the client is controlled by the configuration parameter ENABLE RCS-E SWITCH as defined in section A.1.11 of [RCC.07]. Crane service providers will always set the value of the parameter ENABLE RCS-E SWITCH to "1" in accordance with requirement R16-1-1.
  - The purpose of the RCS switch defined in section 2.9.1.4 of [RCC.07] is to enable/disable relevant RCS services when the RCS client uses a packet switched network. In Crane the RCS Switch shall control the activation of the relevant RCS services independent from the access network to fulfil the requirement R16-1-1.

The following additional requirements apply to section 2.9.1.4 of [RCC.07]:

- Table 43 of [RCC.07] applies with the following addition. If "RCS Switch" is "disabled" and the IMS APN is used, the client shall register in addition to the SMS over IP service as defined in [PRD-IR.92].
- The following additional table applies if the client uses a non 3GPP access network for RCS services.

RCS Switch	Access Network to use for RCS services	Result
Disabled	Non 3GPP	RCS client shall not register on the IMS network.
Enabled	Non 3GPP	Standard configuration, the client shall register in IMS for any

		supported and active RCS services
--	--	-----------------------------------

**Table 53:RCS Switch behaviour in non-3GPP networks**

- If the user changes the value of the RCS Switch from "enabled" to "disabled" and the client is in RCS-CS or RCS-AA device mode then it shall terminate existing sessions and cancel existing requests for RCS services. If the device is VoLTE capable and the IMS registration covers VoLTE, then the client shall re-register to remove the services apart from IP Voice Call via VoLTE/VoHSPA and IP Video Call via ViLTE, SMS over IP and Standalone Messaging (see also section 2.9.1.4 of [RCC.07]). In all other cases the client shall de-register from IMS.
- If the user changes the value of the RCS Switch from "enabled" to "disabled" and the client is in RCS-VoLTE or RCS-VoHSPA device mode, then it shall terminate existing sessions and cancel existing requests for services other than IP Voice Call via VoLTE/VoHSPA and IP Video Call via ViLTE, SMS over IP and Standalone Messaging (see also section 2.9.1.4 of [RCC.07]). It shall re-register in IMS with only the relevant ICSI and feature tags of [PRD-IR.92][PRD-IR.92],[PRD-IR.92] [PRD-IR.94] [PRD-IR.94]or [PRD-IR.58] respectively.
- If the user changes the value of the RCS Switch from "disabled" to "enabled" and the client is not registered for VoLTE or VoHSPA, then the client shall register in IMS for any supported and active RCS services.
- If the user changes the value of the RCS Switch from "disabled" to "enabled" and the client is registered for VoLTE or VoHSPA, then it shall re-register in IMS to add the feature tags of any supported and active RCS services according to configuration.
- If the RCS Switch is set to "disabled" and the client is registered in IMS for VoLTE or VoHSPA and
  - it receives an OPTIONS request it shall respond with 200 OK but no RCS feature tags in the contact header
  - it receives an INVITE or MESSAGE request with RCS feature tags in the accept-contact header, it shall respond with 480 Temporarily Unavailable.
- If the RCS Switch is set to "disabled", then the client shall not invoke the RCS client autoconfiguration mechanism defined in section 2.3.3 of [RCC.07] in accordance with the requirements in US2-3.
- If the RCS Switch is set to "disabled", and a client or network trigger for device configuration applies as defined in 2.3.3.2 of [RCC.07] no device configuration shall be invoked. The trigger for device configuration shall be cached locally in the client.
- If the user changes the value of the RCS switch from "disabled" to "enabled" and no valid configuration is available for the used identity or a client or network trigger for device configuration has been cached locally in the client, then the client shall invoke the RCS client autoconfiguration mechanisms.
- If the RCS Switch is set to "disabled", the client shall not synchronise with the common message store if a trigger as defined in section 3.2.6.2.3 of [RCC.07] applies.

- If the user changes the value of the RCS switch from "enabled" to "disabled", the RCS client shall log-out from a session with the Common Message Store.
- If the user changes the value of the RCS switch from "disabled" to "enabled" the RCS client shall take this as a trigger for synchronization with the Common Message Store.

*R16-19-3* The requirements for user story US16-2 shall be implemented locally on the device. The value of the parameter is used by the client to populate the User Alias as defined in 2.5.3.3 of [RCC.07].

*R16-19-4* The term 'IP Voice Call' is interpreted as IR.51 Voice over Wi-Fi in this context. The requirements for user story US16-3 shall be implemented locally on the device. The client configuration is only relevant if the service provider has activated the IP Voice Call on the device via the PROVIDE IR51 VOICE configuration parameter defined in section 10.3.2 of this document and the Service Provider has determined that the switch to enable or disable IP voice calls is displayed to the user Via the configuration parameter IR51 SWITCH UX as defined in section 10.3.2 of this document. If IP Voice Call is disabled by the user the device shall behave as if it has been disabled by the Service Provider (see section 10.3 of this document).

*R16-19-5* As a clarification to the requirements for user story US16-4, if SMS is provided by means of the Short Message Service as defined in [3GPP TS 23.040] or the Short Messaging Service over IP as defined in IR.92 (see section 4.3.1 of this document) it shall be noted that the SMS STATUS REPORT to notify the sender of a successful delivery is sent by the Service Centre and not by the receiving device. Therefore it is not the recipient controlling sending of a Delivery Notification. Instead the sender has the ability to request delivery report for sent short messages To prevent the SC to send SMS STATUS report the originating client shall not request an SMS STATUS REPORT when submitting a short message. If SMS is provided via Standalone Messaging, both the sender is able to control the request for delivery report and the receiver to control sending of delivery reports. The client is advised to provide a homogenous user experiences if multiple technologies are supported and active to provide SMS.

*R16-19-6* The configuration parameter defined in the requirements for user stories US16-5 and US16-6, controls the retrieval behaviour (immediate or deferred retrieval) of the MMS user agent of the integrated messaging client if MMS is provided by the client via Multimedia Messaging Service as defined in section 4.3.1 of this document.

If the device detects a roaming situation and the user has disabled MMS download in roaming case, then the MMS user agent should apply deferred retrieval behaviour. The user should be notified of a received MMS at the time of reception of the MMS notification.

If the device detects a roaming situation and the user has enabled MMS download in roaming case, then the MMS user agent should apply the retrieval behaviour as determined by the "MMS automatic download" setting of US16-5.

If MMS is provided by the client via Standalone Messaging as defined in section 4.3.1 of this document, then the client shall set the user



preferences to defer standalone messages. For the handling of deferred standalone messaging refer to section 3.2.1.4 of [RCC.07].

*R16-19-7* The requirements for user story US16-7 shall be implemented locally on the device.

*R16-19-8* If generating notifications about messages being displayed is disabled in accordance with the requirements for user story US16-8, then a client receiving a message or file shall disregard the disposition notification header with value “display” and not generate a notification for “displayed”.

*R16-19-9* The configuration parameters for automatic acceptance of File Transfer of US16-9 shall be implemented locally on the device. The parameters shall overwrite the service provider auto acceptance settings provided by the FT AUT ACCEPT defined in section A.1.4 of [RCC.07]. The FT AUT ACCEPT value received in the client configuration provides the default settings of the FT Auto Accept parameter controlled by the user. Once the user has altered the settings the value of FT AUT ACCEPT from the device configuration becomes irrelevant.

*R16-19-10* The requirements for user stories US16-10 to US16-18 shall be implemented locally on the device.

## Annex A

### A.1 Personal Card format

Current implementations of the vCard standard by different device manufacturers leads today to data loss of certain contact information, when this information is exchanged among devices or synced with network address books. An RCS compliant device shall support receiving at a minimum, vCard 2.1 [vCard21] and vCard 3.0 formats [RFC2425], [RFC2426], and may support also the Personal Contact Card (PCC) format [CAB\_TS].

The following fields are considered key fields. No data of these fields should be lost when contact information is exchanged by any means (peer to peer contact sent, uploaded, synchronised, etc.):

- Name
- Telephone numbers
- Email addresses
- Address information
- Personal information

The Minimum subtypes that should be supported are defined in the PCC definition in [CAB\_TS]:

- Name: Composed names (such as “Jean-Baptiste”) shall be supported properly
- Personal Information
  - Nickname
  - Photo
  - Birthdate
  - Comment
- Telephone number: At least the following subtypes of telephone number shall be supported:
  - Land home
  - Land work
  - Land other
  - Mobile home
  - Mobile work
  - Mobile other
  - Fax work
  - Fax other
  - Beeper
  - Other

Email addresses: The following subtypes shall be supported:

1. Email work 1
2. Email work 2
3. Email home 1
4. Email home 2

## 5. Other

- Address information
  - Address
  - Geographic Position
  - Time zone

Sending and receiving a contact card via File Transfer is technically the same as sending any other file.

If the format for pushing a contact card file is vCard 2.1 or 3.0 formats, the MIME (Multipurpose Internet Mail Extensions) type that shall be used for the File Transfer is “text/vcard”.

If the format for pushing the contact card is CAB (Converged Address Book) 1.0 PCC XML format, then the CAB PCC MIME type “application/vnd.oma.cab-pcc+xml” shall be used.

On the receiving side, after the receiving RCS user accepts the contact card file delivered through File Transfer, the receiving RCS client shall apply the mapping of the RCS supported fields between the received format (CAB PCC XML for example) and the used format of the local address book database<sup>4</sup>.

vCard 3.0 format is recommended in RCS.

If the receiving side does not support the offered format identified in the a=file-selector attribute of the SIP INVITE SDP, it should reject the File Transfer invitation with an error response indicating it does not support the content-type, which then causes the sending side to initiate a second File Transfer, this time sending the contact card in a different format.

---

<sup>4</sup> If the conversion between PCC and vCard is required, please see **Error! Reference source not found.** section 5.4.3 “Format Adaptation”.

## A.2 Emoticon conversion table

### Standard Emoticons

Emoticons	Character sequences	Examples describing graphical renditions
Happy, smile	☺ or :)	A happy or smiling face
Sad	:( or :(	A sad face
Wink	;-) or ;) or ;o) or ;O)	A winking face
Big grin	:-D or :D or :oD or :-d or :d or :od or :Od or :OD	A big grin face
Confused	:-/ or :-\	A confused face
Blushing, embarrassed	:-") or :") or :> or :> or :-\$ or :\$	A blushing, embarrassed face
Stick-out tongue	:-P or :P or :oP or :-p or :p or :op or :OP or :Op	A stick-out tongue face
Kiss, red lips	:-* or :*	A kissing face or red lips
Shocked, surprised	:-O or :-o or :o or :O	A shocked, surprised face
Angry	:-@ or :@ or X-( or X(or x-( or x( or xo( or XO(	An angry face
Cool, sunglasses	B) or B-) or (H) or (h) or Bo) or BO)	A face with sunglasses
Worried	:-S or :S or :-s or :s or :oS	A worried face
Devilish	>:-) or >:) or >:o) or >:O)	A devilish face
Crying	;--( or ;:( or :'-( or :'( or ;,o( or :'o( or ;,O( or :'O(	A crying face
Laughing	:-)) or :)) or :o)) or :O))	A laughing face
Straight face, disappointed	:-  or :  or :o  or :O	A straight face
Angel, innocent	O:-) or O:) or o:-) or o:)	An innocent face
Nerd	:-B or :B	A nerdish face
Sleepy	-O or  O or  -o or  o	A sleepy face
Rolling eyes	8-) or 8) or 8o) or 8O)	A rolling eyes face
Sick, ill	:-& or :& or ;o& or :O&	A sick/ill face
Shhh! No speak, lips sealed	:-SS or :SS or :ss or :-ss	A face with sealed lips
Thinking, pensive	:-? or :?	A pensive face
Raised eyebrow, sarcastic look	/:-) or /:) or /:o) or /:O)	A raised eyebrow face or a face with a sarcastic look
Rose, flower	@):-	A rose
Cup of coffee	~o)	A cup of coffee
Drink, cocktail	)-	A cocktail glass

Emoticons	Character sequences	Examples describing graphical renditions
Idea (light bulb)	*:-) or *-:)	A light bulb
Love struck, heart	(L) or <3	A heart
Beer	(b) or (B)	A pint of beer
Broken Heart	(u) or (U) or \Z/	A heart broken in two
rock on!	\m/	A smiling face with rockstar fingers
pirate	:ar!	A face with eye patch
silly	8-}	A face with wobbly mouth and spinning eyes
applause	=D>	A face with clapping hands
Penguin	<(')	A small penguin
Music Note	-8	A semi quaver
Star	(*)	A gold star
Clock	(o) or (O)	A clock face
Pizza	(pi) or (PI)	A slice of pizza or a whole pizza
Money	(mo) or (MO)	Coins or notes or coins and notes
Sheep	(bah) or (BAH)	A sheep
Pig	:8)	A pig's face
Sun	(#)	A shining sun
Rain Cloud	(st) or (ST)	A cloud with rain or cloud with rain drop
Umbrella	(um) or (UM)	An open umbrella
Aeroplane	(pl) or (PL)	A plane
Birthday Cake	(^)	A cake with candles
Party!	<:o)	A face wearing a party hat and blowing a party blower
Film	(~)	A roll of film or strip of film
Gift	(g) or (G)	A gift wrapped present with bow
Email	(e) or (E)	An open envelope
Phone	(t) or (T)	A hand receiver with cable
Wave	:-h	A face with hand waving
Big hug	>:D<	A face with hands hugging itself

### A.3 Unicode Standard “Emoji” Emoticons

The list of required Emoji that must be graphically rendered and offered to the user, and the mapping to relevant Unicode blocks, is detailed in document “joyn Blackbird Unicode Standard Emoji Emoticons version 1.0”, available from

<http://www.gsma.com/network2020/wp-content/uploads/2013/05/RCS-joyn-Blackbird-Unicode-Standard-emoji-emoticons-v1-0-2.pdf>.

## Annex B Document Management

### B.1 Document History

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
1.0	15/05/2015	New document	PSMC	Wade Owojori / GSMA

### B.2 Other Information

Type	Description
Document Owner	RCS Product Group
Editor / Company	Wade Owojori / GSMA

It is our intention to provide a quality product for your use. If you find any errors or omissions, please contact us with your comments. You may notify us at [prd@gsma.com](mailto:prd@gsma.com)

Your comments or suggestions & questions are always welcome.