RCS Universal Profile Service Definition Document

Version 1.0

16 November 2016

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 © 2016 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.

Salesforce EX1032
Salesforce, Inc. v. IQX Corp.
IPR2026-00477

Table of Contents

1 Introduction 6
1.1 Purpose of the Universal Profile 6
1.1.1 Structure of this document 6
1.1.2 Universal Profile client scope 6
1.2 Conventions 7
1.3 Requirement and Technical Realisation Classification 7
1.4 Terms and Abbreviations 7
1.5 Table of references 13
2 Device Provisioning 15
2.1 Description 15
2.2 User Stories and Feature Requirements 15
2.2.1 Activation of RCS services 15
2.2.2 Configuration of the user´s primary device by requesting user identity 16
2.2.3 Multiple RCS instances 17
2.2.4 SIM swap 18
2.2.5 User consent 18
2.2.6 Secondary Devices 20
2.2.7 Error Management 21
2.2.8 Provisioning push 22
2.2.9 Dual SIM Devices 22
2.3 Technical Information 23
2.3.1 Overview 23
2.3.2 Technical Implementation of User Stories and Service requirements 24
3 Capability Discovery and Service Availability 29
3.1 Description 29
3.2 User Stories and Feature Requirements 30
3.3 Technical Information 32
3.3.1 Overview 32
3.3.2 Configuration Parameters 34
3.3.3 Handling of capability exchange triggers in messaging 38
3.3.4 Technical implementation of user stories and requirements 38
4 Operator Messaging 40
5 1-to-1 Messaging 40
5.1 Description 40
5.2 User Stories and Feature Requirements 40
5.3 Technical information 53
5.3.1 Overview 53
5.3.2 Network Fallback Support Capability 55
5.3.3 Client behaviour 56
5.3.4 Network Behaviour 64
5.3.5 Chat Message revocation 65
5.3.6 Geolocation Push Fallback 67

5.3.7 Configuration Parameters 69
5.3.8 Technical Implementation of User Stories and Service Requirements 79
6 Group Chat 84
6.1 Description 84
6.2 User Stories and Feature Requirements 84
6.3 Technical Information 93
6.3.1 Overview 93
6.3.2 Technical Implementation of User Stories and Service requirements 94
7 File Transfer 97
7.1 Description 97
7.2 User Stories and Feature Requirements 98
7.3 Technical Information 109
7.3.1 Overview 109
7.3.2 File Transfer Fallback 109
7.3.3 Configuration Parameters 115
7.3.4 Technical Implementation of User Stories and Service requirements 117
8 Audio Messaging 123
8.1 Description 123
8.2 User Stories and Feature Requirements 123
8.2.1 Sending Audio Messages 124
8.2.2 Notification on Receiving Audio Messages 125
8.2.3 Receiving Audio Messages 125
8.3 Technical Information 126
8.3.1 Overview 126
8.3.2 Technical Implementation of User Stories and Service Requirements 127
9 Messaging for Multi-Device 129
9.1 Description 129
9.2 User Stories and Feature Requirements 129
9.3 Technical Information 134
9.3.1 Overview 134
9.3.2 Technical Implementation of User Stories and Service Requirements 135
10 Green Button Promise for Voice 139
10.1 Description 139
10.2 User Stories and Feature Requirements 139
10.3 Technical Information 142
10.3.1 Overview 142
10.3.2 Configuration parameters 142
10.3.3 Technical Implementation of User Stories and Service Requirements 144
11 Green Button Promise for IP Video Call Services 145
11.1 Description 145
11.2 User Stories and Feature Requirements 146
11.3 Technical Information 149
11.3.1 Overview 149
11.3.2 Technical Implementation of User Stories and Service Requirements 150

12 Enriched Voice Calling 152
12.1 Description 152
12.2 General 152
12.3 Technical Information for the General Requirements 152
12.4 User Stories and Feature Requirements for the Enriched Pre-call experience 153
12.5 Technical Information for the Enriched Pre-call experience 157
12.5.1 Overview 157
12.5.2 Technical Implementation of User Stories and Service Requirements 157
12.6 User Stories and Feature Requirements for the Enriched In-call experience 158
12.6.1 General Requirements 158
12.6.2 “Live Video” 158
12.6.3 Share any file during call 160
12.6.4 Exchanging messages 161
12.6.5 Location Push 162
12.6.6 Enriched Calling In-call sharing with Non-Enriched Calling enabled contacts 163
12.7 Technical Information for the Enriched In-call experience 163
12.7.1 Overview 163
12.7.2 Technical Implementation of User Stories and Service Requirements 164
12.8 User Stories and Feature Requirements for Interactive In-call experience 166
12.8.1 Live Sketch Sharing 166
12.8.2 Specific Requirements for a live sketch on an image 170
12.8.3 Specific Requirements for a live sketch on a map 170
12.9 Technical Information for Interactive In-call services 171
12.9.1 Overview 171
12.9.2 Shared Sketch 172
12.9.3 Specific Shared Image Sketch Requirements 172
12.9.4 Specific Shared Map Sketch Requirements 172
12.10 User Stories and Feature Requirements for the Enriched Post-call experience 172
12.10.1 Enriched Calling Post-call experience with Non-Enriched Calling enabled contacts 174
12.11 Technical Information for the Enriched Post-call experience 174
12.11.1 Overview 174
12.11.2 User Stories and Feature Requirements for the Enriched Post-call experience 174
12.11.3 Enriched Calling Post-Call experience with Non-Enriched Calling enabled contacts 175
12.12 User Stories and Feature Requirements for Enriched Call content in Logs and media contact centric view 175
12.12.1 Technical Information for Enriched Call Logs experience 177
13 rcsVVM Service 177
14 APIs 177
14.1 Description 177

14.2 User Stories and Feature Requirements 178
15 Plugins and UI Hooks 181
15.1 Description 181
16 Security against Malware 182
16.1 Description 182
16.2 User Stories and Feature Requirements 182
16.3 Technical Information 183
16.3.1 User Authentication 183
16.3.2 Encryption 184
16.3.3 Storage of Authentication and Identification Data 184
16.3.4 SIM State Handling 184
16.3.5 Applicability of Authentication Methods 185
16.3.6 Technical Implementation of User Stories and Service requirements 186
17 Data Off 190
17.1 Description 190
17.2 User Stories and Feature Requirements 190
17.3 Technical Information 192
17.3.1 Overview 192
17.3.2 Technical Implementation of User Stories and Service requirements 192
18 RCS Settings 194
18.1 Description 194
18.2 User Stories and Feature Requirements 194
18.3 Technical Information 198
18.3.1 Technical Implementation of User Stories and Service Requirements 198
19 Multi Device Voice and Video 202
19.1 Description 202
19.2 User Stories and Feature Requirements 202
Annex A Supporting requirements 209
A.1 Personal Card format 209
A.2 Emoticon conversion table 210
A.3 Unicode Standard “Emoji” Emoticons 212
A.4 Panoramic photo view 212
Annex B Multiple Client handling on Android™ OS 216
B.1 Multiple Client handling on Android™ OS version superior or equal to 7.0 216
B.2 Multiple Client handling on Android™ OS version prior to 7.0 217
Annex C Configuration Parameters 220
Annex D Document Management 237
D.1 Document History 237
D.2 Other Information 237

1 Introduction

1.1 Purpose of the Universal Profile

The Rich Communication Services (RCS) Universal Profile represents a set of globally shared RCS specifications. This Service Defintion Document (SDD) lists all the User Stories and Feature Requirements, based on the Common Core V2.0 specification and the Pre-Universal Profiles. The Universal Profile describes a single, global RCS implementation that will be deployed worldwide. The aim of this profile is to reduce the variation that exists today across various RCS profiles in order to simplify large-scale deployment. The Universal Profile is targeted at Operating System (OS) developers and Original Equipment Manufacturers (OEM) for open market device implementations. The focus of requirements is on native device implementations implemented at the OS or device manufacturer level. It is acknowledged that downloadable applications may face limitations that prevent such implementations from fulfilling the complete feature set.

The SDD provides user stories and feature requirements and is complemented by the RCS Universal Profile technical specification to describe a prioritized set of features which Mobile Network Operators (MNOs) can launch.

1.1.1 Structure of this document

The document details how features are to be implemented from a functional requirements point of view and details specifics that may influence how certain functions behave, creating an overall guide for OEMs and application developers.

1.1.2 Universal Profile client scope

The Universal Profile can be delivered in two ways for users:

1. Implemented natively within the device by the OS developer or 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 its 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 cases where implementation of a feature in a downloadable client differs from the native experience, these are described separately within the relevant section.

The profile includes some sections that come without a technical realisation (0, 15 and 19). As such they are not in scope for implementations in this version of the universal profile. The requirements are indicative only since they may change following the technical feasibility assessment and are provided for information in case this information on future evolutions would be relevant for the design decisions of an implementation.

For section 9 (Multi-Device Messaging) based on the current state of specifications IMAP access to the Common Message Store is the the only enabler available to fulfil a significant part of the requirements. There is however work ongoing in the industry to define an alternative method of accessing the Common Message Store which may be adopted in

future versions of the Universal Profile. To accommodate this possible change in the future releases, in this version it is optional for clients to implement section 9 and the requirements related to backup and restore of messages and files in sections 5, 6, 7 and 8.

1.2 Conventions

It is a shared understanding by the standardising RCS MNOs that any service described in the RCS standard may or may not be offered by any given MNO.

NOTE: For device manufacturers and client developers requirements are classified based on the conventions defined in section 1.3 of this document.

For the purpose of this document, user stories are identified using the following numbering convention: “USN.N”, where US= User Story and N= the associated user story e.g. US2.2.

The associated requirements are identified using the following numbering convention: “RN-N-N, where “R” = requirement e.g. R2-2-1. Sub requirements will appear as a third level e.g. R-2-2-1-1.

1.3 Requirement and Technical Realisation Classification

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

Table 1: Requirements Classification

1.4 Terms and Abbreviations

Term	Description (contains technical and functional terms)
3GPP	3rd Generation Partnership Project
Active device or interface	A device or interface will be active for a conversation’s “session” if the user has either started a conversation, or sent events outside of a session from that device or responded to an incoming event with an event listed in R9-3-4 on that device/interface. A session is established and associated with that conversation. Further events sent within the conversation will be sent only to that device in real-time and will be synchronised with other (inactive) devices as required. Any given user can only have one active device / interface at any given point in time for an active session.
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

Term	Description (contains technical and functional terms)
	user has multiple RCS devices available to him at all (using this capability information shared).
AKA	Authentication and Key Agreement
AMR	Adaptive Multi-Rate
A-Party	The party that initiates a communication event e.g. creates and sends a chat message or File Transfer or initiates a call to the B-Party.
APN	Access Point Name
App	Smartphone application.
App ID	Unique identifier for an application.
API	Application Programming Interface
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, File Transfer or call from the A-Party.
Call Composer	A view on the device that allows the A-Party to enrich outgoing voice calls with pre-call content before placing the call.
Call Log	The view on the device displaying all the user's call events, e.g. incoming, outgoing, and missed calls. Call logs usually offer a view containing all call events ordered chronologically, plus a detailed view of a single call event or call events with a specific Contact.
Capability / Availability	A contact has a device registered for RCS service that can initiate or respond to a requested RCS service.
CFB	Call Forward Busy
CFS	Client Fallback to SMS incl. Revocation – one of the two procedures of Delivery Assurance in Integrated Messaging.
Chat Message	A single text message that was conveyed from one user to another using the RCS Chat service.
CLIP	Calling Line Identification Presentation
CLIR	Calling Line Identification Restriction
Common Message Store (CMS)	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.
CPIM	Common Profile for Instant Messaging
CPM	Converged IP Messaging
CS	Circuit Switched
CW	Call Waiting

Term	Description (contains technical and functional terms)
Default Messaging Client	In the case of multiple diallers on a device, the client chosen by the user to act as the default dialler for setting up and receiving voice and video calls.
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 composing purposes.
Delivery Assurance	A mechanism in Integrated Messaging that improves the timely delivery of messages and files. The procedures that Delivery Assurance uses are Client Fallback to SMS incl Revocation (CFS) and Network Fallback to SMS (NFS).
Delivery Notification	Indication that a message was successfully received by the B-Party device.
DELIVERY TIMEOUT	A duration parameter set by the MNO 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	When the message has been displayed in the Chat view on the receiving device.
Direct Delivery	In multi-device messaging, when an event (e.g. Chat Message, File Transfer, Audio Message, or Geolocation Push) is received, it is received on all of the recipient's registered and connected devices at the same time. When an event is sent from any of the registered and connected devices, it is sent to all of the sender's other registered and connected devices at the same time.
DNS	Domain Name System
DTMF	Dual Tone Multi-Frequency
Dual SIM device	A device where two different identities, provided by two different SIMs, are active at the same time.
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.
Enriched Voice Calling	The ability to share content before, during and after a voice call.
EUCR	End User Confirmation Requests
E-UTRAN	Evolved UMTS (Universal Mobile Telecommunications System) Terrestrial Radio Access Network
Events	Events as used in this SDD are messages, content and notifications in the context of Operator Messaging.
External Loudspeaker	Speaker on the device which amplifies the audio of the call when activated.

Term	Description (contains technical and functional terms)
Feature Tag	An IARI Tag assigned to a RCS functionality allowing to identify and route the RCS traffic accordingly.
Federated Device	A common term used for all devices federated under the identity of a specific user (federated devices always comprise one primary and one or more secondary devices).
FQDN	Fully Qualified Domain Name
Front Camera	Camera placed on the display side of a communication device.
GBA	Generic Bootstrap Architecture
GIF	Graphics Interchange Format
Global Settings	In a multi-device setup, Global Settings are settings which are changed on one device and change the corresponding setting on any federated devices or interfaces as well (as opposed to Local Settings).
GPRS	General Packet Radio Service
HOS	Home Operator Services
HSPA	High Speed Packet Access
HTML	Hyper Text Markup Language
HTTP	Hyper Text Transfer Protocol
IARI	IMS Application Reference Identifier
ICSI	IMS Communication Service Identifier
IMAP	Internet Message Access Protocol
IMDN	Instant Message Disposition Notification
IMS	Internet Protocol (IP) Multimedia Subsystem
IMSI	International Mobile Subscriber Identification.
Inactive device or Interface	A device or interface not currently active in a multi-device scenario.
Interconnected RCS Service	An RCS Service that can be accessed between users of MNOs 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.
Integrated Messaging	An MNO 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.
JPEG	Joint Photographic Experts Group
KB	KiloByte (i.e. 1024 bytes)
LED	Light Emitting Diode
Local Settings	In a multi-device setup, Local Settings are settings which are changed on one device without any impact on corresponding settings on any federated devices or interfaces (as opposed to Global Settings).
LTE	Long Term Evolution
MDV[2]	Multi device Voice and Video

Term	Description (contains technical and functional terms)
Messaging event	Associated with any of the services listed in R9-3-4 and includes all types of messages, files, content, new message notifications, previews, icons and message status notifications (sent and received).
MIME	Multipurpose Internet Mail Extensions
MMS	Multimedia Messaging service
MNO	Mobile network operator.
Multi-Device Support	RCS Service that enables a user to register more than one device under a single identity.
Multi Device Voice and Video	An MNO service that allows to use SIM based and SIM less devices to make voice and / or video calls (and supporting services around these) under one identity.
Multi-SIM	Multi-SIM is an MNO-individual solution to federate SIM-based devices for offering a multi device solution to customers. Multi-SIM solutions may or may not be based on SIMs with identical identities.
MSISDN	Mobile Subscriber Integrated Services Digital Number, i.e. mobile phone number.
Native RCS Device	A device with an RCS client deeply integrated by the OEM or OS developer (as opposed to a downloaded RCS client).
NFS	Network Fallback to SMS – one of the two procedures of Delivery Assurance in Integrated Messaging.
OEM	Original Equipment Manufacturer.
“offline” user	A user who is known to be RCS enabled and not currently registered to the RCS service.
OMA	Open Mobile Alliance
On-Net	Communication or signalling that does not go across the interworking interface (NNI) between networks or MNOs.
“online” user	A user who is known to be RCS enabled and is currently registered to the RCS service.
OS	Operating System
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).
OTP	One Time Password
P-CSCF	Proxy Call Session Control Function
Primary Device or Primary Interface	Device which contains the SIM that matches the identity which the client uses to register in IP Multimedia Subsystem (IMS).

Term	Description (contains technical and functional terms)
Primary SIM	In the context of a Multi Device solution, the Primary SIM shall be the SIM that provides the identity of the Primary Device or Interface and all federated Secondary Devices or Interfaces.
PS	Packet Switched
RCS	Rich Communication Services
RCS 1-to-1 Messaging	Can either be standalone messaging or 1-to-1 chat as defined in RCC.07
RCS Alias name	A name that is defined by the user that represents the user as a Chat participant on B-Party devices, if no Contact exists in the contact list.
RCS-enabled	Capable of the RCS service, activated and ready to operate when the network conditions allow.
rcsVVM enabled device	A device provisioned for RCS service that can manage Visual Voice Mail messages stored in the Common Message Store using the RCS client.
Reachable	The UE can receive service notifications irrespective of RCS service registration or connection to the cellular network.
Rear Camera	Opposite to the front camera positioned on the back of the device.
Seamless Messaging	An MNO messaging service whereby the user is not aware of the messaging technology used but the device / network determines which messaging technology is used.
Secondary Device or Secondary Interface	Terms used to describe any access to a user's RCS account and service features from a device or interface not containing the SIM associated with the primary identity. A user may have several secondary devices and/or interfaces available to access their RCS service, including devices containing SIMs not associated with the user's primary identity.
Service availability	Service availability is a state of a specific user that is determined using Capability Discovery processes.
SG	Signalling Gateway
SIM	Subscriber Identity Module
SIP	Session Initiation Protocol
SMS	Short Message Service
SRVCC	Single Radio Voice Call Continuity
SSL	Secure Socket Layer
SSO	Single Sign-On
Standalone Message	A single text message that was conveyed from one user to another using the RCS Standalone Messaging service.
T&C	Terms & Conditions
TE	Technical Enabler
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.
TLS	Transport Layer Security

Term	Description (contains technical and functional terms)
Trusted Wi-Fi	Trusted Wi-Fi" refers to a Wi-Fi connection offered by the Service Provider or via a third party trusted by the service provider.
UE	User Equipment
UI	User Interface
URI	Uniform Resource Identifier
UX	User Experience
VoLTE	Voice over Long Term Evolution
VVM	Visual Voice Mail.
Voice Mail System (VMS)	The network system that allows users to listen to voice messages, delete voice messages, and compose voice messages.
Wi-Fi	Trademark of Industry Consortium "Wi-Fi Alliance" used as synonym for WLAN (Wireless Local Area Network)
XCAP	XML Configuration Access Protocol
XDMS	XML Document Management Server
XML	Extensible Markup Language
xMS	The traditional MNO messaging services known as Short Message Service (SMS) and Multimedia Messaging Service (MMS).

1.5 Table of references

Ref	Doc Number	Title
[1]	[3GPP TS 22.140]	3GPP TS 22.140, release 10, Multimedia Messaging Service (MMS); Stage 1 http://www.3gpp.org/DynaReport/22140.htm
[2]	[3GPP TS 23.040]	3GPP TS 23.040, release 10, Technical realization of the Short Message Service (SMS) http://www.3gpp.org/DynaReport/23040.htm
[3]	[3GPP TS 24.008]	3GPP TS 24.008, release 10, Mobile radio interface Layer 3 specification; Core network protocols; Stage 3 http://www.3gpp.org/DynaReport/24008.htm
[4]	[3GPP TS 24.167]	3GPP TS 24.167, release 12, 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; 3GPP IMS Management Object (MO) http://www.3gpp.org/DynaReport/24167.htm
[5]	[CAB_TS]	OMA Converged Address Book (CAB) Specification, Approved Version 1.0, 13 November 2012http://www.openmobilealliance.org
[6]	[NG.102]	IMS Profile for Converged IP Communications Version 3.0 17 May 2016 http://www.gsma.com/
[7]	[PRD-IR.51]	IMS Profile for Voice, Video and SMS over Wi-Fi Version 4.0 23 May 2016 http://www.gsma.com/
[8]	[PRD-IR.67]	GSMA PRD IR.67 - "DNS/ENUM Guidelines for Service Providers & GRX/IPX Providers" Version 10.0 24 April 2014 http://www.gsma.com/
[9]	[PRD-IR.92]	GSMA PRD IR.92 - "IMS Profile for Voice and SMS" Version 10.0 19 May 2016

Ref	Doc Number	Title
		http://www.gsma.com/
[10]	[PRD-IR.94]	GSMA PRD IR.94 - "IMS Profile for Conversational Video Service" Version 11 24 May 2016 http://www.gsma.com/
[11]	[RCC.07]	GSMA PRD RCC.07 version 6.0- "Rich Communication Suite 6.0 Advanced Communications Services and Client Specification" 18 March 2016 http://www.gsma.com/
[12]	[RCC.09]	GSMA PRD RCC.09 RCS 6.0 Endorsement of OMA CPM 2.1Message Storage, Version 6.0 18 March 2016 http://www.gsma.com/
[13]	[RCC.10]	GSMA PRD RCC.10 Rich Communication Suite 6.0 Endorsement of OMA CPM 2.1 Interworking Version 5.0 18 March 2016 http://www.gsma.com/
[14]	[RCC.11]	GSMA PRD RCC.11 Rich Communication Suite 5.3 Endorsement of OMA CPM 2.0 Conversation Functions Version 5.0 18 March 2016 http://www.gsma.com/
[15]	[RCC.12]	GSMA RCS 5.1 Endorsement of OMA SIP/SIMPLE IM 1.0, Version 1.0 13 August 2012 http://www.gsma.com/
[16]	[RCC.14]	GSMA PRD RCC.14 Service Provider Device Configuration Version 3.0 18 March 2016 http://www.gsma.com/
[17]	[RCC.15]	GSMA PRD RCC.15 IMS Device Configuration and Supporting Services Version 2.0 18 March 2016 http://www.gsma.com/
[18]	[RCC.20]	GSMA PRD RCC.20 Enriched Calling Technical Specification Version 2.0 18 March 2016
[19]	[RCC.53]	GSMA PRD RCC.53 joyn Device API Specification Version 3.0 23 June 2015 http://www.gsma.com/
[20]	[RCC.55]	GSMA PRD RCC.55 [TAPI-Security]: RCS Extensibility: Terminal API and Network API Security Version 2.0 23 June 2015 http://www.gsma.com/
[21]	[RFC2425]	A MIME Content-Type for Directory Information IETF RFC http://tools.ietf.org/html/rfc2425
[22]	[RFC2426]	vCard MIME Directory Profile IETF RFC http://tools.ietf.org/html/rfc2426
[23]	[RFC5547]	A Session Description Protocol (SDP) Offer/Answer Mechanism to Enable File Transfer IETF RFC http://tools.ietf.org/html/rfc5547
[24]	[vCard21]	vCard, The Electronic Business Card, A versit Consortium Specification, 18 Sep 1996 http://www.imc.org/pdi/vcard-21.doc
[25]	[OMA-CAB]	Converged Address Book (CAB) Specification,

Ref	Doc Number	Title
		Approved Version 1.0, 13 November 2012 http://www.openmobilealliance.org
[26]	[PRESENCE2MO]	OMA Management Object for Presence SIMPLE 2.0, Approved Version 2.0, 10 July 2012 http://www.openmobilealliance.org
[27]	[SUPLMO]	OMA Management Object for SUPL, Candidate Version 2.0 – 27 Jan 2011 http://www.openmobilealliance.org/
[28]	[XDMMO]	OMA Management Object for XML Document Management 1.1, http://www.openmobilealliance.org
[29]	[OMA-MMS-CONF]	OMA MMS Conformance Document, Version 1.3 – 28 Jan 2008 http://www.openmobilealliance.org

2 Device Provisioning

2.1 Description

An MNO 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.

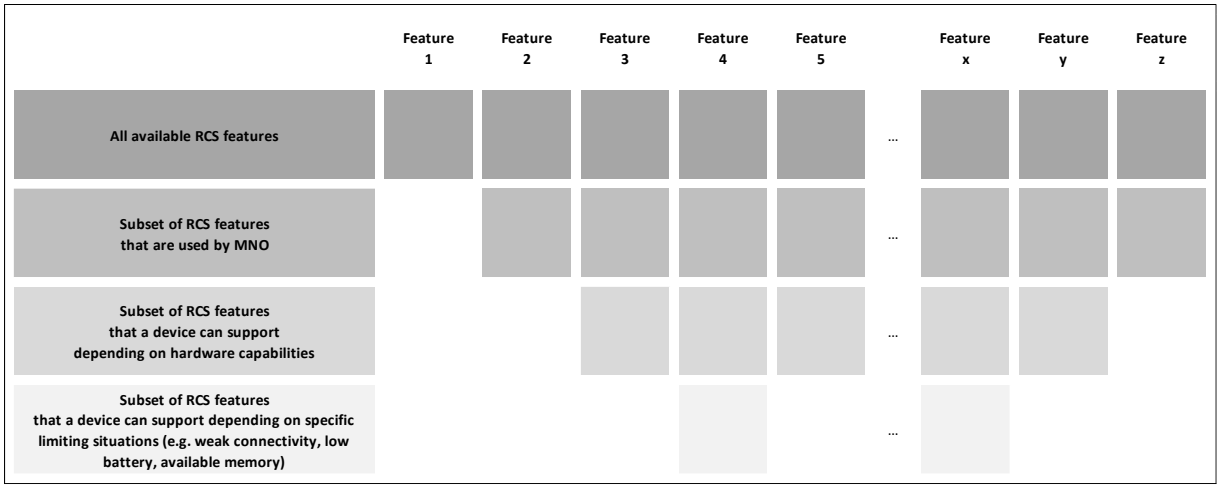

Figure 1: RCS features and their availability depending on MNO choice, device capability, and specific limiting situations.

2.2 User Stories and Feature Requirements

2.2.1 Activation of RCS services

US2-1 **As a user, I want RCS services to be on by default in my device without having to do anything. As an MNO, I want my RCS services to be enabled for my users by default without user interaction.**

R2-1-1 By default, the RCS master switch shall be enabled if the device was provisioned by the MNO.

R2-1-2 The user shall be able to turn the master switch off at any time.

US2-2 **As a user, I want my device to activate RCS services as required in an unobtrusive way.**

R2-2-1 Any available RCS services shall be activated on a device:

R2-2-1-1 When the RCS Master switch is switched on.

R2-2-1-2 When the messaging app or dialler app associated with the RCS service is set as the default messaging client or dialler respectively.

R2-2-2 RCS service activation shall happen either over cellular, or non-cellular networks.

R2-2-3 RCS messaging features shall only be available when the default messaging app is RCS capable.

R2-2-4 RCS enriched calling features shall only be available when the default dialler app is RCS capable.

R2-2-5 When a client is permanently removed from a device or otherwise permanently deactivated, it shall attempt to inform the service provider.

2.2.2 Configuration of the user´s primary device by requesting user identity

US2-3 **As an MNO, I want my RCS users to verify their identity before they use the RCS service.**

R2-3-1 When automatic identification of the user is not possible, the user shall be prompted to provide (by manually typing in) their MSISDN (Mobile Subscriber Integrated Services Digital Number).

R2-3-2 Automatic identification of the user shall be considered not possible when:

- The MNO doesn't offer any automatic identification process.
- After one week since the first automatic identification attempt.

R2-3-3 The user shall be informed why the device is asking him to provide his MSISDN:

R2-3-3-1 This manual MSISDN identification shall be prompted in a context relevant to the services being activated: for example only when the user enters the RCS app relating to the services activated (messaging app or dialler app).

R2-3-4 The user shall be able to skip the manual identification process. In such case, the user can not benefit of RCS services until the client is configured either through the automatic configuration process or through a new manual identification process.

R2-3-4-1 When a user has skipped the process, manual identification shall not be prompted again until the device's next reboot unless automatic identification has been completed in the meanwhile which makes the manual identification irrelevant.

R2-3-4-2 User prompts for manual identification shall be placed in context, i.e. when the user accesses the (native) messaging application on the device.

R2-3-4-3 The maximum number of retries for manual identification shall be 3.

R2-3-5 For entering the MSISDN the user shall be presented with a numeric keypad. When a user enters his MSISDN into the manual identification process, the device shall ensure that the information entered is likely to be of a valid MSISDN format.

R2-3-6 To ensure validity of the provided MSISDN, a verification process shall take place:

R2-3-6-1 A SMS with a one-time password is sent to the device. A silent SMS is preferred if supported by MNO's network.

R2-3-6-2 The one time password included in the SMS may be intercepted by the RCS provisioning process or be manually entered by the user and verified.

R2-3-7 When the verification process has been completed successfully, the provisioning process shall be completed without any further user interaction.

R2-3-8 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 an incorrect MSISDN), the user shall be informed that the process is taking longer than expected and cannot be completed at this stage.

R2-3-9 In this case, the user shall be prompted with the previously given MSISDN (so that the user can amend it if necessary) and shall be provided with an opportunity to retry.

2.2.3 Multiple RCS instances

US2-4 **As a user, I want to download as many RCS applications (messaging clients and diallers) as I choose, and use them without any additional manual configuration**

NOTE: It is up to the MNO to determine how to provision additional RCS applications/instances.

R2-4-1 It should be possible for multiple RCS applications (e.g. multiple messaging applications and multiple diallers) to be active and working at the same time on a device.

NOTE: This requirement cannot be satisfied before device Application Programming Interfaces (APIs) are available from the native RCS implementation.

R2-4-2 Only one messaging 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.

R2-4-3 Only one dialler shall manage the user notifications of incoming calls and call-related information (e.g. enriched calling) at a time and act as the default dialler for making outgoing calls. This shall be known as the Default Dialler.

R2-4-4 If more than one messaging client is active and working at the same time, the user shall be able to choose which one of these clients will act as the Default Messaging Client.

R2-4-5 If more than one dialler is active and working at the same time, the user shall be able to choose which one of these clients will act as the Default Dialler.

R2-4-6 Legacy messaging clients not supporting RCS should not be able to operate as the Default Messaging Client.

R2-4-6-1 On devices where non-RCS clients are able to operate as the Default Messaging Client, RCS messaging services shall only be available when the Default Messaging Client supports RCS.

R2-4-7 Legacy diallers not supporting RCS Enriched Calling should not be able to operate as the Default Dialler.

R2-4-7-1 On devices where non-RCS clients are able to operate as the Default Dialler, RCS Enriched Calling shall only be available when the Default Dialler supports RCS

2.2.4 SIM swap

US2-5 **As a user, I want to use different SIM cards without losing any of my data**

R2-5-1 In the event of a Subscriber Identity Module (SIM) swap (using a SIM with different identity), if a configuration associated with the SIM (either because the device is able to resolve the MSISDN or via the International Mobile Subscriber Identification (IMSI)) is available in the device then it shall be used; otherwise the use case is equivalent to first time use of the service (activation of RCS services as defined in 2.2.1.). Independent of the outcome, user data (e.g. configuration, contacts, messaging history, call logs, etc...) shall not be deleted from the device in the event of a SIM swap

2.2.5 User consent

This section does not apply to markets that don't require users to accept Terms & Conditions (T&C).

For markets which require users to accept T&C before using RCS, two scenarios can be applied, display of "User Message" or display of "End User Confirmation Request".

User Message

US2-6 **As an MNO, I want to be able to provide information and require consent BEFORE my users use the RCS service.**

R2-6-1 Upon MNO discretion a popup showing EITHER Terms & Conditions OR a Welcome Message (OR no popup 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”).

R2-6-2 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).

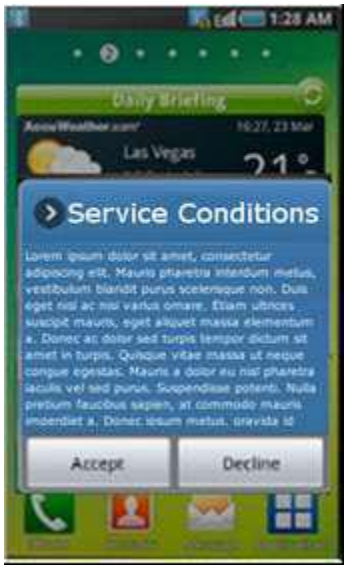

Figure 2: Example Terms & Conditions pop-up

R2-6-3 As soon as the user is presented with the popup, the RCS service shall be active on the device.

NOTE: This means that if the user leaves the screen without any action it is equivalent to an acceptance of the User Message.

R2-6-4 If the user declines the User Message, RCS services shall not be available on the device, (for details see R2-6-2 and Figure 2).

R2-6-5 In case of decline, a retry algorithm shall be able to retrigger the service activation and T&C 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.

R2-6-5-1 Any retry to ask the user for confirmation of the User Message shall be placed in context, i.e. when the user accesses the native messaging application on the device.

End User Confirmation Request

US2-7 **As an MNO, I want to be able to provide information and require consent from my users AFTER the RCS service has been activated**

R2-7-1 Upon MNO 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.

R2-7-2 The display of that message shall be able to come with EITHER one OR two buttons to respond by the user.

R2-7-3 The MNO shall be able to determine the button texts (e.g. 'accept') of that popup.

R2-7-4 The responses to the message shall be relayed back to the network.

R2-7-5 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.

R2-7-6 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,. In this case, the user shall still use the legacy services such as: SMS/MMS/Circuit Switched (CS) Call provided by the MNO on the device.

R2-7-7 In case the RCS services are deactivated, an RCS set-up entry point shall become visible in the device (e.g. settings).

R2-7-8 Upon MNO policies, additional messages may be displayed to the user.

US2-8 **As an MNO I want to request additional information from my users during first-time registration in order to fulfil specific security purposes.**

R2-8-1 Upon MNO discretion users can be requested to enter additional information during first-time registration in order to fulfil specific security requirements set by the MNO.

NOTE: Details are covered in Security against Malware, see section 16.

US2-9 **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.**

R2-9-1 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 "about" page").

2.2.6 Secondary Devices

US2-10 **As a user, I want to use RCS services on other RCS enabled devices other than my primary device.**

R2-10-1 Any device for which there is a compatible RCS application shall become a secondary device by downloading and installing an RCS application.

R2-10-2 When a user wants to use their primary identity in a second or subsequent device, they shall follow a specific authentication process.

R2-10-3 If the application is to be shared by several MNOs, it shall request the user, during the secondary device's authentication process, to choose among the available options. As an alternative, the application could be MNO and country specific, therefore not needing to request this information.

R2-10-4 During the secondary device's authentication process the user shall be prompted to type in a valid MSISDN.

R2-10-5 After successful completion of R2-10-4 a password shall be sent over SMS to the user's primary device.

R2-10-6 In case the user enters and sends an invalid MSISDN in R2-10-5, the UI (User Interface) shall respond according toR2-11-1.

R2-10-7 After successful completion of R2-10-5 the user shall *be* requested to enter the password to complete the provisioning process.

NOTE: Since the SMS with the one time password is sent in this case to the primary device but the device to be configured may be a different one, the application on the secondary cannot intercept the SMS. Therefore this SMS is readable and the user will be requested to input the one time password to complete the provisioning.

R2-10-8 When the secondary device authentication has successfully completed, a completion or welcome message may be displayed.

2.2.7 Error Management

US2-11 **As an MNO, I want technical errors to be handled with minimal user interaction**

The user may get any of the following errors:

R2-11-1 Reception of SMS (see R2-3-6-1, R2-10-5) takes too long or is never received.

NOTE: There are two possible causes:

1. The network does not deliver the SMS.
2. The user made a mistake when typing the MSISDN and the SMS is sent to a different device (also see R2-10-6). 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 up to MNO's discretion).

R2-11-2 Temporary unavailable: Applies to internal errors during configuration/provisioning or configuration server unreachable. The device shall reattempt provisioning at a later stage (i.e. at the next device start-up).

R2-11-3 Permanently unavailable: In case the MNO does not want to provide RCS services to a particular subscription an MNO defined error message shall be displayed if it is required by the MNO and the provisioning process is stopped.

R2-11-4 If the user terminates the configuration process before the process is completed. Further configuration attempts shall automatically start once the user connects to a cellular network.

2.2.8 Provisioning push

US2-12 **As an MNO, I want to be able to push configuration settings in special cases.**

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

R2-12-1 The MNO shall be able to push configuration settings to new or existing RCS users (e.g. in the case of changing parameters).

R2-12-2 The MNO shall be able to push configuration settings in case the network is upgraded to a new RCS release.

R2-12-3 The MNO shall be able to push configuration settings when the device is permanently disabled from using RCS but the user would like to start using RCS.

2.2.9 Dual SIM Devices

US2-13 **As a user of a device that has more than one SIM (module or eSIM) installed in the device, I want to select the SIM that is active for RCS.**

R2-13-1 On first boot-up of the device, the user shall be prompted to select the SIM that shall be used for the active RCS service.

R2-13-1-1 The user shall only be prompted to select one SIM to be active for RCS, if both SIMs are RCS capable.

R2-13-1-2 The user shall only be offered to select SIMs of MNOs who can offer RCS service.

R2-13-1-3 The user shall be notified of the active RCS SIM without being prompted to select one, when there is only one SIM that's RCS capable.

R2-13-1-4 MNOs that offer RCS services should be able to inform the user about their RCS service, capabilities that are implemented and potential billing implications.

R2-13-2 The user shall be able to change the selection to another SIM anytime from the device settings.

R2-13-2-1 MNOs information about the RCS service (as in R2-13-1-4) shall be available to be accessed at a later point in time.

R2-13-2-2 If the user changes the active RCS SIM from the device settings, the previous RCS MNO shall be informed about the de-selection of the service.

NOTE: It is expected that MNOs who are informed about customers de-select their service that they will de-provision the user's identity and will no longer report the RCS capability for this user identity to other users (on-net or cross-net) on incoming capability requests.

US2-14 **As a user, I want to enjoy the benefits of enriched calling whenever I make/ receive the call over active RCS SIM.**

R2-14-1 The user shall have all the entry points enabled to trigger the enriched calling when active RCS SIM is chosen for outgoing calls.

R2-14-1-1 The user shall have no possibility for making enriched calling when SIM other than active RCS SIM is chosen for outgoing calls.

R2-14-1-2 When user makes a voice call to another RCS user with the identity from active RCS SIM, enriched calling (pre-call, in-call and post-call) shall be possible

R2-14-1-3 Incoming enriched calls should be possible only for calls made to the active RCS SIM identity, since the other SIM identity is not RCS capable.

US2-15 **As a user, I want to be provided with enhanced messaging capabilities when available regardless of the SIM I choose for RCS services.**

R2-15-1 When creating a new 1-to-1 Messaging conversation, the proposed identity shall be the identity that supports RCS. The proposed messaging service shall be RCS whenever the B-Party is known to be an RCS user in line with the rules of Integrated or Seamless Messaging.

R2-15-2 When answering a message in an existing messaging thread, the proposed user ID shall be maintained. The user shall be able to switch to the other identity (SIM). The rules of Integrated or Seamless Messaging (as configured by the MNO) shall apply.

R2-15-3 In the conversation history of a user/ group, the messages exchanged shall be marked with the SIM slot used for communication, regardless of the messaging technology.

R2-15-4 While using RCS for messaging, user shall not be prompted to choose SIM for outgoing messages.

2.3 Technical Information

2.3.1 Overview

2.3.1.1 Provisioning

Provisioning 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 specified in [RCC.14] being in scope. For the HTTP based mechanism, section 2.3.3.2 of [RCC.07] and its subsections shall apply in their entirety. If the network is able to do automatic authentication of a primary device based on the access, section 2.2 of [RCC.14] shall be followed. Otherwise for a primary device automatic identification based on the SIM or based on the IMSI as specified in section 2.4 and 2.3 of [RCC.14] respectively might still be possible. As specified in section 2.3 of [RCC.14], a client on a primary device shall request the user for the MSISDN only when those mechanisms fail and when the MSISDN cannot be obtained through other means. Provisioning of secondary devices shall follow section 2.5 of [RCC.14].

The device shall assume that RCS is available on the user's network if Domain Name System (DNS) resolution of the HTTP configuration URL is possible using the MCC and MNC obtained from the SIM card. The rcs_profile parameter shall be included in the HTTP GET requests and set to "UP_1.0".

If an active RCS client is disabled (e.g. due to toggling the master switch referred to in US2-1 or following the activation of another client as a result from the requirements in section 2.2.3), a HTTP configuration request with the rcs state parameter set to -4 (as described in [RCC.07]) shall be sent to the network at the first possible occasion. When the user re-enables a disabled RCS client that had been active before, a HTTP configuration request will be sent to verify whether the available version of the RCS configuration parameters is still valid.

2.3.1.2 User Consent

User consent and welcome messages shall be realised using the MSG characteristic defined in sections 2.2.3 and 4.1 of [RCC.14] or using End User Confirmation Requests (EUCR) as specified in section 3.1 of [RCC.15].

2.3.1.3 Multi-Client

Handling of multiple instances relies on a fundamental principle: only one RCS stack shall be active (i.e. registered to the IMS) at any given time on a device.

To ensure that, a device-local solution is required which will therefore be OS specific.

For Android™ devices, procedures described in Annex B apply.

2.3.2 Technical Implementation of User Stories and Service requirements

R2-16-1 The requirements in US2-1 and R2-2-1 and its sub requirements shall be realised locally on the device.

R2-16-2 R2-2-2 shall be realised as described in [RCC.07] section 2.3.3.1 and 2.3.3.2 with only the HTTP solution being in scope.

R2-16-3 R2-2-3 and R2-2-4 shall be realised locally on the device.

R2-16-4 For R2-2-5, shall set the rcs state to -4 in the configuration request and follow client codes and procedures defined in section 2.3.3.2.1 of [RCC.07].

R2-16-5 R2-3-1 shall be realised locally on the device.

R2-16-6 Provisioning on networks with automatic identification (see requirement R2-3-2) shall be done as described in section 2.3.1.1. If the network cannot authorize the user based on the access (as described in requirement R2-3-2 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.

R2-16-7 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 2.3.1.1 referring to section 2.3 of [RCC.14] and its subsections that provide the procedure required in requirements R2-3-2, along with the error handling described in section 2.3.4of [RCC.14]. 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.

R2-16-8 R2-3-3 and its sub requirements shall be realised locally on the device

R2-16-9 R2-3-4 and its sub requirements shall be realised locally on the device

R2-16-10 R2-3-5 shall be realised locally on the device

R2-16-11 R2-3-6 and its sub requirements shall be realised as described in section 2.3 of [RCC.14] using the SMS format being described in section 2.3.3 of [RCC.14] if the SMS should be handled silently.

R2-16-12 R2-3-7 shall be realised locally on the device

R2-16-13 R2-3-8 and R2-3-9 shall be realised locally on the device

R2-16-14 On Android™ devices, Requirements R2-4-1**,** R2-4-2 and R2-4-3 are linked to the ability of the embedded RCS stack to be used by other messaging applications than the native client.

NOTE: Multi-client solutions for other OSs are for further study. Where relevant solutions on such OSs will align with the concepts used on Android™.

R2-16-15 When the embedded RCS stack is not opened to other applications than the native client, technical solutions described for requirements R2-4-6-1 and R2-4-7-1 apply.

R2-16-16 On Android™ devices requirement R2-4-4 is implemented locally on the device with the Android setting related to the Default SMS app.

R2-16-17 On Android™ devices, R2-4-5 is implemented locally on the device with the Android™ setting related to the Default Dialler (or phone) application.

R2-16-18 The technical feasibility of requirements R2-4-6 and R2-4-7 depend on either evolutions of the Android™ Operating System or device specific implementation to ensure that restriction.

R2-16-19 On Android™ devices whose OS version is superior or equal to 7.0, requirement R2-4-6-1 depends on the availability of an embedded RCS stack opened to other application than the native RCS client:

- On a non RCS device or an embedded RCS device where the stack cannot be used by other applications than the native client: if the messaging application set as Default Messaging Client supports RCS messaging services (using its own stack), the associated stack shall register RCS messaging services to the IMS and announce RCS messaging services in capability exchanges. Any other RCS client previously set as Default SMS app should unregister RCS messaging and Enriched Calling services from the IMS.
- On an embedded RCS device where the stack can be accessed by other applications than the native clients, the required behaviour is:

- if the messaging application set as the Default SMS app supports RCS messaging services using the embedded RCS stack, then this stack shall:
  - announce RCS messaging services in IMS registrations
  - announce support of RCS messaging services in capability exchanges
- if the messaging application set as the Default SMS app does not support RCS messaging services using the embedded RCS stack, then this stack shall:
  - not announce RCS messaging services in IMS registrations
  - not announce support of RCS messaging services in capability exchanges

R2-16-20 On Android™ devices whose version is superior or equal to 7.0, requirement R2-4-7-1 is handled differently according to:

- On a non RCS device or an embedded RCS device where the RCS stack cannot be used by other applications than the native client:
  - if the dialler set as Default Dialler supports the Enriched Calling features, these services will only be provided when this dialler can use the RCS stack of the messaging application set as the default SMS app to implement Enriched Calling services. In that case, this RCS stack shall register Enriched calling services to the IMS and announce them in capability exchange.
  - if the dialler set as the Default Dialler does not support Enriched Calling features, the RCS client if set as default SMS app shall:
    - not register the Pre-Call, Shared Sketch, Shared Maps, Video Share, and Post-Call feature tags on the IMS network.
    - not announce support of Pre-Call, Shared Sketch, Shared Maps, Video Share and Post-Call services in capability exchanges.
- On an embedded RCS device where the RCS stack can be accessed by other applications than the native RCS client, the required behaviour is:
  - if the dialler set as the Default Dialler supports the Enriched Calling features using the embedded RCS stack, then this stack shall:
    - register the Pre-Call, Shared Sketch, Shared Maps, Video Share and Post-Call feature tags on the IMS network.
    - announce support of Pre-Call, Shared Sketch, Shared Maps, Video Share and Post-Call services during capability exchanges.
  - if the dialler set as the Default Dialler does not support Enriched Calling, then the embedded RCS stack shall:
    - not register the Pre-Call, Shared Sketch, Shared Maps, Video Share and Post-call feature tags.
    - not announce support of Pre-Call, Shared Sketch, Shared Maps, Video Share and Post-Call services during capability exchanges.

R2-16-21 R2-5-1 shall be realised locally on the device as described in section 2.1 of [RCC.14].

R2-16-22 As mention in section 2.3.1.1, configuration of additional devices shall be done as described in section 2.5 of [RCC.14] realising the requirements in section US2-10.

R2-16-23 The user consent before use of the service described in user story US2-6 shall be realised through the mechanism for providing User Messages in the HTTP configuration described in section 2.2.3 and 4.2 of [RCC.14]. This mechanism shall be supported by the RCS clients and may be used upon the service provider's discretion.

R2-16-24 As described in section 2.2.3 of [RCC.14] the User Message mechanism supports requirements R2-6-1and R2-6-4.

R2-16-25 Requirements R2-6-2, R2-6-5 and R2-6-5-1 shall be implemented locally on the device.

NOTE: The retry algorithm described is to be realised in the device. An MNO can opt for more retries through the Provisioning Push mechanism described in US2-12.

R2-16-26 For requirement R2-6-3 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.

R2-16-27 The user consent after activation of the service described in user story US2-7 shall be realised through the mechanism End User Confirmation Request mechanism described in section 3.1 of [RCC.15]. 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.

R2-16-28 As described in section 3.1 of [RCC.15] the End User Confirmation Request mechanism supports requirements R2-7-1, R2-7-2, R2-7-3 and R2-7-4. For requirement R2-7-2, 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.

R2-16-29 Requirement R2-7-5 shall be implemented locally on the device

R2-16-30 For requirements R2-7-6 and R2-7-7 the network shall disable the RCS client by triggering a client reconfiguration using the procedure defined in R2-16-36 and R2-16-37 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].

R2-16-31 For requirement R2-7-8, [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 previous one.

R2-16-32 As described in section 2.2.5 of [RCC.14] an MNO 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 R2-8-1. This same non-transparent handling of the SMS can be used to realise this requirement on networks where automatic identification is not possible.

R2-16-33 Requirement R2-9-1 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.

R2-16-34 If the subscriber cannot be provisioned due to MNO policy (i.e. a permanent unavailability as described in requirement R2-11-3), the service provider can include a message as described in sections 2.2.3 and 4.2 of [RCC.14] in a response disabling the RCS client (i.e. RCS DISABLED STATE set to -1).

R2-16-35 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 R2-11-1) 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.

R2-16-36 A SMS shall be sent to the device with a specific format defined in section 3 of [RCC.14] for the push request for initial configuration of a device on which RCS was permanently disabled (i.e. as a consequence of R2-16-35 and R2-16-36 required in R2-12-1 and R2-12-3), and a reconfiguration of an active RCS device (required in R2-12-1 and R2-12-2), shall be enough to trigger a new configuration of a primary device.

R2-16-37 For the reconfiguration of primary and additional devices on which RCS is active already (required in R2-12-1and R2-12-2), 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].

R2-16-38 An RCS enabled SIM shall be discovered based on successful DNS resolution of Fully Qualified Domain Name (FQDN) of Auto-configuration server. This should happen regardless of the type of network (Packet Switched (PS) network or Wi-Fi).

R2-16-39 After discovering the SIM to be supporting RCS as per the procedures in R2-16-38, the client shall fetch the configuration data from Auto-configuration server. When provisioning the user with RCS for the first time, MNO might render a welcome message with list of services/ features to educate the user as described in R2-6-1. This welcome message serves as a medium for MNO to educate/ promote the RCS services and it does not necessarily be correlated with the use of Terms & Conditions

R2-16-40 The client should store the welcome message received from network against the SIM as additional information so that user could revisit the details at later point.

R2-16-41 For requirements R2-13-1-1 and R2-13-1-2, the client shall follow the discovery procedure as described in R2-16-38.

R2-16-42 Requirement R2-13-1-3 shall be implemented locally on the device.

R2-16-43 For requirement R2-13-1-4, the client shall follow the mechanism described in R2-16-39.

R2-16-44 Requirements R2-13-2 and R2-13-2-1 shall be implemented locally on the device.

R2-16-45 For requirement R2-13-2-2, when user changes the default RCS SIM from one MNO to another, client shall

- send HTTP GET request to the ex-MNO with rcs_state parameter set to value -4
- initiate provisioning and registration procedures with new MNO

NOTE: When the user changes the active RCS SIM when there is no data connectivity, the changes shall take into effect after device regains data connectivity

R2-16-46 For requirements R2-14-1, R2-14-1-1 and R2-14-1-2, the client shall be realised locally on the device and when applicable enriched calling shall be provided as described in section 12.

R2-16-47 For requirement R2-14-1-3, a service discovery request targeted at the identity associated to the non-RCS enabled SIM will fail and as such the other party will not be aware that enriched calling is possible and treat the call as a non-enriched call.

R2-16-48 Requirements R2-15-1, R2-15-2, R2-15-3 and R2-15-4 shall be implemented locally on the device. SIM slot information is not stored in the network. When synchronising with the Common Message Store as described in section 9, any retrieved messages are related to the SIM slot of the RCS SIM.

3 Capability Discovery and Service Availability

3.1 Description

Capability discovery is a process which enables RCS users to know the availability of the set or subset of RCS services that 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

3.2 User Stories and Feature Requirements

US3-1 **As a service provider, I can configure the device capability discovery or service availability behaviour.**

R3-1-1 It is at the discretion of the individual MNO to enable or disable RCS capability discovery and service availability in their network and on their devices.

R3-1-2 When both RCS capability discovery and service availability are disabled on a given network and their devices, all RCS service requirements requiring RCS capability discovery and service availability requests are expected to be always available and selectable by the user.

R3-1-3 All RCS MNOs shall respond to each and every RCS capability discovery or service availability request that originates from another MNO or device indicating the agreed interworking capabilities of a given user.

US3-2 **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.**

R3-2-1 The device shall make visible to the user whether a contact is RCS-enabled and if so, for which RCS services or categories they are capable and available for at a given point in time.

R3-2-2 The device shall make visible to the user the detected RCS capabilities for contacts following a contact list scan or an individual contact capability check.

R3-2-3 When displaying capabilities of a non RCS contact, the device shall only make visible services that are known to be compatible with defined RCS services.

R3-2-4 For 1-to-1 Messaging in its Integrated Messaging variant (as defined in ‘US5-2: Variant 1 – Integrated Messaging), there shall not be any RCS service entry points when the recipient is known to be a non- RCS user.

R3-2-5 For Enriched Calling (as defined in section 12 'Enriched Voice Calling'), there shall only be a single service entry point (Post-call Note, as in R12-50-1) when the recipient is known to be a non- RCS user.

R3-2-6 When more than one RCS feature can deliver a similar service, the RCS capability and service availability information should be made visible to the user under a general RCS service category via an icon/label/button. This is done to avoid user confusion when similar RCS capabilities use different underlying services for service delivery.

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 MNOs can configure the appearance of RCS Enriched Calling and Video Call service entry points on the device (on a per-device basis) in one of the following ways:

R3-3-1-1 **Variant A**: The service entry point shall be visible and selectable by the user if there is a high likelihood that the service can be established successfully at that time. If the service is unlikely to be established successfully, the service entry point shall be greyed out and not selectable. This variant applies for any phone number including RCS and non RCS contacts.

R3-3-1-2 **Variant B:** The service entry point shall be visible and selectable by the user if there is a high likelihood that the service can be established successfully at that time. If the service is unlikely to be available, the appearance of the service entry point shall change but remain visible and selectable for any phone number including RCS and non RCS contacts.

R3-3-1-3 **Variant C:** The service entry point shall be visible and selectable by the user for any phone number including RCS and non RCS contacts**.**

NOTE 1: In the case user B is a non RCS user with Video over Long Term Evolution (ViLTE), during call setup confirmation of the ViLTE capability is to be considered to mean there is a high likelihood for a successful video call upgrade.

NOTE 2: “Likely to succeed” means capability or service availability exchange indicates end-to-end support. “Likely to fail” means capability or service availability exchange indicates “not available at this time”.

R3-3-2 If the MNO has decided to enable RCS contact list scan, then the device shall scan the contact list to find out which of the contacts are enabled for which RCS services, in the following ways:

R3-3-2-1 On the first time a different SIM is connected to a RCS device, the device shall perform an initial scan of the full contact list.

R3-3-2-2 After installation and/or set up of the RCS application, and after each re-configuration of the RCS service which impacts capability discovery, the device shall perform a scan of the contact list for all contacts which are not associated with valid RCS capability (or RCS non-capability) information.

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

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

NOTE: If this contact is RCS enabled, their current RCS capabilities shall be displayed.

R3-3-3-2 When opening that contact from the contact list.

R3-3-3-3 When starting a conversation with that contact (e.g. when adding a contact to the “To:” field of a new message.)

R3-3-3-4 When opening a conversation or thread with that contact.

R3-3-3-5 When entering a potentially valid number into the dialler.

R3-3-4 The information whether a given contact is RCS enabled or not shall be updated every time a chat message or File Transfer event is received and when a delivery or display notification for a sent message or file is received.

R3-3-5 The MNO shall have the ability to limit the impact of capability and availability checks based on the following:

R3-3-5-1 An MNO defined minimum interval duration shall exist between two queries sent to the same RCS contact.

R3-3-5-2 An MNO defined minimum interval duration shall exist between two queries sent to the same non-RCS contact.

R3-3-5-3 An MNO defined telephone number prefix setting.

R3-3-5-4 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.

R3-3-5-5 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 Each response to a capability/service availability request/update shall include the current or most recently available capability/availability information.

R3-3-7 The MNO may respond to capability requests with current user capabilities or service availabilities which are stored on the capability or service availability server.

3.3 Technical Information

3.3.1 Overview

When enabled, Capability Discovery and Service Availability shall be realised based on two main Technical Enablers (TE):

TE1: Session Initiation Prototocl (SIP) Options Exchange as specified in [RCC.07] Sections 2.6, 2.6.1.1, 2.7, 2.7.1.1

TE2: Presence Based Exchange as specified in [RCC.07] Sections 2.6, 2.6.1.2, 2.7, 2.7.1.1, 3.7.4, A.1, A1.1, A.2.8

The two implementations are compatible through the co-existence solutions [RCC.07] Section 2.6.1.3.

These enablers provide indications on the following

- capability information (i.e. whether a contact supports a service) and
- service availability information (i.e. whether a contact is currently likely in conditions that allow successful establishment of the service)

TE2 provides this information using the presence service descriptions as described in section 2.6.1.2 of [RCC.07] which would indicate just service availability from which capability information can be derived (i.e. if a service is currently available for use with a contact, that contact is assumed to support the service). For TE1, a similar approach shall be followed, but there the use of the “automata” tag allows to indicate that a contact supports a service (i.e. capability information) without indicating service availability as described in section 2.6.1.1 of [RCC.07].

In the profile defined in this document Service Availability shall be the basis to indicate to the user that a service can likely be established successfully for the following services and for determining whether the following services can be used with a contact:

- IP Video Call (see section 11 and 12)
- Pre-Call services (see section 12)
- Post-Call services (see section 12)
- Chat and File Transfer when latched to SMS (see section 5 and 7 respectively

In-call services can only be available within a call. Therefore their Service Availability shall be verified at the start of every call. This applies to the following services:

- Video Share (see section 12)
- Interactive in-call services (Shared Map/Shared Sketch, see section 12)

Capability information shall be used for determining whether the following services can be used with a contact:

- Chat when not “latched” (see section 5)
- Group Chat (see section 6)
- File Transfer when not “latched” (see section 7)
- File Transfer fall-back to SMS (see section 7)
- Geolocation Push (see section 5)
- Geolocation Push fall-back to SMS (see section 5)

Capability information and service availability information obtained through the capability exchange enablers will be cached on the device according to the requirements in section 3.2. Within this cache different expiry policies are applicable for capability information and service availability. The configuration parameters controlling this are described in section 3.3.2.

When encountering an event related to a contact that doesn’t correspond to the the cached capability information of that contact, a client shall refresh those cached capabilities by initiating a Capability Discovery and Service Availability request. This shall be done when:

- A 1-to-1 SIP request to an RCS enabled contact results in a SIP 404 response or
- A Geolocation Push or File Transfer via HTTP request is received from a contact for which the corresponding capability wasn’t part of the cache or
- For TE1, a SIP OPTIONS request carrying at least one RCS feature tag is received from a non-RCS contact.
- A contact initiates an enriched calling pre-call, post-call or in-call service for which the corresponding capability wasn’t part of the cache

NOTE: Reception of a Chat or Standalone Message from a non-RCS contact is not included because taking into account possible future evolutions of the profile described in this document that could be the result of interworking. An IP Video Call from such a contact is excluded because that may come from a user that only supports IP Video Call.

3.3.2 Configuration Parameters

3.3.2.1 New Configuration Parameters

The following configuration parameters are introduced to manage the user experience based on retrieved capability and service availability information of a contact:

Configuration parameter	Description	Parameter usage
VIDEO AND ENCALL UX	This parameter controls the visibility and selectability of the User Experience (UX) service entry point for Video Call and Enriched Calling: 0,(default): The Video Call and Enriched Calling service entry point will be conditionally visible and conditionally selectable. In the case where based on the capability exchange the service is considered to be available (see section 3.3.1), the corresponding service entry point is visible and selectable. In the case when the capability exchange fails fails or indicates that the service is not available, the corresponding service entry point colour will change and the service entry point will become unselectable. 1: The Video Call and Enriched Calling service entry point will be conditionally visible and always selectable. In the case where based on the capability exchange the service is considered to be available (see section 3.3.1), the corresponding service entry point is visible and selectable. In the case when the capability exchange fails or indicates that the service is not available, the corresponding service entry point will change and remain selectable. The service availability will have no impact on the selectability of the entry point. NOTE: The VIDEO AND ENCALL UX behaviour is valid for any phone number. NOTE: if either video call or enriched calling is not enabled (see section 11 and 12), the corresponding service entry points shall not be shown regardless of the setting of the VIDEO AND ENCALL UX parameter	Optional Parameter

Table 2: Video Call and Enriched Calling Service Entry Point UX Configuration Parameter

This parameters is included in the UX tree defined in section 5.3.7.

<u>Node: /<x>/UX/videoAndEncallUX</u>

Leaf node that describes the visibility and selectability of the video Call and Enriched Calling UX service entry point.

If not instantiated, the same UX service entry point shall be used.

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

Table 3: UX MO sub tree addition parameters (videoAndEncallUX)

- Values:
  0, the Video Call and Enriched Calling service entry point will be conditionally visible and conditionally selectable
  1, the Video Call and Enriched Calling service entry point will be conditionally visible and always selectable
- Post-reconfiguration actions: When the value is changed, the client shall reflect this change in the UI whenever a UI screen is opened that includes the relevant service entry points in a UI screen.
- Associated HTTP XML characteristic type: “videoAndEncallUX”

The following configuration parameters are introduced to manage the expiry of availability information of a contact::

Configuration parameter	Description	Parameter usage
SERVICE AVAILABILITY INFO EXPIRY	This parameter controls expiration of cached service availability information of contacts. NOTE: The services for which service availability (and thus the cached information for which the expiry is controlled by this parameter) is relevant are listed in section 3.3.1. Its value shall indicate the validity time of cached availability information in seconds. Default value: 60	Optional Parameter

Table 4: Video Call and Enriched Calling Service Entry Point UX Configuration Parameter

This parameter is included in the Client Control tree defined in section 5.3.7.

<u>Node: /<x>/ClientControl/serviceAvailabilityInfoExpiry</u>

Leaf node that describes the validity of the availability information cached in the terminal in seconds.

If not instantiated, the same UX service entry point shall be used.

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

Table 5: Client Control MO sub tree addition parameters (serviceAvailabilityInfoExpiry)

- Values: The time in seconds

- Post-reconfiguration actions:
  - When increasing the value, the newly configured expiry value shall be applied to newly cached availability information only
  - When decreasing the value, the client shall consider the expiry of the currently cached capabilities to be the new value and start monitoring from the moment of reconfiguration
- Associated HTTP XML characteristic type: “serviceAvailabilityInfoExpiry”

3.3.2.2 Redefined parameters

The following parameter defined in [RCC.07] shall be used with the following definition in the context of this profile.

Configuration parameter	Description	Parameter usage
CAPABILITY INFO EXPIRY	When using the capability discovery mechanism and with the aim of minimising the traffic, an expiry time is set in the capability information for real-time and non-real-time communication services fetched using SIP OPTIONS or Presence. When capability information was obtained more recently than the value configured for this parameter, it shall be considered as being still valid. . When set to 0, the cached capabilities shall be considered to never expire and shall be invalidated only by a conclusive capability and service availability exchange indicating that they are no longer valid NOTE: The services for which Capability Information (and thus the cached information for which the expiry is controlled by this parameter) is relevant are listed in section 3.3.1. Default value:2592000 (30 days)	Optional Parameter

Table 6: Video Call and Enriched Calling Service Entry Point UX Configuration Parameter

This leads to the following formal definition replacing the one in section A.2.8 of [RCC.07].

Node: /<x>/CapDiscovery/capInfoExpiry

Leaf node that describes the validity of the capability and service availability information cached in the terminal

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

Table 7: Capability MO sub tree addition parameters (capInfoExpiry)

- Values: The validity time in seconds, 0 indicates that there is no expiry
- Post-reconfiguration actions:

  - When changing from a positive value to 0, the already cached capability information shall be considered to never expire
  - When changing from 0 to a positive value, the client shall consider the expiry of the currently cached capabiltiies to be the newly configured value and start monitoring from the moment of reconfiguration
  - When increasing the value, the newly configured expiry value shall be applied to newly cached capabilities only
  - When decreasing the value, the client shall consider the expiry of the currently cached capabiltiies to be the newly configured value and start monitoring from the moment of reconfiguration

- Associated HTTP XML characteristic type: “capInfoExpiry”

3.3.3 Handling of capability exchange triggers in messaging

For messaging following its realisation as defined in sections 5, 6, 7 and 8, capability information is not necessarily required at all times when coming across the Capability Exchange trigger points defined as part of requirement R3-3-3. In messaging only the following trigger points would be relevant:

- R3-3-3-3 for its use in the messaging context and
- the trigger points referred to in R3-3-3-4.

For those entry points an actual capability exchange shall be done only ifwhen all of the following conditions are fulfilled:

- Capability Exchange is enabled (i.e. CAPABILITY DISCOVERY MECHANISM as defined in section A.1.10 of [RCC.07] is set to 0 or 1) and
- the capability exchange is allowed based on the conditions configured by the operator (i.e. according to the CAPABILITY DISCOVERY ALLOWED PREFIXES, NON RCS CAPABILITY INFO EXPIRY client configuration parameters defined in section A.1.10 of [RCC.07] and section 3.3.2) and
- Chat is enabled (i.e. CHAT AUTH as defined in section 5.3.7 is set to 1) and
- at least one of the following conditions is fulfilled:

  - the Chat Capability Information for the contact is unknown or
  - The contact is known to be Chat capable, but for last message a client fall-back to SMS was done (i.e. Latching as required in section 5.2) and no valid Service Availability information is available for Chat with that Contact (based on the configured value for SERVICE AVAILABILITY INFO EXPIRY defined in section 3.3.2.1).

If those conditions are not applicable, the trigger point should not result in a capability exchange request.

3.3.4 Technical implementation of user stories and requirements

R3-4-1 For Requirement R3-1-1 the MNO shall be able to configure the device through the CAPABILITY DISCOVERY MECHANISM client configuration parameter as described in Section A.1.10 [RCC.07]

R3-4-2 Requirement R3-1-2 shall be implemented locally on the device.

R3-4-3 It is recommended the network return response code 404 (not a RCS customer) or 480, 408 when the RCS customer is not registered or a 200 response with agreed interworking service tags when receiving capability polling requests from other networks or devices to satisfy requirement R3-1-3 as described in [RCC.07].

R3-4-4 Requirements R3-2-1 and R3-2-2 shall follow TE1 or TE2. The rest of the requirements under R3-2-3, R3-2-4, R3-2-5 and R3-2-6 shall be implemented locally on the device. The available services for requirement R3-2-3 are voice calling, Operator Messaging with RCS messaging being available if configured through the corresponding configuration parameters.

R3-4-5 Service providers need to configure how RCS service entry points are displayed and made selectable as described in requirement R3-3-1 using the VIDEO CALL and ENCALL UX configuration parameter described in section 3.3.2 if they wish to select variant A (R3-3-1-1) or Variant B (R3-3-1-2). If they wish to use Variant C (R3-3-1-3), they should disable Capability Exchange by setting the CAPABILITY DISCOVERY MECHANISM client configuration parameter defined in Section A.1.10 [RCC.07] to 2 or by not providing that parameter. As defined in R3-1-2 this shall then result in the desired behaviour.

R3-4-6 Requirements under R3-3-2 shall follow 2.6.2 [RCC.07]. The MNO can control whether the RCS contact list scan is enabled through the DISABLE INITIAL ADDRESS BOOK SCAN client configuration parameter.

R3-4-7 Requirements under R3-3-3 shall follow 2.6.2.1, 2.6.3.1, 3.3.6.3, and 3.3.4.1.3 of [RCC.07] and where applicable section 3.3.3.

R3-4-8 Requirement R3-3-4 shall be implemented locally on the device, updating the expiry for the cached Capability information of that contact according to the value set in the CAPABILITY INFO EXPIRY client configuration parameter when this value is not set to 0.

R3-4-9 Requirements R3-3-5 shall follow TE1 or TE2 capability discovery optimizations defined in 2.6.3, 2.6.4, and A.1.10 of [RCC.07] and section 3.3.1 and 3.3.2 of this document.

R3-4-9-1 The operator defined minimum interval duration referred to in R3-3-5-1 shall be based on the configuration of the SERVICE AVAILABILITY INFO EXPIRY and CAPABILITY INFO EXPIRY client configuration parameters defined in section 3.3.2

R3-4-9-2 The interval referred to in R3-3-5-2 shall be configured through the NON RCS CAPABILITY INFO EXPIRY client configuration parameter defined in section 3.3.2.2

R3-4-9-3 Requirement R3-3-5-3 shall follow 2.6.4.1 [RCC.07] with the prefixes being configured through the CAPABILITY DISCOVERY ALLOWED PREFIXES client configuration parameter defined in section A.1.10 of [RCC.07]..

R3-4-9-4 For R3-3-5-4, the cache shall be managed as described in section 3.3.1

R3-4-9-5 Requirement R3-3-5-5 applies only to TE1.

R3-4-10 Requirement R3-3-6 shall be implemented locally on the device for TE1 and as described in section 2.6.1.2 of [RCC.07] for TE2.

R3-4-11 Requirement R3-3-7 shall be provided by the Presence Application Server for TE2 and may be provided by an OPTIONS Application Server (as defined in section 2.6.1.1.5 of [RCC.07]) for TE1.

4 Operator Messaging

Operator Messaging was a separate section to describe the mechanisms that determine the messaging service that is used under any given frame conditions in the Global Common Core specification [RCC.61]. In an effort to reduce complexity, the requirements have been simplified and integrated into the sections 5 (1-to-1 Messaging) and 7 (File Transfer).

5 1-to-1 Messaging

5.1 Description

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

5.2 User Stories and Feature Requirements

US5-1 **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.**

R5-1-1 The Operator Messaging Application shall combine the composing of:

- 1-to-1 Messages
- File Transfer

with SMS (and MMS, if configured by the MNO) messages.

R5-1-2 All messaging entry points on a device shall ensure access to the full Operator Messaging experience.

NOTE: For native implementations.

US5-2 **Variant 1 - Integrated Messaging: As a user, I want full visibility about the Messaging Service that is used for sending a message or a file.**

R5-2-1 The device shall determine and propose the best messaging service available at any point in time to the user.

R5-2-1-1 The user shall be able to configure the device so that either the automatically determined 1-to-1 Messaging service is selected, or a user preference applies (see US18-12 and subsequent requirements).

R5-2-2 Delivery Assurance shall be supported and can be implemented using either Network Fallback to SMS (NFS) or Client Fallback to SMS incl. Revocation (CFS).

R5-2-2-1 'Chat' shall be proposed as the selected Messaging Service only for recipients known to be RCS users for which the messaging technology is not currently latched to SMS (only applies to CFS, see section R5-2-4-6) in each of the following cases:

R5-2-2-1-1 The A-party device is registered to the RCS platform.

NOTE: This includes connectivity via cellular coverage or Wi-Fi.

R5-2-2-1-2 The A-party device is in "Flight Mode", i.e. the user set the cellular data switch to off and the CS connectivity is set to off.

R5-2-2-1-3 The A-party device is not connected to cellular coverage and the user has set the cellular data switch for home network on the device to "on".

NOTE: When not registered in the cases above, messages shall be queued for delivery when the device is reconnected. The user shall be notified that these messages are queued for delivery.

R5-2-2-2 'SMS' shall be proposed as the Messaging Service in each of the following cases:

R5-2-2-2-1 The recipient is not known to be an RCS user.

R5-2-2-2-2 The recipient is an RCS user for whom the technology was latched to SMS (see section R5-2-4-6).

R5-2-2-2-3 The A-Party device is neither connected to cellular coverage nor registered to RCS and the user has set the cellular data switch for home network on the device to "off".

NOTE: Messages shall be queued for delivery when the device is reconnected. The user shall be notified that these messages are queued for delivery.

R5-2-2-2-4 The A-Party device is not online but is connected to cellular coverage.

R5-2-2-3 The full content of the chat messages shall be delivered to the recipient irrespective of the messaging service that has been used (1-to-1 Chat or SMS).

R5-2-2-4 The A-Party user shall be able to differentiate Chat messages from SMS messages the user has created.

R5-2-2-5 The B-Party user shall be able to differentiate incoming chat messages from incoming SMS messages.

R5-2-3 If 1-to-1 Chat Messages cannot be instantly delivered by RCS, the terminating leg should invoke 'Network Fallback to SMS'.

NOTE: NFS does not influence the behaviour of legacy (joyn Blackbird or joyn Crane Priority Release) clients but optimizes the Chat message delivery whatever the originating client version.

R5-2-3-1 If the terminating leg indicates support of Network Fallback to SMS to the universal profile A-Party client (or a later version), the A-Party user shall not be prompted to send a chat message as SMS (i.e. no CFS).

R5-2-4 If 1-to-1 Chat Messages cannot be delivered by RCS within an MNO configurable period of time and the terminating network does not support NFS, the client shall use the procedures of CFS to ensure Delivery Assurance.

R5-2-4-1 The procedures of CFS shall be used on any universal (or later version) client only if the terminating leg has indicated the support for CFS.

R5-2-4-2 While typing, Capability Discovery may change the messaging service to be used from SMS to Chat.

R5-2-4-3 If delivery of a 1-to-1 Chat message could not be confirmed after an MNO configurable period of time, the client shall offer the option to send the message as SMS.

R5-2-4-4 The user shall have the option to automate the user interaction for CFS. The following options shall be selectable:
- Always ask
- Never ask and always send as SMS
- Never ask and never send as SMS

R5-2-4-4-1 The user shall have the option to see this selection or change this decision at any point in the RCS settings section.

NOTE 1: Steps 3 (R5-2-4-5-3 below) to Step 4b (R5-2-4-5-5 below) are only presented to the user if the device is configured to “Always Ask” and would be automatically processed accordingly if the device is configured to “Never Ask and always send as SMS”.

NOTE 2: The user selection to automatically send as SMS shall have no impact on MMS being used as a fallback for File Transfer.

R5-2-4-5 The following steps describe how and when the revocation and send as SMS procedure shall be applied:

R5-2-4-5-1 Step 1: User A has created a Chat message and this message has been sent.

R5-2-4-5-2 Step 2: Delivery for that Chat message has not yet been confirmed within an MNO configurable period of time. If the A-Party device lost connectivity during this period, then Step 3 shall not occur until the A-Party device is connected again for an MNO configurable time, to allow update of message status notifications.

R5-2-4-5-3 Step 3: The user shall be presented with a message "Your Chat message could not be delivered instantly, do you want to change to an SMS message?" and a confirmation request for the user to select (yes / no) shall be shown.

If a delivery notification for the Chat message is received before the user has selected their response (yes/no), the confirmation request shall be removed, and the original Chat message shall be indicated as 'delivered' (or 'displayed', if applicable).

R5-2-4-5-4 Step 4a: If the user selects "Yes", then
- a revocation for the original Chat message shall be triggered,
- the original Chat message shall be removed from the conversation history once the revocation has been confirmed as successful, and
- an SMS message shall be sent and appear in the conversation history. This SMS will display content similar to the original Chat message, the timestamp of the moment the user confirmed the sending by SMS and an indication of the sending service "SMS".

Subsequent sent messages that are in 'pending' or 'sent' status shall be covered by the same user selection (same procedure applies), and latching as described in section R5-2-4-6 shall be applied.

Failure of one of these steps, shall not mean that the other steps are not executed. This may lead to duplicated messages.

R5-2-4-5-5 Step 4b: If the user selects "No", a revocation of the original Chat message shall not be triggered and an SMS shall not be sent. The Chat message status shall be updated according to the delivery status. The suggested messaging service shall remain Chat. As long as the user stays within the conversation thread, they shall not be asked again.

R5-2-4-6 SMS Latching: When sending a message to a known CFS contact, a universal client shall by default propose to use 1-to-1 Chat. If during the last message exchange the client had to fall-back to SMS and there has been no indication since that the contact is RCS online again (e.g. capability exchange or use of another RCS service), SMS shall be used as the default messaging service. This means that once there has been a fall-back to SMS, subsequent messages shall continue to be sent as SMS until RCS availability is confirmed.

R5-2-4-6-1 SMS shall also be used whenever the client has already fallen back to 'SMS link' for File Transfer: subsequent messages shall continue to be sent as SMS until RCS availability is confirmed (e.g. capability exchange or use of another RCS service).

NOTE: The use of CFS for Chat and File Transfer is subject to users allowing it in user settings (see section 18).

R5-2-5 Before sending a message, the A-Party messaging interface shall clearly display whether a message will be sent as SMS or Chat.

R5-2-5-1 When opening the conversation or before entering the first character of a message, the client logic shall propose the Messaging Service (either SMS or Chat) to be used for that message.

R5-2-5-2 Before sending a message, the client shall indicate to the user whether a message will be sent as SMS or 1-to-1 Chat.

R5-2-5-3 The user shall be able to change the proposed messaging service on a per message and on a general basis.

NOTE 1: Details of changing the proposed messaging service on a general basis are specified in section US18-12.

NOTE 2: Changing the proposed messaging service on a per message basis shall be a “one click experience” on UI level.

R5-2-5-4 A manual user selection of a Messaging 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.

R5-2-5-5 The creation of a new conversation shall trigger the automatic selection of the proposed Messaging Service.

US5-3 **Variant 2 - Seamless Messaging: As a user, I want to send a message without knowing about the underlying technology / service that is being used to convey my messages / file shares. I want the MNO to deliver the message the best possible way to the intended recipient(s).**

As a user, I don’t want my Messaging Application to show the Messaging Service being used when messages are displayed in my inbox.

As a user, I want to fully rely on my MNO to convey the Messaging Service to ensure quickest and most reliable message delivery.

R5-3-1 The RCS client can be configured to automatically send RCS messages when connected and registered for the RCS service.

R5-3-2 The RCS client will not show or visually indicate to the user the technology / service used to convey the message from the device.

R5-3-3 The MNO should interwork any RCS message sent from the RCS device (regardless of technology / service) to ensure the best possible message delivery to an intended recipient.

R5-3-4 The Seamless Messaging composer shall select RCS as the Messaging and File Transfer Service when no network connection is available and not registered for RCS services. These messages shall be queued for delivery when the device is reconnected. The user shall be notified that these messages are queued for delivery.

R5-3-5 When the device is connected to cellular coverage but not registered to the RCS platform, the delivery mechanism from the Seamless Messaging App shall be SMS.

NOTE: All other RCS services will not be available.

R5-3-5-1 If the user selects other RCS services (non text messaging) when in this mode these messages will be queued for delivery until the device is reconnected. The user shall be notified that these messages are queued for delivery.

R5-3-6 When the device is connected to cellular coverage with data but not registered to the RCS platform, the sending mechanism from the Seamless Messaging App shall be xMS.

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

R5-3-7 When the device is registered for RCS services, the sending mechanism from the Seamless Messaging App shall be RCS.

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

R5-3-8 When the device is registered for RCS services 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.

Seamless Messaging - Selected Messaging Service					
User A - Sender	Connected to Cellular network	Yes	Yes	No	No
	Registered to RCS	Yes	No	Yes	No
User B - Receiver	Connected to Cellular network	n/a			
	Registered to RCS				
Selected service		**RCS**	**xMS***	**RCS**	**RCS***
* On-device caching of unsent RCS messages/files required, and the user shall be informed.					

Table 8: Table to explain and summarise static conditions for Seamless Messaging

US5-4 **As a user, I want to send Messages to my contacts.**

NOTE: This document describes the Messaging Service functionality for contacts on-net or on an Interconnected RCS service. Other contacts may have less functionality available.

R5-4-1 Any RCS user shall be able to send a Message to Contacts in the contact list or by entering the contact's MSISDN.

R5-4-2 The user shall have the option to send a message at any time by entering an existing chat conversation and continue.

NOTE: The 1-to-1 conversation 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 messaging history or the option to resume the chat at a later time.

R5-4-3 The messaging service that is used to convey the messages is determined by either the ruleset of Integrated Messaging or the ruleset of Seamless messaging.

R5-4-3-1 The MNO shall be free to choose <u>either</u> Integrated Messaging <u>or</u> Seamless messaging.

R5-4-3-2 In Integrated Messaging, the user can influence the proposed messaging service according to requirements under US18-12.

US5-5 **As a user, I want to see the status of my sent Messages.**

R5-5-1 For A-Party, the following message states shall be supported:

R5-5-1-1 Message Pending: Transfer of the Message in progress *(e.g. queuing on device)*.

R5-5-1-2 Message Sent: confirmation that the message has been correctly accepted by the A-Party's network.

R5-5-1-3 Message Delivered: Confirmation that the message has been delivered to the B-Party device.

R5-5-1-3-1 For legacy SMS messages sent from a device, Delivery Notifications may be supported upon user choice or network default configuration.

R5-5-1-4 For Integrated Messaging: If a message was delivered applying NFS, the A-Party client shall be able to differentiate between a message that was terminated as Chat and a message that was terminated as SMS. For example, the user shall be able to understand whether or not to expect a Delivery Notification.

R5-5-1-5 Message Displayed: When the message has been displayed in the Chat view on the receiving device. As per US18-7 and the related requirements, the user shall have the option to disable sending the feedback that the message was displayed.

NOTE: Message Displayed status may not be supported by all networks. Incoming "displayed" notifications may be ignored by these networks and not forwarded to the user.

R5-5-1-5-1 For legacy SMS messages sent from a device, appropriate means shall be used to inform the user that "Message Displayed" is not available (e.g. by greying out Display Notification as soon as the Delivery Notification is displayed).

R5-5-1-5-2 For Integrated Messaging: If a message was delivered applying NFS, the A-Party client shall be able to differentiate between a message that was terminated as Chat and a message that was terminated as SMS. For example, the

user shall be able to understand whether or not to expect a Display Notification.

R5-5-1-6 Message sending 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 (Sending the message may be re-triggered manually by the user).

R5-5-2 If the sending device is offline at the time a notification is received, notifications shall be updated once the sending device is online again.

R5-5-3 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.

R5-5-4 The ‘failed’ status notification shall never be aggregated but presented separately to the user.

R5-5-5 Message states only apply to messages to recipients which do not blacklist the sender. In case the sender is blacklisted, the valid sending message states shall be “pending”, “sent”, “failed” and “delivered”.

US5-6 **As a user, I want to include small graphics into my Messages.**

NOTE: Small graphics can express mood, fun or icons to explain a thing or a status in a graphical, easy to use and understandable manner. Examples are ☺, ☏, 💣 and ☯.

R5-6-1 It shall be possible to add small graphics when creating a message by adding from a selection of graphical elements in the messaging application.

NOTE: Standards for conversion of text strings to Emoji are described in Annex “Emoticon conversion table”, Annex A.3.

R5-6-2 It shall be possible to add a few basic small graphics when creating a 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.

R5-6-3 The graphical elements that are used may vary between implementations, but the conveyed meaning must not be changed.

R5-6-4 Small graphics shall be displayed properly in any representation of the messages on the user interface, which includes the conversation thread as well as any notifications or previews of messages in pop-ups or dedicated screens.

US5-7 **As a user, I want to see when the other party is currently writing a Message.**

R5-7-1 The other party shall be able to see an “is typing” notification whenever the creator of a message is typing.

NOTE: Networks may not support “is typing” notification. In this case, networks may ignore incoming “is typing” notifications.

US5-8 **As a user, I want to ensure that my messages reach their destination as reliably and quickly as possible.**
As a user, I want to send text Messages to my contacts even when they're temporarily offline (e.g. device switched off). I expect them to receive these Messages as soon as they can be terminated.

R5-8-1 Void

R5-8-2 The MNO shall ensure all 1-to-1 messages and related messaging services originating from a device shall be conveyed in a manner that will ensure the quickest delivery to the recipient.

R5-8-2-1 Store and Forward shall be available and provided by every RCS Service Provider to host messages for its RCS users on the terminating leg when these users are offline.

R5-8-3 It shall be possible to send a message to a B-Party user when they are offline.

NOTE: If the B party receives the message using another service before re-registering to RCS, then the B-party shall not be notified of the message – this avoids message duplication.

US5-9 **As a user, I want to receive text Messages from my contacts. 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.

R5-9-1 Any RCS user shall be able to receive message(s) that are sent to them.

R5-9-2 Any message exchanged in the Chat Conversation shall be received without any form of acceptance of the message.

NOTE: MMS may be restricted by user settings.

R5-9-3 The user shall see any Messages and File Transfer events exchanged with a single contact grouped into one Conversation thread.

R5-9-3-1 Any application allowed to manage (read, write, view) xMS on a device shall also be allowed to manage (read, write, view) RCS messages. Any application allowed to manage (read, write, view) RCS on a device shall also be allowed to manage (read, write, view) xMS messages.

R5-9-3-2 Any application selected by the user as the default messaging application shall manage xMS and RCS messages (incl. File Transfer).

R5-9-4 If messages are received that exceed the number of characters that the application is able to display properly, the application shall cut off characters that cannot be displayed properly and inform the user about the fact that only a part of the message can be displayed.

US5-10 **As a user, I want to be notified at any time my device receives a new Message. I want notifications of rapidly sequenced incoming Messages intelligibly aggregated and counted.**

R5-10-1 On receiving a message, the user shall be notified.

R5-10-2 Rapid sequence of incoming Messages or File Transfers in one Conversation shall be consolidated into one audible notification per Conversation. Consolidation of visual notifications is not affected.

R5-10-3 The visual notification shall be permanently removed after the user has opened the message or seen the file download (link).

US5-11 **As a user, I want audible notifications in line with device settings.**

R5-11-1 For audio notifications, device audio related settings shall prevail.

US5-12 **As a user, I want to view my sent and received Messages in a time-based order.**

R5-12-1 All messages exchanged 1-to-1 with the same contact shall be threaded in the same thread in a timely order.

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).

R5-12-2 The order of messages shall be in line with the order messages have been sent and received on the device.

R5-12-3 Incoming and outgoing messages shall be displayed interlaced.

R5-12-4 Sent messages shall be inserted into the Conversation thread as they have been sent.

US5-13 **As a user, I want to see the timestamp associated with each of my sent and received messages.**

R5-13-1 The date and time associated with each chat message shall be displayed adjusted to the current device date and time.

R5-13-1-1 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.

R5-13-1-2 Timestamps for received messages shall be based on the UTC timestamp that comes with each message, aligned with the selected device time zone.

US5-14 **As a user, I want conversations which contain unread messages to be differentiated from conversations that contain messages I have seen.**

NOTE 1: This requirement shall be valid for Messaging for Multi-Device as well.

NOTE 2: 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.

R5-14-1 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.

R5-14-2 The visual notification shall be permanently removed after the user has opened the message on any connected device (in case of multi device).

US5-15 **As a user, I want to know who is participating in Chat Conversation at any point in time.**

R5-15-1 If the sender of a message is not in my contact list, the sender's RCS Alias name, if available, shall be presented in addition to the sender's MSISDN. Representation of Alias names shall be differentiated from contact list matches. The support of RCS Alias shall be MNO configurable.

NOTE: The Alias (as specified in US18-2) is created by the message sender.

R5-15-2 If neither contact name nor the RCS Alias are available, the B-Party shall be represented by their MSISDN.

US5-16 **As a user, I don't want to feel restricted by Message size limits.**

R5-16-1 Messages (incoming and outgoing) shall allow for up to 8192 bytes length.

NOTE: MNO defined parameter.

US5-17 **As a user, I want to exchange multi-media content in my 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', section 7.

R5-17-1 The user shall be able to select and send Multi Media in Conversations.

NOTE: Details on multi-media content share are covered in 'File Transfer', section 7.

R5-17-2 The user shall be able to receive Multi Media in Conversations.

NOTE: Details on 'multi-media content share' are covered in 'File Transfer', section 7.

R5-17-3 The user shall be able to browse any media that was exchanged in the particular 1-to-1 Conversation in an aggregated view.

US5-18 **As a user, I want to maintain multiple Conversations in parallel.**

R5-18-1 Multiple parallel conversations (with different recipients) and Group conversations shall be supported at any given point in time.

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 may be stored on the network.

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

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

R5-19-3 In case the MNO 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 my device always be in sync with the messages stored on the network.**

R5-20-1 1-to-1 Messaging shall support storage on the network.

US5-21 **As a user, I want to restore my Conversations from the Common Message Store (e.g., but not limited to, after wiping device or purchasing a new device).**

R5-21-1 The user shall have the option to restore Conversations from the Common Message Store (e.g., but not limited to, in case of handset replacement or automated local memory removal of messages on device to free up memory space).

US5-22 **As a user, I want to delete complete Conversations.**
As a user, I want to select and delete single and multiple nonadjacent messages in a conversation thread.

R5-22-1 Any Messages or entire conversations that have been deleted by the user shall no longer be available on the Common Message Store.

NOTE: Deletion on other devices of the same identity is described in ‘Messaging for Multi-Device’, section 9.

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

R5-23-1 The user shall be able to receive a voice call when actively engaged in a conversation and return to the message conversation when the voice call was ended.

R5-23-2 The user shall be able to receive a video call when actively engaged in a 1-to-1 messaging conversation or Group Chat Conversation and return to the conversation when the video call ends.

US5-24 **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) from the 1-to-1 Messaging Application.**

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.

R5-24-1 The 1-to-1 messaging conversation shall be a service entry point to initiate a Geolocation Push.

R5-24-2 There may be other service entry points available on the device to initiate a Geolocation Push (e.g. Contact Card, call log).

R5-24-3 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 an online map display or a 'screenshot' with map picture.

R5-24-4 For Geolocation Push, the rules of Delivery Assurance as described in section 0 shall apply if the MNO supports Integrated Messaging.

R5-24-5 If Geolocation Push is delivered using SMS, the recipient's device shall be able to detect that it's a Geolocation Push and display that event as an icon.

R5-24-5-1 The icon shall make visible to the user that they received a location.

R5-24-5-2 If the user selects the icon, the service shall be performed as if the Geolocation Push would have been transferred as a RCS message.

US5-25 **As a user, I want to view an automatically detected position on map and have the ability to change this manually before sending.**

R5-25-1 If the current position is to be sent, the location shall be automatically detected and suggested to the end user.

R5-25-2 The user shall have the option to preview and correct the automatically detected position on a map view before sending.

R5-25-3 The Geolocation Push Service shall support sending of a location from other applications (e.g. mapping apps).

US5-26 **As a user, I want to tag positions or locations with a text field.**

R5-26-1 The user shall have the option to tag a position or location with a free text field before sending.

US5-27 **As a user, I want to receive positions / locations in a map view.**

NOTE: These functions are not provided by the RCS implementation.

R5-27-1 When receiving a position or location, the RCS Geolocation Push user shall have the ability to see the position / location on a map.

R5-27-2 When receiving a position or location, the RCS Geolocation Push user shall be able to see any tags that were added by the sender.

R5-27-3 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.

US5-28 **As a user, I want to send many 1-to-1 messages and files by selecting multiple recipients.**

R5-28-1 The client shall make clear to the user the differences between multiple 1-to-1 message and a Group Chat.

R5-28-2 The user shall be able to create a distribution list for multiple 1-to-1 messages.

R5-28-2-1 The distribution list shall be available as a service entry point for multiple 1-to-1 messages.

R5-28-3 The user shall be able to create multiple 1-to-1 messages by selecting 1-to-1 messaging and add more than one participant as recipients.

R5-28-3-1 A distribution list shall be created in this case.

R5-28-3-2 The distribution list of a multiple 1-to-1 message shall be stored on the device and be accessible for the user after sending the message, e.g. for sending another message or file instantly or later.

R5-28-3-3 The user shall be able to manage distribution lists for multiple 1-to-1 messages: Name distribution list (e.g. football team), add and remove recipients, or delete an entire distribution list.

R5-28-4 All messages and files that are sent to a distribution list are treated on the originating and terminating devices similar to explicit 1-to-1 messages or file transfers.

R5-28-5 Recipients of messages sent to a distribution list are not aware of the other recipients who are on the list and receive similar messages.

US5-29 **As an MNO, I would like to control the use of multiple 1-to-1 messages.**

R5-29-1 To prevent Spam distribution, the MNO shall be able to limit the list of recipients.

R5-29-1-1 The MNO shall be able to set the possibility of unlimited participants.

R5-29-2 The MNO shall be able to determine the messaging service(s) that are used to convey multiple 1-to-1 message distribution.

R5-29-2-1 The rules of Seamless Messaging and Integrated Messaging shall apply if RCS is used to deliver messages.

5.3 Technical information

5.3.1 Overview

This section covers the functional requirements for the client to select and apply the service behaviour specified in the previous section. For some services, the desired requirements may be provided by multiple technologies. This section deals with the co-existence of the technologies and specifies the selection rules taking into account the following services:

- The **1-to-1 Messaging service** can be provided based on:
    - The RCS 1-to-1 Chat service following the Open Mobile Alliance (OMA) Converged IP Messaging (CPM) technical realisation defined in section 3.3 of

[RCC.07] and extended by functionality provided in this section. In order for the RCS 1-to-1 Chat service to be used it shall be enabled by the service provider via the configuration parameter CHAT AUTH as defined in section 5.3.7.2 and the client shall be registered in IMS. The client configuration parameter CHAT MESSAGING TECHNOLOGY defined in sections A.1.4.3 and A.2.6 shall be set to 1. The client shall advertise the chat capability in accordance with the definitions of sections 2.6.1.1.2 and 2.6.1.2.5.1 of [RCC.07] based on the procedures specified in section 3.3. RCS 1-to-1 Chat delivery is driven by Delivery assurance requirements described in section 5.2. For the Service Providers that have deployed other RCS versions with RCS Chat 1-to-1 service based on OMA SIMPLE IM procedures, deploying an OMA SIMPLE IM to OMA CPM and vice versa interworking function will be needed. The interworking procedures will be covered in a separate document.

NOTE: As per section 3.3.4.3 of [RCC.07] and [RCC.11], there is no message included in the SIP INVITE.

- The RCS Standalone messaging service as defined in section 3.2 of [RCC.07]. In order for the RCS Standalone messaging service to be used it shall be enabled by the service provider via the configuration parameter STANDALONE MSG AUTH as defined in sections A.1.4.3 and A.2.1 of [RCC.07] and the client shall be registered in IMS.
- The Short Messaging Service as defined in [3GPP TS 23.040] or the Short Messaging Service over IP as defined in IR.92.

This profile assumes that the Service Provider deploys one of the following options with regards to enabled RCS 1-to-1 messaging technologies:

1. Only RCS Standalone messaging service is enabled (i.e. STANDALONE MSG AUTH set to 1) or
2. Only RCS 1-to-1 Chat service is enabled (CHAT AUTH is set to 1) or
3. RCS 1-to-1 Chat and RCS Standalone messaging service are enabled (i.e. STANDALONE MSG AUTH is set to 1 and CHAT AUTH is set to 1)

NOTE: For Service Providers that deploy the first option in combination with the Group Chat service (i.e. GROUP CHAT AUTH is set to 1) and choose to interwork with Service Providers that deploy the second option through interworking their RCS Standalone messages to an RCS 1-to-1 Chat session and vice versa, an interworking function will be deployed. The implementation of the interworking procedures is for further study.

- The **Geolocation Push service** can be provided based on:
  - The RCS Geolocation Push service realised as defined in section 3.10 of [RCC.07]. In order for the RCS Geolocation Push service to be used it shall be enabled by the service provider via the configuration parameter PROVIDE GEOLOC PUSH as defined in sections A.1.8 and A.2.1 of [RCC.07] and the client shall be registered in IMS.

- The **1-to-Many Messaging service** can be provided based on the services listed under the 1-to-1 Messaging service.

  - If the RCS Standalone messaging service is enabled, the 1-to-Many Messaging service is provided based on the procedures described in [RCC.11].
  - Otherwise, if the RCS Standalone messaging service is not enabled, the 1-to-Many Messaging service is provided as 1-to-1 Messaging service per single recipient.

  The 1-to-Many messaging service is enabled if the MAX 1 TO MANY RECIPIENTS configuration parameter defined in section 5.3.7 is present with a value other than "0"..

5.3.2 Network Fallback Support Capability

Delivery Assurance in this profile relies on a capability indication mechanism during the initiation of a 1-to-1 Chat session (see section 5.3.3.3). The capability indication is used by the network to indicate which fallback mechanism shall be applied for messages sent by a client in this 1-to-1 chat session. The capability indication is used by the network to indicate its support for either

- the network fallback procedure, where the network is responsible for providing the fallback (also called Network Fallback to SMS, or NFS), or
- the message revocation, where the client is responsible for the fallback (also called Client Fallback to SMS or CFS).

The indication is provided by the feature tags defined in Table 9.

tag	Description
+g.gsma.rcs.msgrevoke	Message Revocation is supported (as defined in section 3.3.4.1.10.3 of [RCC.07])
+g.gsma.rcs.msgfallback	Network interworking is supported

Table 9: Feature tags used to indicate network support for chat fallback mechanisms

Only one of the network indications defined in Table 9 can be present in a 1-to-1 Chat session, i.e. they are mutually exclusive.

The indication and the support of a network fallback mechanism is mandatory in the profile defined in this document. This includes service provider deployments supporting termination of 1-to-1 Chat sessions only.

If the network indicates support of network fallback, the network shall take responsibility for delivering the message using the most suitable path. Therefore if the terminating network has provided this indication the client shall not apply procedures to monitor the delivery of chat messages and fallback.

When the CHAT REVOKE TIMER is set to a value higher than 0 and the network indicated capability is message revocation, the client shall apply procedures to monitor the delivery of chat messages and fallback. For integrated messaging configured clients (i.e. MESSAGING UX set to 1), the SMS fallback shall be enabled on the client based on the MESSAGING

FALLBACK DEFAULT client configuration parameter and user selection. For seamless messaging configured clients (i.e. MESSAGING UX is set to 0), there is no user authorisation required for the SMS fallback.

When SMS latching is triggered, the client shall cache this event for future interactions with this contact unless Chat service is re-selected. This cached information shall affect the capability exchange triggers (see section 3.3) and the messaging technology selection (see section 5.3.3.1).

When the CHAT REVOKE TIMER parameter is set to 0 or the SMS fallback is disabled on the client and the network indicated capability is message revocation then the client behaviour is based on the terminating network chat delivery policies (e.g. store and forward will be applied if the recipient cannot be reached).

NOTE: For Standalone Messaging, it is assumed that both the originating and the terminating network will offer interworking to xMS, where the former is used when sending a Standalone Message to a non-RCS user or a user of an operator with whom no interworking agreement for Standalone Messaging is offered. The latter option would be used towards RCS users who's primary device is offline, but reachable. This is considered to be providing the delivery assurance for Standalone Messaging.

5.3.3 Client behaviour

5.3.3.1 Technology selection rules

5.3.3.1.1 1-to-1 Messaging service

The technology selected for the first message in a 1-to-1 Conversation shall be based on:

- the RCS 1-to-1 messaging technologies enabled i.e. RCS Standalone messaging and/or RCS 1-to-1 Chat.
- the chat capability of the contact (i.e. based on the last capability exchange that was executed according to the triggers defined in section 3)

The technology selection rules apply for the case where the originating client is registered for RCS services. If the client is not registered for RCS services specific handling is applied based on the MESSAGING UX client configuration parameter setting.

If RCS 1-to-1 Chat is disabled and RCS Standalone messaging is enabled then RCS Standalone messaging is the selected technology.

If RCS 1-to-1 Chat is enabled and RCS Standalone messaging is disabled then

- if the recipient supports the RCS Chat service then the RCS 1-to-1 Chat service is the selected technology for the initiation of a conversation, otherwise
- if the recipient does not support the RCS Chat service then SMS is the selected technology

If both RCS 1-to-1 Chat and RCS Standalone messaging are enabled then

- if the recipient supports the RCS 1-to-1 Chat service then the RCS 1-to-1 Chat service is the selected technology for the initiation of a conversation, otherwise
- if the recipient does not support the RCS 1-to-1 Chat service then RCS Standalone messaging is the selected technology.

If the RCS 1-to-1 Chat Messaging technology is selected for a 1-to-1 conversation, the technology may change during the conversation based on the network fallback procedures defined in this document.

If the RCS 1-to-1 Chat Messaging technology and the initiation of a RCS 1-to-1 Chat session fails then the client shall

- send an RCS Standalone message if RCS Standalone Messaging is enabled, otherwise
- send a SMS.

If the RCS 1-to-1 Chat Messaging technology is selected for a 1-to-1 conversation and sending of a RCS 1-to-1 Chat message fails with one of the following MSRP response codes

- 400 request was unintelligible
- 403 attempted action is not allowed
- 501 recipient does not understand the request method

the client shall

- send an RCS Standalone message if RCS Standalone Messaging is enabled, otherwise
- send a SMS.

If the RCS Standalone messaging service is selected for a 1-to-1 conversation, originating or terminating network fallback may be applied based on Service provider policies.

If the RCS Standalone messaging service is selected and sending an RCS Standalone message returns an one of the following responses:

- 380 Alternative Service
- 408 Request Timeout
- 486 Busy Here
- 487 Request Terminated

the client shall immediately resend the message as an xMS. For other error responses the client will retry the message before falling back to xMS..

Table 10 provides an overview of the technology selection and fallback scenariosen for 1-to-1 messaging conversations.

Enabled technologies	Terminating network chat fallback mechanism indicated	Non -RCS recipient	RCS recipient with Chat capability	RCS recipient with no Chat capability
RCS Standalone messaging only	N/A	RCS Standalone messaging	RCS Standalone messaging	RCS Standalone messaging
RCS 1-to-1 Chat Messaging only	Revocation supported	SMS	RCS 1-to-1 Chat Messaging unless latched to SMS	SMS
	Interworking supported	SMS	RCS 1-to-Chat Messaging	SMS
RCS 1-to-1 Chat and RCS Standalone messaging	Revocation supported	RCS Standalone messaging	RCS 1-to-1 Chat Messaging unless latched to SMS	RCS Standalone messaging
	Interworking supported	RCS Standalone messaging	RCS 1-to-1 Chat Messaging	RCS Standalone messaging

Table 10: Messaging technology selection for 1-to-1 conversation initiation when A party is online

5.3.3.1.2 Geolocation Push service

If the RCS Geolocation Push service is enabled (i.e. PROVIDE GEOLOC PUSH is set to 1) and the Chat service is enabled (i.e. CHAT AUTH is set to 1), the client shall follow the procedures defined in section 3.10 of [RCC.07]:

If a message for RCS Geolocation Push is subject to delivery assurance as defined in this document, the client shall apply the procedures defined in section 5.3.6. If a message for RCS Geolocation Push is subject to delivery assurance as defined in this document and the receiver does not support the procedures defined in section 5.3.6, the client shall send the location based on the rules defined in section 5.3.3.1.1:

- Selecting an RCS Standalone message if RCS Standalone Messaging is enabled, otherwise
- Selecting an SMS.

If the RCS Geolocation Push service is enabled (i.e. PROVIDE GEOLOC PUSH is set to 1), the RCS 1-to-1 Chat service is disabled (i.e. CHAT AUTH is set to "0") and the RCS Standalone messaging service is enabled, the regular Geolocation Push service defined in section 3.10 of [RCC.07] cannot be used due to its dependency on Chat. Therefore the

location information shall be sent as a text message based on the technology selection rules described in 5.3.3.1.1. For the format of the message, the procedures defined in section 5.3.6 shall be applied (i.e. it shall depend on whether the recipient indicated the Geolocation Push via SMS capability defined in section 5.3.6.2).

For sending location information towards non RCS users, the 1-to-1 Messaging technology selection rules towards non-RCS users defined in section 5.3.3.1.1 shall apply.

5.3.3.1.3 1-to-Many messaging service

The availibity of the 1-to-Many messaging service and the maximum number of participants allowed for 1-to-Many messaging services shall be controlled by the MAX 1 TO MANY RECIPIENTS parameter defined in section 5.3.7. The MAX 1 TO MANY RECIPIENTS configuration parameter is applicable regardless of which technology is selected.

If the RCS Standalone messaging service is enabled, the RCS Standalone message service shall be selected based on procedures described in in sections 7.2.1 and 9.1 of [RCC.11] for sending a CPM Standalone Message to an ad-hoc group whereby the client shall set the copyControl attribute for all recipients to “BCC”.

If the RCS Standalone messaging service is not enabled, the technology selected for the many 1-to-1 messaging services is based on the 1 TO MANY SELECTED TECHNOLOGY client configuration parameter value (see section 5.3.7.1). If the Chat service is selected via the 1 TO MANY SELECTED TECHNOLOGY configuration parameter, the procedures for technology selection and delivery assurance apply on a single recipient basis as defined for the RCS 1-to-1 Chat service.

5.3.3.2 Chat Fallback Mechanism management

When initiating a 1-to-1 Chat session, the client complying with this profile shall monitor the delivery of the messages exchanged in the session based on the feature tags defined in Table 9:

- If a SIP 200 OK response is received as final response, the client shall behave as follows based on the presence or absence of the feature tags defined in section 5.3.2.2.
    - If the Contact header in the 200 OK response included the message revocation feature tag defined in section 5.3.2.2while the CHAT REVOKE TIMER client configuration parameter is configured with the value 0 or if applicable the SMS fall-back is disabled on the client, the client shall assume delivery for any messages based on the terminating network delivery policies (e.g. store and forward will be applied if the recipient cannot be reached).
    - If the Contact header in the 200 OK response includes the message revocation feature tag defined insection 5.3.2.2, the CHAT REVOKE TIMER client configuration parameter is set to a value higher than 0 and if applicable the SMS fall-back is enabled on the client, the client shall apply monitoring of the delivery for any messages sent within the session as defined in section 3.3.4.1.10.1.1 of [RCC.07] (i.e. through a timer based on the CHAT REVOKE TIMER client configuration parameter).

- If the message revocation feature tag defined in section 5.3.2.2 is absent in the Contact header of the 200 OK response, then the client shall not monitor the delivery of any messages that it sends in the Chat session.

For a client invited to a 1-to-1 Chat session (excluding a session for delivering stored messages or notifications), behaviour shall be as follows:

- If the Contact header field included in the SIP INVITE request included the message revocation feature tag defined in section 5.3.2.2 while the CHAT REVOKE TIMER client configuration parameter is configured with the value 0 or if applicable SMS fall-back is disabled on the client, the client shall assume the delivery of any messages that it sends in the Chat session according to the terminating network delivery policies (e.g. store and forward will be applied if the recipient cannot be reached).
- If the Contact header in the SIP INVITE request includes the message revocation feature tag defined in section 5.3.2.2and the CHAT REVOKE TIMER client configuration parameter is set to a value higher than 0 and if applicable SMS fall-back is enabled on the client, the client shall monitor the delivery of any messages that it sends in the Chat session as defined in section 3.3.4.1.10.1.1 of [RCC.07] (i.e. through a timer based on the CHAT REVOKE TIMER client configuration parameter).
- If the message revocation feature tag defined in section 5.3.2.2 is absent in the Contact header of the SIP INVITE request, then the client shall not monitor the delivery of the messages that it sends in the Chat session.

5.3.3.3 Procedures for Client SMS Fall-back

If according to the procedures defined in section 5.3.3.2 the client runs for messages in a conversation a timer based on the CHAT REVOKE TIMER client configuration parameter and the client receives "delivery" disposition notifications for all messages in the conversation, then the client shall stop the timer.

The client shall start a timer based on the CHAT REVOKE TIMER client configuration parameter for the next message sent in the conversation considering the message revocation capability indicated in accordance with the procedures defined in section 5.3.3.2.

1. If the timer based on the CHAT REVOKE TIMER client configuration parameter is running for at least one conversation and if
    a. the client registers in IMS successfully due to a previous de-registration (e.g. due to user setting or data-off) and if the value of the RECONNECT GUARD TIMER configuration parameter defined in section 5.3.7 is not set to "0", then the client shall start the reconnection guard timer with the value provided in the RECONNECT GUARD TIMER configuration parameter defined in section 5.3.7, or
    b. the client re-connects to the Proxy Call Session Control Function (P-CSCF) due to a previous loss of connection to the P-CSCF and if the value of the RECONNECT GUARD TIMER configuration parameter defined in section 5.3.7 is not set to "0", then the client shall start the reconnection guard timer with the value provided in the RECONNECT GUARD TIMER configuration parameter defined in section 5.3.7.
    c. The reconnect guard timer shall start if

i. a success response is received from the network for an initial registration or re-registration resulting from the client procedures to re-connect to the P-CSCF, otherwise
ii. at the time of P-CSCF connection re-gain.

2. If the timer based on the CHAT REVOKE TIMER client configuration parameter expires, then processing commences with step 3.
3. The client shall check whether the reconnection guard timer is running. If yes, then processing commences with step 5, otherwise processing commences with step 4.
4. If the client
    a. is not registered in IMS due to missing data connection (e.g. data off, loss of connection to the P-CSCF and registration expired), then the client shall wait until data connection is regained.
    b. If the data connection is regained then the client shall send an initial registration as per procedures of section 2.4 of [RCC.07].
    c. has stored a valid IMS registration but it has previously detected a loss of connection to the P-CSCF, then the client shall wait until data connection is regained.

    If the data connection is regained
        i. and the IMS registration is valid (e.g. registration is not expired, the client IP address did not change, access network did not change), then the client shall send a re-registration as per procedures of section 2.4 of [RCC.07].
        ii. and the IMS registration is not valid (e.g. registration is expired, the client IP address did change), then the client shall send an initial registration as per procedures of section 2.4 of [RCC.07].

    If the initial registration or the re-registration is successful, then
        iii. if the value of the RECONNECT GUARD TIMER configuration parameter defined in section 5.3.7 is set to "0" then processing commences with step 6.
        iv. otherwise, the client shall start the reconnection guard timer with the value provided in the RECONNECT GUARD TIMER configuration parameter defined in section 5.3.7. Processing commences with step 5.
    d. otherwise, in all other cases where the client is registered in IMS, processing commences in step 6.
5. If the reconnection guard timer is running and
    a. if "delivery" disposition notifications have been received for all messages in the conversation, then the reconnection guard timer shall be stopped by the client. The client shall stop the message fall-back processing.
    b. if the client detects a loss of connection to the P-CSCF or it is de-registered, the reconnection guard timer is stopped and processing commences with step 4
    c. If the reconnection guard timer expires the processing commences with step 6.
6. The client shall verify whether connectivity for sending SMS messages exists. If connectivity for sending of SMS messages exists, then processing commences with step 7. Otherwise, the client
    a. shall wait until connectivity for SMS is regained again.

   b. If the connection to the P-CSCF is lost or the client is de-registered from IMS while waiting for connectivity for sending of SMS messages, the client shall stop waiting for SMS connectivity and continue processing in step 4.
   c. If "delivery" disposition notifications have been received for all messages in the conversation, then the client shall stop waiting for SMS connectivity. The client shall stop the SMS fall-back processing.
   d. Once connectivity for sending SMS is regained, then processing commences with step 7.

7. If a user authorisation is required for the SMS fall-back for this conversation, then the client shall invoke a user interaction. Otherwise processing commences with step 8.
   a. If the client receives "delivery" disposition notifications for all messages in the conversation, then the client shall abort the user interaction and stop the message fall-back processing.
   b. If the user interaction results in the user authorisation of the SMS fall-back, then the procedure commences with step 4. The client shall retain the user authorisation of the SMS fall-back for the subsequent processing, i.e. the client shall not invoke the user interaction again.
   c. If the user interaction results in rejection of the message fall-back, then the client shall stop message fall-back processing.
8. The client shall create a Message Revoke request for the oldest chat message of the conversation for which no "delivery" disposition notification has been received and which has not been processed for SMS fall-back. The client shall send the Message Revoke request to the network. Message revocation shall be implemented as defined in section 5.3.5 of this document. If the value of the configuration parameter CFS TRIGGER defined in section 5.3.7
   a. is set to "1", then
      i. if the Message Revocation request fails due to loss of connection to the P-CSCF, then the client shall continue processing with step 4.
      ii. if the client receives a success response (200 OK) to the Message Revoke request, then the client shall
         1. start an operation timer to supervise the processing of the Message Revocation, otherwise
         2. not send a fall-back SMS and consider the chat message as processed for SMS fall-back. The client shall continue with the procedure in step 8 until all messages in the conversation have been processed.
      iii. If the client receives a "delivery" disposition notification for the message to be revoked, it shall stop SMS fall-back handling.
      iv. If the client receives a Message Revocation response from the network with a "success" result, then the client shall stop the operation timer and shall send the fall-back SMS following the procedures for fall-back according to the type of message (e.g. chat message, file transfer).
      v. If the client receives a Message Revocation response from the network with a "failure" result, then the client shall stop the operation timer and shall not send the fall-back SMS and consider the chat message as processed for SMS fall-back. The client shall continue with the procedure in step 8 until all messages in the conversation have been processed.

vi. If the client detects a loss of connection to the P-CSCF or the client is de-registered from IMS (e.g. due to user settings), then the client shall stop the operation timer and shall send the fall-back SMS following the procedures for fall-back according to the type of message (e.g. chat message, file transfer). If there is at least one message in the conversation for which no "delivery" notification has been received and which has not been processed for SMS fall-back the client shall continue processing with step 4, otherwise is shall stop SMS fall-back handling.

vii. If the operation timer expires then the client shall send the fall-back SMS following the procedures for fall-back according to the type of message (e.g. chat message, file transfer).

viii. If submission of the SMS to the network fails (e.g. no SMS connectivity), then the client shall suspend the processing of SMS fall-back and apply the client procedures for the handling of failed SMS message submissions.

ix. If the submission of the SMS is confirmed by the network with a success response, then the client shall consider the chat message as processed for SMS fall-back. The client shall trigger SMS latching and cache this status for the contact. The client shall continue with the procedure in step 8 until all messages in the conversation have been processed.

x. If the submission of the SMS is rejected by the network with a failure response, then the client shall stop processing of the SMS fall-back and apply the client procedures for the handling rejected SMS message submissions

b. is set to "0" or is not present then the client shall send the fall-back SMS following the procedures for fall-back according to the type of message (e.g. chat message, file transfer) and the Message Revoke request at the same time.

i. If the Message Revoke request fails due to loss of connection to the P-CSCF and there is at least one message in the conversation for which no "delivery" notification has been received and which has not been processed for SMS fall-back, then the client shall continue processing with step 4, otherwise the client shall stop processing of SMS fall-back.

ii. If submission of the SMS to the network fails (e.g. no SMS connectivity), then the client shall suspend the processing of SMS fall-back and apply the client procedures for the handling failed SMS message submissions.

iii. If the submission of the SMS is confirmed by the network with a success response, then the client shall consider the chat message as processed for SMS fall-back. The client shall trigger SMS latching and cache this status for the contact. The client shall continue with the procedure in step 8 until all messages in the conversation have been processed.

iv. If the submission of the SMS is rejected by the network with a failure response, then the client shall stop processing of the SMS fall-back and apply the client procedures for the handling rejected SMS message submissions.

v. The outcome of the Message Revocation operation does not alter the processing requirements of the client with regard to SMS fall-back.

However the client may need to inspect the outcome of the Message Revocation operation to satisfy the requirements for the presentation of the message status to the user.

5.3.3.4 Disposition Notifications

For the messages sent in a Chat session, the client shall request in the Instant Message Disposition Notification (IMDN) Common Profile for Instant Messaging (CPIM) header an Interworking Disposition Notification as defined in Appendix O of [RCC.11], if during the setup of the session the terminating network has indicated support for interworking using the corresponding feature tag defined in Table 9. As defined in [RCC.07], the client shall also request a Delivery and a Display notification.

When receiving an Interworking Disposition Notification as defined in Appendix O of [RCC.11], the client shall consider the message to have been delivered and interworked. The client shall thus not assume that a Delivery and a Display notification will follow.

5.3.4 Network Behaviour

5.3.4.1 Chat Fallback Mechanism Management

Service Providers supporting the RCS 1-to-1 Chat service as defined in section 5.3.1 shall support network fallback. This profile assumes that the fallback is performed in the network serving the recipient of the message. RCS 1-to-1 Chat Fallback in the network serving the sender of the message is out of the scope of this document. The following procedures shall be implemented:

- When handling an SIP INVITE request for a 1-to-1 Chat session, if the messaging server in the originating network supports the client fallback delivery assurance procedure, then it shall add either the message revocation feature tag as defined in section 5.3.3.2 in the Contact header field of the SIP INVITE request sent towards the terminating client based on the chat fallback mechanism that is supported. If the the messaging server in the originating network supports the network fallback delivery assurance procedure as defined in section 5.3.3.2 no additional actions are required when handling an SIP INVITE request for a 1-to-1 Chat session.
- When handling an SIP INVITE request for a 1-to-1 Chat session, the messaging server in the terminating network supports the client fallback delivery assurance procedure procedure it, then it shall add either the message revocation feature tag as defined in section 5.3.3.2 in the Contact header field in every 200 OK to the SIP INVITE request sent towards the originating client. If the the messaging server in the terminating network supports the network fallback delivery assurance procedure procedure as defined in section 5.3.3.2 no additional actions are required when handling an SIP INVITE request for a 1-to-1 Chat session.

NOTE: For networks with RCS Standalone messaging service enabled that enable only receiving 1-to-1 chat messages (i.e. CHAT AUTH is set to 0 and GROUP CHAT AUTH is set to 1) that choose to interwork with Service Providers that enable only RCS 1-to-1 Chat service (option 2) by deploying RCS Standalone message to RCS 1-to-1 Chat session interworking function the above procedure can be fulfilled by the interworking function.

The terminating network shall always return a SIP 200 OK response to a SIP INVITE request for 1-to-1 chat session since the network takes responsibility for delivering the message in the best way possible regardless of the connectivity status of the client.

If the terminating network supports Message Revocation, this shall be implemented as defined in section 5.3.5 of this document.

5.3.4.2 Indicate delivery as SMS

When a network complying with this profile supports interworking and it delivers the message through interworking to SMS, it shall generate an interworking notification as defined in Appendix O of [RCC.11] when such a notification was requested in the IMDN Disposition-Notification CPIM header of the message that was interworked. In that case, the network shall not generate a Delivery disposition notification. If IMDN Disposition-Notification CPIM header didn't include a request for an interworking notification, the network shall generate a Delivery Notification instead.

NOTE: Since according to section 5.3.3.4 a client complying with this profile will always have requested an interworking notification, this requirement to generate a regular Delivery notification is intended to support clients of previous RCS versions.

5.3.5 Chat Message revocation

Message Revocation shall be implemented as defined in section 3.3.4.1.10 of [RCC.07], but only the client of the sender of the message shall initiate the MessageRevoke request. Section 3.3.4.1.10.1.2 of [RCC.07] for MessageRevoke requests sent by the Messaging Server is not applicable. Additional clarifications and requirements apply:

- The Service Provider policy defined in section 3.3.4.1.10.1.1 of [RCC.07], to send Message Revoke requests in the case that a 486 Busy Here response is received does not apply. Instead the client shall initiate a Message Revoke request based on the procedures described in section 5.3.3.2.
- Message revocation is applicable for chat messages used for File Transfer via HTTP as defined in section 7 or Geolocation Push as defined in section 5.3.6 if an appropriate fallback mechanism is applicable for the message.
- Message Revoke requests and MessageRevokeResponse requests are not sent with CPIM headers, and a delivery and/or displayed notification shall not be requested.
- There is no store and forward for the Message Revoke requests and the MessageRevokeResponse requests.
- For the Message Revoke request section 3.3.4.1.10.1.1 of [RCC.07] applies. The client shall send a SIP MESSAGE request according to the rules and procedures of [RCC.11] with the clarifications listed here. In this SIP MESSAGE request, the client:

    1. shall include an Accept-Contact header field with the CPM IMS Communication Service Identifier (ICSI) for Session Mode Messaging similarly to the case for IMDNs carried in SIP MESSAGE requests;
    2. shall add a dedicated Accept-Contact header field carrying the Message Revoke feature tag defined in section 3.3.4.1.10.3 of [RCC.07] along with the *require* and *explicit* parameters;

3. shall include the Content-Type header field with the value set to the message revocation content-type application/vnd.gsma.rcsrevoke+xml, as described in section 3.3.4.1.10.4 of [RCC.07];
4. shall include the address of the originating RCS Client that has been authenticated as per [RCC.11];
5. shall include a User-Agent header field as specified in [RCC.11];
6. shall set the Request-URI of the Message Revoke request to the address of the target contact of the message that is requested to be revoked;
7. shall not include the device identifier of the original sender of the message in the MessageRevokeResponse request;
8. shall set the body of the Message Revoke request, as follows:
   a. The <Message-ID> element set to the value of the imdn.message-ID of the original message that is requested to be revoked,
   b. The <From> element set to the URI of the sender of the message,
   c. The <To> element set to the URI of the recipient of the message.
9. Similar to section 5.4 of [RCC.11] for IMDNs, shall include the same Conversation-ID and Contribution-ID header field values used for the message being revoked.
10. shall send the SIP MESSAGE request according to the rules and procedures of [RCC.11].

- For the MessageRevokeResponse request section 3.3.4.1.10.2 of [RCC.07] applies. The Messaging Server shall send a SIP MESSAGE request according to the rules and procedures of [RCC.11] with the clarifications listed here. In this SIP MESSAGE request, the Messaging Server handling the Message Revoke request:

  1. shall include an Accept-Contact header field with the CPM ICSI for Session Mode Messaging similarly to the case for IMDNs carried in SIP MESSAGE requests;
  2. shall add a dedicated Accept-Contact header field carrying the Message Revoke feature tag defined in section 3.3.4.1.10.3 of [RCC.07] without the *require* and *explicit* parameters;
  3. shall include the Content-Type header field with the value set to the message revocation content-type application/vnd.gsma.rcsrevoke+xml as described in section 3.3.4.1.10.4 of [RCC.07];
  4. shall include the address of the intended recipient RCS Client, where the Messaging Server initiates the MessageRevokeResponse on behalf of the intended recipient that has been authenticated as per [RCC.11];
  5. shall include a User-Agent header field of the Messaging Server as specified in [RCC.11];
  6. shall set the Request-URI of the MessageRevokeResponse request to the address of the contact that sent the message that is requested to be revoked;
  7. shall set the body of the MessageRevokeResponse request, as follows:
     a. The <Message-ID> element set to the value of the imdn.message-ID of the original message that is requested to be revoked,
     b. The <From> element set to the URI of the sender of the message,
     c. The <To> element set to the URI of the recipient of the message,
     d. The <result> element set to the revoke result;

8. Similar to section 5.4 of [RCC.11] for IMDNs, shall include the same Conversation-ID and Contribution-ID header field values used for the message being revoked.
9. shall send the SIP MESSAGE request according to the rules and procedures of [RCC.11].

- For chat messages that are under retry delivery attempt due to Messaging Server store and forward functionality, the result of the MessageRevokeResponse shall be “failed”.
- The client shall ignore any MessageRevokeResponse request for chat messages that it does not recognize based on the Message-ID (corner case).

5.3.6 Geolocation Push Fallback

5.3.6.1 Registration

A client supporting the rendering of the user data of a short message for Geolocation Push as defined in section 5.3.6.2 and the procedures for "geo" URI defined in section 5.3.6.4 shall add the feature tag defined in Table 11 in the Contact header field of the SIP REGISTER requests that it initiates.

5.3.6.2 Geolocation Push via SMS Capability

5.3.6.2.1 Based on SIP OPTIONS

A client supporting this profile shall add the feature tag defined in Table 11 in the Contact header field of the SIP OPTIONS requests and responses.

RCS service	Tag
Geolocation Push via SMS	+g.3gpp.iari-ref="urn%3Aurn-7%3A3gpp-application.ims.iari.rcs.geosms"

Table 11: SIP OPTIONS tag for Geolocation Push via SMS

5.3.6.2.2 Based on Presence

A client supporting this profile shall include in the capabilities that announces in the Presence document the following capability:

Geolocation Push via SMS
Service-id: +g.3gpp.iari-ref=*org.3gpp.urn:urn-7:3gpp-application.ims.iari.rcs.*geosms
Version: 1.0
Contact address type: tel / SIP URI

5.3.6.3 Geolocation Push URI for fallback

A client supporting Geolocation Push fallback shall be able to

- generate, using RCS Location information data, and
- resolve and render

a “geo” URI according to [RFC5870].

For the purpose of Geolocation Push fallback the "geo" URI format of [RFC5870] is extended by a new parameter to carry a "label". The usage of the "label" parameter shall follow the definitions for the "label" in Geolocation Push defined in section 3.10 of [RCC.07].

"Geo" URI parameters extending [RFC5870] are defined in Table 12.

Parameter	Value Restriction	Value Definition
rcs-l	Constrained	Contains a label that can be used to tag the nature of the location (e.g. indicate that it's the home or provide an address, name of restaurant, etc.) in the context of Geolocation Push. If the label parameter is absent, the location that is shared is assumed to be the sharing users own position. NOTE: non ASCII and reserved characters have to be represented using percent encoding in accordance with [RFC5870].

Table 12: "geo" URI Parameter Extensions

Note: It is recommended that implementations ensure that the maximum length of the URLs does not exceed the length of the user data of one short message.

5.3.6.4 Sender procedures

If the originating client decides to fallback to SMS for a Geolocation Push message and the recipient supports Geolocation Push via SMS as indicated by the capability defined in section 5.3.6.2 then the sender client shall use the position and the label of the RCS Location information data sent in the Geolocation Push message and generate a "geo" URI as defined in section 5.3.6.3.

5.3.6.5 Receiver procedures

On reception of a SMS message, the client shall parse the user data of the message.

If the user data contains a "geo" URI as defined in [RFC5870], then the client shall apply the UX procedures defined for suppression and replacement of the "geo" URI string. The client shall apply the rules for the presence and absence of the "label" via the "geo" URI extension defined in section 5.3.6.3 in accordance with the definitions of section 3.10 of [RCC.07].

5.3.6.6 Network Procedures for Fall Back for Geolocation Push

The procedures in the network for fallback for Geolocation Push are network internal and therefore outside of the scope of this document. However, to facilitate a solution at a later time, as specified in section 5.3.6.1 the User Equipment (UE) shall include the IMS Application Reference Identifier (IARI) defined in Table 11 in the Contact header field of the SIP REGISTER request along with the rest of the feature tags the UE is required to include, as described in [RCC.07]. The format of the SMS messages sent shall follow the format defined for the client-based fallback described in section 5.3.6.4.

5.3.7 Configuration Parameters

5.3.7.1 New configuration parameters

To provide the required MNO control of the 1-to-1 Messaging behaviour, the following parameters are added to those that are available in [RCC.07], [RCC.14] and [RCC.15]:

Configuration parameter	Description	RCS usage
MESSAGING UX	This parameter controls whether the UX for messaging shall be the seamless messaging (0, default value) or the integrated messaging experience (1) NOTE: When receiving a provisioning document from a legacy network, this parameter is not provided resulting in the default behaviour.	Optional Parameter
USER ALIAS AUTH	This parameter controls whether the client is authorised to offer the user alias function to the user. The following values are defined: The client is not authorised for user alias handling. The client shall not offer the user a Ux to manage the user alias used for RCS services. For mobile originated RCS transactions, the client shall never add a user alias as defined in section 2.5.3.4 of [RCC.07]. If the client receives a user alias as defined in section 2.5.3.4 of [RCC.07] in a mobile terminated RCS transaction, the client shall discard the value, i.e. it is neither displayed to the user nor stored in the communication history. The client is authorized to offer the user functions related to the user alias handling (default). The definitions of [RCC.07], specifically section 2.5.3.4, and the user alias related functional requirements of this document apply.	Optional Parameter
MESSAGING FALLBACK DEFAULT	This parameter is applicable only when MESSAGING UX is set to 1 and CHAT REVOKE TIMER is set to a value higher than 0. It controls the default setting for the client switch controlling the user dialog when according to the rules in section 5.2 an RCS 1 to 1 Chat message or RCS Geolocation Push message should be resent as SMS, The default can be set to: **0 (Default Value),** never ask the user to confirm the retransmission as SMS and always send as SMS, **-1,** never ask the user to confirm the retransmission as SMS and never send as SMS **1**, always ask the user to confirm whether the message should be sent as SMS instead.	Optional parameter

RECONNECT GUARD TIMER	This parameter is applicable when CHAT REVOKE TIMER is set to a value higher than 0. It provides the minimum time the client shall be registered in IMS prior to sending a message revocation request for a chat message when the revocation timer (i.e. CHAT REVOKE TIMER) expired. Default value: 120 seconds	Optional parameter
CFS TRIGGER	This parameter is applicable when CHAT REVOKE TIMER is set to a value higher than 0. It controls the trigger for the client to fallback to SMS when revocation procedures apply. 0 (default), the client shall fall back to SMS and send the Message Revoke request right after sending the SMS 1, the client shall fall back to SMS right after receiving the MessageRevokeResponse request with the value of the result equal to “success”	Optional parameter
MAX 1 TO MANY RECIPIENTS	This parameter is applicable when CHAT AUTH or STANDALONE MSG AUTH is set to 1 and it provides the maximum contacts allowed to be included in the distribution list of the 1-to-Many messaging service. 0 (default): the 1-to-Many Messaging service is disabled 1: the client can add unlimited number of recipients >1: integer value that indicates the maximum total number of recipients that can be included in the distribution list	Optional parameter
1 TO MANY SELECTED TECHNOLOGY	This parameter is applicable when the RCS Standalone messaging service is disabled (i.e. STANDALONE MSG AUTH is set to 0) and it controls the selected messaging technology for the 1-to-Many messaging service. 0 (default): SMS is selected 1: RCS 1-to-1 Chat service is selected	Optional parameter
DISPLAY NOTIFICATION SWITCH	This parameter controls whether sending of Display Notifications is enabled/disabled on the recipient’s client. 0 (default), Enable sending Display Notifications, The user may still disable it using the Display Notification setting 1, Disable sending Display Notifications. The Display Notification setting is not available to the user.	Optional parameter

Table 13: Additional Configuration Parameters to control 1-to-1 Messaging behaviour

The MESSAGING UX, USER ALIAS AUTH and MESSAGING FALLBACK DEFAULT parameters are added to the UX tree with the following formal definition:

<u>Node: /<x>/UX</u>

The parameters used to control the UX of the client are placed under this interior node.

Status	Occurrence	Format	Min. Access Types
Required	One	node	Get

Table 14: UX MO sub tree addition node

- Values: N/A
- Associated HTTP XML characteristic type: “UX”

Node: /<x>/UX/messagingUX

Leaf node that describes whether the seamless messaging experience or the integrated messaging experience shall be used.

If not instantiated, the seamless messaging experiences shall be used.

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

Table 15: UX MO sub tree addition parameters (messagingUX)

- Values:
  0 (default), the client shall use the seamless messaging experience
  1, the client shall use the integrated messaging experience
- 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: “messagingUX”

Node: /<x>/UX/userAliasAuth

Leaf node that describes whether the client is authorised for user alias handling for RCS services.

If not instantiated, user alias handling as defined in this document based on the implementation in section 2.5.3.4 of [RCC.07] shall be applied by the client.

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

Table 16: UX MO sub tree addition parameters (userAliasAuth)

- Values:
  0, the client is not authorised for user alias handling
  1 (default), the client is authorised for user alias handling
- Post-reconfiguration actions:
  If the configuration parameter value transits from 0 to 1, or the parameter is added with value 1 to the client configuration, the client shall unhide the UX elements for the management of the user alias.
  If the configuration parameter value transits from 1 to 0 or the configuration parameter is removed, then the client shall hide the UX element for the management of the user alias. A stored user alias value of the client user shall be deleted.

The new value of the configuration parameter shall be stored and applied from this time on.

- Associated HTTP XML characteristic type: “userAliasAuth”

Node: /<x>/UX/msgFBDefault

Leaf node that describes the default setting of the switch controlling whether the user should confirm a retransmission of a 1 to 1 RCS Chat message or RCS Geolocation Push message as SMS.

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

Table 17:UX MO sub tree addition parameters (msgFBDefault)

- Values:
  -1, the default setting of the switch is to never ask the user to confirm the retransmission and never do the fallback
  0 (default value), the default setting of the switch is to never ask the user to confirm the retransmission and always do the fallback.
  1, the default setting of the switch is to always ask the user to confirm the retransmission as SMS
- Post-reconfiguration actions: Change the setting of the switch, if it hasn’t been toggled by the user before.
- Associated HTTP XML parameter ID: “msgFBDefault”

Node: /<x>/UX/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 18: UX MO sub tree addition Service Provider Extension Node

- Values: N/A
- Associated HTTP XML characteristic type: “Ext”

This lead to the following UX tree:

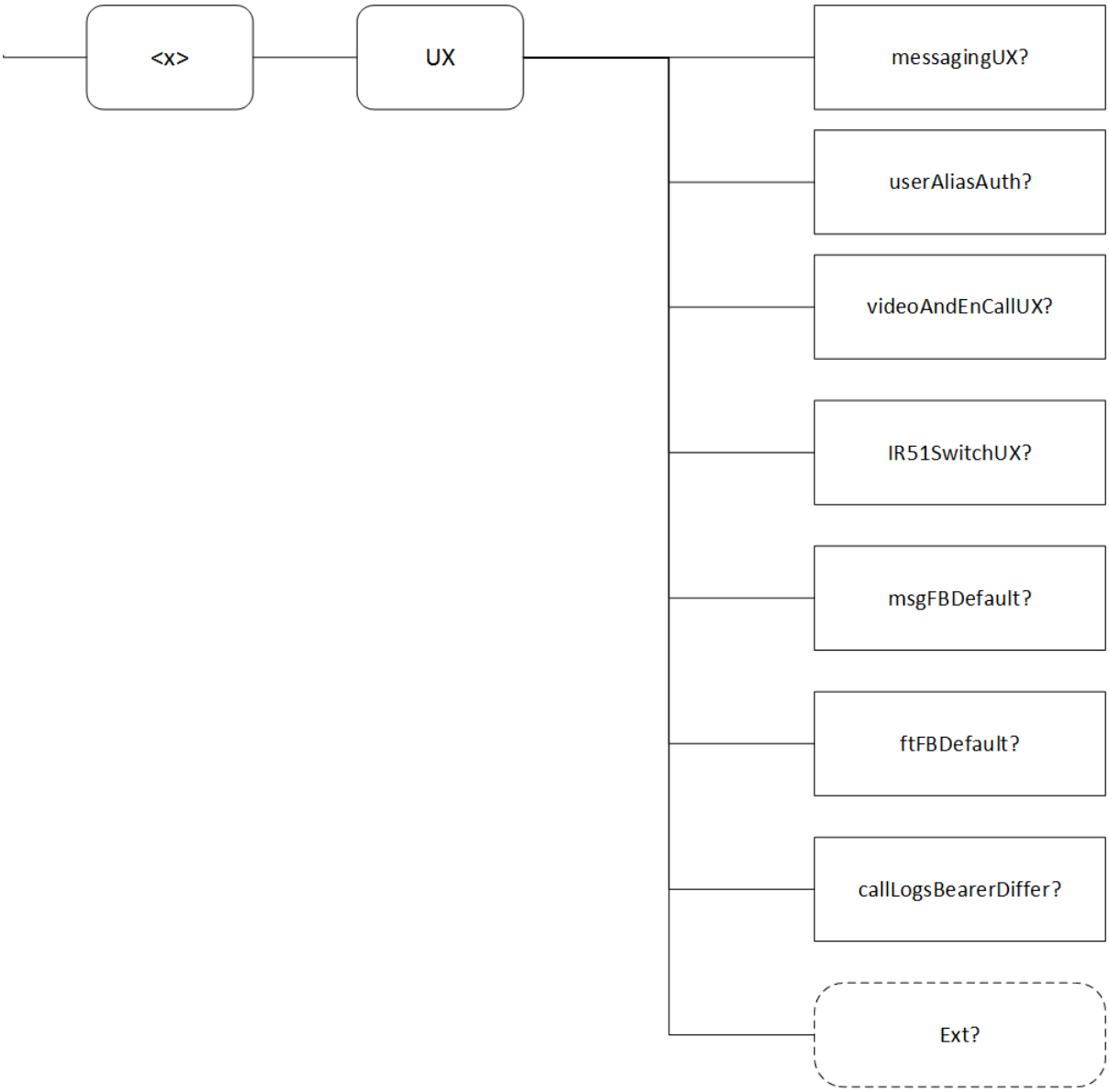

Figure 3: UX MO tree

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

```
<characteristic type="UX">
    <parm name="messagingUX" value="X"/>
    <parm name="userAliasAuth" value="X"/>
    <parm name="videoAndEnCallUX" value="X"/>
    <parm name="IR51SwitchUx" value="X"/>
    <parm name="msgFBDefault" value="X"/>
    <parm name="ftFBDefault" value="X"/>
    <parm name="callLogsBearerDiffer" value="X"/>
    <characteristic type="Ext"/>
</characteristic>
```

Table 19: UX MO sub tree associated HTTP configuration XML structure

The USER RECONNECT GUARD TIMER, CFS TRIGGER, MAX 1 TO MANY RECIPIENTS and 1 TO MANY SELECTED TECHNOLOGY parameters are added to the Client Control subtree with the following formal definition:

Node: /<x>/ClientControl

Common Core related parameters used to control the client behaviour are placed under this interior node.

Status	Occurrence	Format	Min. Access Types
Required	One	node	Get

Table 20: ClientControl MO sub tree addition node

- Values: N/A
- Associated HTTP XML characteristic type: “clientControl”

Node: /<x>/ClientControl/reconnectGuardTimer

Leaf node that provides the minimum time the client shall be registered in IMS prior to sending a message revocation request for a chat message.

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

Table 21: Client Control MO sub tree addition parameters (reconnectGuardTimer)

- Values: integer value defining the timeout to be used in seconds
- Post-reconfiguration actions: Start using the provided value the next time when regaining connectivity while a Chat message is pending to be delivered.
- Associated HTTP XML parameter ID: “reconnectGuardTimer”

Node: /<x>/ClientControl/cfsTrigger

Leaf node that controls the client trigger to fallback to SMS when revocation procedures apply.

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

Table 22: Client Control MO sub tree addition parameters (cfsTrigger)

- Values:
  0 (default): the client shall fall back to SMS and send the Message Revoke request right after sending the SMS
  1: the client shall fall back to SMS right after receiving the MessageRevokeResponse request with the value of the result equal to “success”
- Post-reconfiguration actions: Start using the provided value the next time revocation request shall be sent.
- Associated HTTP XML parameter ID: “cfsTrigger”

Node: /<x>/ClientControl/max1toManyRecipients

Leaf node that provides the maximum number of contacts allowed to be included in the distribution list of the 1-to-Many messaging service.

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

Table 23: Client Control MO sub tree addition parameters (max1ToManyRecipients)

- Values:
  0 (default): the 1-to-Many Messaging service is disabled
  1: the client can add unlimited number of recipients
  >1: integer value that indicates the maximum total number of recipients that can be included in the distribution list
- Post-reconfiguration actions:
  If the configuration parameter value transits from 0 to a value higher than zero, or the parameter is added with value higher than zero to the client configuration, the client shall unhide the UX elements for the management of the distribution lists.
  If the configuration parameter value transits from a value higher than 0 to 0 or the configuration parameter is removed, then the client shall hide the Ux elements for the management of distribution lists. Any stored distribution lists shall be deleted.
  The new value of the configuration parameter shall be stored and applied from this time on.
- Associated HTTP XML parameter ID: “max1ToManyRecipients”

Node: /<x>/ClientControl/1toManySelectedTech

Leaf node that allows selecting the 1-to-1 messaging technology to be used for the 1-to-Many messaging service.

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

Table 24: Client Control MO sub tree addition parameters (1toManySelectedTech)

- Values:
  0 (default): SMS is selected
  1: RCS 1-to-1 Chat service is selected
- Post-reconfiguration actions: Start using the provided value the next time when sending a 1-to-Manny message.
- Associated HTTP XML parameter ID: “1toManySelectedTech”

Node: /<x>/ClientControl/displayNotificationSwitch

Leaf node that controls whether the sending of Display Notification is enabled/disabled on the recipient’s client.

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

Table 25: Client Control MO sub tree addition parameters (displayNotificationSwitch)

- Values:
  0 (default), Enable sending Display Notifications, The user may still disable it using

the Display Notification setting
1: Disable sending Display Notifications, The Display Notification setting is not available to the user.

- Post-reconfiguration actions: Start using the provided value the next time when receiving a message that requires Display Notification.
- Associated HTTP XML parameter ID: “displayNotificationSwitch”

Node:/ <x>/ClientControl/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 26: ClientControl MO sub tree addition Service Provider Extension Node

Values: N/A

- Associated HTTP XML characteristic type: “Ext”

This lead to the following Client Control sub tree

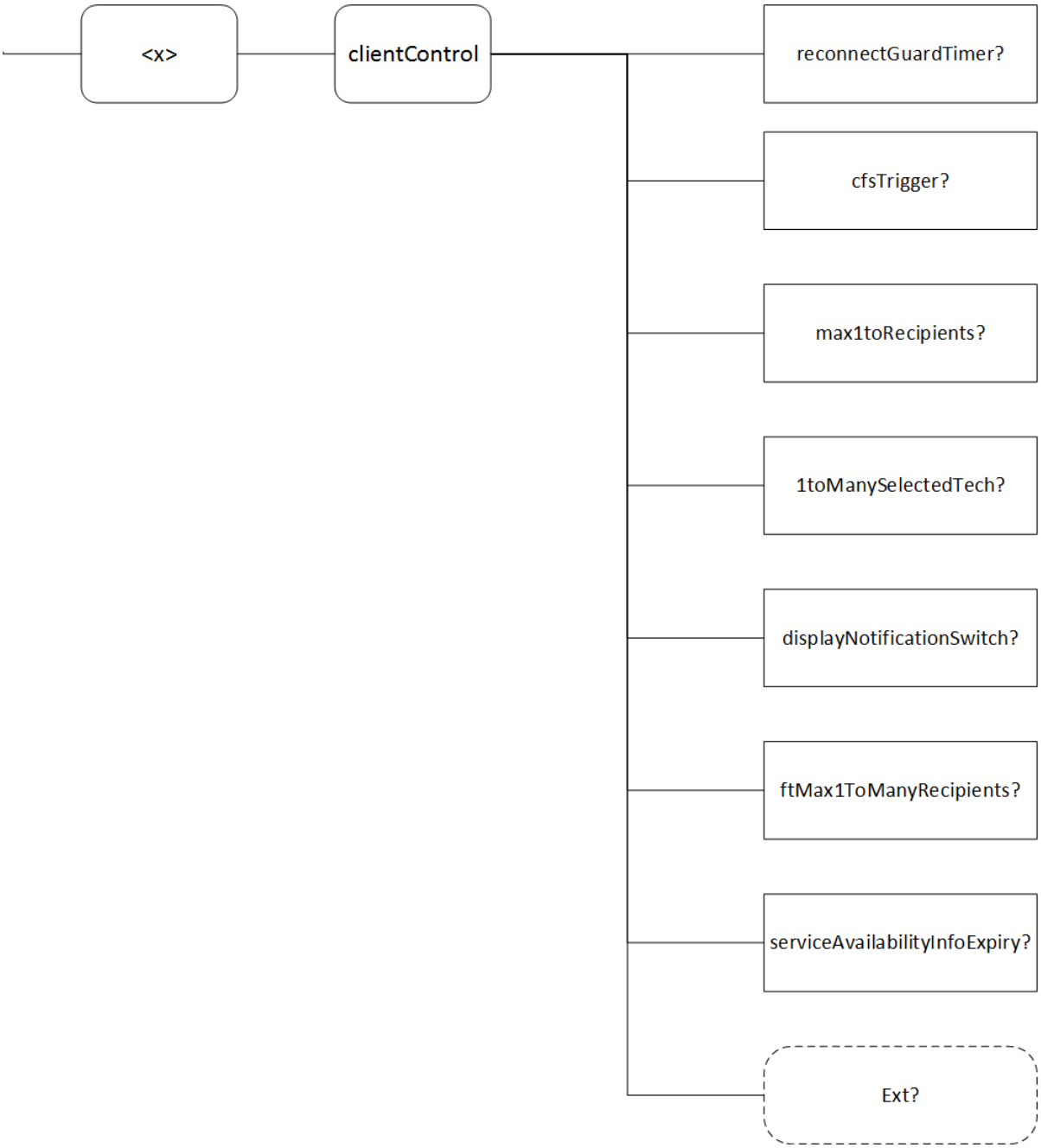

Figure 4: Client Control MO sub tree

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

```
characteristic type="clientControl">
    <parm name="reconnectGuardTimer" value="X"/>
    <parm name="cfsTrigger" value="X"/>
    <parm name="max1toManyRecipients" value="X"/>
    <parm name="1toManySelectedTech" value="X"/>
    <parm name="displayNotificationSwitch" value="X"/>
    <parm name="ftMax1ToManyRecipients" value="X"/>
    <parm name="serviceAvailabilityInfoExpiry" value="X"/>
    <characteristic type="Ext"/>
</characteristic>
```

Table 27: ClientControl sub tree associated HTTP configuration XML structure

5.3.7.2 Existing configuration parameters with updated definition

To provide the required behaviour for 1-to-1 Messaging service, the definition of the following parameters is updated:

Configuration parameter	Description	RCS usage
CHAT AUTH	This parameter Enables/Disables the sending of Chat service. When set to **0,** initiation of 1-to-1 chat session is disabled. When set to **1**, initiation of 1-to-1 chat sessions is enabled. When this parameter is set to **1**. GROUP CHAT AUTH parameter shall also be set to **1**.	Mandatory Parameter
GROUP CHAT AUTH	This parameter Enables/Disables the Group Chat service and receiving 1-to-1 chat session invitations. If set to **0** the Group Chat service and receiving 1-to-1 chat invitations is disabled. When set to **1** the Group Chat service and receiving 1-to-1 chat invitations is enabled. If CHAT AUTH is set to **0**, GROUP CHAT AUTH can be enabled or disabled. If CHAT AUTH is set to **1**, GROUP CHAT AUTH shall be set to **1**.	Mandatory parameter

Table 28: Redefined Configuration Parameters to control 1-to-1 Messaging behaviour

This leads to the following new definitions:

Node: /<x>/Services/ChatAuth

Leaf node that represents the authorisation for the user to send the chat messages

The node shall be instantiated if the rcsDisabledState node is not provided.

Status	Occurrence	Format	Min. Access Types
Required	One	bool	Get, Replace

Table 29: Services MO sub tree addition parameters (ChatAuth)

- Values: 0, 1
  0- Indicates that initiating 1-to-1 chat sessions is disabled
  1- Indicates that initiating 1-to-1 chat sessions is enabled
- Post-reconfiguration actions: The client should be reset and should perform the complete first-time registration procedure following a reconfiguration (i.e. HTTP) as described in section 2.3.1.1 of [RCC.07].
- Associated HTTP XML parameter ID: “ChatAuth”

Node: /<x>/Services/GroupChatAuth

Leaf node that represents the authorisation for the user to receive chat messages and use the group chat service

Status	Occurrence	Format	Min. Access Types
Required	One	bool	Get, Replace

Table 30: Services MO sub tree addition parameters (GroupChatAuth)

- Values: 0, 1
  0- Indicates that Group Chat service and receiving 1-to-1 chat session invitations is disabled
  1- Indicates that Group Chat service and receiving 1-to1 chat session invitations is enabled
- Post-reconfiguration actions: The client should be reset and should perform the complete first-time registration procedure following a reconfiguration (i.e. HTTP) as described in section 2.3.1.1 of [RCC.07].
- Associated HTTP XML parameter ID: “GroupChatAuth”

5.3.8 Technical Implementation of User Stories and Service Requirements

R5-30-1 Requirements R5-1-1 and R5-1-2 shall be implemented locally on the device.

R5-30-2 Requirement R5-2-1 shall be implemented locally on the device.

R5-30-3 Requirements R5-2-2-1 and R5-2-2-2 and their sub requirements are implemented locally on the device based on the current connectivity state and the available information on the B-party as a consequence of the capability exchange (see section 3.3) and as specified in section 5.3.3.1.

R5-30-4 Requirements R5-2-2-3, R5-2-2-4 and R5-2-2-5. shall be implemented locally on the device

R5-30-5 Requirement R5-2-3 shall be realised based on the interworking procedures in [RCC.07] and the applicable specifications it refers to.

R5-30-6 Requirement R5-2-3-1 shall be realised through the procedures in section 5.3.3.2.

R5-30-7 Requirement R5-2-4 shall be realised through the procedures in section 5.3.3.2 and revocation procedures defined in section 3.3.4.1.10 of [RCC.07] and the additional clarifications of section 5.3.5.

R5-30-8 Requirement R5-2-4-1 shall be realised based on the client configuration parameter CHAT REVOKE TIMER defined in [RCC.07] and the network indication for the support of revocation as specified in section 5.3.2.

R5-30-9 Requirement R5-2-4-2 shall be implemented locally on the device.

R5-30-10 Requirement R5-2-4-3 shall be implemented locally on the device based on the value configured for the client configuration parameter CHAT REVOKE TIMER defined in A.1.4.3 and A.2.6 of [RCC.07].

R5-30-11 Requirement R5-2-4-4 and its sub requirements shall be implemented locally on the device with the default for the user setting being configured

through the MESSAGING FALLBACK DEFAULT client configuration parameter defined in section 5.3.7.

R5-30-12 Requirement R5-2-4-5 and its sub requirements shall be implemented on the device using the revocation procedures defined in section 3.3.4.1.10 of [RCC0.7 RCS6.0 UNI] with the timeout on regaining connectivity required in requirement R5-2-4-5-2 being controlled through the RECONNECT GUARD TIMER parameter defined in section 5.3.7. For sending the SMS in parallel with the Message Revoke requests required in requirement R5-2-4-5-4, the CFS TRIGGER parameter defined in section 5.3.7 shall be set to zero.

R5-30-13 Requirement R5-2-4-6 shall be implemented locally on the device.

R5-30-14 Requirement R5-2-4-6-1 shall be implemented locally on the device. It is applicable when selected user settings resulting from Service Provider configuration or user selection for both undelivered RCS chat messages and undelivered RCS files allow SMS fallback and latching (i.e. set to always resend undelivered RCS chat messages as SMS and always resend undelivered RCS Files as SMS link)

R5-30-15 Requirement R5-2-5 and its sub requirements shall be implemented locally on the device.

R5-30-16 Requirements R5-3-1 and R5-3-2 shall be implemented locally on the device.

R5-30-17 Requirement R5-3-3 shall be implemented based on the selected 1-to-1 messaging technology. When RCS 1-to-1 Chat is selected, interworking on the network serving the recipient of the message can be performed based on procedures described in sections 5.3.2, 5.3.3 and 5.3.4. When RCS Standalone messaging is selected, originating or terminating fallback may be applied based on Service provider policies.

R5-30-18 Requirements R5-3-4, R5-3-5, R5-3-6, R5-3-7, R5-3-8 and their sub requirements shall be implemented locally on the device.

R5-30-19 Requirements R5-4-1 and R5-4-2 shall be implemented locally on the device.

R5-30-20 Requirement R5-4-3-1 shall be realised by configuring the MESSAGING UX parameter defined in section 5.3.7.

R5-30-21 Requirement R5-4-3-2 is realised as specified in section 18.3.

R5-30-22 For the message transfer states of requirement R5-5-1 the following technical implementation applies:

- **Pending**: When the user presses the button to send the message until the first success response is received from the network. For RCS 1-to-1 Chat message or RCS Standalone message, it may be in this state for some time when the user is not registered with the IMS core (e.g. offline or airplane mode). For SMS, it may be in this state when the user is not available for sending SMS.

- **Sent**: For RCS 1-to-1 Chat message, a MSRP 200 OK is received. For RCS Standalone message pager mode, a SIP 200 OK is received from the network. For RCS Standalone message Large Message Mode, a SIP 200 OK response is received to the SIP BYE request sent by the client once the Standalone message has been successfully transferred via MSRP. For SMS, the message is successfully submitted to the network.
- **Delivered**: For RCS 1-to-1 Chat message or RCS Standalone message, when receiving the Delivery Notification with status set to “delivered”. Requirement R5-5-1-3-1 is realised based on the procedures described in [3GPP TS 23.040] upon receiving a delivery report of the short message. Requirement R5-5-1-4 shall be realised based on the Interworking disposition notification as specified in section 5.3.3.4.

NOTE: An originating client may receive for a chat message both a delivery and an interworking disposition notification, e.g. due to support of multi device in the terminating network. Reception of the delivery disposition notification overwrites the "interworking" status of the message".

- **Displayed**: For RCS 1-to-1 Chat message or RCS Standalone message, when receiving the Displayed Notification with the status set to “displayed”. Requirement R5-5-1-5-1 shall be implemented locally on the device. Requirement R5-5-1-5-2 shall be realised based on the Interworking disposition notification as specified in section 5.3.3.4. Displayed status is not applicable if the client received an interworking notification but no delivery notification.

R5-30-23 **Error**: For 1-to-1 RCS Chat message or RCS Standalone message, when an error is received as specified in [RCC.07] and the applicable specifications it refers to.

R5-30-24 Notifications on delivery status information as defined in R5-5-2 shall be stored and forwarded in the Store and Forward server as specified in section 3.3.4.1.5 of [RCC.07].

R5-30-25 Requirements R5-5-3, R5-5-4 and R5-5-5 shall be implemented locally on the device.

R5-30-26 For the requirements in user story US5-6 the device shall support the encoding and display of the graphical elements as defined in Annexes A.2 and A.3.

R5-30-27 The indication that the other party is typing in requirement R5-7-1 is based on the reception of the "isComposing" indication as defined in section 3.3.4.1 of [RCC.07]. The "isComposing" indication can only be transferred within an active RCS 1-to-1 Chat session. “isComposing” indication cannot be transferred when other messaging technology is selected based on the messaging technology selection rules defined in this section. The client shall send the "isComposing" indication only if a RCS 1-to-1 Chat session exists for the conversation the user is typing in. When there is no active

session, session initiation is triggered when the user sends a message and consequently there is no “isComposing” indication for the first message sent. There is no “isComposing” indication for messages delivered through Store and Forward delivery procedures.

R5-30-28 Requirement R5-8-2 is fulfilled based on sections 5.3.1 to 5.3.7.

R5-30-29 Requirement R5-8-2-1 shall be implemented as defined in sections 3.3.4.1.4 and 3.3.4.1.5 of [RCC.07].

R5-30-30 Requirement R5-8-3 is fulfilled based on sections 5.3.1 to 5.3.7.

R5-30-31 Requirement R5-9-1 shall be implemented as defined in sections 5.3.1 to 5.3.7.

R5-30-32 For requirement R5-9-2, the client 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.

R5-30-33 Requirement R5-9-3 and R5-9-4 shall be implemented locally on the device.

R5-30-34 The requirements of user stories US5-10 and US5-11 shall be implemented locally on the device.

R5-30-35 Requirement R5-12-1 shall be implemented locally on the device.

R5-30-36 For the requirements R5-12-2, R5-12-3 and R5-12-4 the client shall support the following procedure.

- It is the responsibility of the Messaging Server to deliver chat messages in the correct order, so the Client can rely on it when sorting received messages. The client shall interleave the sent and received messages in the chronological order. The client shall interleave received messages based on the value of the CPIM Message-Direction header value (as referred to from section C.1.9 of [RCC.11]) as sent or received or, if absent as received message. The client shall interleave client originated messages as sent message.
- 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. The client shall interleave messages based on the value of the Multipurpose Internet Mail Extensions (MIME) Message-Direction header defined in Annex C.1.3 of [RCC.07].

R5-30-37 The requirements of user story US5-13 shall be implemented locally on the device. As a clarification, the timestamp for "sent" messages received via the 1-1 chat service or the Common Message Store is taken from the CPIM DateTime header in accordance with the technical implementation of R5-12-2, R5-12-3 and R5-12-4.

R5-30-38 The requirements of user story US5-14 shall be implemented locally on the device.

R5-30-39 To satisfy the requirements of US5-15 the client shall apply the following procedure:

If the configuration parameter USER ALIAS AUTH defined in section 5.3.7 is set to 0 then the client shall:

- Not offer the user to manage a user alias used for RCS communications.
- Not send a user alias for mobile originated chat sessions and
- Discard the user alias received in mobile terminated chat session messages, i.e. the user alias is not displayed and not stored in the local communication history.

If the configuration parameter USER ALIAS AUTH defined in section 5.3.7 is set to 1 or it is not present, then:

- The client shall offer the user to manage a user alias used for RCS communications.
- For mobile originated chat transactions, the client shall add a user alias if set by the user as defined in section 2.5.3.4 of [RCC.07].
- If the client receives a user alias as defined in section 2.5.3.4 of [RCC.07] in a mobile terminated chat session and the originator address does not match an address book contact, the client shall display the user alias it to the user.
- The client shall store the user alias in the local chat communication history.

In addition, the client implementation shall respect the requirements of the post reconfiguration actions defined for the configuration parameter USER ALIAS AUTH in section 5.3.7.

R5-30-40 For the realization of requirements of user story US5-16 the client shall enforce the max message size for sending messages as defined by the configuration parameter MAX SIZE IM defined in section A.1.4.3 and A.2.6 of [RCC.07].

R5-30-41 For requirements R5-17-1 and R5-17-2 section 7.3 applies.

R5-30-42 Requirement R5-17-3 shall be implemented locally on the device.

R5-30-43 Requirement R5-18-1 shall be implemented locally on the device.

R5-30-44 Requirements R5-19-1 and R5-20-1 are fulfilled by deploying a Common Message Store in [RCC.07], [RCC.09] and [RCC.11].

R5-30-45 Requirement R519-2 is fulfilled based on Service Provider policies.

R5-30-46 Requirement R5-19-3 shall be implemented locally on the device.

R5-30-47 For requirement R5-21-1, a dedicated Message Store client shall be implemented on the device as defined in section 4.1 of [RCC.07], [RCC.09] and [RCC.11].

R5-30-48 For requirement R5-22-1, the client shall delete messages and conversations in the Common Message Store after local deletion as defined in section 4.1.6.6 of [RCC.07].

NOTE: Because the enabler used to provide the Common Message Store may change in future versions of the profile defined in this document (see section 1.1.2), in this version of the profile it is optional for clients to provide these implementations for the requirements of US5-19 to US5-22.

R5-30-49 The requirements of US5-23 shall be implemented locally on the device.

R5-30-50 The requirements of the user stories US5-24 to US5-27 are implemented via the RCS Geolocation Push service defined in section 3.10 of [RCC.07] and the additional procedures defined in section 5.3.6.

R5-30-51 Requirements R5-28-1, R5-28-2, R5-28-3, R5-28-4 and R5-28-5 shall be implemented based on the 1-to-Many Messaging service procedures defined in sections 5.3.1 and 5.3.3.1.

R5-30-52 For requirement R5-29-1, the MAX 1 TO MANY RECIPIENTS parameter defined in section 5.3.7 shall be configured.

R5-30-53 For R5-29-2, the 1 TO MANY SELECTED TECHNOLOGY parameter defined in section 5.3.7 shall be configured.

R5-30-54 Requirement R5-29-2-1 shall be implemented locally on the device.

6 Group Chat

6.1 Description

Group Chat allows users to exchange chat messages with a number of contacts. All contacts are aware of each other, replies will always be distributed to the entire group of participants.

6.2 User Stories and Feature Requirements

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

R6-1-1 Any RCS user shall be able to create a Group Chat Conversation by selecting capable (for this service) contacts from the contact list and invite them to a Group Chat.

R6-1-2 It shall be possible to create a 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 being created.

R6-1-3 Any (for this service capable) RCS user shall be able to participate in a Group Chat Conversation after the invite to that Group Chat has been confirmed (by automatic confirmation or manual confirmation).

R6-1-4 The MNO shall be able to set a maximum number of participants in a Group Chat Conversation. To ensure interoperability, the MNO shall allow 100 participants for each Group Chat conversation where participants from other networks are included.

R6-1-5 It shall only be possible to set up a new Group Chat Conversation if the initiating user is connected to the RCS platform.

R6-1-6 When starting a new Group Chat, the inviting user or initiator shall invite at least two other Group Chat capable participants. The restriction of at least three participants in a Group Chat shall only apply to the creation of a Group Chat, i.e. a Group Chat containing only two participants is perfectly valid if previous Group Chat participants have left or other invited participants had never joined.

R6-1-7 When a user tries to create a new Group Chat with the same list of participants and the same Group Chat subject title as an existing one, then the client shall jump to the existing Group Chat and not create a new one.

R6-1-8 When a user tries to create a new Group Chat with the same list of participants as an existing one but not with the same Group Chat subject title, then a new Group Chat shall be created.

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

R6-2-1 When Creating a Group Chat Conversation, it shall be possible for the initiator to define a subject title and a Group Chat icon.

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”). If no Group Chat icon has been defined, a placeholder Group Chat icon shall be used.

R6-2-3 The Group Chat icon shall be represented in the list of chat conversations similar to contact icons for 1-to-1 Messaging conversations. The selection mechanism, including possible resize, crop or aspect ratio correction tools, shall be similar to the procedures that are offered by the device for contact pictures.

R6-2-4 It shall be possible to maintain more than one Group Chat with identical Group Chat subject titles.

R6-2-5 Any Group Chat participant shall be able to change the subject of the Group Chat and / or Group Chat icon at any time locally on their devices.

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

R6-3-1 Participants in a Group Chat Conversation shall be able to add new participants from their contact list.

R6-3-2 It shall not be possible to add new Group Chat participants in a Group Chat Conversation once the maximum number of participants has been reached as configured by the MNO (see R6-1-4).

R6-3-3 It shall be possible to add participants to a Group Chat if they are offline at the time where the addition takes place.

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

R6-3-4 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 online or offline- from the time the new participants are accepted (either by automatic confirmation or manual confirmation of the user when online).

US6-4 **As a user, I want to know who is participating in a Group Chat Conversation at any point in time.**

R6-4-1 Any participant in a Group Chat Conversation shall be able to see a list of participants at any point in time.

R6-4-2 If the sender of a Group Chat Message is not in my contact list, the sender's RCS Alias name if available, shall be presented in addition to the participant's MSISDN.

R6-4-3 Representation of Alias names shall be differentiated from contact list matches. The support of RCS Alias shall be MNO configurable.

NOTE: The Alias (as specified in US18-2) is created by the message sender.

R6-4-4 If neither Contact name nor RCS Alias is available, a participating contact shall be represented with the MSISDN in the list of Group Chat participants.

R6-4-5 In the case where new Group Chat participants join the Group Chat, all other Group Chat participants shall be notified.

R6-4-6 In the case where Group Chat participants leave the conversation, all other Group Chat participants shall be notified.

US6-5 **As a user, I may not want to deal with Group Chat invites and acceptances.**

R6-5-1 The MNO shall be able to configure the device in a way that any user who was invited to a Group Chat Conversation shall automatically become a participant of that Group Chat Conversation – no invite / acceptance 'handshake process' required.

R6-5-2 The user shall be able to see who originally set up the Group Chat.

R6-5-3 Auto-accept for Group Chat shall be MNO configurable; if an MNO decides to not support auto-accept, the invited user becomes participant in a Group Chat once the participation was confirmed manually.

US6-6 **As a user, I want to send text Group Chat Messages to an existing Group Chat Conversation.**

R6-6-1 Any participant in a Group Chat Conversation shall be able to send messages to all Group Chat participants.

R6-6-2 If the originating user tries to send messages to other Group Chat participants while offline, the messages shall be queued locally on the device and sent out once the device is online again.

US6-7 **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.**

R6-7-1 Any message exchanged in the Group Chat Conversation shall be received on other participants' devices without any form of acceptance of the message.

US6-8 **As a user, I want to send Group Chat Messages to my Group Chat participants even when they're temporarily offline (e.g. device switched off). I expect them to receive these Group Chat Messages when they come online again.**

R6-8-1 In case any participant in a Group Chat Conversation is currently offline, any message(s) or updates to the list of Group Chat participants shall be delivered once the user is back online.

R6-8-2 The MNO shall be able to set the storage duration for store & forward cases (deferred messaging) based on individual MNO 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.

US6-9 **As a user, I want to include small graphics into my Group Chat Messages.**

NOTE: Small graphics can express mood, fun or icons to explain a thing or a status in a graphical, easy to use and understand manner. Examples are ☺, ☎, 💣 and ☯.

R6-9-1 It shall be possible to add small graphics when creating a Group Chat message by adding from a selection of graphical elements in the ChatGroup Chat application.

NOTE: Standards for conversion of text strings to Emoji are described in the Annex "Emoticon conversion table", Annex A.3

R6-9-2 It shall be possible to add a few basic small graphics when creating a Group 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

R6-9-3 The graphical elements that are used may vary between implementations, but the conveyed meaning must not be changed.

NOTE: The conversion of text strings to graphics for any type of smileys shall affect any representation of the messages on the user interface, which includes the conversation thread as well as any notifications or previews of messages in pop-ups or dedicated screens.

US6-10 **As a user, I don't want to feel restricted by Group Chat Message size limits.**

R6-10-1 Group Chat Messages (incoming and outgoing) shall allow to send and receive up to 8192 bytes.

NOTE: MNO defined parameter.

R6-10-2 If Group Chat messages are received that exceed the number of characters that the application is able to display properly, the application shall cut off characters that cannot be displayed properly and inform the user about the fact that only a part of the message can be displayed.

US6-11 **As a user, I want to see the status of my sent Group Chat Messages.**

R6-11-1 For A-Party, the following message states shall be indicated to the user:

R6-11-1-1 Message Pending: Transfer of the Chat Message in progress (e.g. queuing on device).

R6-11-1-2 Message Sent: confirmation that the message has been correctly accepted by the A-Party's network.

R6-11-1-3 Message Delivered: Receiving devices have noticed that a message has been received by the device.

NOTE 1: The Delivery Notification is intended to inform the sender of the message about the delivery status of the message or file transfer. Other participants of the Group Chat are not expected to receive the message delivery status.

NOTE 2: Networks may not support "Message Delivered" in Group Chat. In this case, there are no outgoing notifications generated, and incoming "Message Delivered" notifications in Group Chat may be ignored.

R6-11-1-4 Message Displayed: When the message has been displayed in the Chat view on the receiving device. As per US18-7 and the related requirements, the user shall have the option to disable the feedback that the message was displayed.

R6-11-1-5 Message sending 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). (Sending the message may be re-triggered manually by the user).

R6-11-2 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.

US6-12 **As a user, I want to see when the other party is currently writing a Group Chat Message.**

R6-12-1 The other party shall be able to see an "is typing" notification whenever a new Chat Message is being created.

NOTE: Networks may not support "is typing" notification. In this case, networks may ignore incoming "is typing" notifications.

US6-13 **As a user, I want to be notified at any time my device receives a new Group Chat Message.**

R6-13-1 On receiving a Group Chat message, the user shall be notified.

R6-13-2 For audio notifications, device audio related settings shall prevail.

US6-14 **As a user, I want notifications of rapidly sequenced incoming Group Chat Messages intelligibly aggregated and counted.**

R6-14-1 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.

R6-14-2 The visual notification shall be permanently removed after the user has opened the message.

US6-15 **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.**

R6-15-1 Any Group Chat shall be represented with Subject title and Group Picture (and possibly unread message identifier) in the list of Chat Conversations.

US6-16 **As a user, I want conversations which contain unread messages to be differentiated from conversations that contain messages I have seen.**

NOTE 1: This requirement shall be valid for Messaging for Multi-Device as well.

NOTE 2: Unseen files or file download notifications cover events that use File Transfer as an enabler e.g., but not limited to, Audio Messaging or vCard share.

R6-16-1 Group Chat Conversations with unread messages, unseen files or file download notifications shall be marked accordingly.

US6-17 **As a user, I want to receive Group Chat Messages from any of the contacts participating in a Group Chat Conversation.**

R6-17-1 Any RCS user shall receive Group Chat Message(s) that are sent to Group Chat Conversations the user participates in at any point in time.

R6-17-2 Group Chat Messages shall be received straight in the inbox; no hand-shake acceptance shall be required.

R6-17-3 Any participant of a Group Chat shall only be able to see messages that have been exchanged between the time of joining the Group Chat and leaving the Group Chat.

R6-17-4 It shall not be possible for any participant of a Group Chat Conversation to see any messages that possibly have been exchanged before the participant has joined the Group Chat.

US6-18 **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', section 7.

R6-18-1 The user shall be able to select and send Multi Media elements in Group Chat Conversations.

R6-18-2 The user shall be able to receive Multi Media elements in Group Chat Conversations.

R6-18-3 The user shall be able to browse any media that was exchanged in the particular Group Chat in a aggregated view.

US6-19 **As a user, I want to view my sent and received Group Chat Messages in a time-based order.**

R6-19-1 All messages exchanged within the same Group Chat Conversation shall be threaded in the same group chat thread in timely order.

R6-19-2 The order of messages shall be in line with the order messages have been sent and received on the device.

R6-19-3 Incoming and outgoing messages shall be displayed interlaced.

R6-19-4 Outgoing messages shall be inserted into the Group Chat Conversation thread as they have been sent.

US6-20 **As a user, I want to see the timestamp associated with each of my sent and received messages.**

R6-20-1 The date and time associated with each chat message shall be displayed adjusted to the current device date and time.

R6-20-1-1 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.

R6-20-1-2 Timestamps for received messages shall be based on the UTC timestamp that comes with each message, aligned with the selected device time zone.

US6-21 **As a user, I want any Group Chat Conversations to permanently reside on my phone, and I can resume that group whenever I decide to do so.**

R6-21-1 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.

R6-21-2 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.

R6-21-3 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:

R6-21-3-1 Session related information is not shown to the user, i.e. 'Chat closed' shall not be displayed at the UI level.

R6-21-3-2 Simply writing a new message and hitting 'Send' shall be enough to continue a Group Chat that has timed out at network level.

R6-21-3-3 When the user hits 'Send' the Group Chat session is set up and the user message is also sent.

R6-21-3-4 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 active participants.

R6-21-3-5 Group Chat follows up in the same Chat window, keeping the full history of the session.

R6-21-3-6 While the Group 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.

US6-22 **As a user, I want to maintain multiple 1-to-1 Messaging and Group Chat Conversations in parallel.**

R6-22-1 Multiple parallel 1-to-1 Messaging and Group Chat conversations shall be supported at any given point in time.

US6-23 **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 Group Chat.

R6-23-1 Any participant in a Group Chat Conversation shall be able to leave that Group Chat at any point in time.

R6-23-2 Any participant who has left a Group Chat Conversation shall no longer receive any new messages or updates to the participants list.

R6-23-3 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.

R6-23-4 Re-joining a previously left Group Chat Conversation shall be possible by the user being re-invited by another (still active) Group Chat participant.

R6-23-5 Manually deleting a Group conversation from the list of chat conversations automatically triggers leaving the Group Chat, i.e. the participant is removed from the list of Group Chat participants.

NOTE: A user warning may be given by the device that the deletion of a Group Chat removes the participant from the GC entirely.

R6-23-6 Deleting one, more or all messages within a Group Chat conversation (without removing the Group Chat conversation thread from the list of conversations) does not trigger leaving the Group Chat.

R6-23-7 Participants shall be automatically removed from the Group if the corresponding user account / subscription is no longer valid.

NOTE: Details of the subscription validity are at the discretion of the individual MNO.

US6-24 **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.

R6-24-1 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.

R6-24-2 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.

US6-25 **As a user, I want to send Group Chat Messages from secondary devices with identical capabilities compared to primary device capabilities.**
As a user, I want my device to always be in sync with the Group Chat Messages on the network even in case of multiple devices.

R6-25-1 Group Chat shall support Multi-Device Usage.

US6-26 **As a user, I want my Group Chat messages backed up on the Common Message Store which is trusted and safe.**

R6-26-1 All Group Chat Conversations may be stored on the network.

NOTE 1: If the user has not been part of a Group Chat Conversation from the very beginning, or left the Group Chat Conversation while other Group Chat participants continued, only the part of the Group Chat Conversation between joining and leaving the Group Chat shall be stored.

NOTE 2: Details of storage are at the individual MNO discretion.

US6-27 **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).**

R6-27-1 The user shall have the option to restore Group Chat Conversations from the Common Message Store *(e.g. in case of handset replacement)*.

US6-28 **As a user, I want the ability to share my current position or a selected location with any of my Groups from the Messaging Application.**

R6-28-1 The user shall have the ability to share positions or locations from any Group Chat conversation.

R6-28-2 Recipients participating in the Group Chat shall be able to receive any position or location in the Group Chat, irrespectively whether their RCS version supports the “Geolocation Push” service or not.

NOTE: Legacy mode may be provided by a link to an online map display or a ‘screenshot’ with map picture.

NOTE: Requirements defined under US5-27 detailing the service in addition to the above listed Group Chat specific requirements are valid accordingly.

6.3 Technical Information

6.3.1 Overview

The Group Chat service is provided based on the Group Chat technical enabler defined in section 3.4 of [RCC.07] with the exceptions described below.

[RCC.07] allows service providers to implement the Group Chat experience based on SIMPLE IM or CPM. In accordance with the definitions in section 5.3.1 only CPM is supported as messaging technology in the profile described in this document.

In order for the Group Chat service to be used it shall be enabled by the service provider via the configuration parameter GROUP CHAT AUTH as defined in section 5.3.7.2 and the client shall be registered.

NOTE: For the Service Providers that have deployed other RCS versions with RCS Group Chat service based on OMA SIMPLE IM procedures, deploying an OMA SIMPLE IM to OMA CPM and vice versa interworking function will be needed.The interworking procedures will be covered in a separate document.

Closed Group Chat as defined in section 3.4.4.2 of [RCC.07] is not supported in the profile defined in this document.

The option for the Service Provider to offer Group Chat interworking with SMS/MMS is not supported in the profile defined in this document.

As a clarification to the procedures in section 3.4.4. of [RCC.07] the client shall only invite or add contacts to a Group Chat knowing to have the Chat capability as defined in section 2.6.1.1.2 or 2.6.1.2.5.1 of [RCC.07] based on the procedures of capability discovery defined in section 3 of this document.

In the profile defined in this document a client receiving a SIP 403 error response including a warning header set to “127 Service not authorized” in result of the procedure to restart a Group Chat shall not automatically initate a new Group Chat as defined in section 3.4.4.1.7 of [RCC.07]. Instead the client shall apply the Ux behaviour as defined for the case where the user has voluntarily left the Group Chat.

6.3.2 Technical Implementation of User Stories and Service requirements

R6-29-1 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 GROUP CHAT AUTH parameter defined in section5.3.7.2.
- The procedures for initiation of a group chat and the conditions for the client to select capable contacts are defined in section 3.4.4.1.1 of [RCC.07].
- For R6-1-2, the new Group Chat shall be created as a separate session as specified in section 3.4.4 of [RCC.07] without reference to the ongoing 1-to-1 session .
- For requirement R6-1-4, the MNO can configure the maximum number of participants in a Group Chat by means of the MAX_AD-HOC_GROUP_SIZE parameter defined in section A.1.3 of [RCC.07]. The MNO hosting a Group Chat can configure the maximum number of participant by setting a policy for the [RFC5475] maximum-user-count. To meet the requirement of R6-1-4 service providers need to set the values accordingly. 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 by the client as defined in section 3.4.4.1.2 of [RCC.07].
- Requirement R6-1-6 for the restriction upon Group Chat creation shall be implemented locally on the device. To satisfy the requirement of R6-1-6 for the closure of a Group Chat, the service provider's conforming to the profile defined in this document may choose to set the value of the minimum number of participants allowed in a Group Chat as defined in section 3.4.4.1.3.3 of [RCC.07] to either "2" or "1". If a client attempts to restart a Group Chat with 1 or 2 participants left and it receives a SIP 404 error response then the client shall not initate a new Group Chat with the same Group Chat ID as defined in section 3.4.4.1.7 of [RCC.07] and apply a Ux behaviour as for a terminated Group Chat instead.
- Requirements R6-1-7 and R6-1-8 shall be implemented locally on the device.

R6-29-2 The requirement R6-2-1 shall be implemented as follows:

The client of the initiator of the Group Chat shall send the subject of the Group Chat Conversation as defined in section 7.3.1.2 of [RCC.11]. The Controlling Function shall process the subject as defined in section 9.2.1 and 9.2.10 of [RCC.11].

The client of the initiator of the Group Chat shall set the icon of the Group Chat via the CPM Group Session Data Management as defined in section 6.8 of [RCC.11]. The Controlling Function shall process the client request as defined in sections 6.8, 9.2.12 and 9.2.14 of [RCC.11].

R6-29-3 The requirements R6-2-2 shall be implemented locally on the device.

R6-29-4 The requirement R6-2-3 shall be implemented locally on the client. The client shall resize the Group Chat icon to have a maximum file size of 10 Kilo-Bytes(KB) The Group Chat Icon shall only be sent by use of the "file-info" element of the icon set request defined in section 6.8.1 of [RCC.11].

R6-29-5 The requirement R6-2-4 shall be implemented locally on the device.

R6-29-6 The requirement R6-2-5 shall be implemented locally on the device.

R6-29-7 For user story US6-3, the client shall allow members of a Group Chat Conversation to add new participants as defined in section 3.4.4.1.2 of [RCC.07]. The technical implementation defined for R6-1-4 shall be taken into account. Requirement R6-3-5 shall be implemented locally on the device based on the received notification and the indicated participant status.

NOTE: To avoid sending notifications to participants twice in short succession, the conference focus may 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.

R6-29-8 In order to be able to display the list and status of users in a group conversation as required in user story US6-4 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 R6-4-3 and R6-4-4 is implemented as defined in section 2.5.3.4 of [RCC.07]. The ability of the MNO to control the support of user alias is provided by means of the client configuration parameter USER ALIAS AUTH defined in section 5.3.7.1 of this document.

R6-29-9 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 US6-5. Service Providers should enforce auto accept for an invitation to a Group Chat by setting the value of the configuration parameter IM SESSION AUTO ACCEPT GROUP CHAT and IM SESSION START as defined in section A.1.3.3 of [RCC.07].

R6-29-10 For the requirements of user story US6-6, 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 of [RCC.07] and send the message to it.

R6-29-11 The client shall not implement client UI procedures to accept reception of messages or group chat invitations to fulfil the requirements of user story US6-7.

R6-29-12 The requirements of user story US6-8 is fulfilled by means of the Group Chat Store and Forward functionality described in section 3.4.4.3 of [RCC.07].

R6-29-13 The implementation of the graphics in a Group Chat conversation in the requirements of US6-9 shall be supported by clients as defined in Annex A.2 and A.3.

R6-29-14 For the realization of the requirements R6-10-1 the client shall enforce the max message size for sending messages as defined by the configuration parameter MAX SIZE IM defined in section A.1.4.3. of [RCC.07]. Service Providers need to set the value as indicated in R6-10-1.

R6-29-15 The requirement R6-10-2 shall be implemented locally on the device.

R6-29-16 For the realisation of the requirements in user story US6-11, the status indication for group chat messages and File Transfer sent in the Group Chat are the same as defined for RCS 1-to-1 Chat messages in section 5 and for files in section 7. When requesting, sending and receiving disposition notifications in a Group Chat, the client shall respect the definitions of section 3.4.4.1.5 of [RCC.07].

R6-29-17 Notifications on delivery status information as defined in R6-11-2 shall be stored for offline users and forwarded in the Messaging Server as specified in section 3.4.4.3 of [RCC.07].

R6-29-18 The requirements for US6-12 to display typing notifications is implemented same as for RCS 1-to-1 Chat via "isComposing" notification as defined in section 3.4.4. of [RCC.07]

R6-29-19 The requirements for user stories US6-13 and US6-14 are implemented locally on the device.

R6-29-20 The requirement of user story US6-15 is implemented locally on the device in alignment with the requirements of user story US6-2.

R6-29-21 The requirement of user story US6-16 is implemented locally on the device.

R6-29-22 The requirements of user story US6-17 shall be implemented locally on the device. The client shall not apply any UI procedures for the acceptance of the delivery of single messages.

R6-29-23 Sending of Multimedia in a Group Chat, as defined in the requirements of user story US6-18, is done via the File Transfer defined in section 7 of this document. Transmission of File Transfer via HTTP in a Group Chat shall follow the procedures defined in section 3.4.4 and 3.5.4.8 of [RCC.07].

R6-29-24 For the requirements in user story US6-19 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.

R6-29-25 The requirements of user story US6-20 shall be implemented locally on the device.

R6-29-26 The requirements of user story US6-21 shall be implemented locally on the device based on the Group Chat life cycle definitions in section 3.4.4 of [RCC.07].

R6-29-27 The requirements of user story US6-22 shall be implemented locally on the device.

R6-29-28 The requirements of user story US6-23 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 in accordance with the definitions for invitation to a new Group Chat, see user story US6-5.

R6-29-29 The client implementation shall ensure that the Group Chat handling as defined in R6-23-5 initiates a request to the network to voluntarily leave the Group Chat.

R6-29-30 The requirement for automatic removal from the Group Chat defined in R6-23-7 shall be implemented by the service provider by administrative triggers to terminate CPM session as defined in section 8.7 of [RCC.11]. In addition the Messaging Server hosting a given Group Chat should implement the procedure for removal of participants on IMS profile removal as defined in section 3.4.4.1.3.1 of [RCC.07].

R6-29-31 The requirements of user story US6-24 shall be implemented locally on the device.

R6-29-32 The requirements of user stories US6-25 through to US6-27 are implemented as defined in section 3.4.4.1.8 of [RCC.07] and based on the definitions in section 9 of this document.

NOTE: Because the enabler used to provide the Common Message Store may change in future versions of the profile defined in this document (see section 1.1.2), in this version of the profile it is optional for clients to provide this implementation for the requirements of US6-25 to US6-27.

R6-29-33 The implementation of user story US6-28 shall be based on Geolocation Push in a Group Chat as defined in section 3.10.4 of [RCC.07].

7 File Transfer

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 device, but there shall be other service entry points as well.

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 If the originating device is offline, File Transfer cannot be sent from the device.

R7-1-1-1 The device implementation may allow the user to create an RCS File Transfer in that case.

R7-1-1-2 The File Transfer status is ‘pending’ and the A-Party user is informed about this status.

R7-1-1-3 The File Transfer shall be executed once the originating device is online again without further user interaction.

NOTE: When the originating device is offline, at operator discretion MMS may be used to send the file when the MMS service is enabled on the device and network conditions allow (e.g. sufficient connectivity for MMS but the device is not registered for RCS).

R7-1-2 Any RCS user shall be able to transfer a file to Contacts in their contact list or by entering the contact’s MSISDN

R7-1-3 File Transfer shall allow transfer of any files 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.

R7-1-4 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.

R7-1-5 The following file types per content type shall be supported by any RCS device in the way that content can be generated or displayed / replayed:

R7-1-5-1 Pictures in Joint Photographic Experts Group (JPEG) format shall be supported.

R7-1-5-2 Panoramic Photos shall be supported (as guidelines describe in Annex A.4).

R7-1-5-3 Pictures in animated Graphics Interchange Format (GIF) format shall be supported actively:

R7-1-5-3-1 When opening a messaging thread containing a GIF file transfer, this file shall be animated automatically and run once when visible.

R7-1-5-3-2 After that, the user is able to trigger the animation again whenever clicking on the object (a visual indication that the animation can be retriggered should be associated with the file).

R7-1-5-4 Audio files in MP3 format shall be supported.

R7-1-5-5 Video Files in MPEG4 format shall be supported.

R7-1-5-6 vCards in .vcf format shall be supported (for details see US7-17)

R7-1-6 Any RCS device shall have the liberty to support (generation / replay) other formats in addition to the formats listed in R7-1-5.

R7-1-7 If the recipient is not RCS capable, but the originating device is connected to RCS, the originating device shall use one of the MNO configurable options below:

R7-1-7-1 File Transfer legacy support:

The file shall be uploaded and the sending device creates a SMS containing the link that allows the recipient to download the file with minimal user interaction. This link shall be accompanied by a 'cover note' in local language that conveys the following message: "You have received a file that originates from the sender as indicated. If you wish to download the file, please click the link:". The link shall use the format of a "short link" that allows the user to identify the sender as their MNO which is a trusted party. (If technically required, it might be the originating network identifier as well).

R7-1-7-2 MMS

NOTE: In no case there should be an attempt to send RCS to non-RCS users and wait for the fail result.

R7-1-8 The user shall be able to change the proposed File Transfer service on a per file and on a general basis.

NOTE: Details of this function are specified in section US18-14.

US7-2 **As a user, I want to ensure that my files reach their destination as reliably and quickly as possible.**

R7-2-1 If File Transfer cannot be instantly delivered by RCS, the B-Party network should apply Delivery Assurance.

R7-2-1-1 The B-Party network shall notify the A-Party network and client that the file delivery is ensured by the B-party network.

R7-2-2 If the A-Party client is made aware that "CFS" is available <u>and</u> a file is not confirmed to be delivered within an MNO configurable period of time via RCS File Transfer, the A-Party user (who is registered on RCS) shall be informed and have the opportunity to notify the recipient with a download link based on SMS.

R7-2-2-1 The user shall have the option to automate the user interaction for Client Fallback to SMS link.
The following options shall be selectable:
- Always ask
- Never ask and always send as SMS link
- Never ask and never send as SMS link

R7-2-2-1-1 The user shall have the option to view and/ or change this decision at any point in the RCS settings section.

NOTE: Steps 3 (R7-2-2-2-3 below) to Step 4b (R7-2-2-2-5 below) are only presented to the user if the device is configured to “Always Ask” and would be automatically processed accordingly if the device is configured to “Never Ask and always send as SMS”.

R7-2-2-2 Details of how and when the revocation of the RCS link and “Send as SMS link” procedure shall be applied:

R7-2-2-2-1 Step 1: User A has created a File Transfer and the file has been sent.

R7-2-2-2-2 Step 2: Delivery for that File Transfer has not yet been confirmed within an MNO configurable period of time. If the A-Party device should have been offline during this period, the following Step 3 shall not be triggered unless the A-Party device was ‘online’ for an MNO configurable time after reconnection, to allow update of File Transfer status notifications.

R7-2-2-2-3 Step 3: The user is presented with a message “Your File Transfer has been successfully uploaded, but the notification for the recipient could not be delivered instantly. Do you want to change to an SMS notification?” and a confirmation request for the user to select (yes / no) input.

If during the display of that message, before user confirmation, a delivery notification for that File Transfer comes in, the user request for “Send as SMS link” shall be removed, and the original File Transfer shall be indicated ‘delivered’ (or ‘downloaded’, if applicable).

R7-2-2-2-4 Step 4a: If the user selects “Yes”, then
- a revocation for the original download link notification shall be triggered,
- the original File Transfer (thumbnail element) shall be removed from the conversation history once the revocation has been confirmed successful,
- an SMS link shall be sent in the background.
- A second File Transfer is generated in the A-party client as a thumbnail of the original File (consistent behaviour compared to Chat / SMS experience), with the sending service indication “SMS”.
- If the user has sent more than one File or message, then the decision to send as SMS (link) shall apply to all events

in ‘sent’ or ‘pending’ status.
- Failure of one of these steps, shall not mean that the other steps shouldn’t be executed. This may lead to duplicated File Transfer access messages on the recipient’s device.
- File Transfer latching shall be applied (as described in R7-2-2-3).

R7-2-2-2-5 Step 4b: If the user selects “No”, a revocation of the original download link notification shall not be triggered, neither an SMS link shall be sent.
- The File Transfer status is updated according to the delivery status.
- The RCS File Transfer notification to the recipient user will stay in the store & forward of the terminating network (according to terminating MNO policies).

R7-2-2-3 File transfer latching: When sending a File to a known CFS enabled contact, a universal client shall by default propose to use FT. If during the last FT exchange the client has applied CFS (SMS link) and there has been no indication since that the contact is online again (e.g. capability exchange or use of another RCS service), SMS link shall be used as the default sending service.

R7-2-2-4 SMS link shall also apply if the client has already fallen back to SMS for text messaging: subsequent File transfers shall continue to be sent as SMS or SMS link until RCS availability is confirmed (e.g. capability exchange or use of another RCS service).

US7-3 **As a user, I want to transfer a file from multiple service entry points on my device.**

R7-3-1 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.

R7-3-2 The user shall have the option to send files to multiple 1-to-1 contacts, as described in requirements of US5-28.

US7-4 **As a user, I want to see the status of any file I sent (including those which have not been delivered (yet)).**

R7-4-1 File Transfer shall support delivery status notifications per individual file (sender device):

R7-4-1-1 File Transfer ‘Pending’ – Transfer of the file has been triggered but not actually started (e.g. queuing on device).

R7-4-1-2 File Transfer ‘In Progress’ – File Transfer started but not completed.

R7-4-1-3 File Transfer ‘Cancelled’ – the sender has cancelled the File Transfer during the File Transfer ‘In Progress’.

R7-4-1-4 File ‘Sent’ - transmission of the File Transfer request has been successfully completed.

R7-4-1-5 File ‘Delivered’ – the file has been successfully delivered to the recipient’s device.

R7-4-1-5-1 For pictures, file ‘Delivered’ shall be reported whenever the preview thumbnail has been successfully delivered to the recipient’s device. If the entire file has been pushed to the device without a preview-thumbnail (e.g. in case of auto-download), then its arrival on the recipient’s device shall trigger the file ‘Delivered’ status notification.

R7-4-1-5-2 For audio messages and other file types, the file ‘Delivered’ status is triggered when the recipient’s device has been informed there is a file available for download.

NOTE: It is important not to use the confirmation of full file download to trigger ‘Delivered’ as, in case of auto-download set to ‘off’ by the user and Delivery Assurance, this could lead to duplicates.

R7-4-1-5-3 The A-Party user shall know whether or not to expect a ‘Delivered’ notification for a File Transfer or other restrictions that are caused by Delivery Assurance application.

R7-4-1-6 File ‘Displayed’ - the content of the file was brought to the user’s attention by display of the file transfer notification in the messaging thread on the active screen.

R7-4-1-6-1 ‘Displayed’ notifications are not available for legacy support and Delivery Assurance cases. The originating client shall be made aware and the user shall be made aware of the reduced feature set of legacy support, similar to missing ‘Displayed’ notification in 1-to-1 Chat.

R7-4-1-7 File Transfer ‘Failed’- the expected outcome of the operation could not be confirmed by the network (In this case: file ‘Sent’, file ‘Delivered’ or file ‘Displayed’ status notifications have not been received) and the device does not attempt to send the message again).

R7-4-2 When a ‘Failed’ status notification occurs, sending the message again may be triggered manually by the user. 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 again.

US7-5 **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.

R7-5-1 Selecting a picture file format that can be rendered by the sending device shall offer the user 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.

R7-5-2 The user shall have the option to configure the image resizing feature as described in US18-9 and the related requirements.

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.

US7-6 **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.**

R7-6-1 On selecting a video file, the user shall have the option to resize the video resolution to a smaller file size in order to save memory, network load and transfer time. The user shall see what the file size would be after that resizing option is applied.

US7-7 **As a user, I don't want to perceive a restriction in file sizes that I want to transfer.**

R7-7-1 The service provider shall set the File Transfer limit to 100MB.

R7-7-2 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.

US7-8 **As a user, I want to transfer a file to multiple users at a time within a Group Chat.**

R7-8-1 File Transfer within a Group Chat shall transfer the file to all participants of the Group Chat.

NOTE: The sender side shall only send the file once over the network in this case.

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, it is not possible for the sender to stop the process of File Transfer.

US7-10 **As a user, I want to transfer a file to multiple users at one time from the gallery or a file browser.**

R7-10-1 The Operator Messaging Service selection shall be made based on capabilities of the participants and cannot be determined before the participants are selected.

R7-10-2 To prevent Spam distribution, the MNO shall be able to limit the list of recipients.

R7-10-2-1 The MNO shall be able to set the possibility of unlimited participants.

R7-10-3 If the user selection of recipients does include one or more contacts not known to be RCS capable, the file shall be delivered based on MNO configuration:

R7-10-3-1 The file shall be uploaded to the RCS File Transfer server and

R7-10-3-1-1 The File Transfer is carried out as multiple 1-to-1 File Transfers.

R7-10-3-1-2 The File Transfer is visible in existing or to be set up 1-to-1 Chat conversations with each recipient.

R7-10-3-1-3 For recipients who are RCS capable, RCS File Transfer shall be used to deliver the file.

R7-10-3-1-4 For recipients who are not RCS capable, the network shall generate a "short link" that allows the user to identify the MNO that provides the download link as a trusted source. This link shall be accompanied by a 'cover note' in local language that conveys the following message: "You have received a file that originates from the sender as indicated. If you wish to download the file, please click the link:"

R7-10-3-2 MMS

R7-10-3-3 The file shall be uploaded and distributed using SMS with link for all recipients.

R7-10-4 The file shall be transferred as RCS File Transfer in Group Chat, if all of the selected contacts are RCS capable.

US7-11 **As a user, I want to transfer a file with my Contact(s) even when they're temporarily offline (e.g. device switched off).**

R7-11-1 In case Delivery Assurance is implemented (CFS or NFS), store and forward may not be applied or only applied temporarily and the request for delivery may be forwarded instantly according to the rules defined for File Transfer Delivery Assurance.

R7-11-2 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.

US7-12 **As a service provider, I want to limit how long a file is available on the network for offline users.**

R7-12-1 The MNO 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.

US7-13 **As a user, I want the device to notify me about new incoming files in a similar way to new incoming messages. I want notifications of rapidly sequenced incoming Chat Messages intelligibly aggregated and counted.**

R7-13-1 On receiving a file or preview thumbnail, the user shall be notified.

R7-13-2 Notifications for File Transfer shall be aggregated similar to Chat Messages as described in US5-10 and related requirements.

R7-13-3 For audio notifications of a new File Transfer request, device settings shall prevail.

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.

R7-13-4 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.

US7-14 **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.

R7-14-1 Incoming files shall be displayed within a new or existing Chat Conversation.

R7-14-2 Files shall be threaded in the conversation as an event similar to messages. The same ruling for order of messages as specified in ‘

R7-14-3 1-to-1 Messaging’ and ‘Group Chat’, shall be applied to files.

R7-14-4 1-to-1 Messaging or 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).

R7-14-5 1-to-1 Messaging 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.

US7-15 **As a user, I want to see incoming files as a thumbnail preview (or generic icon if content cannot be rendered on a 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).

R7-15-1 In case “File Transfer Auto-Accept” is set to off:

R7-15-1-1 The incoming File Transfer presents a thumbnail preview of the file, including file size, on the receiving device first.

R7-15-1-2 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), or 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.

R7-15-1-3 Selection of the preview icon on the receiving device shall trigger the download of the full file to the user's device.

R7-15-1-4 The user shall have the option to delete the thumbnail preview without downloading the content.

R7-15-1-5 A "download all" option may be available to trigger the download of all the content of a displayed conversation history.

R7-15-2 On the B-Party client, if a File Transfer download link was delivered using Delivery Assurance, the link shall not be displayed in plain text but an icon shall represent the link to ensure a user experience as close as possible to the full RCS experience.

R7-15-2-1 Handling of the file, including display of a picture, should be managed by the RCS application. It should be avoided, if technically possible, to change the application and e.g. open a browser.

R7-15-2-2 The file size shall be visible to the B-Party user before the download.

R7-15-2-3 The B-Party user shall be informed accordingly, if the file download is not possible due to missing connectivity.

R7-15-2-4 The B-Party client shall visually differentiate between File Transfer and Geolocation Push by using different icons.

R7-15-2-5 The B-Party client should visually differentiate between different file types (e.g. known formats of picture, audio, music and video) by using different icons.

R7-15-2-6 Once the B-Party device is online again, it shall automatically download the content from the server if the user has enabled File Transfer auto-download in the user settings.

R7-15-2-7 If auto-download of the File Transfer cannot be performed, the user shall be prompted to download the file.

R7-15-2-8 If the File Transfer content is a picture that can be rendered by the B-Party device, the generic icon in the chat conversation with A-party shall be replaced with a thumbnail view of the actual picture after download.

R7-15-2-9 The B-Party client may offer functionality that allows the http-link to be seen in plain text by the user, e.g. in a 'Details' menu of the message.

R7-15-2-10 If the recipient of the link is a legacy RCS device, then the Uniform Resource Locator (URL) should be in a format that allows the user to

see that the link comes from his MNO, which is a trusted party. (If technically required, it might be the originating network identifier as well). This link shall be accompanied by a 'cover note' in local language that conveys the following message: "You have received a file that originates from the sender as indicated. If you wish to download the file, please click the link:"

NOTE: "Legacy RCS device" in this context is an RCS enabled device which does not convert a Delivery Assurance FT link to an icon.

R7-15-2-11 HTTP links received as content of a chat message (not in the context of Delivery Assurance) shall be displayed in plain text format.

R7-15-3 In case File Transfer Auto-accept is set to on:

R7-15-3-1 The user does not have to accept the download for each received File Transfer.

R7-15-3-2 The file is automatically downloaded and can be accessed in the Chat Conversation.

R7-15-4 The MNO shall have the option to set the default value for "File Transfer Auto Accept" via the device provisioning process.

R7-15-5 The user shall have the option to select or deselect "File Transfer Auto-Accept".

US7-16 **As a user, I want to have a visible notification about the status of received files.**

R7-16-1 File Transfer shall support status notifications per individual file (receiver device):

R7-16-1-1 In case of auto accept off- thumbnail preview received – indication that a file is waiting for download trigger on a receiving network.

R7-16-1-2 File Transfer in progress on receiving device – file transfer started but not completed.

R7-16-1-3 Cancelled – the receiver shall have the option to cancel the File Transfer during the File Transfer process.

R7-16-1-4 File downloaded.

R7-16-1-5 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 the option to ask the sender to re-send the file.)

US7-17 **As a user, I want to transfer a Contact's information from the contact list to other RCS users.**

R7-17-1 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 A.1 ‘**Personal Card format**’.

R7-17-2 Devices shall be capable to render vCard files in .vcf format according to RCS standard (see Annex A.1 ‘**Personal Card format**’) and offer to store received Contacts in the device contact list.

US7-18 **As a user, I want to be able to resume interrupted File Transfers**

NOTE: On sending and receiving side.

R7-18-1 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).

R7-18-2 If the receiver’s device does not have enough storage space to download the full file,

R7-18-2-1 A notification shall be provided to the receiver before downloading the full file.

R7-18-2-2 Storage space shall be freed up manually by the receiver before download attempt shall be possible.

R7-18-2-3 The user shall have the option to re-start the file download as long as the MNO storage time (as in R7-12-1) has not expired.

US7-19 **As a service provider, I want to be able to limit the size of the files that are transferred.**

R7-19-1 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.

US7-20 **As a user, I want to administrate File Transfers in Chat and Group Chat Conversations intuitively.**

R7-20-1 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 sent and received files backed up on the Common Message Store which is trusted and safe.**

R7-21-1 Any successfully sent and received files may be stored on the network.

NOTE: Details of storage are at the individual MNO discretion.

R7-21-2 In case the MNO deletes files from the Common Message Store (e.g. for capacity limitation) these files shall not be deleted from local consumer equipment

US7-22 **As a user, I want to restore my sent and received files from the network MNO storage**

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 my device to always be in sync with the stored files on the network even in case of multiple devices.**

NOTE: Details on synchronisation and secondary device use will be described in 'Messaging for Multi-Device', page 129.

R7-23-1 If automatic backup & restore or multi-device usage is enabled, all user devices shall always maintain synchronisation of sent and received files.

NOTE: Details on synchronisation and secondary device use will be described in 'Messaging for Multi-Device', section 9.

7.3 Technical Information

7.3.1 Overview

The File Transfer service is provided based on the File Transfer Enabler defined in section 3.5 of [RCC.07] extended by functionality provided in this section.

The File Transfer enabler supports File Transfer via MSRP and File Transfer via HTTP. The profile defined in this document only supports File Transfer via HTTP. Therefore the client configuration parameter FT DEFAULT MECH defined in section A.1.5 of [RCC.07] is provided by the service provider with the fixed value "HTTP". The client shall advertise the capability for File Transfer via HTTP in accordance with the definitions of section 3.5.4.8.1 of [RCC.07].

The File Transfer technology is derived by the client as result of the capability discovery as defined in section 3 of this document. A RCS contact is considered to be File Transfer capable if the File Transfer via HTTP capability is present.

7.3.2 File Transfer Fallback

7.3.2.1 Introduction

The procedures for File Transfer fallback defined in this section enable RCS clients to provide a File Transfer experience if RCS is not available end-to-end. The definitions in this section replace the definitions for File Transfer fallback in section 3.5.4.8.6 of [RCC.07].

The procedures for File Transfer fallback are applicable if

- a File Transfer is subject to delivery assurance via client fallback to SMS or
- a file is transmitted to a non RCS capable recipient or a RCS capable recipient without File Transfer capability.

The procedures for File Transfer Fallback rely on transport of File Transfer specific content via SMS messages.

7.3.2.2 File Transfer via SMS Capability

The profile defined in this document defines a new client capability for the support of the File Transfer via SMS service. A client supporting the rendering of the user data of a SMS message for File Transfer as defined in section 7.3.2.6 and the procedures for the HTTP(s) URI processing defined in section 7.3.2.4 shall advertise its capability

- via the media feature tag defined in Table 31 in SIP OPTIONS requests and responses for capability discovery or
- via the service description defined in Table 32 in presence documents for capability discovery

in accordance with the definitions for capability discovery defined in section 3 of this document.

RCS service	Tag
File Transfer via SMS	+g.3gpp.iari-ref="urn%3Aurn-7%3A3gpp-application.ims.iari.rcs.ftsms"

Table 31: SIP OPTIONS tag for File Transfer via SMS

RCS service	Service Description
File Transfer via SMS	Service-id: *org.3gpp.urn:urn-7:3gpp-application.ims.iari.rcs.ftsms* Version: 1.0 Contact address type: tel / SIP URI

Table 32: Service Description for File Transfer via SMS

A client supporting the profile defined in this document shall add the media feature tag defined in Table 31 in the Contact header field of SIP REGISTER requests.

7.3.2.3 HTTP Message Body Schema Extension

The HTTP Content Server should be able to assign a user friendly URL to a file uploaded by the client via the upload procedures defined in section 3.5.4.8.3.1 of [RCC.07] in addition to the existing URL for file download. The user friendly URL can be conveyed by the HTTP Content Server to the client via the "branded-url" element defined in the schema in Table 33.

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema targetNamespace="urn:gsma:params:xml:ns:rcs:rcs:up:fthttpext"
            xmlns:xs="http://www.w3.org/2001/XMLSchema"
            xmlns="urn:gsma:params:xml:ns:rcs:rcs:up:fthttpext"

            elementFormDefault="qualified"

            attributeFormDefault="unqualified">

        <xs:element name="branded-url" type="xs:anyURI"/>
</xs:schema>
```

Table 33: HTTP Message Body schema Extension

The "branded-url" element shall be added as an extension to the "data" element of the "file info" element of the HTTP Message Body schema defined in section 3.5.4.8.3.1 of [RCC.07].

Clients receiving the "branded-url" element in a HTTP Content Server response body shall forward the element unaltered to recipients when using the HTTP message body.

The nature and structure of the URL value in the "branded-url" element is left to the discretion of the service provider of the HTTP Content Server.

7.3.2.4 Parameter Definition for HTTP URL for File Transfer fallback

A client supporting File Transfer fallback need to be able to determine additional meta information related to the file located on a HTTP Content Server by parsing the HTTP Content Server file URL.

A HTTP URL locating a file on a HTTP Content Server is identified by the HTTP Content Server FQDN defined in section 3.5.4.8.4 of [RCC.07].

The URL locating a file on a HTTP Content Server is complemented with meta-information describing the file using the URL parameters defined in Table 34.

Parameter	Type	Value
s	Integer	Identifies the size of the file in bytes The presence of the parameter is mandatory, if the URL locating a file on a HTTP Content Server contains additional meta data describing the file.
t	String	Value of the Multipurpose Internet Mail Extensions (MIME) content-type header of the file as defined in [RFC2045]. Note: reserved characters in the content-type header value have to be represented using percent encoding in accordance with [RFC3986]. The presence of the parameter is mandatory, if the URL locating a file on a HTTP Content Server contains additional meta data describing the file.
e	String	Combined date and time in UTC time zone in ISO8601 basic format, i.e. YYYYMMDDThhmmssZ. It indicates the date and time of expiry of the file, e.g. 20170419T135227Z The presence of the parameter is mandatory, if the URL locating a file on a HTTP Content Server contains additional meta data describing the file.

Table 34: HTTP URL parameters for File Transfer fallback

The URL configuration parameters defined in Table 34 shall be appended to the URL locating a file on the HTTP Content Server using Hyper Text Markup Language (HTML) form encoding respecting the definitions of [RFC3986].

It is recommended that implementations ensure that the maximum length of the URL locating a file on a HTTP Content Server does not exceed the length of the user data of one SMS message. However if the string exceeds the maximum length of the user data of a SMS message, then the sending client shall apply the procedures for concatenation of SMS as defined in [3GPP TS 23.040].

7.3.2.5 Sender Procedures

The procedures defined in this section apply

- if the user requests to send a file to a recipient with no RCS capabilities or a recipient with RCS capabilities but without support of the File Transfer service defined in section 7.3.1. In this case the user may prefer to send the message via MMS or as a "text message with a link". The operator is able to provide a default selection via the configuration parameter FT HTTP FALLBACK defined in section 7.3.3.2.
- if a chat message conveying a File Transfer via HTTP is subject to client fallback as defined in section 5.3.3.

7.3.2.5.1 Sending of a File to a Recipient with no File Transfer Capability

If the user requests to send a file to a recipient with no RCS capabilities or a recipient with RCS capabilities but without support of the File Transfer service defined in section 7.3.1, then

- if the user or the client has selected MMS to transfer the file and the file complies or can be converted to comply with the formats and codecs defined in [OMA-MMS-CONF], then the client shall compose a MMS message and send it following the procedures defined in [3GPP TS 23.140], otherwise
- the client shall upload the file to the HTTP Content Server as defined in section 3.5.4.8.3.1 of [RCC.07].
- If successful, the client shall check whether the HTTP message body received from the HTTP Content Server contained an "branded-url" element in the file-info element with type "file", then
- if the "branded-url" element is present it shall use its value, otherwise
- it shall use the value of the "url" attribute contained in the data element of the file-info element with type "file",
- compose a new message containing the URL next to some explanatory text indicating the purpose of the message and send it to the recipient via
- RCS Standalone Messaging, if enabled as defined in section 5.3.1, otherwise
- via SMS.

7.3.2.5.2 File Transfer Client Fallback

If the originating client has uploaded a file to the HTTP Content Server for a File Transfer via HTTP and the client applies monitoring of the delivery of chat messages within the 1-to-1 Chat session in accordance with the definitions in section 5.3.3.2, then the client shall keep the data of the HTTP Content Server response body at least until the delivery of the chat message is confirmed.

Precondition for the application of File Transfer via SMS is that the client has uploaded a file to the HTTP Content Server as defined in section 3.5.4.8.3.1 of [RCC.07] and has received and kept the data of the HTTP Content Server response body.

If the originating client decides to fall back to SMS for a File Transfer as result of the procedures for client fallback as defined in section 5.3.3 and the recipient supports File Transfer via SMS, as indicated by the capability defined in section 7.3.2.2, then the originating client

- shall inspect the URL value of the "url" attribute contained in the data element of the file-info element with type "file" received in the HTTP message body received from the HTTP Content Server to determine whether URL parameters as defined in Table 34 are present, then
- if there is none of the URL parameters defined in Table 34 present, then the client shall generate
    - a “s” parameter as defined in Table 34 using the value extracted from the file-size element of the file-info element with type “file” included in the HTTP message body of the response
    - a “t” parameter as defined in Table 34 using the value extracted from the content-type element of the file-info element with type “file” included in the HTTP message body of the response
    - an “e” parameter as defined in Table 34 using the value extracted from the “until” attribute contained in the data element of the file-info element with type “file” included in the HTTP message body of the response
    - append it to the URL using HTML form encoding respecting the definitions of [RFC3986]
- otherwise use the URL unaltered
- add the URL value to the user data of a SMS message and
- send the SMS message to the recipient address.

If the originating client decides to fall back to SMS for a File Transfer as result of the procedures for client fallback as defined in section 5.3.3 and the recipient does not support File Transfer via SMS via the capability defined in section 7.3.2.2

then the client

- shall check whether the HTTP message body received from the HTTP Content Server contained an "branded-url" element in the file-info element with type "file", then
- if the "branded-url" element is present it shall use its value, otherwise
- it shall use the value of the "url" attribute contained in the data element of the file-info element with type "file",
- add the URL next to some explanatory text indicating the purpose of the message to the user data of a SMS message and
- send the SMS message to the recipient address.

7.3.2.6 Receiver Procedures

On reception of a SMS message, the client shall parse the user data of the message.

If the user data contains a HTTP(s) URL and the FQDN of the URL conforms to the definitions of the HTTP Content Server URI as defined in section 3.5.4.8.4 of [RCC.07], then the client shall apply the UX procedures defined for suppression and replacement of the HTTP Content Server URI. The client shall take the URL parameters for File Transfer fallback as defined in section 7.3.2.4 into account. When retrieving the file, the client shall use the URL as received in the user data of the SMS message.

7.3.2.7 Network Procedures for Fall Back for File Transfer

7.3.2.7.1 HTTP Content Server

Service providers complying with the profile defined in this document should add the HTTP URL parameters defined in Table 34 in the HTTP Content Server response body defined in section 3.5.4.8.3.1 of [RCC.07] to the value of the "url" attribute of the "data" element of the "file-info" element with the "type" attribute set to "file".

Service providers complying with the profile defined in this document should add a "branded-url" element containing a user friendly URL in the "file-info" element with the "type" attribute set to "file". The "branded-url" element shall follow the syntax defined in section 7.3.2.3.

A sample HTTP Content Server response body with a "url" parameters extended as defined in Table 34 and a "branded-url" element defined in Table 33 is shown in Table 35.

```
<?xml version="1.0" encoding="UTF-8"?>
<file xmlns="urn:gsma:params:xml:ns:rcs:rcs:fthttp"
      xmlns:e="urn:gsma:params:xml:ns:rcs:rcs:up:fthttpext">
      <file-info type="thumbnail">
          <file-size>82</file-size>
          <content-type>image/jpeg</content-type>
          <data url="https://ftcontentserver.rcs.mnc001.mcc262.pub.3gppnetwork.org/..."
          until="2017-04-22T19:30:00Z"/>
      </file-info>
      <file-info type="file">
          <file-size>32464</file-size>
          <file-name>example.jpg</file-name>
          <content-type>image/jpeg</content-type>
          <data
          url="https://ftcontentserver.rcs.mnc001.mcc262.pub.3gppnetwork.org/...?t=image%2Fjpeg&s=32464
          &e=20170422T193000Z"
          until="2017-04-22T19:30:00Z"/>
          <e:branded-url>https://www.operator.com/...</e:branded-url>
      </file-info>
</file>
```

Table 35: Sample HTTP Content Server response body

7.3.2.7.2 Network Interworking

The procedures in the network for File Transfer fallback are network internal and therefore outside of the scope of this document. As defined in section 7.3.2.2, the client shall add the media feature tag defined in Table 31 in the Contact header field of the SIP REGISTER allowing the network to detect the client capability. The formats of SMS messages resulting

from the network interworking procedures shall follow the formats defined for the client-based fallback defined in section 7.3.2.5.

7.3.3 Configuration Parameters

7.3.3.1 New Configuration Parameters

To provide operator control of the client's File Transfer behaviour the following new configuration parameters are defined for the profile defined in this document.

Configuration parameter	Description	RCS usage
FT MAX 1 TO MANY RECIPIENTS	This parameter controls the number of recipients for the one to many sending of a File Transfer. 0 (default): no limitation in the number of recipients positive integer value: indicates the maximum total number of recipients of a File Transfer.	Optional parameter
FT FALLBACK DEFAULT	This parameter is applicable only when MESSAGING UX is set to 1. It controls the operator default of the client switch controlling the user dialog when according to the rules in section 5.2 a Chat message associated with a File Transfer is subject to SMS fallback. **0** (Default Value), never ask the user to confirm the fallback to File Transfer via SMS and always fall back, **-1**, never ask the user to confirm the fallback to File Transfer via SMS and never fall back **1**, always ask the user to confirm the fallback to File Transfer via SMS	Optional parameter

Table 36: Configuration Parameters for File Transfer Control

The FT FALLBACK DEFAULT configuration parameter is added to the UX tree defined in section 5.3.7.1 based on the following definition.

<u>Node: /<x>/UX/ftFBDefault</u>

Leaf node that describes the operator's default setting client switch to control the user dialog for File Transfer fallback to SMS.

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

Table 37: UX MO sub tree addition parameters (ftFBDefault)

- Values:

  -1, never ask the user to confirm the fallback to File Transfer via SMS and never fall back
  0 (default value), never ask the user to confirm the fallback to File Transfer via SMS and always fall back.
  1, always ask the user to confirm the fallback to File Transfer via SMS

- Post-reconfiguration actions:
  Change the user setting, if it hasn't been toggled by the user before.
- Associated HTTP XML parameter ID: "ftFBDefault"

The configuration parameter FT MAX 1 TO MANY RECIPIENTS is added to the Client Control MO tree defined in section 5.3.7.1 based on the following definition.

Node: /<x>/ClientControl/ftMax1ToManyRecipients

Leaf node that provides the maximum number of recipients allowed for a File Transfer to multiple recipients.

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

Table 38: Client Control MO sub tree addition parameters (ftMax1ToManyRecipients)

- Values:
  0 (default): the client can send a File Transfer to an unlimited number of recipients
  Positive integer value: indicates the maximum total number of recipients a File Transfer can be sent to.
- Post-reconfiguration actions:
  There are no action at the time of re-configuration.
- Associated HTTP XML parameter ID: "ftMax1ToManyRecipients"

7.3.3.2 Existing Configuration Parameters with updated Definition

The profile defined in this document updates the definition of the configuration parameters defined in [RCC.07] as follows.

Configuration parameter	Description	RCS usage
FT HTTP FALLBACK	This parameter provides the operator default of the technology to transfer files to contacts not supporting File Transfer via HTTP. The parameter can take the following values: 0: MMS (default value) 1: text message with a link.	Optional parameter

Table 39: Configuration Parameters for File Transfer Control

The definitions of the configuration parameter "ftHTTPFallback" of the IM management object subtree defined in section A.2.6 of [RCC.07] are updated as follows:

Node: <x>/ftHTTPFallback

Leaf node that describes the operator's default setting client switch to control the user dialog for File Transfer fallback to SMS.

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

Table 40: IM MO sub tree addition parameters (ftHTTPFallback)

- Values: 0, 1
  - 0, MMS is used (default)
  - 1, Text message with a link us uses
- Post-reconfiguration actions: there is no action required at the time of re-configuration.
- Associated HTTP XML parameter ID: “ftHTTPFallback”

7.3.4 Technical Implementation of User Stories and Service requirements

R7-24-1 For the requirements of user story US7-1 the following definitions apply:

- The File Transfer is provided by the technical enabler described in section 7.3.1 of this document updated by the procedures for File Transfer Fallback defined in section 7.3.2 of this document.
- The File Transfer service shall be offered to the user if the service provider's client configuration enables the File Transfer via HTTP service via the FT DEFAULT MECH parameter set to value "HTTP" as defined in sections 3.5.4.8.1 and A.1.5 of [RCC.07].

R7-24-2 The requirements of R7-1-1 are implemented locally on the device.

R7-24-3 The requirement R7-1-2 is implemented locally on the device. For details of the technology selection for the transfer a file to RCS and non RCS contacts refer to R7-1-7 and the corresponding technical implementation.

R7-24-4 The requirement R7-1-3 is implemented locally on the device for the case of File Transfer to more than one recipient refer to the technical implementation defined for US7-8 and US7-10.

R7-24-5 The capability required in R7-1-4 is a basic function of the File Transfer enabler.

R7-24-6 The requirements of R7-1-5 and R7-1-6 are implemented locally on the device.

R7-24-7 The requirement of R7-1-7 to enable MNO configuration of the File Transfer legacy support mechanism is provided by means of the client configuration parameter FT HTTP FALLBACK defined in section 7.3.3.2

R7-24-8 The requirement R7-1-7-1 is applicable

- if the configuration parameter FT HTTP FALLBACK defined in section 7.3.3.2 is set to "1" or the user has selected File Transfer fallback as the mechanism as defined in requirement R7-1-8, or
- .if the configuration parameter FT HTTP FALLBACK defined in section 7.3.3.2 is set to "0" or the user has selected MMS as the mechanism as defined in requirement R7-1-8 and the file does not conform with the formats and codecs defined in [OMA-MMS-CONF].

The procedure defined in section 7.3.2 applies.

R7-24-9 The requirement R7-1-7-2 is applicable if the configuration parameter FT HTTP FALLBACK defined in 7.3.3.2 is set to "0" or the user has selected MMS as the mechanism as defined in requirement R7-1-8. and the file conforms with the formats and codecs defined in [OMA-MMS-CONF]. The procedure defined in section 7.3.2 applies.

R7-24-10 The requirement R7-1-8 is implemented locally on the device. Once the user has altered the setting of the File Transfer fallback mechanism selection on a general basis and the value of the configuration parameter FT HTTP FALLBACK is re-configured via the service provider device provisioning, then the client shall ignore the value provided by the service provider.

R7-24-11 The requirement R7-2-1 is implemented via the procedures for delivery assurance defined in section 5.3 of this document.

R7-24-12 The requirement R7-2-1-1 is implemented via the network indication of support of delivery assurance as defined in section 5.3 of this document.

R7-24-13 The requirement R7-2-2 is implemented via the procedure for delivery assurance via client fallback as defined in section 5.3 of this document. If the user has confirmed the client fallback via download link, then the sending client shall invoke the procedures for File Transfer fallback as defined in section 7.3.2 of this document. An operator default for the user setting to confirm a client fallback to SMS via download link is managed via the FT FALLBACK DEFAULT configuration parameter defined in section 7.3.3.1.

R7-24-14 The requirements of user story US7-3 shall be implemented locally on the device.

R7-24-15 The requirements of user story 7-4 shall be implemented as follows. The implementation depends on the file transport technology used:

- **Pending**:
  For File Transfer via HTTP and File Transfer Fallback; when the user initiated sending of the file until the first HTTPs 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 via HTTP; from the reception of the first success HTTP response from the network until a MSRP 200 OK is received from the network for the chat message carrying the File Transfer via HTTP message body content.

  For File Transfer Fallback; from the reception of the first success HTTP response from the network until a successful SMS submit confirmation is received from the network for the SMS message carrying the File Transfer Fallback link.

- **Cancelled**:
  If the user has cancelled the File Transfer as described in the user story US7-9.
- **Sent**:
  For File Transfer via HTTP; if a MSRP 200 OK is received from the network for the chat message carrying the File Transfer via HTTP message body content.

  For File Transfer Fallback; if a successful SMS submit confirmation is received from the network for the SMS message carrying the File Transfer Fallback link.
- **Delivered**:
  For File Transfer via HTTP, when receiving the Delivery Notification.

  For File Transfer via SMS; when receiving the delivered status report for the SMS message carrying the File Transfer Fallback link.
  The requirement R7-4-1-5-3 shall be realised based on the Interworking disposition notification as specified in section 5.3.3.4, i.e. the client should indicate that the user should not expect a displayed status for the message in this case.

NOTE: An originating client may receive for a chat message both a delivery and an interworking disposition notification, e.g. due to support of multi device in the terminating network. Reception of the delivery disposition notification overwrites the "interworking" status of the message".

For File Transfer Fallback, when receiving the SMS delivery report. The client should indicate to the user not to expect a displayed status for the message in this case.

- **Displayed:**
  For File Transfer via HTTP, when receiving the Display Notification. If Interworking Disposition notification has been received but no delivery notification, as defined in section 5.3.3.4, then the displayed status is not applicable.

  The requirement R7-4-1-6-1 shall be realised based on the Interworking disposition notification as specified in section 5.3.3.4, i.e. the client should indicate that the user should not expect a displayed status for the message in this case.

  For File Transfer Fallback, not applicable.
- **Failed:**
  The failed state applies whenever the processing to send the File Transfer fails and theclient does not attempt to transfer the file anymore. As a clarification, a File Transfer cannot enter the "failed" status anymore after it entered the "sent" status.

R7-24-16 Notifications on delivery and display status information as per requirement R7-4-2 shall be processed for store and forward as follows:

- IMDN in the messaging server as specified in section 3.3.4.1.5 of [RCC.07]
- SMS delivery status reports as specified in [3GPP TS 23.040].

R7-24-17 The requirements of US7-5 shall be implemented locally on the device. When transferring a large image using File Transfer, the client may 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

R7-24-18 The requirement of user story US7-6 shall be implemented locally on the device.

R7-24-19 The file size limits required in the user story US7-7 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].

R7-24-20 The technical implementation of the requirements of user story US7-8 is defined in section 3.5.4.8 of [RCC.07] and the technical definitions for Group Chat defined in section 6.3 of this document.

R7-24-21 To cancel the sending of a File Transfer as required in user story US7-9 the client shall interrupt the ongoing HTTP file upload flow at the time of user input.

R7-24-22 The requirements in use case US7-10 shall be implemented locally on the device based on the following mechanisms:

R7-24-22-1 For the requirement 7-10-2 the RCS capability shall be discovered via the capability discovery defined in section 3. To identify recipients being RCS capable the client shall check the capability of recipients as defined in section 6.3, 7.3.1 and 7.3.2 of this document.

R7-24-22-2 T he requirement R7-10-2 and R7-10-2-1 shall be implemented on the client based on the operator control configuration parameter FT MAX 1 TO MANY RECIPIENTS defined in section 7.3.3 of this document.

R7-24-22-3 The requirement R7-10-3-1 is applicable

- if at least one recipient has no Chat capability as defined in section 6.3 of this document and if the configuration parameter FT HTTP FALLBACK defined in section 7.3.3.2 is set to "1", or

- all recipients have the Chat capability as defined in section 6.3 of this document and the configuration parameter FT HTTP FALLBACK defined in section 7.3.3.2 is set to "1" but the number of recipients exceeds the value of the configuration parameter MAX_AD-HOC_GROUP_SIZE defined in section A.1.4.1 of [RCC.07].

  As a clarification, the client shall upload the file to the FT Content Server only once and determine per target address whether File Transfer over HTTP or File Transfer fallback is to be used in accordance with the capabilities of the recipient.

R7-24-22-4 The requirement R7-10-3-2 is applicable if

- at least one recipient has no Chat capability as defined in section 6.3 of this document and if the configuration parameter FT HTTP FALLBACK defined in section 7.3.3.2 is set to "0", or

- all recipients have the Chat capability as defined in section 6.3 of this document and the configuration parameter FT HTTP FALLBACK defined in section 7.3.3.2 is set to "0" but the number of recipients exceeds the value of the configuration parameter MAX_AD-HOC_GROUP_SIZE defined in section A.1.4.1 of [RCC.07].

R7-24-22-5 The requirement R7-10-4 is applicable if all recipients have the Chat capability as defined in section 6.3 of this document and the number of recipents does not exceed the value of the configuration parameter MAX_AD-HOC_GROUP_SIZE defined in section A.1.4.1 of [RCC.07]. For the implementation of File Transfer in a Group Chat refer to section 6.3 of this document.

R7-24-23 The technical implementation of File Transfer Store and Forward of user story US7-11 is defined in sections 3.5.4.8 of [RCC.07]. For the technical implementation of Delivery Assurance for File Transfer refer to the technical implementation of US7-2. The client shall determine the validity of the file for download from the file-info element for the file from the HTTP message body content as defined in section 3.5.4.8.3.1 of [RCC.07] for File Transfer via HTTP or from the URL parameter defined in section 7.3.2.4 of this document for File Transfer fallback. If the client attempts to download the file from the HTTP Content Server as defined in section 3.5.4.8.3.2 of [RCC.07] and it receives a HTTP 404 NOT FOUND error, then the client shall assume that the file has expired.

R7-24-24 The requirement of user story US7-12 is provided by the Service Provider's policy on the messaging server or the HTTP Content Server.

R7-24-25 The requirements of user stories US7-13 and US7-14 shall be implemented locally on the device.

R7-24-26 The requirements of user story US7-15 shall be implemented locally on the device.

R7-24-26-1 The Service Provider provides the default selection of auto download via the FT AUT ACCEPT parameter defined in section A.1.5 of [RCC.07]. Once the user has changed the preferences for auto download of files the client shall ignore the settings of the configuration parameter FT AUT ACCEPT.

R7-24-26-2 To ensure the service behaviour for auto-download for files of all sizes as defined in US7-15 the Service Provider shall apply for the configuration parameter FT WARN SIZE the same value as for FT MAX SIZE or FT MAX SIZE INCOMING respectively, see also section 3.5.4.8.3.2 of [RCC.07].

R7-24-26-3 The client shall use the parameters of the file-info element of the HTTP message body content as defined in section 3.5.4.8.3.1 of [RCC.07] for File Transfer via HTTP or from the URL parameter defined in section 7.3.2.4 of this document to support the user experience defined in US7-15.

R7-24-26-4 The thumbnail preview for File Transfer shall be implemented as defined in section 3.5.4.8 of [RCC.07].

R7-24-27 The requirements of R7-16-1 shall be implemented locally on the device based on the procedures defined in section 3.5.4.8.3.2 of [RCC.07] and the clarifications for the sub-requirements.

R7-24-27-1 The requirement of R7-16-1 is implemented locally on the device. During the processing of a reception of a File Transfer the client shall take the following requirements into account:

R7-24-27-2 For requirement R7-16-1-1, the client shall send a delivery disposition notification on reception of a chat message for File Transfer via HTTP if the message body content does not include a file-info element of type “thumbnail”. The client shall send a delivered disposition notification on successful download of the thumbnail in accordance with the procedures in section 3.5.4.8.3.2 of [RCC.07] if the message body of the chat message for File Transfer via HTTP included a file-info element of type “thumbnail”. The requirement is not applicable if the RCS client processes File Transfer fallback as defined in section 7.3.2 of this document.

R7-24-27-3 For requirement R7-16-1-3, if the user cancels the download then the client shall abort the HTTP file download. This requirement is applicable for File Transfer and File Transfer fallback.

R7-24-27-4 For the requirement R7-16-1-4, for File Transfer the client shall send a display disposition notification after the content of the file was brought to the user’s attention by display of the file transfer notification in the messaging thread on the active screen, see also requirement R7-4-1-6.

R7-24-27-5 For the implementation of requirement R7-16-1-5 the client shall take the definitions of section 3.5.4.8.3.2 of [RCC.07] into account.

R7-24-28 To implement the requirements of US7-17 refer to Annex A.1 of this document.

R7-24-29 The requirement of US7-18 shall be implemented based on the procedures defined in

- section 3.5.4.8.3.1 of [RCC.07] for resume on the client when sending File Transfer or File Transfer fallback.
- section 3.5.4.8.3.2 of [RCC.07] for resume on the client when receiving File Transfer or File Transfer fallback.

R7-24-30 The file size limits defined in the user story US7-19 are configured via the FT MAX SIZE parameter defined in section A.1.5 of [RCC.07].

R7-24-31 The requirements of user story US7-20 shall be implemented locally on the device.

R7-24-32 For the implementation of user stories US7-21 through US7-23 refer to section 9 of this document.

NOTE: Because the enabler used to provide the Common Message Store may change in future versions of the profile defined in this document (see section 1.1.2), in this version of the profile it is optional for clients to provide this implementation for the requirements of US7-21 to US7-23.

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’ with the following refinements detailed below.

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 It shall be possible to record and send an Audio Message in Chat and Group Chat conversations.

R8-1-2 Audio Messaging shall use File Transfer Store & Forward as defined in the File Transfer section 7.

R8-1-3 Audio Messaging service shall be capable of sharing exactly one Audio Message at a time.

R8-1-4 The Audio Message shall stay within limits of the File Transfer maximum size limits as defined in the File Transfer section 7.

R8-1-5 Interruptions in transfer of Audio Messages shall be handled as defined in the File Transfer section 7.

8.2.1 Sending Audio Messages

R8-1-6 Any RCS user shall be able to send an Audio Message to Contacts in the contact list or by entering the contact's MSISDN.

R8-1-7 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.

R8-1-8 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.

R8-1-9 Audio Messaging shall support status notification per individual Audio Message (sender side) as described in user story US7-4 and the supporting requirements.

R8-1-10 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 section.

R8-1-11 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.

R8-1-12 Sent Audio Messages shall be displayed and available for playback from a Chat Conversation which is associated with the participant(s) concerned.

R8-1-13 Audio Message recording shall be limited to either ten minutes or a duration based on the maximum file size supported by the MNO, whichever is smaller.

R8-1-13-1 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.

R8-1-13-2 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 conversation.**

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 7.

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 It shall be possible to receive and play an Audio Message in a 1-to-1 Messaging and a Group Chat conversation.

R8-2-6 For Audio Messaging, the rules of File Transfer Auto-Accept shall be in line with the according requirement/s in the File Transfer section.

R8-2-7 A user will be notified, as soon as they come online, of Audio Messages sent to them whilst they were offline as soon as they become online again.

R8-2-8 If the receiving device does not have enough space to store the incoming Audio Message, the regulations in requirement R7-18-2 shall apply.

R8-2-9 When a user plays back an Audio Message, it shall be played through the devices 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 in the File Transfer section.

R8-3-2 Audio Messages shall be stored on a central MNO storage in accordance with the requirements defined the File Transfer section 7.

R8-3-3 Any Audio Messages shall be available on secondary devices and interfaces in accordance with requirements in the File Transfer section and requirements specified in the Messaging for Multi-Device section 9.

R8-3-4 Audio Messages shall be available for playback from the 1-to-1 Messaging or Group Chat conversation by sending and receiving parties.

R8-3-4-1 When an audio message is opened, the user shall be presented with playback, stop and forward / rewind options to operate the audio player.

R8-3-4-2 The user shall have the option to easily respond to a received audio message with an audio message from the opened audio message player.

R8-3-5 Audio Messages shall be saved in the conversation history along with messages and files in a chronological order (as per ordering requirements specified in 1-to-1 Messaging and Group Chat sections).

R8-3-6 Audio Messages shall be displayed with information on the message's time and date and duration.

R8-3-6-1 The icon that is used to represent the audio message in the conversation thread shall be differentiated from an icon that is used for other audio files, e.g. music files.

R8-3-7 In the case of Multi-Device, all requirements in the File Transfer section 7 and in the Multi-Device Messaging section 9 shall apply.

R8-3-8 Incoming Audio Messages shall be represented in Chat Conversations in accordance with requirements in the File Transfer section 7.

R8-3-9 Status notifications for incoming Audio Messages shall be supported in accordance with requirements in the File Transfer section 7.

8.3 Technical Information

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 File Transfer requirements and technical procedures, as per section 7, 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 set to a hard limit of 600 seconds (10 minutes).

8.3.2 Technical Implementation of User Stories and Service Requirements

R8-3-10 Audio Messaging shall be done as described in section 3.11 of [RCC.07] and following the File Transfer requirements and technical procedures, as per section 7.

R8-3-11 As a file can be sent to one or more contacts, requirement R8-1-1 is supported. The recording shall be implemented locally on the device.

R8-3-12 As Audio Messaging is based on the File Transfer mechanism as per section 7, it inherits from the File Transfer features:

R8-3-12-1 Store and Forward is one of these features, hence, requirement R8-1-2 is supported.

R8-3-12-2 Interruptions in transfer of Audio Messages, hence, requirement R8-1-6 is supported.

R8-3-13 Requirement R8-1-3 shall be implemented locally on the device.

R8-3-14 Requirement R8-1-4 shall be implemented locally on the device taking the FT MAX SIZE (refer to Table 76 of [RCC.07]) parameter value into consideration.

R8-3-15 Requirement R8-1-6 and its sub requirements are UI related and shall be implemented locally on the device.

R8-3-16 Requirement R8-1-7, uses the procedure defined for File Transfer, as per section 7 to exchange Audio Messages to a group of contacts.

R8-3-17 Requirement R8-1-8 shall be implemented locally on the device.

R8-3-18 Requirement R8-1-9 is supported via the File Transfer corresponding requirement (section 7).

R8-3-19 Requirement R8-1-10 is supported by the ability to cancel a File Transfer (see section 7).

R8-3-20 Requirement R8-1-11 shall be implemented locally on the device.

R8-3-21 As an Audio Message is a file, it shall be part of a Chat conversation as required by requirement R8-1-12. 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]):

R8-3-21-1 The File Disposition is located in the file-disposition attribute of the file-info element of the main file.

R8-3-22 Requirement R8-1-13 shall be implemented locally on the devices with a maximum length of either a hard 10 minutes limit or, if shorter, on the duration derived from the FT MAX SIZE parameter.

R8-3-23 Requirements R8-1-13-1 and R8-1-13-2 shall be implemented locally on the device.

R8-3-24 As an Audio Message is a file:

R8-3-24-1 Notifications shall be triggered, hence, requirement R8-2-1 is supported.

R8-3-24-2 Sorting as per requirement R8-2-3 is supported.

R8-3-24-3 Action resulting to the selection of a visual notification as per requirement R8-2-4 is supported.

R8-3-25 Requirement R8-2-2 shall be implemented locally on the device.

R8-3-26 Requirement R8-2-5 is supported with the File Disposition being set to ‘render’, making the Audio Message playable in a 1-to-1 Chat or Group Chat

R8-3-27 As an Audio Message is a file:

R8-3-27-1 It shall comply with the rules of File Transfer Auto-Accept as described in ‘section 7’, fulfilling R8-2-6.

R8-3-27-2 Requirement R8-2-7 uses the Store and Forward mechanism as defined in section 7.

R8-3-27-3 Requirement R8-2-8 uses management of local storage space as required in section 7.

R8-3-28 Requirement R8-2-9 shall be implemented locally on the device.

R8-3-29 Requirement R8-2-10 shall be implemented locally on the device.

R8-3-30 As an Audio Message is a file:

R8-3-30-1 Deletion as required in section 7, File Transfer, is supported, fulfilling requirement R8-3-1.

R8-3-30-2 Storage in the Common Message Store as defined in section 7, is supported, fulfilling requirement R8-3-2.

R8-3-30-3 Requirements R8-3-3 and R8-3-7 use Common Message Store features as defined in section 9.

NOTE: Because the enabler used to provide the Common Message Store may change in future versions of the profile defined in this document (see section 1.1.2), in this version of the profile it is optional for clients to provide an implementation for this requirement.

R8-3-30-4 Availability of Audio Messages from the Chat and Group Chat conversation follows the one defined for File Transfer as required in

section 7, fulfilling requirement R8-3-4. The File Disposition being set to ‘render’ allows the Audio Message to be played directly from the Chat. Requirements R8-3-4-1 and R8-3-4-2 shall be implemented locally on the device.

R8-3-30-5 Requirement R8-3-9 uses status notifications for incoming Audio Messages for incoming File Transfer request as described in section 7.

R8-3-31 R8-3-5 shall be implemented locally on the device.

R8-3-32 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 sections 5, 6 and 7. The duration is retrieved from the <playing-length> element of the File Transfer via HTTP message body as defined in Table 55 of [RCC.07].

R8-3-33 R8-3-6-1 shall be implemented locally on the device via a pre-embedded specific icon associated to the Audio Message.

R8-3-34 R8-3-8 shall be implemented locally on the device.

9 Messaging for Multi-Device

9.1 Description

Multi-device Messaging allows users to view, receive, send and manage their RCS messages, xMS messages and RCS-based content from devices and interfaces other than the mobile device containing the SIM. Examples of secondary devices include, but are not limited to, non-native interfaces on smartphones containing a SIM other than the primary SIM, SIM-based or SIM-less tablets or laptops. The devices may connect using any kind of data connection (e.g. mobile data, Wi-Fi).

For device federation principles, please consult Section 19 “Multi-Device Voice and Video”.

9.2 User Stories and Feature Requirements

NOTE: Because the enabler used to provide the Common Message Store may change in future versions of the profile (see section 1.1.2) and because the Common Message Store is an essential part of multi-device messaging, in this version of the profile it is optional for clients to provide an implementation for the requirements in this section.

US9-1 **As an RCS user, I shall be able to connect to and access my RCS messaging services from all of my RCS-enabled devices and interfaces.**

R9-1-1 There shall be one single primary mobile device for the set of multiple devices belonging to a user. The user shall be addressed through the MSISDN associated with that single primary mobile device.

R9-1-2 The A-Party user shall not be aware that they are communicating with the B party’s primary or secondary device or interface.

R9-1-3 Multi-device features shall be available to all users, including those with only a single interface. This means that, including, but not limited to, when an MNO has deployed Multi Device Messaging, backup and restore may be provided to all their RCS users including those with a primary device only.

R9-1-4 When first connecting to the multi-device service, the user shall be introduced to the concept of multi-device, including the benefits of cloud storage and the ability to access messages, content and contacts from multiple devices.

US9-2 **As an RCS user with multiple RCS-enabled devices and interfaces I shall have available all the RCS messaging features that my service provider offers me on any of my devices or interfaces.**

As an RCS user with multiple devices, I shall always be able to receive communications on my primary device whenever under either cellular but no data coverage or cellular on data coverage regardless of the connectivity state of the secondary device(s) and interface(s)

NOTE: For some services this may mean only receiving a notifications about the waiting content (e.g. notification of incoming File Transfer).

R9-2-1 An RCS user with multiple RCS-enabled devices and interfaces shall be able to perform all of the following actions on all of these online devices and interfaces.

R9-2-1-1 Receive any of the services and any pertaining notifications listed in R9-3-4.

R9-2-1-2 Reply to any of the services listed in R9-3-4.

R9-2-1-3 Create and send any of the services listed in R9-3-4.

R9-2-1-4 Forward, delete and resend any of the services listed in R9-3-4.

R9-2-2 The primary mobile device shall also be able to perform the above actions R9-2-1-1 and R9-2-1-3 when connected to mobile cellular network only (i.e. when not connected to mobile data or Wi-Fi). In this case, it is acceptable that functional limitations of the services apply (e.g. SMS limitations apply to text messages).

NOTE: For some services this may mean only receiving a notification about the waiting content (e.g. notification of incoming File Transfer).

US9-3 **As an RCS user with multiple RCS-enabled devices I shall have access to all my SMS/ MMS (if offered by the MNO), RCS 1-to-1 Messaging, RCS Group Chat messages, message states and RCS-related content (including files and events related to services listed in R9-3-4) from any of my devices and interfaces. As a user, I shall be able to manage all of the above messages and content in the same way on every device and interface (i.e. in the same way as on the primary device).**

R9-3-1 A user's complete set of conversation histories shall be stored on a network repository

NOTE: This is the Common Message Store or CMS.

R9-3-2 This store shall be used for RCS-enabled devices and interfaces to be able to receive up-to-date message and conversation histories.

R9-3-3 All contents on the Common Message Store shall be kept for an MNO-configurable period of time and/or up to a configurable quota size per user.

R9-3-4 A conversation history shall include all events that a user has sent and received during that conversation on any of their devices and/or interfaces. An event can be a message, a piece of content, or a message or content notification associated with any of the following services the user has access to:

R9-3-4-1 SMS,

R9-3-4-2 MMS,

R9-3-4-3 1-to-1 messages,

R9-3-4-4 Group Chat messages,

R9-3-4-5 Geolocations,

R9-3-4-6 vCards,

R9-3-4-7 Audio Messages,

R9-3-4-8 Files.

R9-3-5 All events belonging to and content associated with the services listed in R9-3-4 shall be made available to all of the user's RCS-enabled devices and interfaces. This applies even when these services and events are being managed by another application on the device.

R9-3-6 An RCS user with multiple RCS-enabled devices shall have the messaging services that are available to them on the primary device also available on their secondary devices and interfaces.

R9-3-7 An RCS user with multiple RCS-enabled devices and/or interfaces shall perceive the reception of events belonging to services listed in R9-3-4 to be real time on any device or interface.

R9-3-8 Events (messages, content, and notifications) shall be made available across devices and interfaces so that, for each conversation, the most recent events are updated first.

R9-3-9 In the same way as on a primary device, when File Transfer content is made available to devices and interfaces, the files themselves shall only be downloaded automatically in full when the Auto-Accept parameter value is set to "on". When the Auto-Accept parameter is set to "off", File Transfer events shall be represented by their thumbnails or preview icons, which the user can select in order to trigger the download of that particular file on that device or interface. A "download all" option may be available to trigger the

download of all the content of the displayed conversation history on that device if desired.

US9-4 **As a user, I want to be notified of new messages and content on all of my RCS devices and interfaces in an appropriate way, so as not to be annoyed by repetitive and irritating notifications.**

R9-4-1 An RCS user with multiple RCS-enabled devices and/or interfaces shall receive notifications of new incoming events belonging to services listed in R9-3-4 on all their registered and connected RCS-enabled devices and interfaces if the user is not currently using the conversation thread associated with the new incoming event on any of their devices at that time.

R9-4-2 An RCS user with multiple RCS-enabled devices and/or interfaces who is using a conversation thread (i.e. not timed out) on one device or interface shall not receive notifications for incoming events belonging to that thread on other devices or interfaces.

NOTE: A user is considered to be "using" a conversation thread when they have performed any of the following actions within an agreed pre-defined timeout:

- Opening the thread (including unlocking the device screen and returning to the thread),
- Making any selection within the thread (including opening the message composer, typing, adding content, accepting a file transfer invitation when AUTO-ACCEPT is OFF, opening a received file, sending or deleting a message).

A user is no longer considered to be using the conversation thread when:

- The message thread has been "closed" on that interface (i.e. any other screen is displayed, including the gallery).
- A pre-defined agreed timeout has elapsed after no user activity in that thread. (No user activity means no further input in the conversation thread UI by the user nor navigation within the conversation thread).

A user is not considered to be using a conversation when receiving messages from the other party, placing or accepting a call to another party from the thread, auto-accepting file transfer content, automatic message sending (e.g. SMS fallback, automatic resending), typing/sending/deleting messages directly from a notification without opening the message thread ("quick reply"), joining a group chat.

R9-4-3 An RCS user with multiple RCS-enabled devices and/or interfaces opening and responding to a new incoming event belonging to services listed in R9-3-4 on one of their devices/interfaces shall trigger the clearing of notifications for that same message on their other RCS-enabled devices and interfaces (i.e. if the message is read on one device/interface, it is marked as "read" on other devices and interfaces).

R9-4-4 When an RCS user opens an event or marks it as "read", the event shall be marked as "read" on all other devices and interfaces.

R9-4-5 When an RCS user (A-Party) sends a file (or File Transfer-based event such as an Audio Message) to another RCS user (B-Party) who has multiple RCS-enabled devices and the File Transfer is sent outside of an existing Chat conversation (session), the notification will arrive on all of the B-Party's RCS-enabled devices and/or interfaces which are online.

R9-4-6 When an RCS user (A-Party) transfers a file (or File Transfer based event such as an Audio Message) to another RCS user (B-Party) who has multiple RCS-enabled devices and interfaces inside an existing conversation (session), then the preview icon or file shall arrive on the B-Party's device or interface depending on the Auto-Accept setting (i.e. ON/OFF).

R9-4-7 If an RCS user (A-Party) is using a conversation thread with another RCS user (B-Party) with multiple RCS-enabled devices and the B-Party is using a mobile or cellular-equipped device to chat, it is possible that the B-Party loses their data connectivity. In this case, the conversation shall persist between user A and user B on the B-Party's device following the rules of Seamless Messaging or Delivery Assurance as applicable.

US9-5 **As a user, I want to make sure my participation in Group Chat conversations is consistent across all my RCS devices and interfaces.**

R9-5-1 An RCS user who has chosen to leave a Group Chat on one of their connected devices or interfaces shall stop receiving any further updates from that Group Chat on their other devices and interfaces.

US9-6 **As a user, I want to make sure that deleted content is handled sensitively and appropriately across all my RCS devices and interfaces.**

R9-6-1 Any events associated with services listed in R9-3-4 that are deleted by a user on any of his RCS-enabled devices or interfaces shall also be deleted from the Common Message Store and their other RCS-enabled devices and interfaces.

R9-6-1-1 When deleting an event, the user may be warned that it will also be deleted from their other devices and interfaces. A "don't ask again" prompt may be offered.

R9-6-2 Any content that has been deleted from the Common Message Store by the system (e.g. content expiry) shall not be deleted from any of the user's devices or interfaces.

R9-6-3 Any content deleted or removed from a device or interface that was not explicitly deleted by a user action or consent shall not be deleted from the Common Message Store (nor any other device or interface).

NOTE: SIM swap will not delete locally stored content on the device. Factory reset will not cause deletion on the Common Message Store.

US9-7 **As a user, I want to be able to log in and out of secondary devices and interfaces as I choose. As a user, I want to be able to continue a conversation on a different device or interface from the one I used to start it on.**

R9-7-1 An RCS user with multiple RCS-enabled devices and interfaces shall be able to log out of an identity on a secondary device or interface and another user will be able to log into that device or interface with a different identity.

R9-7-2 An RCS user with multiple RCS-enabled devices or interfaces shall be able to start a messaging conversation (1-to-1 Messaging and/or xMS) from one of their devices / interfaces and continue it from any of their other devices. / interfaces.

R9-7-3 The user shall be able to continue the conversation on another device or interface by opening the messaging thread associated with the conversation they would like to pursue on that device / interface.

US9-8 **As an RCS user, I can have multiple conversations active at the same time using different devices and / or interfaces (e.g. I am chatting to Alice using my mobile, whilst at the same time chatting to Bob using my tablet).**

R9-8-1 It shall be possible for an RCS user A with multiple connected RCS-enabled devices and / or interfaces to have multiple conversations with different Contacts at the same time from the same or from different devices / interfaces.

R9-8-2 Multiple RCS app or RCS web-based interfaces for a user shall be able to run on a device at the same time, for the same or different RCS identities.

NOTE: Limitations can apply when trying to use multiple RCS identities on the same device.

US9-9 **As an RCS user, I want to be able to change specific multi-device settings on any device, and for some settings to be kept up to date on all my devices and interfaces.**

R9-9-1 A user shall be able to change their RCS settings as defined in section 17 on any of their devices and interfaces.

9.3 Technical Information

9.3.1 Overview

In this profile, the multi-device service is limited to messaging service only (i.e. voice and video for multi-device are deferred to next release of the universal profile). The multi-device service offers the following RCS services; 1-to-1 Chat, Standalone Messages, Group Chat, Audio Messaging, Geolocation Push, and File Transfer as defined in this profile. In addition to the supported RCS services, multi-device is using backup, restore, and synchronization features via Common Message Store (CMS) as described in section 4.1 of [RCC.07] and in [RCC.09].The messaging for multi-device technical realisation provided in this section is based on the direct delivery model for CPM session based messaging that is defined in CPM 2.1 and endorsed by [RCC.11], and [RCC.07].

During a session based chat (i.e. 1-to-1 Chat or Group Chat), all the RCS user's registered and connected devices maintain the same conversation view to the user. When a message is received, it is delivered to all connected and registered devices at the same time. When a message is sent from any of the connected devices, it is sent to all other connected devices with direction indication that it is a sent message. Offline devices with the exception of the

primary device which is reachable via cellular, during a session based chat will not receive any notification. When an offline device comes online (i.e. becomes a registered and connected device) during a session based chat, it will synchronise with CMS to receive missed messages. The primary device, which is only reachable via cellular connectivity, will receive CPM based messages as xMS via network interworking. When primary device is offline, it is unaware of the messages sent by other devices. Devices which missed the CPM session based conversation, will receive the conversation via CMS synchronisation or via xMS for the primary device only in cellular coverage.

Similar to the single device case, two mechanisms can be used for Capability Discovery; SIP Options and Presence Capability Discovery. The Capability Discovery mechanism shall be configured as mentioned in section 3.

- SIP Options Capability Discovery: Two technical realisations, either without SIP Options Application Server or with SIP Options Application Server as described in section 2.6.1.1.5 of [RCC.07]. SIP OPTIONS Application Server is recommended to be used for multi-device messaging.

- Presence Capability Discovery: The capabilities of each of the user's devices are announced in a Presence Document that is published by using SIP PUBLISH as defined in section 2.6.1.2.2 of [RCC.07]. The Presence Server shall perform aggregation policy based on the rules identified in section 5.5.3.2.1 of [OMA PRS_TS] and section 6.1.3 of [OMA PDE v1.4].

NOTE: It is assumed that the client when configured for Single or Dual Registration (based on the valued of the RCS VOLTE SINGLE REGISTRATION client configuration parameter) maintains the RCS registration regardless of the user activity. It is for further study whether Dual Registration clients and secondary devices may use alternative delivery transports and consequently adopt more efficient connection models that take user activity into account. In that case, the impact on the technical procedures of this section will need to be assessed.

9.3.2 Technical Implementation of User Stories and Service Requirements

R9-10-1 R9-1-1 shall be realised as described in section 2.11 of [RCC.07] and section 2.5 of [RCC.14]. The shared user identity shall be the MSISDN of the primary device, and all the secondary device(s) shall use this identity.

R9-10-2 For R9-1-2 the device, either primary or secondary, shall announce its unique identity to its home network using sip.instance or GRUU as in section 2.11.2 of [RCC.07], and the home network shall ensure that the device identity is not passed to the other party.

R9-10-3 For R9-1-3 the multi-device features described in the overview section are available to the user per [RCC.07]. Multi-device features available to single interface are based on the technical realisation as explained in the appropriate section of single device RCS service in this document. Multi-device and single device shall also support messaging backup and restore via CMS as defined in section of 4.1 of [RCC.07].

R9-10-4 For R9-1-4 introduction message describing the benefits of multi-device features shall be provided by the operator as described in section 2.3.1.2.

R9-10-5 For R9-2-1 including its sub-requirements multi-device for Chat, Group Chat, Geolocation Push, Audio Messaging, and File Transfer shall be realised based on the direct delivery model to all the registered and connected RCS clients. The client shall use direct delivery procedures as given in the following sections:

- section 8.2.2.1 of [RCC.11] for CPM session invitation
- section 8.3.2.1 of [RCC.11] for handling CPM session responses and multiple MSRP media streams
- section 8.6.1 of [RCC.11] for procedures upon receiving MSRP
- section 8.6.2 of [RCC.11] for procedures upon sending MSRP

R9-10-6 R9-2-2 can be fulfilled as described in the below two scenarios:

1. For the multi-device user to reply a message from a primary device that is not connected to mobile data or Wi-Fi, the primary device shall fall-back as described in section 5. The xMS messages shall be stored in the CMS as specified in section 4.1.4 of [RCC.07] in order to provide synchronisation capability for other connected and registered multi-device.
2. For the multi-device user to receive a message in a primary device that is not connected to mobile data or Wi-Fi, the CPM Participating Function shall perform network interworking and deliver the SMS message to the primary device based on the procedures specified in section 8.3.1 of [RCC.11] for CPM Standalone Messages, and section 8.3.2 of [RCC.11] for CPM Session based messaging. Delivery policies in terminating network CPM Participating Function and interworking results shall follow the procedures specified in section 8.3.6 and section 8.3.7 of [RCC.11].

R9-10-7 R9-3-1, R9-3-2, R9-3-3, R9-3-4 are realised by the use of Common Message Store (CMS) as realised in section 4.1 and 4.1.4 of [RCC.07] and the synchronisation of multi-device as described in section 4.1.6.8 of [RCC.07]. The storage folder and objects for the RCS services and legacy messages can be technically realised as in section 5.2 of [RCC.09]. The RCS client and server procedures of CMS can be technically realised as described in section 6 and 7 of [RCC.09].

The quota size per user in the CMS is configured per operator policy.

R9-10-8 R9-3-5 shall be fulfilled as described for R9-3-1, R9-3-2, R9-3-3, R9-3-4. When these events are being managed by another application on the device, only one RCS application shall be active at time. When the user switches to another application, that application will synchronise with CMS.

R9-10-9 R9-3-6 shall be fulfilled by the operator authorising the use of equivalent services on the secondary devices. For example, a secondary device may

receive incoming xMS as Standalone Messages or via CMS, and may send xMS as Standalone Messages.

R9-10-10 R9-3-7 shall follow the technical realisation of R9-2-2 and R9-2-1 including their sub-requirements and requirements R9-3-1, R9-3-2, R9-3-3, R9-3-4. The client synchronisation triggers are specified in section 4.1.6.8 of [RCC.07]. When a user opens a conversation thread, the client shall give priority to synchronise that thread.

R9-10-11 R9-3-8 shall be realised based on section 4.1.6.8 of [RCC.07].

R9-10-12 R9-3-9 shall be realised using the client configuration parameter FT AUTO ACCEPT as mentioned in section 3.5.4.8.3.2.1 of [RCC.07]. A Common File Store for File Transfer via HTTP in section 4.1.4.9 of [RCC.07] shall be required as realisation for File Transfer Contents e.g. copy of the thumbnail and content URL links. A “download all” option can be realised by locally implementation in the device to trigger the download of all the content history for that particular device from the content server.

R9-10-13 For R9-4-1, the technical realisation for R9-2-1 applies.

NOTE: Newly registered and connected device may not automatically join the existing CPM session.

R9-10-14 For R9-4-2, when the user is using the conversation thread on one device, all devices shall follow the display notifications and events in the event reporting framework as specified in section 4.1.4.8 of [RCC.07] to determine whether there is activity on the other devices. This means that Participating Function shall forward the events from the event reporting framework to other connected devices. In addition the client shall consider sent messages and istyping notifications as indication of such activity. In case of a user is using a primary device and receiving SMS message (i.e. primary device is not connected to RCS platform), there will be no display notification sent to the Participating Function from this primary device. The other multi-devices belonging to the user may show this message as a new message. When the user is no longer considered to be using the conversation thread, all the devices shall follow the technical realisation of R9-4-1.

R9-10-15 R9-4-3 shall be fulfilled based on R9-4-2.

R9-10-16 R9-4-4 is realised as described in the technical realisation for R9-4-3.

R9-10-17 R9-4-5 and R9-4-6 shall be realised by following section 3.5.4.8 of [RCC.07] and section 4.1.4.9 of [RCC.07]. Direct delivery model is used to send link to all connected and registered devices as R9-2-1. The multi-device “automatic download” option can be realised using the client parameter FT AUTO ACCEPT per R9-3-9 implementation.

R9-10-18 R9-4-7 When B-party loses the data connectivity, the communication between A party and B-Party (multi-device) shall continue using the fall-back mechanism for the primary device that lost data connection as defined in section 5, via Network Interworking in the B-Party network, the CPM Participating Function shall perform network interworking and deliver xMS

message to the primary device that lost data connectivity based on the procedures identified in R9-2-2.

R9-10-19 R9-5-1 is covered as described in section 3.4.4.1.3.1, section 3.4.4.1.3.2 of [RCC.07], and section 8.2.2.3 of [RCC.11]. For offline devices that come back online, the client shall receive an error as specified in section 9.2.4 of [RCC.11].

- Devices that are online and participating in the session at the time of client departure will receive a SIP BYE request with a Reason Header filed with the protocol set to SIP and the reason code to 200.
- There is no technical solution for an indication of the "departed" status to clients in RCS 6.0 via the Common Message Store. Implementations may add a Group State Object to the conversation folder of the Group Chat with an empty value of the attribute "lastfocussessionid".

R9-10-20 R9-6-1 shall be realised per section 4.1.4.8, 4.1.6.6, and 4.1.6.8 of [RCC.07].

R9-10-21 R9-6-1-1 shall be realised locally on the device (both primary and secondary device(s)).

R9-10-22 R9-6-2 shall be realised locally on the device (both primary and secondary devices) based on the information from the CMS synchronisation as described in the last paragraph of section 4.1.6.8 of [RCC.07] i.e. the message is no longer in the CMS and the client wasn't aware that the \deleted' flag had been set.

R9-10-23 R9-6-3 shall be realised by the device not setting the '\Deleted' flag for messages that the user did not intend the delete.

R9-10-24 R9-7-1 shall be locally implemented in the secondary device.

R9-10-25 R9-7-2 shall be realised following the procedures specified in section 2.11.3, 3.2.1.1, 3.4.4.1.7, 3.4.4.1.8 and 3.12.4.2.2.2 of [RCC.07] and [RCC.11]. This requirement also has dependency on R9-1-2.

R9-10-26 For R9-7-3 this requirement shall follow the technical realisation of R9-2-1, R9-2-2, R9-3-1, R9-3-2, R9-3-3, R9-3-4 and R9-7-4.

R9-10-27 R9-8-1 shall be realised using the same procedures as a single device case with the additional requirement that all devices shall include the +sip.instance feature tag in the Contact header field with the same instance identifier value used at registration in any non-REGISTER SIP requests and responses. There is also dependency on local implementation on the device to allow a user to participate in more than one chat session at a time.

R9-10-28 R9-8-2 shall be realised locally on the device. For the primary device, only one client using the common identity shall be active at a time per the procedure in section 2.2.3.

R9-10-29 R9-9-1 shall be locally implemented in the device. Setting changes are based on per device basis.

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/ Voice over Long Term Evolution (VoLTE) devices under various coverage conditions delivered through VoLTE, Wi-Fi Calling and CS voice calling services.

This section describes the User Stories and Service Requirements for the Green Button Promise for Voice Call services and all features around that core.

10.2 User Stories and Feature Requirements

US10-1 **As a user, I want one single entry point to voice calling 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 for voice shall not indicate which voice service will be used to enable the call.

US10-2 **As a user, I 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 MNO specific voice call performance criteria (e.g. call drop rates, successful call setup rates).

R10-2-2 When there is end-to-end support of high definition voice codecs, the voice call shall be delivered with high-quality audio.

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 MNO specific Wi-Fi Calling performance criteria (e.g. call drop rates, successful call setup rates).

R10-3-3 When there is 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 Wi-Fi Calling on my network.**

R10-4-1 The device shall be configured by the network to enable or to / disable the Wi-Fi Calling service per user.

R10-4-2 In case of concurrent availability of voice services fulfilling same performance criteria it shall be up to MNO specific implementation which voice call enabler to use.

US10-5 **As a service provider, I want the user to be able to turn on or turn off Wi-Fi Calling manually.**

R10-5-1 If Wi-Fi Calling is supported by the service provider and Wi-Fi Calling is configured on the device, a Wi-Fi Calling switch in the phone settings shall be visible to allow the user to turn on or turn off Wi-Fi Calling.

R10-5-2 The default position of the Wi-Fi Calling switch shall be based on MNO configuration (ON or OFF).

R10-5-3 If a service provider does not support Wi-Fi Calling, no such Wi-Fi Calling switch shall be shown to the user on the device.

R10-5-4 The user shall be able to manually deselect a Wi-Fi connection from providing Wi-Fi Calling.

US10-6 **As a service provider, I may want to provide emergency call services even if Wi-Fi Calling is being used as the last resort for voice call connectivity.**

R10-6-1 Emergency call services shall always use a cellular voice call where available (including potential national roaming if required by local regulators).

R10-6-2 Emergency call services may use the Wi-Fi connection if no cellular connection is available at the moment the emergency call is placed.

US10-7 **As a service provider, I may want to allow supplementary services both for voice calls on cellular and over a Wi-Fi connection like Calling Line Identification Presentation (CLIP), Call Waiting (CW), Call Hold, Call Forward Busy (CFB), Call Forward Unreachable and Call Forward No Reply.**

R10-7-1 Supplementary Services like CLIP, CW, Call Hold, CFB, Call Forward Unreachable and Call Forward No Reply may be offered by a service provider during any voice call independent of the actual voice service used.

US10-8 **As a user, I want to use Dual Tone Multi-Frequency (DTMF) tones during calls both on cellular and over a Wi-Fi connection.**

R10-8-1 DTMF should be supported during a call over both on cellular and over the Wi-Fi connection in both the sender‘s and receiver’s experience.

US10-9 **As a user, I want to know which connection (Cellular or Wi-Fi) is used for the voice call.**

R10-9-1 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.

R10-9-2 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.

US10-10 **As a user, I want my voice call to continue in case of connectivity change.**

R10-10-1 The terminal shall support call continuity from Long Term Evolution (LTE) to non-LTE connectivity situations and vice versa in cases where LTE connectivity is not available.

R10-10-1-1 This shall be configurable by the MNO.

R10-10-2 The terminal shall support call continuity from Wi-Fi to LTE and vice versa where LTE connectivity is available.

R10-10-3 The terminal shall support call continuity from Wi-Fi to non-LTE connectivity situations and vice versa.

R10-10-3-1 This shall be configurable by the MNO.

US10-11 **As a user not engaged in another ongoing call, I want to have the same options to react to an incoming call independent of the enabling voice service used.**

R10-11-1 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.

US10-12 **As a user engaged in another ongoing call provided by the network, I want to have the same options to react to an incoming call independent of the enabling voice service used.**

R10-12-1 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.

US10-13 **As users in a voice call, we want to be able to mute (and unmute) our own voice (i.e. mute microphone) at any point during the call without interrupting the call.**

R10-13-1 Each user in a Voice Call shall be able to mute (and unmute) their own live audio at any point during the call.

US10-14 **As a user, I want to see each of my voice calls listed in my device's activity and/or call log regardless of the voice service actually used for the call.**

R10-14-1 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.

R10-14-2 Visual differentiation in the call logs between CS / VoLTE calls and Wi-Fi calls shall be provided. It shall be up to the MNO to enable or disable the differentiator.

R10-14-2-1 For calls that changed the bearer during a call, the above visual indication shall be provided for the bearer that was used at the time the call was initiated.

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].

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 profiles of the 3rd Generation Partnership Project (3GPP) Multimedia Telephony service taking access specific differences into account. The clients are expected to support the common set of procedures and the access specific functions described in [PRD-IR.92] and [PRD-IR.51].

Traditional CS voice services are delivered on 2G/3G networks.

RCS IP Voice call is not supported for primary devices.

10.3.2 Configuration parameters

To provide the required MNO control of the Green Button Promise for Voice behaviour, the following parameter is added to those that are available in [RCC.07], [RCC.14] and [RCC.15]:

Configuration parameter	Description	RCS usage
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 (defined in A.1.12 and A.2.1 of [RCC.07]) or PROVIDE IR51 VIDEO (defined in A.1.12 and A.2.1 of [RCC.07]) is set to 1.

CALL LOGS BEARER DIFFERENTIATION	This parameter is applicable when PROVIDE IR51 VOICE is set to 1 and it controls the display of call logs bearer differentiation between cellular service (CS call /IR.92 voice/IR.94 conversational video service) and IR.51 voice/ conversational video service. 0 (default), the display of the call logs between cellular service and IR.51 voice/conversational video service is not differentiated. 1: the display of the call logs for service initiated as cellular service and for service initiated as IR.51 voice/conversational video service is differentiated.	Optional parameter

Table 41: Additional Configuration Parameters to control Green Button Promise for Voice behaviour

The IR51 SWITCH UX and CALL LOGS BEARER DIFFERENTIATION parameters are added to the UX tree defined in section 5.3.7 with the following formal definition:

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
Required	ZeroOrOne	Int	Get, Replace

Table 42: UX MO sub tree addition parameters (IR51SwitchUX)

- Values:
  0 (default value) Wi-Fi switch for IR.51 voice and conversational video services is not visible to the user

  i. Wi-Fi switch for IR.51 voice and conversational video services is visible to the user with default position set to OFF
  ii. 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: The client shall take the potentially changed value into account for displaying Wi-Fi switch position to the user or not.
- Associated HTTP XML characteristic type: “IR51SwitchUX”

Node: /<x>/UX/callLogsBearerDiffer
Leaf node that describes whether the display of the call logs is differentiated between cellular (CS call/IR.51 voice/IR.94 conversational video service) and IR.51 voice/ conversational video service.

If not instantiated, the display of the call logs is not differentiated between cellular service and IR.51 voice/conversational video service.

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

Table 43: UX MO sub tree addition parameters (callLogsBearerDiffer)

- Values:
  0 (default value): the display of the call logs between cellular service and IR.51 voice/conversational video service is not differentiated.

  1: the display of the call logs for service initiated as cellular service and for service initiated as IR.51 voice/conversational video service is differentiated.
- Post-reconfiguration actions: The client shall take the potentially changed value into account for displaying differentiated call logs between cellular service and IR.51 voice/conversational video service to the user or not.
- Associated HTTP XML characteristic type: “callLogsBearerDiffer”

The representation of the parameter in the UX tree and the associated HTTP configuration XML structure with this parameter are shown in section 5.3.7.

10.3.3 Technical Implementation of User Stories and Service Requirements

R10-15-1 Requirements R10-1-1 and R10-1-2 shall be implemented locally on the device.

R10-15-2 The implementation details to meet the key performance criteria of the voice service defined in Requirement R10-2-1 are left to the discretion of the service provider.

R10-15-3 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].

R10-15-4 For requirement R10-3-1, both “trusted Wi-Fi” and “untrusted Wi-Fi” connections shall be implemented based on procedures defined in [PRD-IR.51].

R10-15-5 The implementation details to meet the key performance criteria of the voice service defined in requirement R10-3-2 are left to the discretion of the service provider.

R10-15-6 For requirement R10-3-3, section 3 of [PRD-IR.51] shall apply

R10-15-7 Requirement R10-4-1 shall be fulfilled by configuring the PROVIDE IR51 VOICE parameter defined in sections A.1.12 and A.2.1 of [RCC.07].

R10-15-8 Requirement R10-4-2 is fulfilled based on service provider policy.

R10-15-9 Requirements R10-5-1, R10-5-2 and R10-5-3 shall be fulfilled based on the PROVIDE IR51 VOICE parameter defined in sections A.1.12 and A.2.1 of [RCC.07] and IR51 SWITCH UX parameter defined in section 10.3.2.

R10-15-10 The requirement R10-5-4 shall be implemented locally on the device.

R10-15-11 For requirements R10-6-1 and R10-6-2 section 5.3 of [PRD-IR.51] applies.

R10-15-12 Requirement R10-7-1 shall be fulfilled based on the technical procedures described in section 2.3 of [PRD-IR.92] and section 2.3 of [PRD-IR.51]. In addition Annex A.4 of [PRD-IR.92] applies.

R10-15-13 Requirement R10-8-1 shall be fulfilled based on the technical procedures described in section 3.3 of [PRD-IR.92].

R10-15-14 Requirements R10-9-1 and R10-9-2 shall be implemented locally on the device.

R10-15-15 For requirement R10-10-1 Annex A.3.2 of [NG.102] and 2.2 of [PRD-IR.92] apply.

NOTE: Single Radio Voice Call Continuity (SRVCC) is only defined for moving from LTE to non LTE radio access. During a voice call there will not be a handover from non LTE to LTE access.

R10-15-16 For requirement R10-10-2section 2.18 of [NG.102] shall apply.

R10-15-17 For requirement R10-10-3 Annex A.3.1 of [NG.102] and Annex A.2 of [PRD-IR.51] apply.

R10-15-18 Requirement R10-11-1 shall be implemented locally on the device. For the call termination procedures, for multimedia telephony section 2.2.4 of [PRD-IR.92] and section 2.2.4 of [PRD-IR.51] shall apply. For CS telephony [3GPP TS 24.008] shall apply.

R10-15-19 Requirement R10-12-1 shall be implemented locally on the device. For the call establishment and termination procedures, for multimedia telephony section 2.2.4 of [PRD-IR.92] and section 2.2.4 of [PRD-IR.51] shall apply. For CS telephony [3GPP TS 24.008] applies. For the Communication Hold and the Communication Waiting service, section 2.3 and Annex A.8 of [PRD-IR.92] and section 2.3 of [PRD-IR.51] shall apply.

R10-15-20 Requirement R10-13-1 shall be implemented locally on the device.

R10-15-21 Requirement R10-14-1 shall be implemented locally on the device.

R10-15-22 Requirement R10-14-2 shall be implemented by configuring the CALL LOGS BEARER DIFFERENTIATION parameter defined in section 10.3.2.

11 Green Button Promise for IP Video Call Services

11.1 Description

IP Video calling is an important feature to evolve the Operator calling experience. IP 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 IP Video Call services and all features around that core delivered through ViLTE [PRD-IR.94], Wi-Fi Calling [PRD-IR.51], and RCS IP Video Call [RCC.07].

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 12.6.2 of this document.

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 such a call is possible.

R11-1-2 The IP Video Call shall offer lip sync experience.

R11-1-3 If there are multiple video call services available, the service that provides the higher voice quality (stability and audio quality) shall prevail.

R11-1-4 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 is not offered as part of this one-button experience.

R11-1-5 The entry point to initiate an IP Video Call shall not indicate the enabling IP Video Call service.

US11-2 **As a service provider, I want to configure the availability of the IP Video Call service depending on the different cellular data bearer conditions.**

R11-2-1 It shall be able to configure the availability of the IP Video Call service based on the different cellular data bearers.

US11-3 **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.**

R11-3-1 IP Video Calls shall be possible through a Wi-Fi connection offered by the service provider or via a third party trusted by the service provider as well as any other Wi-Fi connection of the device.

US11-4 **As a service provider, I want the Wi-Fi Video Calling service to be linked with the availability and configuration settings for Wi-Fi (Voice) Calling.**

R11-4-1 The support for Wi-Fi Video Calling shall be linked with the availability and configuration settings for Wi-Fi (Voice) Calling as defined in 'Green Button Promise for Voice', section 10.

US11-5 **As a user, I (i.e. user A) want to know if I can video call user B.**

R11-5-1 The IP Video Call service shall follow procedures described in section 3, Capability Discovery and Service Availability.

R11-5-2 If the A-Party device does not provide a camera (hardware limitation), the IP Video Call service is not available.

US11-6 **As a user receiving an incoming IP video call, I (i.e. user B) want to decide whether to:**

a) **Reject the entire call, or**

b) **Accept the call with transmitting my camera view.**

R11-6-1 The receiver shall be able to accept or reject an incoming IP Video Call.

R11-6-2 If the receiving device does not provide a camera (hardware limitation), a video call capability shall never be reported for capability exchange or service availability updates.

R11-6-3 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).

US11-7 **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.**

R11-7-1 The incoming call screen shall show to the user that the incoming call is a video call.

R11-7-2 The B-Party shall be informed of any video calls they have missed. The notification shall clearly show that the missed call is an IP Video Call.

US11-8 **As a user in an IP Video Call, I want my video call to continue in case of connectivity change.**

R11-8-1 If connectivity changes from LTE to non-LTE (i.e. still on cellular connectivity) and thus IP video call continuity cannot be maintained, the call shall continue as a Voice Call while the user under changing connectivity should be offered to manually start a “live video” share if available.

NOTE 1: Existing flows for initiating and accepting “live video” shall be followed as specified in section 12.

NOTE 2: When downgrading IP Video Call to a Voice Call all Voice Call requirements are applicable as described in section 10, Green Button Promise for Voice.

R11-8-2 The terminal shall support video call continuity from Wi-Fi to LTE and vice versa where LTE coverage is available.

US11-9 **As a service provider, I want the best possible quality of video available to the user throughout the IP Video Call for the radio bearer the user is on.**

R11-9-1 An IP Video Call shall be delivered at the highest video quality that the radio bearer allows.

R11-9-2 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.

R11-9-3 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.

US11-10 **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.**

R11-10-1 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.

US11-11 **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.**

R11-11-1 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.

R11-11-2 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.

R11-11-3 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.

US11-12 **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.**

R11-12-1 Each user in an IP Video Call shall be able to mute (and unmute) their own live audio at any point during the call.

US11-13 **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.**

R11-13-1 The device shall handle the different orientation permutations depending on how the device is rotated during an IP Video Call.

R11-13-2 When rotating the device, the video’s aspect ratio shall be maintained.

US11-14 **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.**

R11-14-1 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.

R11-14-2 If the phone supports two cameras, the front facing camera shall be activated by default when the video transmission is started.

US11-15 **As a user, I want to know which connection (Cellular or Wi-Fi) is used for the IP Video call.**

R11-15-1 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 IP Video calls.

R11-15-2 The indication to show that a Wi-Fi bearer is used or going to be used for the IP video call should be similar to or consistent with the one used for indicating when a Wi-Fi bearer is used or is going to be used for voice calling.

R11-15-3 During an on-going IP Video 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 video and voice call quality.

NOTE: The criteria to decide whether the video and voice quality is acceptable is left to the implementation.

US11-16 **As a service provider, I may want to allow supplementary services during IP Video Calls when another (voice/video) call comes in like CLIP, CW, Call Hold, CFB, Call Forward Unreachable, and Call Forward No Reply**

R11-16-1 Supplementary Services like CLIP, CW, Call Hold, CFB, Call Forward Unreachable, and Call Forward No Reply may be offered by a service provider during an IP Video Call.

US11-17 **As a user, I want to see my (initiated and received) IP video calls in my call logs similar to any other voice call.**

R11-17-1 The IP Video Call must be displayed in the single (voice AND video) call log interface (per contact or global call log).

R11-17-2 In that single log of the user's device, an IP Video Call shall be differentiated with a specific visual reference from a voice call.

R11-17-3 Similar to voice call events, video call events (i.e. not added in-call) shall be differentiated between outgoing and incoming and for incoming whether it was an answered, unanswered or missed video call.

R11-17-4 Visual differentiation in the call logs between an IP Video Call over cellular and over Wi-Fi shall be provided. It shall be up to the MNO to enable or disable the differentiator.

R11-17-4-1 For calls that changed the bearer during a call, the above visual indication shall be provided for the bearer that was used at the time the call was initiated.

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 section 3.9 of [RCC.07].

The three technical enablers shall co-exist based on procedures defined in section 3.9 of [RCC.07].

The RCS IP Video Call service can be used only when the establishment of end to end IR.94/IR.51 conversational video service is not possible.

The three technical enablers for conversational video services shall interact based on the following definitions:

- Capability discovery: If the result of the exchange is that IR.94/IR.51 Conversational Video is supported in one end and RCS IP Video Call is supported in the other, the IP Video Call shall be available to both ends.
- Service initiation and acceptance: An IR.94/IR.51 Conversational Video-only device 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

R11-18-1 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.

R11-18-2 Requirement R11-1-2 is fulfilled based on used technical enablers (as per section 11.3.1 of this document).

R11-18-3 Requirement R11-1-3 is fulfilled based on the used technical enablers for video (as per section 11.3.1 of this document).

R11-18-4 Requirements R11-1-4 and R11-1-5 shall be implemented locally on the device.

R11-18-5 For requirement R11-2-1, 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.1.12 and A.2.1 of [RCC.07]. RCS IP Video call is available in cellular access if Voice over LTE/Voice over Wi-Fi is not enabled on the device. The service provider is able to configure the availability of RCS IP Video call in this case via the parameter PROVIDE RCS IP VIDEO CALL defined in Annex A.1.12 and A.2.1 of [RCC.07].

R11-18-6 For requirement R11-3-1, both “trusted Wi-Fi” and “untrusted Wi-Fi” connections shall be implemented based on procedures defined in [PRD-IR.51].

R11-18-7 Requirement R11-4-1 is fulfilled based on the PROVIDE IR51 VIDEO parameter defined in Annex A.1.12 and A.2.1 of [RCC.07].

R11-18-8 For requirement R11-5-1 section 3.3 of this document shall apply.

R11-18-9 Requirement R11-5-2 shall be implemented locally on the device.

R11-18-10 Requirement R11-6-1 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 3.9.4 of [RCC.07] shall be considered.

R11-18-11 Requirements R11-6-2 and R11-6-3 shall be implemented locally on the device.

R11-18-12 Requirements R11-7-1 and R11-7-2 shall be implemented locally on the device.

R11-18-13 For requirement R11-8-1 Annex A.3.2 of [NG.102] applies. RCS Video Share service initiation for the case that IP Video call continuity cannot be maintained shall be implemented locally on the device. There is no service continuity for RCS IP Video call on connectivity change.

R11-18-14 For requirement R11-8-2, section 2.18 of [NG.102] shall apply.

R11-18-15 Requirement R11-9-1 shall be fulfilled based on section 3 of [PRD-IR.94], 2.4 and 3 of [PRD-IR.51] and 3.9.4.1 of [RCC.07].

R11-18-16 For requirement R11-9-2, for IR.94/IR.51 conversational video service section 3.3 of [PRD-IR.94] shall apply. For RCS IP video call section 3.9.4.1 of [RCC.07] shall apply.

R11-18-17 For R11-9-3, technical procedures are not defined.

R11-18-18 Requirement R11-10-1 shall be implemented locally on the device.

R11-18-19 The user story US11-11 is not applicable for RCS IP Video call in accordance with the definitions in section 3.9.4.1 of [RCC.07]. For IR.94/IR.51 conversational video services the following applies:

R11-18-20 Requirements R11-11-1 and R11-11-3 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 2.2.4 of [PRD-IR.51].

R11-18-21 Requirement R11-11-2 shall be implemented locally on the device.

R11-18-22 Requirement R11-12-1 shall be implemented locally on the device.

R11-18-23 For requirement R11-13-1, for IR.94 conversational video section 2.4.2 of [PRD-IR.94] shall apply. For IR.51 conversational video service, section 2.4.4 of [PRD-IR.51] shall apply. For RCS IP Video Call section 3.9.4.1 of [RCC.07] applies.

R11-18-24 Requirement R11-13-2 shall be implemented locally on the device.

R11-18-25 Requirements R11-14-1 and R11-14-2 shall be implemented locally on the device.

R11-18-26 Requirements R11-15-1, R11-15-2 and R11-15-3 shall be implemented locally on the device.

R11-18-27 For requirement US11-16 section 2.3 of [PRD-IR.94] shall be taken into consideration for Video over LTE and section 2.3 of [PRD-IR.51] for EPC-integrated Wi-Fi. For RCS IP Video call section 3.9.4.1 of [RCC.07] shall be taken into consideration.

R11-18-28 Requirements R11-17-1, R11-17-2 and R11-17-3 shall be implemented locally on the device.

R11-18-29 Requirement R11-17-4 shall be implemented by configuring the CALL LOGS BEARER DIFFERENTIATION parameter defined in section 10.3.2.

12 Enriched Voice Calling

12.1 Description

The Enriched Voice Calling service evolves the current voice call experience throughout all phases of a voice call: before, during and after the voice call.

Enriched Voice Calling covers the following functional areas:

- **Pre-call experience**: Enrichment of the voice call before the voice call is started. A calling user can “compose” and share content that the called party sees when receiving the voice call.
- **In-call experience**: Enrichment of the voice call during the voice call. Either party can share content during a voice call.
- **Post call experience**: Enrichment in case a voice call could not be connected. A calling party can “compose” additional information that will be included with the missed call information on called party’s device when a call remains unanswered.

These features are to be provided only with Voice Services as described in “Green Button Promise for Voice”, section 10 of this document.

12.2 General

US12-1 **As an MNO, I want to select the enriched calling functional areas I offer to my customers.**

R12-1-1 The MNO shall be able to provide Enriched Calling Pre-call features.

R12-1-2 The MNO shall be able to provide Enriched Calling In-call features.

R12-1-3 The MNO shall be able to provide Enriched Calling Post-call features.

NOTE: The Enriched Calling functional areas (as listed above) can be provided by the MNO independently of each other as required.

12.3 Technical Information for the General Requirements

R12-1-4 In order for the Service Provider to enable the Enriched Calling Pre-Call features they shall set the value of the COMPOSER AUTH configuration parameter (see sections A.1.6 and A.2.1 of [RCC.07]) to 1.

R12-1-5 In order for the Service Provider to enable Enriched Calling In-call features they shall configure each service separately:

R12-1-5-1 For “Live Video”, in order the Service Provider to enable end to end IR.94/IR.51 conversational video call, it shall set:

- For Video over LTE, the value of the PROVIDE IR94 parameter to 1 (see sections A.1.12 and A.2.1 of [RCC.07]). This will enable both “Live Video” experience and initiating a Video Call “from scratch” experience.

- For Video over EPC- integrated Wi-Fi, the value of the PROVIDE IR51 VOICE parameter (see sections A.1.12 and A.2.1 of [RCC.07]) and the value of the PROVIDE IR51 VIDEO parameter (see sections A.1.12 and A.2.1 of [RCC.07]) shall be set to 1. This will enable both “Live Video” experience and initiating a Video Call “from scratch” experience.
- For RCS Video Share service, the value of the PROVIDE VS parameter (see sections A.1.6 and A.2.1 of [RCC.07]) shall be set to 1. This will enable “Live Video” experience.

R12-1-5-2 For sharing any file, in order the Service Provider to enable RCS File Transfer service it shall set correctly the values of the FT HTTP CS URI, FT HTTP CS USER and FT HTTP CS PWD parameters (see sections A.1.5 and A.2.1 of [RCC.07]). This will enable both in-call and outside of a call File Transfer experience.

R12-1-5-3 For exchanging messages, in order the Service Provider to enable 1-to-1 messaging it shall enable one of the acceptable options of messaging technologies as specified in section 5.3. This will enable both in-call and outside of a call messaging experience.

R12-1-5-4 For Location Push, in order the Service Provider to enable RCS Geolocation Push service it shall set the PROVIDE GEOLOC PUSH parameter (see sections A.1.8 and A.2.1 of [RCC.07]) to 1. This will enable both in-call and outside of a call RCS Geolocation Push service. When the messaging service is used to carry the location information, the Service Provider shall enable one of the acceptable options of messaging technologies as specified in section 5.3. This will enable both in-call and outside of a call messaging for sending location information experience.

R12-1-5-5 For live sketch on an image, in order the Service Provider to enable Shared Sketch service it shall set the SHARED SKETCH AUTH parameter (see sections A.1.6 and A.2.1 of [RCC.07]) to 1. This will enable in-call experience.

R12-1-5-6 For live sketch on a map, in order the Service Provider to enable Shared Map service it shall set the SHARED MAP AUTH parameter (see sections A.1.6 and A.2.1 of [RCC.07]) to 1. This will enable in-call experience.

R12-1-6 In order for the Service Provider to enable the Enriched Calling Post-Call features they shall set the value of the POST CALL AUTH configuration parameter (see sections A.1.6 and A.2.1 of [RCC.07]) to 1

12.4 User Stories and Feature Requirements for the Enriched Pre-call experience

This section describes the requirements for the Pre-call Call Composer. For all user stories and requirements listed below, it is assumed that the A-Party is Enriched Voice Calling enabled and online (unless otherwise specified). It is acknowledged that the detailed UX design will vary across implementations. The Enriched Calling UI should conform to the native device design approach to present a consistent experience to users.

US12-2 **As a user (A-Party), I want to be able to place a voice call without the need for sharing pre-call content.**

R12-2-1 All voice call entry points remain the same (i.e. no additional enriched voice calling content sharing steps are required to make a non-enriched voice call).

US12-3 **As a user (B-Party), I want to receive and immediately accept or reject voice calls when Pre-Call content is available.**

R12-3-1 The incoming voice call entry point remain the same (i.e. no additional enriched voice calling content sharing steps are required) to accept or reject any incoming call with a single selection, irrespective of any pre-call content being available on the incoming call screen.

US12-4 **As a user (A-Party), I want to provide the B-Party with additional enriched voice calling content.**

R12-4-1 The A-Party shall have the option to share Pre-call content with B-Party.

R12-4-2 The sharing of Pre-call content shall only be available for 1-to-1 voice calls.

R12-4-3 The sharing of Pre-call content shall not be available for IP Video calls.

R12-4-4 For available Enriched Calling capable contacts, the following service entry points for Pre-call services are offered:

R12-4-4-1 The dialler shall offer access to pre-call features for Enriched Calling capable contacts stored in the address book.

R12-4-4-2 The dialler shall offer access to pre-call features when the user manually enters entering an Enriched Calling capable number.

R12-4-4-3 The address book (e.g. contact card, quick contact view) shall offer access to pre-call features.

R12-4-4-4 The call log, when selecting a specific call event shall offer access to pre-call features.

R12-4-4-5 The 1-to-1 messaging conversation view may offer access to pre-call features.

R12-4-5 The following Pre-call content share shall be supported:

R12-4-5-1 Important Call Indicator: an indicator that identifies to the B-Party that the voice call is of high importance.

R12-4-5-2 Pre-call Subject: a message defined by the A-Party, either entered as free text (limited to 1 to 60 characters), or selected from a list of pre-defined subjects.

NOTE: Emoji's (as defined in Annex A.3 of this document) are supported in the Pre-call Subject.

R12-4-5-3 Pre-call Image: an existing image selected from the device gallery, or a new picture taken with the device camera.

R12-4-5-4 Pre-call Location: the current Location of the A-Party. NOTE: The A-Party location is sent as co-ordinates (latitude and longitude), and it is up to the B-Party device to determine how to represent these co-ordinates (e.g. as location map and/or text).

R12-4-6 The A-Party should only be able to share pre-call content if they have the Calling Line Identification Restriction (CLIR) supplementary service disabled. If CLIR is enabled when the user accesses, or attempts to access, the Call Composer, they should be notified (e.g. via a dialog) about the need to reveal their mobile number and, ideally, be provided with a one-click mechanism to disable the CLIR service.

NOTE: If Pre-call content is shared without conveying the A-Party's Calling Line Identification, the content is not displayed on B-party side.

R12-4-7 After selecting the Pre-call content, the A-Party shall be able to preview and remove or change the selected content before pressing the voice call button.

R12-4-8 The A-Party shall be able to edit the Pre-call Location before placing the voice call to a more accurate position in a geographical map or textual address location.

R12-4-9 The user shall have the option to edit the Pre-call Image before placing the call, incl. options to crop and rotate the image. Access to these editing features shall be implemented in a way that allows straightforward selection and sending of a pre-call picture without extra clicks.

R12-4-10 The Pre-call Image shall be automatically downsized to reflect a target file size of approximately 80KB to ensure timely delivery to the B-Party device.

R12-4-11 All Pre-call content should be displayed on the A-Party outgoing call screen after pressing the voice call button.

R12-4-12 After pressing the voice call button, the user shall only be able to toggle the Important Call Indicator.

R12-4-13 Any Pre-call Image and Subject content shared by the A-party shall be made available on the A-party device for easy selection during a later Pre-call use.

US12-5 **As a user (B-Party), I want to view content for an incoming voice call before answering the voice call.**

R12-5-1 All content shared by the A-Party when the voice call button was pressed shall be presented to the B-Party on their incoming call screen.

NOTE: Pre-call content is also expected to be displayed if the device is in a 'locked screen' state.

R12-5-2 Any pre-call content shall not introduce any delay in the display of the incoming call screen on the B-Party device, nor on the B-Party's ability to accept or reject the call.

R12-5-3 Any pre-call content shall not obscure any important control or display elements on the B-Party incoming call screen, incl. accept and reject call buttons, or caller name and/ or number.

R12-5-4 If the B-Party is already engaged in any kind of call (voice call, enriched voice call, video call), and has the Call Waiting service enabled, an incoming voice call that includes the Important Call indicator shall have this indicator displayed on B-Party screen. The availability of other content (i.e. Pre-call Subject, Image, and/or Location) shall also be indicated. If applicable, the B-Party shall have the option to maximize the incoming call notification to view this additional content before accepting or rejecting the call.

NOTE: Standard call handling controls (accept, reject etc.) shall continue to be available in all states.

R12-5-5 The Important Call Indicator shall be represented graphically and/or textually, in a similar way other important events are represented in the device so the users clearly understand it is an important call.

R12-5-6 The Important Call Indicator shall not cause the B-Party device to ring if the device has been set to silent mode.

R12-5-7 Pre-call Images shall be displayed on the B-Party incoming call screen in the same aspect ratio as the original image, and any automatic cropping of the image shall be avoided.

R12-5-8 If a missed call notification is triggered on the B-Party device, the Important Call indicator and the Call Subject shall be visible in this notification.

US12-6 **As a user (A-Party), I want to know whether or not any Pre-Call image will be displayed on the B-Party side when I initiate the enriched voice call.**

R12-6-1 The B-Party device shall notify the A-Party device when a pre-call added image was received, so the A-Party is aware that the image is visible to the B-Party at the time the receiving device is ringing.

NOTE 1: The A-Party can always start the call even without having received this pre-call image delivery indication.

NOTE 2: In general there is no guarantee that the content is displayed on B-Party side, e.g. in case CLIR is enabled.

US12-7 **As a user (B-Party), I want to be able to maximise the incoming call screen, when it is minimized, to see any Pre-call content.**

R12-7-1 If the B-Party incoming voice call indication is minimised, the Important Call Indicator and Subject shall still be displayed in addition to the usual information that is provided for incoming voice calls without the user having to expand the notification.

R12-7-2 If the B-Party incoming voice call indication is minimised, an indication of the availability of other content (i.e. Image, and/or Location) shall be provided. The B-Party shall have the option to maximize the incoming call indication to view this additional content before accepting or rejecting the voice call.

US12-8 **As a user (A-Party and B-Party), while in a call, I want to see Pre-call content on my in-call screen, if no other content (e.g. via In-call Services) has replaced this Pre-call Content during the call.**

R12-8-1 Any Pre-call Image and/or Location shared by the A-Party shall be visible on both the A-Party and B-Party in-call screens, unless replaced by other content during the call.

NOTE: The displayed Location may appear differently on A- and B-Party device.

12.5 Technical Information for the Enriched Pre-call experience

12.5.1 Overview

The Pre-call experience is implemented by the Call composer service, described in section 3.6.4.3 of [RCC.07] and 2.4 of [RCC.20].

[RCC.20] is applicable for the implementation of Enriched Pre-call experience with the following updates:

- The configuration parameters of [RCC.20] are implemented as defined in Annex C.

12.5.2 Technical Implementation of User Stories and Service Requirements

R12-9-1 Requirements R12-2-1, R12-3-1, R12-4-1, R12-4-2, R12-4-3, R12-4-4-1 to R12-4-4-5, R12-4-5-1 to R12-4-5-4 shall be implemented locally on the device. In addition client configuration and capability discovery as described in section 2.1 and 2.2 of [RCC.20] shall be supported.

R12-9-2 Requirement R12-4-6 shall be implemented locally on the device. In addition the device needs to support the ability to check the status of network based supplementary services.

R12-9-3 Requirements R12-4-7, R12-4-8, R12-4-9 and R12-4-10 shall be implemented locally on the device. In addition the call composer procedures as described in section 2.4 of [RCC.20] shall be supported.

R12-9-4 Requirement R12-4-11, R12-4-12 and R12-4-13 shall be implemented locally on the device.

R12-9-5 Requirements R12-5-1 and R12-5-2 shall be implemented as described in section 2.4 of [RCC.20].

R12-9-6 Requirements R12-5-3 and R12-5-4 shall be implemented locally on the device.

R12-9-7 Requirements R12-5-5, R12-5-6, R12-5-7, R12-5-8 shall be implemented locally on the device. In addition the call composer procedures as described in section 2.4 of [RCC.20] shall be supported.

R12-9-8 Requirement R12-6-1 shall be implemented as described in section 2.4.6 of [RCC.20].

R12-9-9 Requirements R12-7-1, R12-7-2, R12-8-1 shall be implemented locally on the device.

12.6 User Stories and Feature Requirements for the Enriched In-call experience

12.6.1 General Requirements

US12-10 **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 on the call with.**

R12-10-1 All In-Call Services shall be made accessible from the in-call screen which is by definition only shown during an ongoing call.

R12-10-2 All In-Call Services shall be delivered in a 1-to-1 voice call.

R12-10-3 All In-Call Services shall be supported independently of the enabling MNO voice service (e.g. CS / VoLTE / Wi-Fi Calling).

NOTE: Subject to minimum data bandwidth and round trip time requirements.

R12-10-4 When a participant of the call puts the call "On Hold", any entry point to In-call Services shall be unavailable.

12.6.2 "Live Video"

"Live Video" will offer users the experience to add their camera view to an ongoing voice call across different bearers triggered by a single button to "add video". This section describes the User Stories and Service Requirements for the "Live Video" services.

US12-11 **As a user in a voice call, I (i.e. A-Party) want to have the ability share my "live video" (i.e. the camera view) from my in-call screen with the other participant of the call (i.e. B-Party) 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.**

R12-11-1 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.

R12-11-2 The entry point to add "live video" to an ongoing voice call shall be a single button independent of the enabling "live video" service.

R12-11-3 If 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.

R12-11-4 If "live video" can be delivered by multiple technical enablers, the one that provides the best end-to-end lip sync experience shall prevail.

R12-11-5 Sending "live video" shall be configurable by the MNO over supported bearers (3G, High Speed Packet Access [HSPA], 4G and Wi-Fi).

R12-11-6 If the underlying voice call is terminated, the "live video" shall be terminated as well.

R12-11-7 The user shall not be able to record the transmitted "live video" (i.e. both receiving and sending "live video").

R12-11-8 There shall be no option to stream a previously recorded video to the other conversation party

US12-12 **As a user, when receiving a "share live video" request, I (i.e. B-Party) want to decide whether to:**

a) Decline the incoming "live video" request and continue with a 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.

R12-12-1 The receiver (B-Party) shall be able to reject an incoming "live video" request and the voice call shall continue.

R12-12-2 The sender (A-Party) shall be notified accordingly about the selection of the receiver (B-Party) i.e. accepting or rejecting the "live video" service.

R12-12-3 If the receiver sends back a "live video", then the stream shall be shown directly on the originator's device without options to accept or reject.

R12-12-4 Upon acceptance of user A's video stream, the camera view is streamed to the receiver (user B) and displayed on the receiver's screen.

R12-12-5 An audio signal played on the recipient's (i.e. B-Party) side may accompany any reception of an incoming "live video" request.

US12-13 **As a B-Party user accepting an incoming "live video" request, I (i.e. B-Party) want the incoming voice to play automatically through a connected headset. If there is no headset connected, then the voice is played on my external loudspeaker.**

R12-13-1 When an incoming "live video" is accepted, the audio part shall be played either via a connected headset (if connected) or via the external loudspeaker (if no headset connected).

US12-14 **As either user sharing video, when I (i.e. A / B-Party) rotate my device, I want the correct video orientation to be displayed on both ends.**

R12-14-1 The device shall handle the different orientation permutations depending on how the device is rotated during a "live video" to ensure the incoming video is always displayed in the right orientation (e.g. not upside down).

US12-15 **As a user sharing "live video" from my camera, I (i.e. A / B-Party) want to toggle between front and rear camera and upon selection video is changed without interruption (if the device supports two cameras).**

R12-15-1 The user shall be able to toggle between transmitting cameras (i.e. front / back) when the phone supports two cameras.

R12-15-2 If the phone supports two cameras, the front camera shall be active by default for transmission of the "live video".

US12-16 **As a user sharing "live video", I (i.e. A / B-Party) want to stop sharing video at any point during the call without interrupting the underlying voice call.**

R12-16-1 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.

US12-17 **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” for the bearer we use.**

R12-17-1 A “live video” over LTE shall provide a higher video quality than available on 3G.

R12-17-2 A “live video” over Wi-Fi shall provide a higher video quality than available on 3G.

R12-17-3 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 that the maximum negotiated when the “live video” was initiated.

R12-17-4 When 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.

US12-18 **As a user sharing “live video”, I want my “live video” stream to continue in case of connectivity changes.**

R12-18-1 The terminal shall support continuity of the “live video” stream in a seamless manner when network conditions allow.

R12-18-2 In the special event where a “live video” stream cannot be maintained in a seamless manner, the call shall continue as a Voice Call while the user under changing connectivity should be offered to manually (re-)start a “live video” share if available.

R12-18-3 In case a “live video” stream cannot be maintained or re-established, the underlying voice call shall continue.

US12-19 **As a user, I want to see (in my call logs) an indication if a “live video” initiated by me or the other party during the call event.**

R12-19-1 Both A-Party and B-Party call logs should identify that a “live video” event occurred during the call.

R12-19-2 Live video content shared during a call is not stored or accessible after the call for either party.

12.6.3 Share any file during call

The functionality to share any file during a call is based on the File Transfer mechanism. File sharing during a call therefore happens within the context and user flows of the ongoing voice or video call.

US12-20 **As a user, I (i.e. A-Party) want to share any file from my in-call screen with the other participant (i.e. B-Party) during the voice call whenever it is possible.**

NOTE: The terms A-Party and B-Party reference the initiator and the recipient of the file sharing, not the initiator or recipient of the voice call (i.e. any participant of the voice call can share a file during a call).

R12-20-1 File Transfer shall be possible during an ongoing voice call while the voice call continues 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.

R12-20-2 When sharing files with the other participant of the call, the same logic as defined in File Transfer, section 7 of this document, shall apply.

R12-20-3 Receiving a file from the other participant of the voice call shall be possible directly from the in-call screen without ending the voice call.

NOTE: This includes the case where other in-call services are also in progress.

R12-20-4 The support of file types and file sizes shall follow the behaviour described in requirement R7-1-5.

R12-20-5 It shall be possible to resize images as described in requirement R7-5-1

R12-20-5-1 Pictures shall be optimised and resized to facilitate a faster transfer experience during a call (i.e. "low file size" as the default selection).

R12-20-6 It shall be possible to resize videos as described in requirement R7-6-1.

R12-20-7 An ongoing File Transfer shall be completed even if the voice call was terminated. After completion a notification *shall* be displayed that the file is now accessible from the call logs or messaging thread.

R12-20-8 Any file shared during a voice call, with the other participant of the call, shall be accessible during the voice call (until dismissed by the user). If the device supports display or play of that file type, the file or a preview of the file shall be displayed on the in-call screen at receiver side. If display/preview of that specific file type is not supported a placeholder indicating the file name and type shall be displayed.

R12-20-9 For photos the same format supported in File Transfer shall be supported for display in the in-call screen.

R12-20-10 While a shared file is displayed within the in-call screen, the user shall have easy access to standard in-call features (e.g. toggle loudspeaker, mute, etc.).

R12-20-11 It shall be possible to open a full-screen file viewer application from the displayed file / preview of the file for further user interaction with the file (e.g. save, edit, share, etc.) for the duration of the ongoing call.

12.6.4 Exchanging messages

Exchanging messages during a call is based on the available messaging functionality but is a simple way to share something written in an ongoing voice call situation. This experience is especially meant to offer the option to the calling parties to exchange or confirm something in written format (e.g. a name, an address, a number etc.).

US12-21 **As a user while in a voice call, I (i.e. A-Party or B-Party) want to send messages to the other call party.**

R12-21-1 Sending and receiving messages shall be possible during an ongoing voice call while the call shall continue seamlessly on the same bearer.

NOTE: This includes the case where other in-call services are also in progress.

R12-21-2 When sending messages to the other participant of the call, the same logic to determine the messaging service as described in '1-to-1 Messaging' (section 5) shall apply.

R12-21-3 Sending messages to the other participant of the call shall be possible directly from the in-call screen.

R12-21-4 Any messages exchanged during a call shall be available to the user after the call similar to the experience of Messaging outside a call as defined in '1-to-1 Messaging' (section 5).

12.6.5 Location Push

Location Push as In-Call Service describes the functionality to allow sending a location or position to the other contact while in a call.

US12-22 **As a user while in a voice call, I (i.e. A-Party / B-Party) want to send "my location" or a "position" from my in-call screen to the other participant of the call.**

R12-22-1 Location Push shall be possible during an ongoing voice call while the call shall continue seamlessly on the same bearer.

R12-22-2 When sending Location Push to the other participant in the call, the same logic as defined in US5-24 shall apply.

R12-22-3 Selecting and sending Location Push to the other participant of the call shall be possible without ending the call.

R12-22-4 Location Push received from the other participant of the call shall be automatically accepted (based on File Transfer configuration) by the B-Party.

R12-22-5 Once accepted and transferred the location or position shall be displayed on the B-Party's in-call screen as a map (pre-) view and / or the actual address of the location.

R12-22-6 An audio signal played on the recipient's side may accompany any reception of an incoming Location Push / Location Push request.

R12-22-7 Any Location Push sent and/or received during a call shall be accessible for the duration of the on-going call (or until removed from the screen by the user).

R12-22-8 It shall be possible to open a full screen map viewer application from the displayed location for further user interaction with the map (e.g. zoom, move map view, find route) during the call.

12.6.6 Enriched Calling In-call sharing with Non-Enriched Calling enabled contacts

US12-23 **As a user, I want to use In-call Services even with contacts who are not Enriched Calling enabled.**

R12-23-1 When sharing files with the other participant of the call, the same logic as defined in File Transfer (section 7) shall apply when the B-Party is not Enriched Calling enabled.

R12-23-2 When sending a Location Push to the other participant of the call, the same logic as defined in US5-24 shall apply when the B-Party is not Enriched Calling enabled.

R12-23-3 When sending a message to the other participant of the call, the same logic as defined in 1-to-1 Messaging (Section 5) shall apply when the B-Party is not Enriched Calling enabled.

12.7 Technical Information for the Enriched In-call experience

12.7.1 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.51voice 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 [PRD-IR.94] and [PRD-IR.51]. 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 Wi-Fi access.
- Sharing any file during a call: Implemented as described in section 7 of this document.
- Exchanging messages: Implemented via the services described in section 5 of this document.
- Location Push: Implemented as described in section 3.10 of [RCC.07].

The client shall indicate support for the listed services based on Capability Exchange mechanism described in section 3.

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).

12.7.2 Technical Implementation of User Stories and Service Requirements

12.7.2.1 General Requirements

R12-24-1 Requirements R12-10-1 shall be implemented locally on the device.

R12-24-2 For requirement R12-10-2, 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.

R12-24-3 For requirement R12-10-3 section 12.7.1 of this document shall be taken into consideration. The in-call services that are supported for the different voice calling services shall be implemented locally on the device.

R12-24-4 Requirements R12-10-4 shall be implemented locally on the device.

12.7.2.2 Live Video

R12-24-5 Requirement R12-11-1 shall be implemented locally on the device based on clarifications provided in section 12.7.1 of this document.

R12-24-6 Requirement R12-11-2 shall be implemented locally on the device.

R12-24-7 For requirement R12-11-3, in case IR.94/IR.51 conversational video is added, section 2.4 of [PRD-IR.94] shall apply.

R12-24-8 Requirement R12-11-4 is in line with the service prioritisation described in section 12.7.1 of this document under the bullet of “Live Video”.

R12-24-9 For requirement R12-11-5, IR.94/IR.51 conversational video service is available only under Evolved UMTS (Universal Mobile Telecommunications System) Terrestrial Radio Access Network (E-UTRAN)/EPC integrated Wi-Fi coverage. For the case of RCS Video Share, the PROVIDE VS parameter defined in Annex A.1.6 and A.2.1 of [RCC.07] shall be set accordingly.

R12-24-10 For requirement R12-11-6, 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.

R12-24-11 For requirements R12-11-7 and R12-11-8, for the RCS Video Share service and in order to prevent recording, the ALLOW VS SAVE parameter as defined in Annex A.1.6 and A.2.10 of [RCC.07] shall be set to zero.

R12-24-12 For requirement R12-12-1, 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.

R12-24-13 Requirement R12-12-2 shall be implemented locally on the device based on the SIP INVITE response.

R12-24-14 Requirements R12-12-3, R12-12-4 and R12-12-5 shall be implemented locally on the device.

R12-24-15 Requirement R12-13-1 shall be implemented locally on the device.

R12-24-16 For requirement R12-14-1, for IR.94 conversational video service section 2.4.2 of [PRD-IR.94] shall apply. For IR.51 conversational video service, section 2.4.4 of [PRD-IR.51] shall apply. For RCS Video Share service, it

shall be implemented following the image orientation extension described in 3.6.4.1.2 of [RCC.07].

R12-24-17 Requirements R12-15-1 and R12-15-2 shall be implemented locally on the device.

R12-24-18 For requirement R12-16-1, 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 3.6.3.7.4 and 3.6.4.7.5 of [RCC.07] shall apply.

R12-24-19 For requirement R12-17-1, 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 3.6.4.1.3 of [RCC.07] shall apply.

R12-24-20 For requirement R12-17-2, for IR.51 conversational video service section 3 of [PRD-IR.51] shall be considered.

R12-24-21 For requirement R12-18-1 handover procedures defined in [PRD-IR.51], [PRD-IR.92] and [PRD-IR.94] 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.

R12-24-22 For requirement R12-18-2, RCS Video Share service initiation for the case that IP Video call continuity cannot be maintained shall be implemented locally on the device.

R12-24-23 For requirement R12-18-3, in case of IR.94/IR.51 conversational video service loss section 2.4 of [PRD-IR.94] shall apply.

R12-24-24 Requirement R12-19-1 shall be implemented locally on the device.

R12-24-25 For requirement R12-19-2, the ALLOW VS SAVE parameter defined in Annex A.1.6 and A.2.10 of [RCC.06 RCS6.0 UNI] shall be set to zero.

12.7.2.3 Share any file during call

R12-24-26 The realisation of requirement R12-20-1 shall be implemented as defined in section 12.7.1 of this document (sharing any file during a call bullet).

R12-24-27 Requirement R12-20-2 shall be implemented as defined in section 7.3.

R12-24-28 Requirement R12-20-3 shall be implemented locally on the device. It is required for the client to be able to identify whether the file transfer is received from the other party in the call and if so to display the file transfer accordingly.

R12-24-29 Requirements R12-20-4, R12-20-5 and R12-20-6 shall follow the procedures described in section 7.3.

R12-24-30 Requirement R12-20-7 shall be implemented based on the procedures defined in section 12.7.1 of this document (sharing any file during a call bullet). The service continuation is not related to the status of the voice call. The display of the notification shall be implemented locally on the device.

R12-24-31 Requirements R12-20-8, R12-20-9, R12-20-10 and R12-20-11 shall be implemented locally on the device.

12.7.2.4 Exchanging messages

R12-24-32 Requirements R12-21-1 and R12-21-2 shall be implemented locally on the device. Sending and receiving of messages during the call shall follow the same methods and procedures as described in section 5.3.

R12-24-33 Requirements R12-21-3 and R12-21-4 shall be implemented locally on the device.

12.7.2.5 Location push

R12-24-34 Requirement R12-22-1 shall be implemented locally on the device. Sending and receiving of location push information during the call shall follow section 12.7.1 of this document (location push bullet).

R12-24-35 For requirement R12-22-2, as per section 3.10 of [RCC.07] RCS File Transfer over MSRP is used to convey the location information during a voice call. For Geolocation Push fallback scenarios during a voice call, the procedures described in section 5.3 shall apply.

R12-24-36 Requirement R12-22-3 shall be implemented locally on the device.

R12-24-37 The client's auto accept behaviour, defined in requirement R12-22-4 shall be implemented locally on the device and it shall be controlled via the FT AUT ACCEPT parameter defined in Annex A.1.5 and A.2.6 of [RCC.07].

R12-24-38 Requirements R12-22-5 to R12-22-8 shall be implemented locally on the device.

12.7.2.6 Enriched Calling In-Call Sharing with Non-Enriched Calling enabled contacts

R12-24-39 Requirement R12-23-1 shall be implemented as defined in section 7.3

R12-24-40 Requirement R12-23-2 shall be implemented as defined in sections 5.3 and 7.3.

R12-24-41 Requirement R12-23-3 shall be implemented as defined in section 5.3

12.8 User Stories and Feature Requirements for Interactive In-call experience

NOTE: in this section, the ‘A-Party’ requesting a live sketch sharing may be either the caller or the recipient of the ongoing voice call. Similarly the ‘B-Party’ receiving a request to a live sketch sharing may be either the caller or the call recipient.

12.8.1 Live Sketch Sharing

US12-25 **As a user (A-Party or B-Party), I want to be able to participate in a live sketch sharing at any time during an on-going voice call.**

R12-25-1 Both parties shall be able to participate in a live sketch sharing at any time during an on-going 1-to-1 voice call.

NOTE 1: Applies even if other in-call services are also in progress.

NOTE 2: A “live video” needs to be stopped by the user to initiate or accept an incoming live sketch sharing request.

NOTE 3: Both parties may be prevented from initiating a new live sketch sharing if they are already participating in a live sketch sharing.

R12-25-2 The on-going voice call shall continue seamlessly on the same bearer when a live sketch sharing is in progress.

US12-26 **As a user (A-Party), I want to be able to request a live sketch sharing with the other calling party at any time during an on-going voice call.**

R12-26-1 During an ongoing voice call, either party shall be able to request a live sketch sharing with the other party in the call directly from the in-call screen.

NOTE: As long as no other live sketch sharing is currently in progress.

R12-26-2 Either party shall not be able to request a live sketch sharing when the other party is not Enriched Calling enabled or if either party does not have data connectivity during the voice call.

R12-26-3 When a participant of the call puts the call On Hold, any entry point to Interactive In-call services shall be disabled.

US12-27 **As a user (A-Party) having requested the other party to a live sketch sharing, I want to see the status of the live sketch sharing request.**

R12-27-1 It shall be made clear to the A-Party that a request has been sent but is not yet accepted (or rejected).

R12-27-2 The A-Party shall be notified if the request to the live sketch sharing has timed out before B-Party accepts or rejects the request.

R12-27-3 The A-Party shall be notified if the request to the live sketch sharing was rejected by the B-Party.

R12-27-4 The A-Party should be able to re-initiate the request to a live sketch sharing to the B-Party if the previous request failed for any reason, or if it timed out or if rejected by B-Party.

US12-28 **As a user (A-Party) having requested the other party to a live sketch sharing, I want to be able to cancel the request to a live sketch sharing before B-Party acceptance.**

R12-28-1 The A-Party should be able to cancel an initiated request to a live sketch sharing before the B-Party has accepted (or rejected) it.

R12-28-2 The B-Party shall be notified if the request to the live sketch sharing is cancelled by the A-Party before they have accepted (or rejected) it.

R12-28-3 The request to a live sketch sharing shall be cancelled automatically if the call ends before the B-Party has accepted (or rejected) it.

NOTE: No separate notification that the request to a live sketch sharing has been cancelled is required in this case.

US12-29 **As a user (A-Party) having requested the other party to a live sketch sharing, I want the request to time out if the B-Party fails to respond.**

R12-29-1 The request to a live sketch sharing should be automatically dismissed or declined if the B-Party has not accepted (or rejected) it after a pre-defined timeout period.

R12-29-2 Both parties shall be notified if the request to a live sketch sharing times out before the B-Party has accepted (or rejected) it.

US12-30 **As a user (B-Party) having been requested to a live sketch sharing, I want to be able to see the request to the live sketch sharing.**

R12-30-1 An incoming request to a live sketch sharing shall trigger an on-screen display indication which requires a response on the B-Party's device, which shall be visible to the B-Party whether or not the in-call screen is currently displayed on their device.

R12-30-2 B-party can accept or reject a request to a live sketch sharing from A-Party.

R12-30-3 An audio signal played on the B-Party's device may accompany the incoming request to a live sketch sharing.

US12-31 **As a user (B-Party) having been requested to a live sketch sharing, I want to be able to accept the request to the live sketch sharing.**

R12-31-1 The B-Party shall be able to accept the live sketch sharing directly from the live sketch sharing request.

R12-31-2 When B-Party accepts the request to the live sketch sharing both A- and B-Party's live sketch screen shall open automatically including the pre-defined background.

US12-32 **As a user (B-Party) having been requested to a live sketch sharing, I want to be able to decline the request to the live sketch sharing.**

R12-32-1 The B-Party shall be able to decline the request to the live sketch sharing.

US12-33 **As a user (A-Party or B-Party) in an on-going voice call with an ongoing live sketch sharing, I want to be able to edit the sketch.**

R12-33-1 During a live sketch sharing, both parties shall be able to edit the sketch, and view any edits they have made in real time.

R12-33-2 During a live sketch sharing, both parties shall be able to view any edits made to the sketch by the other party in as near real-time as possible.

R12-33-3 Editing a live sketch shall allow actions like changing the sketch background, drawing lines on the sketch background itself and changes to the drawings (e.g. changing line colour and line thickness, erasing lines etc.).

US12-34 **As a user (A-Party or B-Party) in an on-going voice call with an ongoing live sketch sharing, I want to be able to move between the main in-call screen and the sketch screen at any time.**

R12-34-1 While a sketch is open, it shall be easy for the user to use the standard in-call features and controls (e.g. end call, toggle loudspeaker, mute, etc.) without ending the shared sketch session.

R12-34-2 Either party shall be able to switch directly between the sketch and the in-call screens at any time without ending the shared sketch session.

US12-35 **As a user (A-Party or B-Party) in an ongoing live sketch sharing during a voice call, I want the incoming voice automatically on a connected headset. If there is no headset connected, then I want the voice to be played on my external loudspeaker.**

R12-35-1 During an ongoing live sketch sharing, the audio part of the ongoing voice call should be played either via a connected headset (if connected) or via the external loudspeaker (if no headset connected).

US12-36 **As a user (A-Party or B-Party) in an on-going voice call with an ongoing sketch sharing, I want to be able to end the live sketch sharing at any time.**

R12-36-1 Either party shall be able to end the live sketch sharing at any time.

R12-36-2 Either party shall be able to end the live sketch sharing directly from their live sketch screen.

R12-36-3 Either party may be able to end the live sketch sharing directly from their in-call screen.

R12-36-4 The live sketch sharing shall end when the associated voice call ends.

NOTE: Live sketch sharing will not end when the user presses the device back or home keys in the live sketch screen.

US12-37 **As a user (A-Party or B-Party) in an on-going voice call previously engaged in a live sketch sharing which has ended, I want to be informed that the sketch ended.**

R12-37-1 Both parties shall be made aware when the live sketch sharing has ended.

US12-38 **As a user engaged in a shared sketch, I want the final sketch to be saved on my device.**

R12-38-1 The sketch shall be automatically saved to both parties' devices when the session ends.

NOTE 1: Sketch can be saved as a 'flat' image, without separately editable background and drawing layers.

NOTE 2: In case of using an image as background, the original image will not be overwritten by the image modified during the live sketch sharing session.

12.8.2 Specific Requirements for a live sketch on an image

US12-39 **As a user (A-Party and B-Party) in an on-going voice call, I want to be able to share a live sketch on an image.**

R12-39-1 An entry point for a live sketch on an image should be provided on the in-call screen.

US12-40 **As a user (A-Party or B-Party) in an on-going voice call with an ongoing live sketch sharing, I want to be able to edit the sketch background.**

R12-40-1 Either party shall be able to change the live sketch background image and/or colour at any time during the live sketch.

R12-40-2 Any change to the live sketch background shall be shown in real-time on both parties' devices.

R12-40-3 Either party shall be able to select an existing image from the device gallery as the live sketch background.

R12-40-4 Either party shall be able to take a new picture from the device camera to use as the live sketch background.

R12-40-5 Either party should be able to select a live sketch background from a selection of pre-defined template backgrounds.

US12-41 **As a user (i.e. A / B-Party) in an on-going voice call with a live sketch open, I want to be able to zoom and move the background image.**

R12-41-1 Both parties should be able to change the scale of the image (zoom in/out), independent of the image being viewed by the other party.

R12-41-2 Both parties should be able to move around the image, independent of the image being viewed by the other party.

NOTE: These changes to the image are <u>not</u> visible to the other party.

US12-42 **As a user (i.e. A / B-Party) in an on-going voice call with an open live sketch sharing, I want to be able to change the line thickness.**

R12-42-1 The default line thickness and colour initially assigned to the both parties when first opening the live sketch should be the thickness and colour they last selected in any previous sketch session (if applicable).

R12-42-2 Either party shall be able to change the thickness of any lines that they draw at any time during the live sketch session (irrespective of any line thicknesses set on initial default).

12.8.3 Specific Requirements for a live sketch on a map

US12-43 **As a user (A-Party and B-Party) in an on-going voice call, I want to be able to share a live sketch on a map.**

R12-43-1 A separate entry point for a live sketch on a map should be provided on the in-call screen (i.e. defaulting to a map background).

R12-43-2 The A-Party's current location should be set as the default location for any new live sketch on a map for both parties.

US12-44 **As a user (i.e. A / B-Party) in an on-going voice call with an ongoing live sketch on a map, I want to be able to interact with the background map.**

R12-44-1 Both parties shall be able to change the scale of the map, independent of the map being viewed by the other party.

R12-44-2 Both parties shall be able to move the map location, independent of the map being viewed by the other party.

NOTE: These changes to the map are not visible to the other party.

US12-45 **As a user (A-Party and B-Party) in an on-going voice call with an ongoing live sketch on a map, I want to know if the other party has made any edits that I cannot currently see on my map view.**

R12-45-1 If the other party has edited a part of the map that the current party is not viewing, then the current party should be made aware that this is occurring.

R12-45-2 If the other party has edited a part of the map that the current party is not viewing, then the current party should be able to view all the edits easily on their screen when desired.

US12-46 **As a user (A-Party and B-Party) in an on-going voice call with an ongoing live sketch on a map, I want some additional map-based controls.**

R12-46-1 Both parties should be able to see each other's locations on the map

R12-46-2 Both parties should be able to easily move the map to their location at any time.

R12-46-3 Both parties should be able to easily move the map to the other party location at any time.

R12-46-4 Both parties should be able to easily move the map to display both locations at any time.

NOTE: If location is disabled on either party's device, the marker for their location will not be shown on the map.

R12-46-5 Both parties should be able to send a location marker to the other party, with this marker being visible on both parties' sketches.

R12-46-6 Both parties should be able to easily move the map to display all locations at any time.

12.9 Technical Information for Interactive In-call services

12.9.1 Overview

The Interactive In-Call Experiences Shared Sketch and Shared Map shall be implemented by the client as described in section 12.8 of this document. The technical implementation shall follow the procedures as described in sections 2.9.7, 2.9.8 and 2.9.10 of [RCC.20]. The protocol to use is described in section 2.9.10 of [RCC.20].

12.9.2 Shared Sketch

R12-47-1 Requirements R12-25-1, R12-26-1, R12-26-2, R12-27-2, R12-27-3, R12-27-4, R12-28-1, R12-28-2, R12-30-2, R12-31-2, R12-32-1, R12-33-1, R12-33-2 shall be implemented locally on the device. In addition, the procedures as described in sections 2.9.7, 2.9.8 and 2.9.10 of [RCC.20] shall be supported.

R12-47-2 Requirements R12-25-2, R12-26-3, R12-27-1, R12-28-3, R12-29-1, R12-29-2, R12-30-1, R12-30-3, R12-31-1, R12-33-3, R12-34-1, R12-34-2, R12-35-1, R12-36-1 to R12-36-4, R12-37-1, R12-38-1 shall be implemented locally on the device.

12.9.3 Specific Shared Image Sketch Requirements

R12-47-3 Requirements R12-39-1 and R12-40-1 shall be implemented locally on the device.

R12-47-4 Requirement R12-40-2 shall be implemented locally on the device. In addition the procedures as described in [RCC.20] section 2.9.7, 2.9.8 and 2.9.10 shall be supported.

R12-47-5 Requirements R12-40-3, R12-40-4, R12-40-5 shall be implemented locally on the device.

R12-47-6 Requirements R12-41-1, R12-41-2, R12-42-1 and RR12-42-2 shall be implemented locally on the device.

12.9.4 Specific Shared Map Sketch Requirements

R12-47-7 Requirements R12-43-2, R12-45-1, R12-45-2, R12-46-1 and R12-46-5 shall be implemented locally on the device. In addition the procedures as described in [RCC.20] section 2.9.7, 2.9.8 and 2.9.10 shall be supported.

R12-47-8 Requirements R12-43-1, R12-44-1, R12-44-2, R12-46-2, R12-46-3, R12-46-4 and R12-46-6 shall be implemented locally on the device.

12.10 User Stories and Feature Requirements for the Enriched Post-call experience

This section describes the use case where a user (A-Party) can add additional information after an unanswered / unsuccessful call to the callee (B-Party). This information updates the existing missed call notification on the B-Party side with an enhanced version that not only provides the missed call information but also provides the B-Party with a reason why the A-Party placed the call.

US12-48 **As a user (A-Party), I want to be presented with on-screen options after an unanswered call so that I can add a reason for the call.**

NOTE: An ‘unanswered’ call is any call attempt that has not been completed as a connection between the A-Party and the B-Party, e.g., but not limited to, B-Party did not answer the call, B-Party rejected the call, or A-Party cancelled the call before B-Party accepted it. A call connected to the B-Party voicemail system is treated as an answered call (as is Call Forwarding).

R12-48-1 If a call was not answered by the B-Party, the A-Party shall have the option to EITHER:

- Write and send a Post-call Note to the B-Party (limited to 1 to 60 characters) OR
- Record and send a Post-call Voice Message (limited to 10 minutes long) to the B-Party

NOTE: Emoji's are supported in Post-call Notes.

R12-48-2 Pre-defined Post-call Notes should be available for the user.

R12-48-3 The Pre-call Subject shall be presented as default Post-call Note.

R12-48-4 The implementation of pre-defined Post-call Notes on the device may offer some or all of the following features:

- The device may store and display previously entered user-defined Post-call Notes.
- An auto-complete function may be available that lists matching existing Post-call Notes while the user is typing.
- The user may be able to select a Post-call Notes from a list of pre-defined and/or previously used notes.
- The user shall have an ability to edit any pre-defined or previously entered and stored Post-call Notes.

R12-48-5 If the B-Party is not connected to data when the call attempt ended, the sending of post-call content shall follow the 1-to-1 Messaging (Section 5) logic.

US12-49 **As a user (B-Party), I want to see an updated and enriched missed call indication on my device if the caller (A-Party) added a reason after the call was not answered by me.**

R12-49-1 Post-call Notes or Voice Messages shall update the existing standard missed call indication on the B-Party's device.

R12-49-2 If no standard missed call indication is displayed on the B-Party's device because the B-Party rejected the call, any Post-call Note or Voice Message shall be displayed in a new indication. It should be made clear to the user that this new indication is for a rejected call.

R12-49-3 If the standard missed call indication has already been dismissed by the B-Party, the Post-call Note or Voice Message shall display a new indication. It shall be made clear to the user that this new indication does not represent an additional new missed call.

R12-49-4 The B-Party shall be able to read the Post-call Note from the associated indication, either directly or by expanding the indication.

R12-49-5 The B-Party shall be able to play the Post-call Voice Message from the associated indication, either directly or by expanding the indication.

R12-49-6 If the initial call was already enriched with a Pre-call Subject by the A-Party (using the Pre-call options), the Post-call Note may replace the initial Pre-call Subject displayed in the indication.

12.10.1 Enriched Calling Post-call experience with Non-Enriched Calling enabled contacts

US12-50 **As a user, I want to be able to send a Post-call Note or Voice Message to contacts who are not Enriched Calling enabled.**

R12-50-1 In case the B-Party is not Enriched Calling enabled then

- A written Post-call Note shall be sent as defined in 1-to-1 Messaging (section 5).
- A recorded Post-call Voice Message shall be sent as defined in 'Audio Messaging' (Section 8).

NOTE 1: Post-call Notes can be sent to non-RCS contacts (leveraging on SMS) and to non-Enriched Calling capable RCS contacts (leveraging on 1-to-1 Messaging)

NOTE 2: Post-call Voice Messages can be sent to non-Enriched Calling capable RCS contacts (leveraging on Audio Messaging). Post-call Voice Messages cannot be sent to non-RCS contacts.

12.11 Technical Information for the Enriched Post-call experience

12.11.1 Overview

The Enriched Post-call experience shall be implemented by the client as described in section 12.10 in this document. The technical realisation of the Post-call experience is described in section 2.5 of [RCC.20].

12.11.2 User Stories and Feature Requirements for the Enriched Post-call experience

R12-51-1 Requirement R12-48-1 shall be implemented locally on the device. The technical implementation of sending the Post-call Note or Post-call Voice message shall be implemented as described in section 2.5 of [RCC.20].

R12-51-2 Requirements R12-48-2, R12-48-3 and R12-48-4 shall be implemented locally on the device.

R12-51-3 Requirement R12-48-5 shall be implemented based on the post call service under consideration. Post-Call Note information shall be sent based on the technology selection rules defined in section 5.3. When Post-Call session fallback is triggered, the text included in the note element of the Post-Call xml shall be extracted and sent using the selected technology as specified in section 5.3. For Post-Call Voice Message, it shall be implemented as defined in section 8.3.

R12-51-4 Requirements R12-49-1 to R12-49-6 shall be implemented locally on the device.

12.11.3 Enriched Calling Post-Call experience with Non-Enriched Calling enabled contacts

R12-51-5 Requirement R12-50-1 shall be implemented based on the Post-Call service under consideration. Sending Post-Call Note or Voice Message information shall be possible even though Post-call service is not confirmed based on capability discovery. For Post-Call Note information, it shall be sent based on the technology selection rules defined in section 5.3. For Post-Call Voice Message, it shall be implemented as defined in section 8.3.

12.12 User Stories and Feature Requirements for Enriched Call content in Logs and media contact centric view

This section describes how the standard logs implementations are extended to include additional Enriched Calling content shared either pre-, during, or post-call. It is acknowledged that the detailed UX design will vary across implementations.

US12-52 **As a user (A-Party and B-Party), I want to be able to see my calling activity with the other party in the message threads.**

R12-52-1 The following rich content shall be available in the message thread for both parties:

- Post Call note
- Post Call voice note
- Messages exchanged
- Files shared (including sketches stored as pictures)
- Location shared during the call

R12-52-2 Any enriched content that was shared by a user (A-Party and B-Party) shall be available in the message thread on A-Party's device.

R12-52-3 Any enriched content that was shared by a user (A-Party and B-Party) shall be available in the message thread on B-Party's device if the A-Party is a known contact in B-party's contact list.

R12-52-4 Post-call enriched content shared with B-Party shall be notified to B-Party as a new 1-to-1 message.

R12-52-5 Pre-call and In-call enriched content shared with B-Party shall not be notified to B-Party as a new message, (if added to the messaging thread) it shall be there but automatically flagged as "read" on B-Party's device.

R12-52-6 The message thread shall identify content received from the B-party using Enriched Calling features as call content (in contrast to messaging content).

R12-52-7 Any Enriched Calling content shall be stored in the B-Party's message thread only if the associated content was presented on the device.

US12-53 **As a user (A-Party and B-Party), I want to be able to see my calling activity with the user in the Call log.**

R12-53-1 The following rich content shall be available in the enriched call log entry for both parties:

- Important flag
- Post Call note or in his absence Subject
- Post Call voice note
- Location shared in pre-call
- Indicators for:
    - Messages exchanged
    - Files shared (including sketches stored as pictures)
    - Location shared during the call

R12-53-2 The following rich In-call content should be available in the enriched call log entry for both parties:

- Messages exchanged
- Files shared (including sketches stored as pictures)
- Location shared during the call

R12-53-3 Rich content that was added in a call (missed call, received call, ongoing call or rejected call) by the A-Party shall be available in the call log on A-Party's device, as part of the enriched call log entry for the respective event.

R12-53-4 Enriched Calling content that was presented on the B-Party's device (miss call, received call, ongoing call or rejected call) shall be available in the call log.

US12-54 **As a user (A-Party or B-Party), I want to have access to content that was shared with a contact within a contact centric view.**

R12-54-1 Specific files shared or exchanged with a contact shall be available to both parties in a contact centric view (e.g. a gallery view).

R12-54-2 The following rich content shall be available in the contact centric view for both parties:

- Files shared in that call
- Sketches stored as pictures during that call

		Call Log	Messaging thread	Contact centric view
Pre- Call	Subject	Shall	Should	
	Importance	Shall	Should	
	Pre-Location	Shall	Should	
	Pre-Image	Should(1)	Shall	Shall
In- Call	Files	Should(1)	Shall	Shall
	Location	Should(1)	Shall	
	Notes	Should(1)	Shall	
	Sketches	Should(1)	Shall	Shall
Post- Call	Note	Shall	Shall	
	Voice note	Shall	Shall	
Messaging	Messages		Shall	
	Files		Shall	Shall
	Location		Shall	

Table 44: Overview of the Enriched Call content representations

NOTE: (1) Content itself is not mandatory but indicator to the content is mandatory

12.12.1 Technical Information for Enriched Call Logs experience

R12-55-1 Enriched content in Logs and media contact centric view shall be implemented locally on the device.

For the Post-Call cases described in R12-48-5, the receiving client will not be able to distinguish whether the sender sent a Post-Call note or message and as a consequence the event will not be included in the call log.

Additionally, the receiving client will not be able to distinguish whether the sender sent a Post-Call audio or file transfer audio message and as a consequence the event will not be included in the call log.

13 rcsVVM Service

This service is considered to be out of scope of the profile defined in this document.

14 APIs

14.1 Description

RCS APIs enable MNOs, OEMs and developers from companies outside of the traditional MNO ecosystem to enrich their services by integrating RCS features into their applications.

Using on-device terminal APIs, MNOs can open up RCS capabilities to developers to propose innovative new services to their customers which increase RCS usage and data traffic consumption.

This chapter covers requirements for the APIs that must be made available to developers on any RCS device. APIs offering the same service features should also be made available to

developers by the MNO via network APIs and integrated into the existing wholesale eco-system which should be evolved to support the richer features and new capabilities that RCS can offer.

NOTE: In this document “developer” means either OEM application developer, MNO application developer or third party developer

14.2 User Stories and Feature Requirements

NOTE: the requirements in this section are indicative and may change significantly once technical feasibility is completed as part of the future versions of the Universal Profile.

US14-1 **As a user, I want to be able to install and use new applications enriched with messaging services and enhanced with new innovative features.**

As a developer, I want to provide innovative applications based on, or using Operator Messaging services without having to implement the full infrastructure necessary to provide such services.

As an MNO, I want to open up my RCS messaging and service data channel infrastructure to developers and third parties so that their applications can be enriched with these RCS features.

R14-1-1 APIs shall be made available for the following RCS services and features:

R14-1-1-1 Capability Discovery,

R14-1-1-2 1-to-1 Messaging, Group Chat,

R14-1-1-3 File Transfer including geo-location,

R14-1-1-4 Audio Messaging,

R14-1-1-5 Video Share, Geolocation Share during a call,

R14-1-1-6 Dedicated service data channel (Extensions), and

R14-1-1-7 Service configuration information that may be 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, FT HTTP CAP ALWAYS ON, etc.).

R14-1-2 All the devices or native RCS implementation shall provide APIs to expose the services listed above to third parties.

R14-1-3 The device’s RCS database containing the user’s messages and content shall be made available to third parties (already provided for SMS today).

R14-1-4 When a user installs an application that uses RCS APIs, the user shall be informed that the application will have access to his RCS services and features.

R14-1-5 Any application with access to the RCS services listed in R14-1-1-1 to R14-1-1-5 above is able to manage and display any event or communication

associated with those services, no matter which application was used to generate the event.

R14-1-6 An application using its own dedicated service data channel to realise a specific feature shall only be able to exchange communications over this dedicated service data channel with other applications authorised to do so. Only such authorised applications shall be able to manage and display the associated communication streams.

US14-2 **As a user, I want to be able to use the application of my choice to handle my existing messaging services, ensuring that I am not overwhelmed with multiple notifications for the same incoming message or incoming event.**

R14-2-1 If more than one application on a device is able to handle the RCS messaging services listed in R14-1-1-1 to R14-1-1-5 above, then the user shall have the ability to choose which one is used as the "default messaging application", i.e. the application used to notify the user of new incoming events and to be the default application used to create and send new events.

R14-2-2 If more than one application on a device is able to handle the same dedicated service data channel (extension), then all of the eligible applications will be able to handle the streams in a similar way (e.g. it could be that several applications notify the user of the same incoming communications stream).

R14-2-3 A user shall be notified once and only once for each incoming message or event for services listed in R14-1-1-1 to R14-1-1-5 above in order to avoid a confusing user experience.

NOTE: See section 2.2.3 for more detailed requirements on multiple client co-existence.

US14-3 **As a user, I want to be able to control which application(s) can access and use my RCS services.**

R14-3-1 An application wishing to use RCS APIs shall follow a verification process when it is installed on a device.

R14-3-2 During installation of an application that uses RCS APIs, the user shall be prompted to accept or reject the application's use of RCS services.

R14-3-2-1 If the user accepts that the application can use RCS services, the application shall be able to access the RCS services listed above along with any communications history associated with these services.

R14-3-2-2 If the user rejects that the application can use RCS services, the application shall not be able to access nor use the RCS services listed above nor the communications history associated with these services.

US14-4 **As a user using an RCS-enabled app, I want to know which of my contacts has RCS services available to them on any of their devices.**

US14-5 **As a user I want to know which of my contacts share any new features or services that are provided to me by an application using a dedicated service**

data channel and be able to communicate with these contacts in the appropriate way.

R14-5-1 An identifier shall be attributed to each of a developer's applications which will allow the application to use the device's RCS services as listed in R14-1-1-1 to R14-1-1-5above.

R14-5-2 An application may create a dedicated data channel to provide a new service. In this case the service shall use an identifier that is used to refer to a new service. This identifier can be shared by other applications as soon as they are authorised to do so by the developer owning the identifier.

R14-5-3 It shall be possible for a developer to authorise several applications to use the same identifier.

US14-6 **As a developer, I want to ensure that users of my application are aware of other contacts supporting the underlying services so that they can communicate with them as much as possible.**

R14-6-1 A user with an application using RCS APIs shall be able to see, if appropriate, which of his contacts also has the same application and/or features provided by it.

R14-6-2 An RCS user exchanging capability information with other RCS users shall include information about any application using a dedicated service data channel API in the capability information shared. This will include capabilities for any applications running on the user's secondary device(s).

R14-6-3 An RCS application using RCS APIs shall be able to request information about the exact capabilities supported by some or all of the user's contacts.

R14-6-4 Capability information for applications on a contact's secondary device(s) shall also be discoverable.

R14-6-5 When an RCS application using a dedicated service data channel API is uninstalled from a device and that service data channel is not supported on any other of the user's devices, the capability information of that service is no longer advertised for that user.

US14-7 **As an MNO, I want to be able to identify applications that use my RCS messaging and service data channel infrastructure and to be able to measure and record how much traffic and service usage is generated by each one.**

As an MNO, I want to make sure that malicious applications using RCS service APIs cannot generate traffic and that any such malicious traffic shall not be transported across the network (i.e. blocked).

As an MNO, I want to make sure that malicious use by applications of my messaging and communications services infrastructure is prevented, for example to make sure that an application cannot masquerade as another.

As an MNO, I want to be able to identify traffic generated by applications using RCS APIs on a per identifier basis and revoke access to these APIs for applications using these identifiers.

R14-7-1 Traffic generated by an application or service using RCS APIs shall be identifiable as such by the MNO on a per identifier basis.

R14-7-2 An MNO shall be able to revoke an application using a given identifier from access to all RCS features and functionality.

R14-7-3 Blocking or revoking applications using a given identifier from sending traffic shall not affect the user's ability to send authorised RCS service traffic from other applications or from their native RCS client.

US14-8 **As a developer, I want my application to be aware of the existence and RCS state of the SIMs currently in the device.**

R14-8-1 Application(s) shall be able to identify which RCS identity is in use by the device at any time.

R14-8-2 Subscribing applications shall be notified by the device when the identity of the SIM that is active for RCS changes.

R14-8-3 Upon user approval, applications shall be able to assign the identity to be used for the RCS services on the device.

15 Plugins and UI Hooks

15.1 Description

Within communication services different users have different needs how they want to express themselves, what they want to share with their communication partners and how they want to experience communication. Plugins are the way how the messaging and voice & video calling experience defined in this document can become more versatile in catering to those unique needs of various consumer segments.

In that context, Plugins are services that extend what users can experience within their communication. Examples of those plugins can be 'Send Money' (i.e. allowing a user to easily transfer money to a communication partner within a conversation), 'share an interactive shopping list' (i.e. allowing to maintain a shopping list within a group conversation, open for each participant to pick, accept or add any of its items), or 'spam caller detection' (i.e. indicating the user the reputation of an unknown Caller-ID on the incoming call screen) and 'video calling filter' (i.e. allowing to put a real-time filter on your own camera stream within an IP Video Call). The list of Plugins is clearly undefined and allows all creativity for third parties to stimulate their development ideas. Plugins are to be supported across all implementations of the Universal Profile in the same way and must not need to be optimised for a single implementation.

The users can easily discover, install and use only the Plugins they are interested in, without having a cluttered and heavy application.

The specification of Plugins will consider monetisation options for MNOs and/or implementation partners.

Detailed requirements for Plugins will be defined and published in a future release of this document.

16 Security against Malware

16.1 Description

Authentication in RCS services on an individual device is currently 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.

16.2 User Stories and Feature Requirements

US16-1 **As a user, I want to use my MNO communication services safely and securely.**

R16-1-1 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.

R16-1-2 Authentication mechanism(s) shall be defined for a user on devices with a SIM. When SIM available on the device, (a) SIM based authentication mechanism(s) shall be used.

R16-1-3 Authentication mechanism(s) which prevent spoofing and other attacks shall be defined for a user on devices without a SIM.

R16-1-4 The Authentication mechanism(s) for devices with or without SIM shall be defined in such a manner that even if the user data is intercepted by the network or any 3rd party applications, the intercepted user data cannot be misused.

R16-1-5 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.

R16-1-6 User interaction to ensure security solutions shall be minimized.

R16-1-7 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.

R16-1-8 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).

US16-2 **As an MNO, I want to customize the enhanced security function.**

R16-2-1 The security solution shall offer the option for the MNO to enable or disable the function with appropriate security control.

R16-2-1-1 Enable or disable over the air.

R16-2-1-2 Enable or disable for selected devices.

R16-2-2 If user interaction is required, the user shall be guided to accomplish the interaction in a way that RCS use of the identity is enabled in a secure way after the set-up process.

US16-3 **As an MNO, I want to ensure that traffic and content generated by an RCS identity is generated by that identity's true user.**

R16-3-1 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.

R16-3-2 All traffic generated by an identity shall be identifiable as such.

16.3 Technical Information

The technical implementation of RCS involves a number of technologies to secure the user network interface. Methods for encryption, user authentication and access authorisation are applied by the client and the network on a per interface and protocol basis. The level of security for the individual technologies depend on the selection of the security measure applied.

16.3.1 User Authentication

The following main user authentication and methods are used in RCS.

R16-4-1 User Authentication via the SIM based Authentication and Key Agreement protocol (AKA). This authentication protocol comes with a high level of security based on shared secrets exchanged between the SIM and the network authentication centre. As a result of the initial authentication the client and network agree keys which are used to encrypt the UNI signalling flow. As an extension to the SIM 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].

R16-4-2 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).

R16-4-3 Network based user identification (e.g. via "header enrichment") 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 SIM based Authentication and Key Agreement protocol. The IP address assigned at the time of bearer set-up is used as the criteria to identify the user within the existing bearer session. Service Provider need to take precautions in securing the trusted network access to prevent fraudulent

IP address claims. The mechanism is insecure since attackers are able to gain unauthorized access to the network services once they got the permission to use a bearer session on behalf of the user.

R16-4-4 User based Authentication via one time password (OTP), whereby the user or the device claims an identity which is challenged via a signalling transaction over a channel with an authentication context for this identity, e.g. the short message service to another device or an external secure token service. Based on the one time authentication a long term authentication context can be generated (SSO) to prevent the need for subsequent authentication transactions. This security measure may be used as an additional measure for another authentication mechanism, e.g. based on the principle of the two factor authentication, which comes in most cases with user impact.

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.

16.3.2 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. Clients conforming to the profile defined in this document shall support the encryption for all signalling and media traffic technologies described in this document.

16.3.3 Storage of Authentication and Identification Data

The RCS client needs 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.

16.3.4 SIM State Handling

If the SIM of a device is used to provide the identity of the user for RCS services and the device leaves the SIM ready state, then the RCS client shall take actions to disable RCS services for the user based on procedures defined in this section. This is caused by the fact that the basis of the user identification and authentication is no longer available to the client if the SIM is not available.

If the client detects that the device is about to leave or left the SIM Ready State (e.g. power off, physical removal of SIM), then the client shall instantly de-register from IMS if the connectivity and security settings allow it. In addition, any other ongoing RCS client session or transaction based on the SIM identity (e.g. a connection with the HTTP Content Server) shall be aborted.

If the device is not in SIM Ready State, a client configuration stored in the client remains valid (in accordance with its validity) but it is in dormant state, i.e. the client does not invoke RCS services, e.g. it does not register in the IMS Network.

If the client recovers the SIM Ready State (e.g. user enters PIN, re-insert the SIM Card in the device), then the client shall check whether the configuration stored in the client

corresponds to the inserted SIM (comparing the IMSI from client configuration with IMSI from SIM).

If the client detects that the IMSI has been changed, then the procedures for SIM change apply as defined in section 2 of this document. Otherwise, the device uses the valid client configuration related to the IMSI of the SIM to enable RCS services again, e.g. to register in the IMS network.

The procedures apply regardless of the access technology used to access RCS services.

16.3.5 Applicability of Authentication Methods

This section gives an overview of the applicability and support requirements of user authentication methods defined in section 16.3.1 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 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 45: 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

Access Point Name (APN) Configuration MO of [RCC.07], see section 2.1.3 of [NG.102].

User Network Interface	Primary Device	
	Applications Using terminal API	Applications 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]
Service Provider Client Configuration Configuration Over non 3GPP networks	Same as device that provides the terminal API	Support of OTP based authentication is mandatory.
IMS Access Authentication	Same as device that provides the terminal API	Support of SIP digest with the credentials from client configuration is mandatory
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
Message Store Server Authentication	Same as device that provides the terminal API	Support of plain password authentication is mandatory.

Table 46: Authentication Mechanisms for non-embedded clients on primary device

16.3.6 Technical Implementation of User Stories and Service requirements

R16-4-5 For the requirements in user story US16-1 the following applies:

R16-4-5-1 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 16.3.1. 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.

R16-4-5-2 HTTP(s) based client configuration in 3GPP access makes use of either the GBA (see R16-4-1) or network based user identification (see

R-16-4-3) as defined in section 2.4 and 2.2 of [RCC.14] respectively. The network based user authentication may be replaced or extended on service provider request the OTP based user authentication (see R16-4-4) as defined in section 2.2 and 2.3 of [RCC.14]. The authentication mechanism is negotiated between client and server as defined in [RCC.14].

R16-4-5-3 As defined in section 2.2.5 of [RCC.14] the service provider may decide to further secure the identification via invocation of the SMS based procedure which adds additional authentication (see R16-4-4). 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].

A client on a device with a SIM not being in SIM Ready State shall not invoke client configuration procedure if the identity associated SIM is used for RCS, see section 16.3.4.

R16-4-5-4 Client configuration transactions carrying user data are encrypted via Transport Layer Security (TLS)/Secure Socket Layer (SSL) as defined in sections 2.2.5 of [RCC.14].

R16-4-5-5 HTTP(s) based client configuration on non 3GPP access for primary and for additional devices makes use of either based on the GBA for a primary device (see R16-4-1) or via the OTP based authentication method (see R16-4-4) as defined in sections 2.3 – 2.5 and 2.6 of [RCC.14].

A client on a device with a SIM not being in SIM Ready State shall not invoke client configuration procedure if the identity associated SIM is used for RCS, see section 16.3.4).

R16-4-5-6 Client configuration transactions are encrypted via TLS/SSL as defined in 2.2.5 of [RCC.14].

R16-4-5-7 The authentication method for IMS access depends on the mode and capability of the RCS device, the type of access and the device configuration. The client shall apply the authentication in IMS as defined in section 2.13.1.2 of [RCC.07].

A client on a device with a SIM not being in SIM Ready State shall not register in IMS if the identity associated SIM is used for RCS, see section 16.3.4.

R16-4-5-8 The encryption of SIP signalling is determined by client configuration as defined in section 2.8 of [RCC.07] and 2.2.2.2 of [RCC.15].

R16-4-5-9 The authentication method for HTTP transaction of File Transfer over HTTP shall be based on digest authentication (see R16-4-2) based on the credentials received by the client via device configuration or via GBA/AKA based authentication on a primary device (see R16-4-4) as defined in sections 3.5.4.8.1 of [RCC.07].

A client on a device with a SIM not being in SIM Ready State shall not

invoke file transfer transactions if the identity associated SIM is used for RCS, see section 16.3.4.

R16-4-5-10 HTTP File Transfer transactions carrying user data are encrypted via TLS/SSL as defined in 3.5.4.8.5 of [RCC.07].

R16-4-5-11 The authentication method for Internet Message Access Protocol (IMAP) sessions for the Common Message Store either based on AKA based on the GBA (see R16-4-1) or is based on basic authentication (see R16-4-2) with the CMS credentials received by the client via device configuration as defined in section 2.13.1.5 of [RCC.07].

A client on a device with a SIM which is not in SIM Ready State shall not login to the Common Message Store if the identity associated SIM is used for RCS, see section 16.3.4.

R16-4-5-12 IMAP sessions are encrypted by use of TLS as defined in section 2.13.1.5 of [RCC.07].

R16-4-5-13 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 R16-4-1) or digest authentication (see R16-4-2) with the IMS credentials received by the client via device configuration or network based user identification (see R16-4-3) as defined in section 2.13.1.4 of [RCC.07].

A client on a device with a SIM which is not in SIM Ready State shall not invoke HTTP/XCAP transactions if the identity associated SIM is used for RCS, see section 16.3.4.

R16-4-5-14 The encryption of HTTP/XCAP is based on TLS as defined in section 2.8 of [RCC.07].

R16-4-5-15 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].

R16-4-5-16 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.

R16-4-5-17 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]. It is mandatory for clients supporting the profile defined in this document to support encryption of RTP.

R16-4-6 For the requirements in user story US16-1 to minimise the user interaction for security solutions a case by case analysis of user interaction flows for device configuration and personalisation 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, e.g. a user readable short message or an external secure token service. There is no security and authentication related user interaction flows in RCS for services other than device configuration and personalization.

R16-4-6-1 “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 SIM or network based user identification. If the MNO 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 described below.

R16-4-6-2 “HTTP(s) based client configuration mechanism over non 3GPP access” as defined in section 2.3 of [RCC.14] may require a 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].

R16-4-6-3 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 2.5 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 2.5.1of [RCC.14] and 2.1.2 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.15] 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 of [RCC.15] is “in-band”.

The user interaction for the input of a PIN on the primary device as defined in section 2.3.3.4.2.3 of [RCC.15] is “in-band”.

R16-4-7 For the requirements in user story US16-2 the following applies.

R16-4-7-1 The enhanced security function can be enabled or disabled by the service provider as defined in section 2.2.5 and 2.3.5 of [RCC.14].

R16-4-7-2 The enhanced security function makes use of general client procedures for the user identification and authorisation. These

procedures have only limited capabilities to convey MNO specific explanatory text. Only the out-of-band transaction provides the service provider with the capability to covey specific information. However this is outside of the scope of this specification.

R16-4-8 For the requirements in user story US16-3 the following applies.

R16-4-8-1 The RCS implementation assumes one common user identity managed across all involved technologies (e.g. SIM, Device Configuration, IMS, 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.

17 Data Off

17.1 Description

Users in many cases switch cellular data usage off locally on their device. To allow the MNO to offer IR 92 / IR 94 and RCS services to their users even in these use cases, the data off switch shall have an MNO configurable impact on the device connectivity. It shall be up to the individual MNO 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.

17.2 User Stories and Feature Requirements

US17-1 **As an MNO, I want to be able to configure the device to use various technologies for the production of MNO communication services even when the cellular data switch on the device is set to ‘off’.**

R17-1-1 For the configuration of MNO voice, video and messaging services, the following technologies / bearers shall be considered in scope:

R17-1-1-1 CS call over 2G and 3G network.

R17-1-1-2 VoLTE call over 4G network.

R17-1-1-3 SMS over 2G and 3G network (including services enabled by SMS).

R17-1-1-4 MMS over 2G, 3G, 4G network.

R17-1-1-5 IR.92 SMS over 4G network (including services enabled by SMS).

R17-1-1-6 RCS Messaging over 2G, 3G, 4G network (including services enabled by RCS Messaging) inside and outside of a call.

R17-1-1-7 RCS File Transfer over 2G, 3G, 4G network including services enabled by RCS File Transfer) inside and outside of a call.

R17-1-1-8 RCS Enriched Calling Pre-Call and Post-Call services over 3G and 4G networks.

R17-1-1-9 Video Share over 3G and 4G networks and Interactive In-call services inside an ongoing call over 2G, 3G, 4G networks.

R17-1-1-10 IR.94 ViLTE over 4G network.

R17-1-1-11 Operator Provisioning over 2G, 3G, 4G networks.

R17-1-2 The availability of the services listed in requirement R17-1-1(with the exception of services listed under R17-1-1-1 and R17-1-1-3 shall be independently configurable on a per-MNO and per customer basis for roaming and on-net as described in Table 47.

R17-1-3 When an MNO has configured services which require a cellular network as "Available", these services shall be available even if the user sets the cellular data switch to 'off'.

R17-1-4 When an MNO has configured services which require a cellular network as "On User Selection", these services shall be available only if the user's cellular data setting is 'on'.

NOTE: It is at sole MNO discretion to decide on the services that shall be offered to their users. The MNO might decide to offer none of the configurable services, a selection of these services or all of the above listed services.

	Service Behaviour on-net	Service Behaviour in Roaming
CS Voice	**Always on**	**Always on**
xMS over CS	**Always on**	**Always on**
VoLTE (IR.92)	**Configurable**	**Configurable**
SMS over IP	**Configurable**	**Configurable**
MMS	**Configurable**	**Configurable**
RCS Messaging	**Configurable**	**Configurable**
RCS File Transfer	**Configurable**	**Configurable**
RCS Enriched Calling (Pre-call and Post-call services)	**Configurable**	**Configurable**
Video Share and Interactive In-Call services	**Configurable**	**Configurable**
ViLTE (IR.94)	**Configurable**	**Configurable**
Provisioning	**Configurable**	**Configurable**
PS data/Internet Access	**Always off**	**Always off**

Table 47: Summary of the availability of PS services over cellular networks when cellular DATA is set to OFF

17.3 Technical Information

17.3.1 Overview

The technical realisation of data off behaviour is applicable to devices in the following way:

- For embedded clients on primary devices using the IMS APN or Home Operator Services (HOS) APN as defined in sections 2.2 and 2.9.1.4 of [RCC.07] the complete behaviour is applicable via the Data Off functionality defined in section 2.9.1.5 of [RCC.07]. In accordance with the definitions of section 2.2 of [RCC.07] this includes downloadable clients that use terminal APIs to access the RCS functionality.
- For embedded clients on primary devices using the internet APN for RCS services as defined in section 2.9.1.5 of [RCC.07] the behaviour is not applicable. It is assumed that the availability of these services in case of data off is determined by the switch controlling the data connection with the internet APN
- For downloadable clients on primary devices, as defined in section 2.2 of [RCC.07] the level of support of the behaviour depends on the level of integration with the native applications, which is limited by the permissions offered by the mobile OS or the OS platform API.
- Secondary devices: Those are access agnostic and as a result the behaviour described is not applicable to such clients. When the cellular data switch is switched off, they would have no data connectivity on cellular networks and as a result in those circumstances they shall not be able to offer any MNO services on such networks.

17.3.2 Technical Implementation of User Stories and Service requirements

For the implementation of the requirements in user story US17-1 the following applies:

R17-2-1 Communication services implemented on primary devices require an IP data connection. In accordance with the definitions in [NG.102] for IP communication devices and in [RCC.07] for RCS devices the data connection is provided in cellular access networks by bearers using the IMS and the HOS APN, both being independently available from the cellular data connection for generic use via the internet APN. Therefore the implementation of the requirements in US17-1 focus on the ability of the MNO to disable the service based on service provider policy, although a bearer is available.

R17-2-2 CS call over 2G network and CS call over 3G network refer to the circuit switched telephony service. In accordance with the requirement for CS voice in Table 47, this service will be available regardless of the cellular data switch (covering R17-1-1-1).

R17-2-3 VoLTE call over 4G network refers to the Multimedia Telephony service over LTE access defined in [IR.92]. The MNO capability to disable/enable VoLTE as required in Table 47 is implemented by the configuration parameter VOLTE DATA OFF defined in section A.1.15 of [RCC.07] (covering R17-1-1-2).

R17-2-4 SMS over 2G and 3G network refers to the SMS service over circuit switched networks, SMS over General Packet Radio Service (GPRS)and SMS over Signalling Gateways (SG). In accordance with the requirement for SMS in Table 47, this service will be available regardless of the cellular data switch (covering R17-1-1-3).

R17-2-5 IR.92 SMS over 4G network refers to the SMS over IP service. In accordance with the requirement for SMS over IP in Table 47, the MNO capability to disable/enable SMS over IP is implemented by the configuration parameter SMS over IP DATA OFF defined in section A.1.15 of [RCC.07] (covering R17-1-1-5).

R17-2-6 MMS over 2G and 3G network and MMS over 4G network refers to the MMS service being access network agnostic, only requiring SMS to carry push notifications. In accordance with the requirement for MMS in Table 47, the MNO capability to disable/enable MMS is implemented by the configuration parameter MMS DATA OFF defined in section A.1.15 of [RCC.07] (covering R17-1-1-4).

R17-2-7 RCS Messaging over 2G, 3G, 4G network refers to the RCS messaging services 1-to-1 Chat, Group Chat and Standalone Messaging. The MNO capability to disable/enable RCS Messaging as required in Table 47 is implemented by the configuration parameter RCS MESSAGING DATA OFF defined in section A.1.15 of [RCC.07] (covering R17-1-1-6).

NOTE: This configuration does disable also the File Transfer. An MNO is thus not able to disable chat or standalone messaging but enable File Transfer.

R17-2-8 File Transfer over 2G, 3G, 4G network refer to the RCS messaging services refers to the File Transfer service. The MNO capability to disable/enable File Transfer as required in Table 47 is implemented by the configuration parameter FILE TRANSFER DATA OFF defined in section A.1.15 of [RCC.07] (covering R17-1-1-7).

R17-2-9 RCS Enriched Calling Pre-Call and Post-Call services over 3G and 4G networks refer to Content Sharing Call Composer and Post-Call services. The MNO capability to disable/enable RCS Enriched Calling as required in Table 47 is implemented by the configuration parameter PRE AND POST CALL DATA OFF defined in section A.1.15 of [RCC.07] (covering R17-1-1-8).

R17-2-10 Video Share services over 3G and 4G networks refers to Content Sharing Video Share service. The MNO capability to disable/enable RCS Enriched Calling as required in Table 47 is implemented by the configuration parameter CONTENT SHARE DATA OFF defined in section A.1.15 of [RCC.07] (covering the Video Share part of R17-1-1-9).

R17-2-11 Interactive In-Call services over 3G and 4G networks refer to Shared Map and Sketch services. The MNO capability to disable/enable Interactive In-Call services as required in Table 47 is implemented by the configuration parameter CONTENT SHARE DATA OFF defined in section A.1.15 of [RCC.07] (covering the interactive In-Call services part of R17-1-1-9).

R17-2-12 IR.94 ViLTE over 4G networks refers to Conversation video over LTE. The MNO capability to disable/enable ViLTE (IR.94) as required in Table 47 is

implemented by the configuration parameter IP VIDEO CALL DATA OFF defined in section A.1.15 of [RCC.07] (covering R17-1-1-10).

R17-2-13 Operator Provisioning over 2G, 3G, 4G networks refers to Device Management. The MNO capability to disable/enable Provisioning as required in Table 47 is implemented by the configuration parameter PROVISIONING DATA OFF defined in section A.1.15 of [RCC.07] (covering R17-1-1-11).

R17-2-14 To enable Messaging for Multi Device an RCS client needs to synchronize conversation history data for RCS messaging, File Transfer, SMS and MMS with the Common Message Store, consuming IP data. To complete the requirements in US17-1 the MNO should have the capability to disable/enable Conversation history synchronization via the configuration parameter SYNC DATA OFF defined in section A.1.15 of [RCC.07].

R17-2-15 For R17-1-2, this shall be realised through the use of the client configuration parameters defined in section A.1.15 of [RCC.07] that provide separate settings to control the roaming and the on-net behaviour.

R17-2-16 For R17-1-3 and R17-1-4, this shall be realised locally on the device based on the configured values of the client configuration parameters defined in section A.1.15 of [RCC.07].

18 RCS Settings

18.1 Description

RCS is a Service Platform for MNOs 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.

Each setting shall only be applicable if the individual MNO has deployed the correspondent service.

18.2 User Stories and Feature Requirements

US18-1 **As a user, I want to switch between RCS instances on one device to ensure smooth operation.**

NOTE: ‘A RCS “Master Switch” shall be available to activate / deactivate the native RCS functionality on the device.

R18-1-1 Switching the master switch off shall disable all associated RCS services on that device.

R18-1-2 There shall be various entry points on the device for the Master Switch, for example:

- Wireless and Networks settings on the device (if available)
- “Messaging” -> “Settings” (if implemented)
- “Messaging” -> “Settings” -> “Chat Service” (if implemented)

R18-1-3 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).

R18-1-4 Any downloaded applications that have been installed on a device shall have its own means to activate / deactivate the application (this may be provided by the application or the operating system of the device).

US18-2 **As a user, I want to be able to set and change an RCS Chat Alias.**

R18-2-1 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.

US18-3 **As a user, I want to enable or disable Wi-Fi Voice Calling and Wi-Fi Video Calling.**

R18-3-1 Users shall be allowed to turn on or turn off Wi-Fi Voice Calling and Wi-Fi Video Calling using one single switch.

R18-3-2 This user setting shall be visible only when Wi-Fi Voice Calling and/or Wi-Fi Video Calling is activated by the MNO.

US18-4 **[For Integrated Messaging] As a user, I want to switch on/off SMS Delivery Notification.**

R18-4-1 The user shall have the option to select or deselect automatically sending a Delivery Notification for SMS they receive in an Integrated Messaging scenario.

R18-4-2 The default setting shall be based on individual MNO configuration.

US18-5 **As a user, I want to enable or disable automatic MMS download.**

R18-5-1 The user shall have the option to enable or disable automatic MMS download in Integrated Messaging.

R18-5-1-1 The default setting shall be “enabled”.

R18-5-2 The user shall have the option to enable or disable the automatic download of MMS whilst they are roaming.

R18-5-2-1 The default setting shall be “disabled”.

US18-6 **As a user, I want to personalise my device and need access to settings that allow me to do so.**

R18-6-1 The user shall have the option to enable or disable the device Light Emitting Diode (LED) for incoming message or File Transfer notification, both in the case of native or downloadable RCS client.

R18-6-1-1 The default setting shall be “enabled”.

R18-6-2 The user shall have the option to enable or disable the device vibration for incoming message or File Transfer notification, both in the case of native or downloadable RCS client.

R18-6-2-1 The default setting shall be “enabled”.

R18-6-3 The user should have the option to personalise other features of the native or downloadable RCS client. Specifically, the following features should be covered:

- Notification sounds for incoming messages (e.g. xMS, 1-to -1 Messaging Group Chat Messages, File Transfers)
- Notification preferences
- Customised ringtones (for Voice calls or IP Video)
- Visual customisation for chat (for example fonts, bubble styles, backgrounds etc.)

US18-7 **As a user, I want to enable or disable the sending of the notification that tells the sender the message was displayed.**

R18-7-1 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, if supported by the MNO.

R18-7-2 The default for this setting shall be “enabled”.

US18-8 **As a user, I want to enable or disable automatic acceptance for File Transfer.**

R18-8-1 The user shall have the option to enable or disable auto-acceptance for incoming File Transfer:

R18-8-1-1 FT Auto Accept: I/O (default value set to I)

R18-8-1-2 FT Auto Accept while roaming: I/O (default value set to O)

US18-9 **As a user, I want to be able to control the image resizing options in RCS File Transfer.**

R18-9-1 The user shall have to option to set one of the following selections:

R18-9-1-1 always resize a selected option which is then stored as default value

R18-9-1-2 always ask

R18-9-1-3 never resize

R18-9-2 The default setting shall be “always ask”.

R18-9-3 For downscaling pictures, the following requirements shall apply:

R18-9-3-1 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 JPEG 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.

R18-9-3-2 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.

R18-9-3-3 If the factor (F) is 1, the original image shall be transferred.

US18-10 **As a user, I want to be able to control the video resizing options in RCS File Transfer.**

R18-10-1 The user shall have to option to set one of the following selections:

R18-10-1-1 Always resize to a selected option which is then stored as default value

R18-10-1-2 Always ask

R18-10-1-3 Never resize

R18-10-2 The default setting shall be “always ask”.

R18-10-3 The resizing options shall be based on OEM / developer choices including the default value of 480p @ 1200kbps.

R18-10-4 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.

R18-10-5 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.).

US18-11 **As a software developer, I want to display on request an ‘about’ page that explains details of the RCS client.**

R18-11-1 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.

US18-12 **As an Integrated Messaging user, I want to influence the proposed service for messages and transferring files.**

R18-12-1 If the MNO configured the device for Integrated Messaging, a setting shall allow the user to select the default sending method to be used when the user sends a message or file. The user is able to select:

- ‘Proposed Messaging Service’ (follow Integrated Messaging behaviour as defined in Integrated Messaging requirements), or
- ‘SMS’ and 'MMS' (if MMS is disabled, the option will be SMS and SMS with link) or
- ‘RCS chat’ and 'RCS File Transfer’.

US18-13 **As an Integrated Messaging user, I want to be able to change my preference for whether undelivered RCS messages will follow the Client Fallback SMS (CFS) mechanism or not. The user shall be able to set one of the following options, applicable in the situations in which CFS takes place (see R5-2-4-4:**

R18-13-1 Always resend undelivered RCS messages as SMS (and don’t ask),

R18-13-2 Always ask,

R18-13-3 Never resend undelivered RCS messages as SMS (and don’t ask).

R18-13-4 The default for this setting shall be configurable by the MNO.

US18-14 **As an Integrated Messaging user, I want to be able to change my preference for whether undelivered RCS files are automatically sent again by SMS link or not.**

R18-14-1 The user shall be able to set one of the following options:

R18-14-1-1 Always resend undelivered RCS Files as SMS link (and don't ask),

R18-14-1-2 Always ask,

R18-14-1-3 Never resend undelivered RCS Files as SMS link (and don't ask).

R18-14-1-4 The default for this setting shall be configurable by the MNO.

US18-15 **As a user, I want to be able to block specific contacts**

R18-15-1 It shall be possible to block specific contacts.

R18-15-2 All incoming communications from an identified blocked contact shall be blocked by the device.

R18-15-3 The user shall not be notified about any incoming communications from a contact on their local device blacklist.

R18-15-4 The blocked sender shall not be notified about the status of being blocked. Operator Messages and file transfers shall indicate the "sent" and "delivered" states as appropriate and shall not indicate "displayed".

R18-15-5 In the case that a blocked contact makes a voice or video call, they will hear a ringtone or busy tone. Any further call treatment is determined by the MNO.

R18-15-6 Exception: In the case where a blocked contact is participating in a Group Chat, the requirements above shall not apply.

US18-16 **As a user, I want to select the active RCS SIM on a Dual SIM Device.**

R18-16-1 The user shall be able to change the selection to another RCS SIM at any time. (See section 2.2.9 which applies in their entirety).

R18-16-2 The switch between SIMs shall only be visible in the case that both SIMs are RCS capable.

18.3 Technical Information

A number of requirements for service configuration parameters on the client are provided.

18.3.1 Technical Implementation of User Stories and Service Requirements

R18-17-1 The technical implementation of the requirements for user story US18-1 to switch between multiple RCS instances on a device are provided in Device Provisioning, see section 2.2.

R18-17-2 The technical implementation of the requirements of US18-1 regarding Master Switch shall be provided by client via the following procedures:

- If the user changes the value of the "Master Switch" from "ON" to "OFF", the client shall send a HTTP client configuration request with the "vers" parameter defined in [RCC.14] set to the value stored for the local client configuration and the "rcs_state" parameter defined in [RCS6.0] to "-4". The client shall expect configuration server responses as defined for client configuration requests with positive integer values in the "vers" request parameter as defined in [RCC.14] and process is accordingly. The client shall keep the lasts client configuration data locally stored.
- If the validity of the configuration XML document expires or it receives a network request for client configuration as defined in section 3 of [RCC.14] and the "Master Switch" is set to "OFF", then the clients shall not send a HTTP configuration request but keep the configuration data locally stored.
- If the user changes the value of the "Master Switch" from "OFF" to "ON" then the client shall send a HTTP client configuration request with the "vers" parameter defined in [RCC.14] and the "rcs_state" parameter defined in [RCS6.0] to the value stored for the local client configuration.
- If the user changes the value of the "Master Switch" from "ON" to "OFF" 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/VoWiFi capable and the IMS registration covers VoLTE/VoWiFi, then the client shall re-register to remove the services apart from IP Voice Call and IP Video Call, SMS over IP (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 "Master Switch" from "ON" to "OFF" and the client is in RCS-VoLTE device mode, then it shall terminate existing sessions and cancel existing requests for services other than IP Voice Calls and IP Video Call and SMS over IP (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.94] respectively.
- If the user changes the value of the "Master Switch" from "OFF" to "ON" and the client is not registered for any of the IP Voice Call, IP Video Call or SMS over IP, then the client shall register in IMS for any supported and active RCS services.
- If the user changes the value of the "Master Switch" from "OFF" to "ON", and the client is registered for any of the IP Voice Call, IP Video Call or SMS over IP, then it shall re-register in IMS to add the feature tags of any supported and active RCS services according to configuration.
- If the "Master Switch" is set to "OFF" and the client is registered in IMS for any of the IP Voice Call, IP Video Call or SMS over IP 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 "Master Switch" is set to "OFF", and Backup & Restore as defined in section 9 is enabled then the client shall not synchronise with the common message store if a trigger as defined in section 4.1.6.8 of [RCC.07] applies.
- If the user changes the value of the "Master Switch" from "ON" to "OFF", the RCS client shall log-out from a session with the Common Message Store.
- If the user changes the value of the "Master Switch" from "OFF" to "ON" and Backup & Restore as defined in section 9 is enabled then the RCS client shall take this as a trigger for synchronization with the Common Message Store.

R18-17-3 The requirements for user story US18-2 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].

R18-17-4 The term ‘IP Voice Call’ is interpreted as IR.51 Voice over Wi-Fi in this context. The requirements for user story US18-3 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 A.1.12 of [RCS6.0] 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. 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.

R18-17-5 As a clarification to the requirements for user story US18-4, 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 5.3.1) 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.

R18-17-6 The configuration parameter defined in the requirements for user stories US18-5, 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 7.3 of IR.92.

R18-17-6-1 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.

R18-17-6-2 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 US18-5.

R18-17-7 The requirements for user story US18-6 shall be implemented locally on the device.

R18-17-8 Requirement R18-7-1 shall be implemented in accordance with the DISPLAY NOTIFICATION SWITCH clent configuration parameter defined in section 5.3.7.1. When display notification is supported by the Service Provider, the DISPLAY NOTIFICATION SWITCH parameter shall be set to 0. If sending notifications about messages being displayed is disabled by the user, then a client receiving a message or file shall ignore the disposition notification header with value “display” and not generate a notification for “displayed”.

When display notification is not supported by the Service Provider, the DISPLAY NOTIFICATION SWITCH parameter shall be set to 1. In this case, the user is not able to enable/disable the Display Notification setting

R18-17-9 .The configuration parameters for automatic acceptance of File Transfer of US18-8 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.

R18-17-10 The requirements for user stories US18-9 to US18-12 shall be implemented locally on the device.

R18-17-11 Requirements R18-13-1 to R18-13-3 shall be implemented locally on the device. For requirement R18-13-4, the MESSAGING FALLBACK DEFAULT client configuration parameter defined in section 5.3.7.1 shall be set.

R18-17-12 Requirements R18-14-1 to R18-14-1-3 shall be implemented locally on the device. For requirement R18-14-1-4, the FT FALLBACK DEFAULT client configuration parameter defined in section 7.3.3.1 shall be set.

R18-17-13 The technical implementation of the requirements of user story US18-15 shall be implemented as follows:

R18-17-13-1 Requirement R18-15-4 shall be implemented locally on the device. For 1-to-1 chat; the procedures of section 3.3.4.1.1 of [RCC.07] shall apply.

R18-17-13-2 For File Transfer via HTTP, Audio Messaging and Geolocation Push; the client shall apply the procedure for the chat message as defined in R18-17-13-1. For chat messages for File Transfer via HTTP or Audio

Messaging the client shall not continue the File Transfer procedure, i.e. not attempt to download the thumbnail or the file from the FT content server.

R18-17-13-3 To satisfy the requirement R18-15-6 the client shall not screen received session invitations or chat messages received in a Group Chat session for originator addresses contained in the local client blacklist.

R18-17-13-4 To satisfy the requirements of R18-15-5, if the client receives an incoming call request for a voice or video call from an address contained in the client local blacklist, then the client shall, based on a client implementation option,

- accept the incoming call request without notifying the user and without answering the call,
- reject the incoming call request based the procedures defined for user determined user busy.

R18-17-13-5 For Enriched Pre-Call and Post call services; if the client receives a session invitation for an RCS Enriched Calling session from an address contained in the client local blacklist, the client shall accept the session request and all received Pre-call and Post-call elements as defined in [RCC.20] but not notify the user.

R18-17-13-6 For a short message received from an originator address contained in the client local blacklist, the client shall confirm the delivery, shall not notify the user and shall discard the short message.

R18-17-13-7 For MMS messages, if the client receives a MMS Notification from an originator address contained in the client local blacklist, the client shall confirm MMS Notification, shall stop processing of the MMS transaction and shall not notify the user.

R18-17-14 The technical implementation of the user story US18-16 shall be implemented locally on the device.

19 Multi Device Voice and Video

19.1 Description

Multi device Voice and Video (MDV[2]) allows the user to make and receive phone calls on a variety of devices and interfaces other than the mobile device containing the primary SIM. Examples of devices include but are not limited to non-native interfaces on smartphones containing a SIM other than the primary SIM, tablets, laptops and connected watches. The devices may connect using any kind of data connection (e.g. mobile data, Wi-Fi).

19.2 User Stories and Feature Requirements

NOTE: the requirements in this section are indicative and may change significantly once technical feasibility is completed as part of the future versions of the Universal Profile.

US19-1 **As a user, I would like to use various connected devices for my preferred MNO voice and video calling service.**

R19-1-1 All devices I use shall use one identity for any incoming or outgoing calls.

R19-1-2 The used identity shall be the MSISDN of the primary device.

NOTE: Any devices which are not the primary device are called secondary device(s).

R19-1-3 A secondary device is linked to the identity of the primary device using the MDV2 federation process.

NOTE: One single secondary device may carry multiple secondary instances which are federated with different identities.

R19-1-4 If an MNO has deployed an RCS Multi Device Messaging (MDM) service, the federation process shall span both MDM and MDV2 processes (from the user perspective).

R19-1-5 Secondary devices may use a SIM to authenticate to the network (not to the MDV2 service!) or use a SIM-less data connection.

R19-1-6 SIM based secondary devices may or may not be linked to the primary identity as part of a Multi-SIM implementation of the MNO.

NOTE 1: If the SIM based device could make and / or receive phone calls under its own identity, this capability shall not be affected by the federation with a primary device.

NOTE 2: Multi-SIM is not in scope of the proposed MDV^2 solution.

R19-1-7 A connected device shall fulfil certain pre-requisites to be used as a primary or secondary device for MDV^2:

R19-1-7-1 The device shall support connectivity to the MNO voice service (details tbd in technical implementation).

R19-1-7-2 The device shall support speaker and microphone.

R19-1-7-3 To allow Video services, the device shall support a video camera and capable display. If these requirements are not met, the device will not support Multi Device Video services.

R19-1-7-4 The device shall support a voice call application compatible with MNO voice calling, incl. a dialler. If Multi Device Video Calling is supported, an MNO video calling application shall be supported.

R19-1-7-5 The device shall support an application that supports the federation process.

R19-1-7-6 The device may support a call log.

R19-1-7-7 The device shall be capable to alert the user.

R19-1-8 There shall be an overview over all federated devices and key settings of these on the primary device.

R19-1-9 The federation process shall be initiated from the primary device. This process shall be secure to prevent abuse.

R19-1-10 The following device types shall be supported (non-exhaustive list):

R19-1-10-1 Primary device: SIM- based (smart) phone

R19-1-10-2 Secondary device: SIM-based Smartphone, feature phone or basic phone (in a Multi-SIM configuration or stand-alone).

R19-1-10-3 Secondary device: tablet computer (SIM based or non-SIM based).

R19-1-10-4 Secondary device: Laptop or PC.

R19-1-10-5 Secondary device: browser-based on any connected device.

R19-1-10-6 Secondary device: fixed line phone (not all MDV features may be supported). (Fixed line phone shall keep their fixed line identity in parallel.)

R19-1-11 All MDV2 calling services and features shall be available (unless stated differently) on any of the federated devices irrespective of the status of any other federated device (including primary device).

US19-2 **As a user, I want to receive calls on any of my MNO voice and/or video capable devices.**

R19-2-1 For incoming calls, the user shall be able to configure a ringing pattern across all federated devices:

R19-2-1-1 Parallel ringing, or

R19-2-1-2 Sequential ringing in the sequence defined by the user, or

R19-2-1-3 Selected devices ringing in a pre-defined sequence (e.g. device 1 first, 15 seconds, then devices 2, 3 and 4 in parallel, then 5).

R19-2-2 Viewing / changing settings for ringing pattern at incoming calls shall be supported on the primary device and the secondary device(s).

R19-2-3 An incoming call shall alert the user on any of the federated devices (regardless of the ongoing activity) to allow the user to accept the call.

R19-2-4 The call can be accepted on any of the devices which are actually alerting the user of an incoming call.

R19-2-5 When the call is answered on one device all other federated devices shall stop alerting the user of an incoming call.

R19-2-6 If the call has been answered by the called party, there shall not be any notification of a missed call on any of the federated devices.

R19-2-7 If the call has not been answered by the called party, all devices shall notify a missed call.

R19-2-8 If a missed call notification has been cleared on one device (e.g. because the user has seen the missed call notification), then the missed call notification shall be immediately cleared on all reachable federated devices.

R19-2-9 If a device is not reachable, then updates on that device are not performed. When a device comes online again, all previous notifications shall be updated.

R19-2-10 Ring tones shall be user configurable across the federated devices, e.g. all ring tones identical across all federated devices or differentiated ringtones across federated devices.

R19-2-11 The minimum set of IR.92 supplementary services shall be available across all devices for incoming calls.

R19-2-12 RCS Enriched Calling services shall be available across all devices that are Enriched Calling capable for incoming calls if supported by the MNO.

R19-2-13 If one device is active in a call, one of the federated devices should still be available for another outgoing call.

R19-2-14 If one device is active in a call, one of the federated devices should still be available for another incoming call.

R19-2-15 The MNO should be able to restrict the number of parallel lines available.

NOTE: This restriction shall not affect the ability of making an emergency call from any device.

R19-2-16 Federated devices can receive incoming MDV[2] calls via MNO managed voice and video services, such as CS, VoLTE, VoWiFi, ViLTE or ViWiFi.

US19-3 **As a user, I want to initiate calls from any of my MNO voice and / or video capable devices.**

R19-3-1 Any device shall be able to initiate a call from different service entry points:

R19-3-1-1 The dialler application.

R19-3-1-2 The contact list application (if available).

R19-3-1-3 The call logs application (if available).

R19-3-2 The minimum set of IR.92 supplementary services shall be available across all devices for outgoing calls

NOTE: Calling Line ID Presentation of outgoing call initiated from secondary device will adopt the MSISDN of the primary device, notwithstanding if secondary device has its own SIM.

R19-3-3 If the user calls his own phone number (identity of the primary device), then any of the other federated devices shall indicate an incoming call and if

accepted, a call between a primary and a secondary device or between two secondary devices shall be established.

R19-3-4 RCS Enriched calling services shall be available across all devices that are Enriched Calling capable for outgoing calls.

R19-3-5 Federated devices can make MDV[2] calls via MNO managed voice and video services, such as CS, VoLTE, VoWiFi, ViLTE or ViWiFi.

US19-4 **As a user, I want to use consistent call logs on all of my federated devices.**

NOTE: Call Log requirements in this section only apply if a device has call logs implemented.

R19-4-1 Each calling event (incoming or outgoing) shall be logged in the call log of the device.

R19-4-2 Call log applications on the device shall support administrative functions such as deleting a selected call log entry.

R19-4-3 Call logs shall support RCS Enriched Calling features if Enriched Calling is supported on that particular device.

R19-4-4 Call logs shall be available across all devices in a consistent way, upon configuration of the user.

R19-4-5 Call logs shall provide the following:

R19-4-5-1 Other party involved in call.

R19-4-5-2 Incoming or outgoing call.

R19-4-5-3 Date and timestamp when the call was established.

R19-4-5-4 Duration.

R19-4-5-5 Enriched Calling media according to Enriched Calling requirements.

R19-4-5-6 Some of the call log information may be available in a “Detailed View” only.

R19-4-5-7 Filter options for display of incoming / outgoing / missed calls / accepted calls / rejected calls.

R19-4-5-8 Voice call / video call differentiator.

R19-4-6 Call logs shall highlight missed call events to guide the user’s attention. Once seen, the highlight shall disappear without dedicated user interaction (i.e. manually clearing notifications).

R19-4-7 Updates of call logs shall be available for the user in real time. The user shall be able to configure the device to balance between real time updates and battery power saving.

R19-4-8 Call logs may offer inclusion from other events (e.g. messaging events) but shall offer the possibility to display pure call related logs.

US19-5 **As a user, I want to be able to administrate my MDV^2 settings.**

NOTE: Any potential suspension of MDV^2 calling service does not affect any other calling service on a particular device

R19-5-1 It shall be possible to suspend the MDV^2 services on a secondary device for that particular secondary device.

R19-5-2 It shall be possible to remotely suspend MDV^2 services on any federated devices from the (online) primary device.

R19-5-3 There shall not be a dedicated 'call suspension function' on a primary device (it is accepted that power off effectively suspends calling services on the primary device).

R19-5-4 It shall be possible to administrate the settings for incoming calls from any of the federated devices.

R19-5-5 All federated devices have access to the same set of settings if stored in online database (not applicable to local device settings).

US19-6 **As a user, I want to use multiple devices for video calls and In-Call services.**

R19-6-1 It shall be possible to separate voice from In-Call service (on devices that support Video Call or Enriched Calling) across two of the federated devices (e.g. keeping audio on a Smartphone device and switch the video part, file share, or geolocation share to a secondary (e.g. large screen) device).

US19-7 **As a user, I want to transfer calls from one device to another federated device.**

R19-7-1 The user shall be able to transfer an ongoing voice or video call (either user initiated or incoming call) from one device to another federated device.

NOTE: The call transfer can be initiated from the device currently active in the call to another federated device as 'Call Push' operation. Alternatively, the user can use 'Call Pull' operation, from another federated device not active in the call, to initiate the call transfer.

R19-7-2 In-Call sharing content shall be accessible on the device that carries the call.

R19-7-3 This call transfer shall be virtually unlimited, i.e. a transferred call be handed over to the next federated device or handed back to the original device at any time.

US19-8 **As a user, I want to have more than one active device on the same call.**

R19-8-1 The user shall be able to make a call or receive a call on one of the federated devices, and add another of the federated devices to that particular call as long as there is at least one of the federated devices active on that call.

R19-8-2 The maximum number of federated devices on the same call equals the number of federated devices.

US19-9 **As an MNO, I want my MDV^2 service to be in line with local regulations.**

R19-9-1 All federated device shall support emergency calls (including actual calling device location).

R19-9-2 Legal interception shall be possible for any made or received calls on primary or secondary device, for both incoming and outgoing calls.

Annex A Supporting requirements

A.1 Personal Card format

Section 3.5.4.9.1 of [RCC.07] does not apply for the profile defined in this document. The following text applies instead.

There is multiple formats for the transfer of Personal Cards. This Annex defines the transfer formats and procedures for Personal Cards in RCS.

A RCS client shall support receiving the following formats:

- the vCard 2.1 format as defined in [vCard21]
- the vCard 3.0 format as defined in [RFC2425] and [RFC2426]

In addition, a RCS client may support receiving the following format:

- the Personal Contact Card (PCC) format defined in [CAB_TS]).

In the profile defined in this document the vCard 3.0 format as defined above shall be used for sending.

Variations in the implementation of Personal Card formats may lead to data loss when Personal Cards are exchanged. To limit the effect, the following fields are considered key fields for RCS. No data of these fields should be lost when contact information is exchanged in RCS.

- **Name:** Composed names (such as “Jean-Baptiste”) shall be supported properly.

- **Personal Information:**

    - Nickname
    - Photo
    - Birthdate
    - Comment

- **Telephone numbers:** 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:

    - Email work 1
    - Email work 2
    - Email home 1
    - Email home 2
    - Other

- **Address information:**
    - Address
    - Geographic Position
    - Time zone

Sending and receiving of a Contact Card using File Transfer via HTTP or File Transfer fallback is technically the same as sending any other file. For details about the File Transfer technologies refer to section 7 of this document.

If the format for transferring a Contact Card is vCard 2.1 or vCard 3.0, then the MIME content type “text/vcard” shall be used for File Transfer.

If the format for transferring the Contact Card is the CAB (Converged Address Book) 1.0 PCC XML format, then the CAB PCC MIME content type “application/vnd.oma.cab-pcc+xml” shall be used for File Transfer.

On the receiving side, if the receiving RCS user adds the Contact Card delivered through File Transfer to the local address book, the receiving RCS client shall apply the mapping of the RCS supported fields between the received format and the used format of the local address book database. For conversion between PCC and vCard formats refer to section 5.4.3 of [OMA-CAB].

If the receiving client does not support the format of a Contact Card, then the client handling for unsupported content types applies.

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	:’-) and :”-) 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

Emoticons	Character sequences	Examples describing graphical renditions
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
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 rock star 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

Emoticons	Character sequences	Examples describing graphical renditions
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
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.

A.4 Panoramic photo view

RCS devices shall be able to record, display and share panoramic pictures in a user-convenient way. The requirements in this Annex A.4 shall be considered as guidelines for the implementations; screen examples are provided to illustrate these requirements but shall by no means mandate any design or UI principles. If a recorded panoramic view covers less than 360 degree full circle pictures the requirements shall be applied accordingly.

Recording Panoramic photos

- The device shall offer the ability to record cylindrical photos.

- Panoramic Photos shall be stored in a compressed mode to limit memory requirements.
- Panoramic Photos shall be recorded in a way that a full 360 degree ‘cylinder’ is recorded or a fraction of the complete 360 degree view.
- Resolution and quality shall allow zoom in to see details.
- Panoramic Photos shall be stored in a location on the device that is easy to find and to select for further operation (e.g. sharing).
- Recording a Panoramic Photo shall be limited to approximately 360 degree circle. If the user stops recording of the panoramic photo before the 360 degree circle is complete, requirements for recording, viewing and sharing shall be valid accordingly.

Viewing Panoramic Photos

- The device shall display Panoramic Photos in a user convenient way.
    - The picture shall be displayed in full display size view of a fraction of the full picture, i.e. the picture is always displayed in full height, areas left and right of the displayed areas can be selected. Black barred areas of the screen shall be avoided.

Figure 5: Maximum zoom out (device in portrait mode)

Figure 6: Maximum zoom out (device in landscape mode)

    - Portrait and landscape mode shall be supported without distortion of the picture.
- The user shall have the option to select from different navigation methods inside a Panoramic Photo:
    - The user shall be able to select the default navigation method for navigating the picture.

- Automatic navigation: the display cylinder rotates automatically at a user definable speed. The default speed shall be convenient for most user applications.

- Finger navigation: the user can navigate the picture by shifting a finger on the screen left and right.

- Gyro navigation: The cylinder section that is on display is selected by moving the phone physically. The sensitivity of the navigation shall be customizable: over-sensitive (i.e. by moving the phone e.g. 90 degrees left or right, the cylinder shall be scrolled by 360 degrees (or proportions of this movement)) or regular (to turn the picture for 180 degrees the phone needs to be turned by 180 degrees).
  NOTE: The setting may be user accessible or fixed by the application, e.g. to allow for 'close to real' navigation with 360 degree glasses.

- For large device use (e.g. PC, Laptop, TV), the application shall offer navigation based on the available input devices (e.g. keyboard or mouse).

Figure 7: Navigation options when fully zoomed out

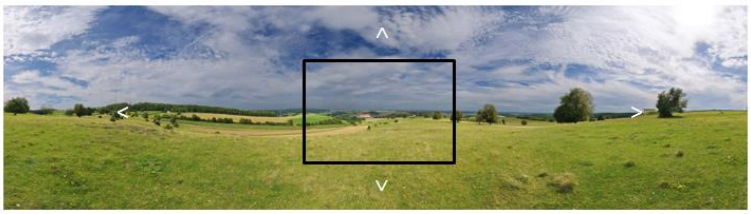

Figure 8: Navigation options when zoomed in

- The user shall be able to zoom in and out again on the Panoramic Photo to focus on details.
- The Panoramic Photo application shall contain a few pre-loaded 360 Degree Photos to allow the user to get used to UI and value of this technology.

Sharing 360 Degree Panoramic photos

- Sharing Panoramic Photos shall be possible using the RCS File Transfer mechanisms.

  - Service entry points for Panoramic Photo sharing shall be in 1- to-1 Messaging, Group Chat, the device gallery and other locations.

- Panoramic Photos shall not be compressed when shared via RCS file transfer, even when "always compress" is a default setting for picture sharing.

    - The user shall be made aware of the impact on data transfer volume and time.
- When receiving a Panoramic Photo, the preview icon shall show the centre of the picture whenever the preview icon appears on the display.
    - Navigation inside the pre-view picture shall be enabled.
    - The application may automatically scroll through the panoramic picture in the preview.
    - Zoom in / out shall not be available.
- Before download, the file size of the Panoramic Photo shall be visible to the end user (if manual file transfer confirmation is required).

Annex B Multiple Client handling on Android™ OS

On Android™ devices, multiple client handling depends on the Android™ OS version running on that device.

Note: Android™ embedded RCS devices implementing the Universal Profile are assumed to be running and Android™ OS version superior or equal to 7.0. RCS downloadable clients cannot follow this rule as they can be downloaded and installed on any Android™ OS version.

B.1 Multiple Client handling on Android™ OS version superior or equal to 7.0

For embedded RCS devices or downloadable applications running on Android™ OS version superior or equal to 7.0:

- On a non RCS device or an embedded RCS device where the stack cannot be used by other applications than the native client, the required behaviour is:
    - Any RCS client (embedded or downloadable application) shall only activate its own RCS stack when it is set as the Default SMS app.
    - Enriched Calling services shall only be enabled when the Default Dialler supports RCS Enriched Calling services and can use the RCS stack of the messaging application set as the Default SMS app to implement Enriched Calling services.
    - Pre-Call, Shared Sketch, Shared Maps, Video Share and Post-Call services shall be disabled:
        - either when the dialler set as Default Dialler does not support Enriched Calling.
        - or when the dialler that supports Enriched Calling is set as Default Dialler but cannot use the RCS stack of the messaging application set as Default SMS app.

NOTE: When the default messaging application is a downloadable application, it is up to the application to provide RCS Enriched calling services even if this downloadable application is not set as default dialler.

- On an embedded RCS device where the RCS stack is opened to other applications than the native clients, the required behaviour is:
    - Any RCS messaging application becoming the Default SMS app should rely on the native RCS stack to implement RCS messaging services.
    - Any Enriched Calling application becoming the Default Dialler should rely on the native RCS stack to implement RCS Enriched Calling services.
    - The embedded RCS stack shall not register the RCS messaging features to the IMS when the messaging application set as the default SMS app does not support RCS messaging features.
    - The embedded RCS stack shall not register the Pre-Call, Shared Sketch, Shared Maps, Video Share and Post-Call features tags to IMS when the Default Dialler does not support Enriched Calling features.

NOTE 1: As a consequence, In-Call Chat and In-Call File Transfer as defined in section 12.4.3 and 12.4.4 are not available when the default SMS app does not support RCS messaging services.

NOTE 2: Once devices using embedded stack with open access to other messaging and dialler applications than the native clients are available in the market, a downloadable RCS application with its own stack should only activate its stack when either installed on a non RCS device or on an embedded RCS device where the RCS stack is not opened to other applications and when set as default SMS app.

On Android™ OS version superior or equal to 7.0, in order for the RCS client or RCS stack to be notified of Default SMS app changes and Default Dialler change, the RCS client shall listen for the broadcast of the Android™ Intents:

- "ACTION_DEFAULT_SMS_PACKAGE_CHANGED".
- "ACTION_DEFAULT_DIALER_CHANGED"

B.2 Multiple Client handling on Android™ OS version prior to 7.0

For downloadable applications running on Android™ version strictly inferior to 7.0 and because the Intent "ACTION_DEFAULT_SMS_PACKAGE_CHANGED" is not available in that case, multiple instance handling shall be implemented locally on the device following one of the two options described below:

Option 1- Retrieve the client list and if other client is active ask the user to disable it

- 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.

Android™ RCS downloadable clients installed on Android™ OS version prior to 7.0 shall define the following meta-data properties in their Manifest.xml file[1].

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 48: Android™ RCS client Manifest meta-data properties

[1] 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.

Android™ RCS downloadable clients installed on Android™ OS version prior to 7.0 shall define a settings screen activity that can be open 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 49: Android meta-data usage

Android™ RCS downloadable clients installed on Android™ OS version prior to 7.0 shall define a publicly readable Shared Preferences using the name "*pckgname.gsma.joyn.preferences*", where '*pckgname*' parameter shall be replaced with 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:

- True: It will mean that the RCS client is enabled (user switch in settings set to ON) and the application has been provisioned successfully.
- 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.

Client start-up behaviour

For the client implementations that choose to implement this option when started for the first time on a device working on Android™ OS whose version is inferior to 7.0 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".

On Android™ OS whose version is strictly inferior to 7.0, client shall indicate

- that it is active by opening its own "pckgname.gsma.joyn.preferences" shared preferences and set its own "gsma.joyn.enabled" property to "True".
- that it has become inactive by opening its own "*pckgname.gsma.joyn.preferences*" shared preferences and set its own "*gsma.joyn.enabled*" property to "False".

Option 2- Retrieve the client list and if other client is installed not attempt provisioning or registration.

For the client implementations that choose to implement this option when the client becomes the Default SMS app or when it is already set as the Default SMS app but there is an application update on a device working on Android™ OS whose version is inferior to 7.0 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 first section of the previous option.
- If an RCS client is found (i.e. their shared preferences with the respective properties described for option 1 are present), the client shall not attempt provisioning or registration.
- If none RCS client is found, the client shall activate its own stack.

  - If the RCS client loses its' Default SMS app status it shall de-register.

Annex C Configuration Parameters

This Annex provides an overview of all configuration parameters that are applicable for the profile defined in this document with indications on whether client configurability is expected or whether clients can assume the parameter to always have a fixed value. Next to that, it indicates for parameters whether there is an aligned value for this profile even if for that parameter client configurability is still expected to allow for future evolution. If this is the case for a parameter configured a numeric range, a client shall where applicable allow both higher and lower values than what is provided.

Parameter	Functional Definition	Syntax Definition for transport using [RCC.14]	Client Configurability	Aligned Value for this profile
IMS Parameters				

Parameter	Functional Definition	Syntax Definition for transport using [RCC.14]	Client Configurability	Aligned Value for this profile
ConRef	[3GPP TS 24.167]	[RCC.15]	Fixed dummy value: *dummy.apn*	
PDP_ContextOperPref	[3GPP TS 24.167]	[RCC.15]	Fixed value: 0	
P-CSCF_Address	[3GPP TS 24.167]	[RCC.15]	Not instantiated	
Timer_T1	[3GPP TS 24.167]	[RCC.15]	Service provider configurable	
Timer_T2	[3GPP TS 24.167]	[RCC.15]	Service provider configurable	
Timer_T4	[3GPP TS 24.167]	[RCC.15]	Service provider configurable	
Private_user_identity	[3GPP TS 24.167]	[RCC.15]	Service provider configurable	
Public_user_identity	[3GPP TS 24.167]	[RCC.15]	Service provider configurable	
Home_network_domain_name	[3GPP TS 24.167]	[RCC.15]	Service provider configurable Recommended to use ims.mnc<MNC>.mcc<MCC>.pub.3gppnetwork.org whereby <MNC> and <MCC> shall be replaced by the respective values of the home network in decimal format and with a 2-digit Mobile Network Code (MNC) padded out to 3 digits by inserting a 0 at the beginning (as defined in [PRD-IR.67]).	
ICSI_List	[3GPP TS 24.167]	[RCC.15]	Tree is instantiated, but no leafs shall be provided.	
LBO_P-CSCF_Address	[3GPP TS 24.167]	[RCC.15]	Tree is instantiated	

Parameter	Functional Definition	Syntax Definition for transport using [RCC.14]	Client Configurability	Aligned Value for this profile
Address (LBO_P-CSCF_Address)	[3GPP TS 24.167]	[RCC.15]	Service provider configurable	
AddressType (LBO_P-CSCF_Address)	[3GPP TS 24.167]	[RCC.15]	Service provider configurable	
Resource_Allocation_ Mode	[3GPP TS 24.167]	N/A	Not instantiated	
Voice_Domain_Preference_E_UTRAN	[3GPP TS 24.167]	[RCC.15]	Service Provider Configurable	
SMS_Over_IP_Networks_Indication	[3GPP TS 24.167]	[RCC.15]	Service Provider Configurable	
Keep_Alive_Enabled	[3GPP TS 24.167]	[RCC.15]	Service Provider Configurable	1
Voice_Domain_Preference_UTRAN	[3GPP TS 24.167]	N/A	Not instantiated	
Mobility_Management_IMS_Voice_Termination	[3GPP TS 24.167]	[RCC.15]	Service Provider Configurable	
RegRetryBaseTime	[3GPP TS 24.167]	[RCC.15]	Service Provider Configurable	
RegRetryMaxTime	[3GPP TS 24.167]	[RCC.15]	Service Provider Configurable	
PhoneContext_List	[3GPP TS 24.167]	N/A	Tree not instantiated	
SS_domain_setting	[3GPP TS 24.167]	[RCC.15]	Service Provider Configurable	
PS_domain_IMS_SS_control_ preference	[3GPP TS 24.167]	[RCC.15]	Service Provider Configurable	
IMS Mode Authentication Type	[RCC.15]	[RCC.15]	Service Provider Configurable	
Realm	[RCC.15]	[RCC.15]	Service Provider Configurable	
Realm User Name	[RCC.15]	[RCC.15]	Service Provider Configurable	
Realm User Password	[RCC.15]	[RCC.15]	Service Provider Configurable	
Transport Protocols: Signalling Cellular	[RCC.15]	[RCC.15]	Service Provider Configurable SIPoTLS recommended	

Parameter	Functional Definition	Syntax Definition for transport using [RCC.14]	Client Configurability	Aligned Value for this profile
Transport Protocols: Signalling Roaming	[RCC.15]	[RCC.15]	Service Provider Configurable SIPoTLS recommended	
Transport Protocols: Signalling Wi-Fi	[RCC.15]	[RCC.15]	Service Provider Configurable	SIPoTLS, if authentication different from IMS AKA is used and thus IPsec is not enabled
Transport Protocols: Real Time Media Cellular	[RCC.15]	[RCC.15]	Service Provider Configurable SRTP recommended	
Transport Protocols: Real Time Media Roaming	[RCC.15]	[RCC.15]	Service Provider Configurable SRTP recommended	
Transport Protocols: Real Time Media Wi-Fi	[RCC.15]	[RCC.15]	Service Provider Configurable	SRTP if authentication different from IMS AKA is used and thus IPsec is not enabled
Transport Protocols: Discrete Media Cellular	[RCC.15]	[RCC.15]	Service Provider Configurable MSRPoTLS recommended	
Transport Protocols: Discrete Media Roaming	[RCC.15]	[RCC.15]	Service Provider Configurable MSRPoTLS recommended	

Parameter	Functional Definition	Syntax Definition for transport using [RCC.14]	Client Configurability	Aligned Value for this profile
Transport Protocols: Discrete Media Wi-Fi	[RCC.15]	[RCC.15]	Service Provider Configurable	MSRPoTLS if authentication different from IMS AKA is used and thus IPsec is not enabled
RCS VOLTE SINGLE REGISTRATION	[RCC.07] NOTE: VoLTE would register immediately on first boot up if relevant. If after autoconfiguration the device is configured to do single registration, the client should send a REGISTER request (re-registration) to add the additional feature tags for RCS.	[RCC.07]	Service Provider Configurable	
RCS State Parameters				
RCS DISABLED STATE	[RCC.07]	[RCC.07]	Service Provider Configurable	
Presence Parameters				
CLIENT-OBJ-DATA-LIMIT	[PRESENCE2MO]	[RCC.07]	Service Provider Configurable if CAPABILITY DISCOVERY MECHANISM is set to 1. Not instantiated otherwise.	
CONTENT-SERVER-URI	[PRESENCE2MO]	N/A	Not instantiated	

Parameter	Functional Definition	Syntax Definition for transport using [RCC.14]	Client Configurability	Aligned Value for this profile
SOURCE-THROTTLE-PUBLISH	[PRESENCE2MO]	[RCC.07]	Service Provider Configurable if CAPABILITY DISCOVERY MECHANISM is set to 1. Not instantiated otherwise.	
MAX-NUMBER-OF-SUBSCRIPTIONS-IN-PRESENCE-LIST	[PRESENCE2MO]	[RCC.07]	Service Provider Configurable if CAPABILITY DISCOVERY MECHANISM is set to 1. Not instantiated otherwise.	
SERVICE-URI-TEMPLATE	[PRESENCE2MO]	N/A	Not instantiated	
RLS-URI	[PRESENCE2MO]	[RCC.07]	Service Provider Configurable if CAPABILITY DISCOVERY MECHANISM is set to 1. Not instantiated otherwise. Recommended Value: presence-rls@ims.mnc<MNC>.mcc<MCC>.pub.3gppnetwork.org whereby <MNC> and <MCC> shall be replaced by the respective values of the home network in decimal format and with a 2-digit MNC padded out to 3 digits by inserting a 0 at the beginning	

Parameter	Functional Definition	Syntax Definition for transport using [RCC.14]	Client Configurability	Aligned Value for this profile
PRESENCE PROFILE	[RCC.07]	[RCC.07]	Fixed Value: 0	
NOTE MAX SIZE	[RCC.07]	N/A	Not instantiated	
LOCATION VALIDITY	[RCC.07]	N/A	Not instantiated	
NON-VIP CONTACTS POLL MAX FREQUENCY	[RCC.07]	N/A	Not instantiated	
XDM parameters				
XCAP Root URI	[XDMMO]	N/A	Not instantiated	
XCAP Authentication user name	[XDMMO]	N/A	Not instantiated	
XCAP Authentication Secret	[XDMMO]	N/A	Not instantiated	
XCAP Authentication type	[XDMMO]	N/A	Not instantiated	
REVOKE TIMER	[RCC.07]	N/A	Not instantiated	
PNB MANAGEMENT	[RCC.07]	N/A	Not instantiated	
Messaging parameters				
PRES-SRV-CAP	[RCC.12]	[RCC.07]	Fixed value: 0	
MAX_AD-HOC_GROUP_SIZE	**[RCC.12]**	[RCC.07]	Service Provider Configurable	50
CONF-FCTY-URI	[RCC.12]	[RCC.07]	Service Provider Configurable Recommended value: chat@conf-factory.<home-network-domain-name> Where <home-network-domain-name> is replaced with the Home Network Domain Name used by the client	

Parameter	Functional Definition	Syntax Definition for transport using [RCC.14]	Client Configurability	Aligned Value for this profile
EXPLODER-URI	[RCC.12]	[RCC.07]	Fixed dummy value: *sip:foo@bar* if STANDALONE MSG AUTH is set to 0, Service Provider Configurable otherwise. Recommended Value: exploder@conf-factory.<home-network-domain-name> Where <home-network-domain-name> is replaced with the Home Network Domain Name used by the client	
CONV-HIST-FUNC-URI	[RCC.12]	[RCC.07]	Fixed dummy value: *sip:foo@bar*	
DEFERRED-MSG-FUNC-URI / MSG-STORE-URI	[RCC.12]	[RCC.07]	Fixed dummy value: *sip:foo@bar*	
CHAT AUTH	Section 5.3.7	[RCC.07]	Service Provider Configurable	
GROUP CHAT AUTH	Section 5.3.7	[RCC.07]	Service Provider Configurable	
STANDALONE MSG AUTH	[RCC.07]	[RCC.07]	Service Provider Configurable	
IM CAP ALWAYS ON	[RCC.07]	[RCC.07]	Fixed Value: 1	
GROUP CHAT FULL STORE FORWARD	[RCC.07]	[RCC.07]	Fixed Value: 0	
GROUP CHAT INVITE ONLY FULL STORE FORWARD	[RCC.07]	[RCC.07]	Fixed Value: 0	
IM CAP NON RCS	[RCC.07]	[RCC.07]	Fixed Value: 0	
IM CAP NON RCS GROUP CHAT	[RCC.07]	N/A	Not instantiated	

Parameter	Functional Definition	Syntax Definition for transport using [RCC.14]	Client Configurability	Aligned Value for this profile
IM CAP NON RCS LIMIT GROUP CHAT	[RCC.07]	N/A	Not instantiated	
GROUP CHAT BREAKOUT ALLOWED PREFIXES	[RCC.07]	N/A	Not instantiated	
IM SESSION AUTO ACCEPT	[RCC.07]	[RCC.07]	Service Provider Configurable	1
IM SESSION START	[RCC.07]	[RCC.07]	Service Provider Configurable	0
IM SESSION AUTO ACCEPT GROUP CHAT	[RCC.07]	[RCC.07]	Service Provider Configurable	
IM SESSION TIMER	[RCC.07]	[RCC.07]	Service Provider Configurable	
MAX SIZE IM	[RCC.07]	[RCC.07]	Service Provider Configurable	8192 (bytes as defined in [RCC.07] section A.2.5)
MAX SIZE STANDALONE	[RCC.07]	[RCC.07]	Service Provider Configurable	1048576 (i.e. 1MB)
MESSAGE STORE URL	[RCC.07]	[RCC.07]	Service Provider Configurable	
MESSAGE STORE USER / PASSWORD	[RCC.07]	[RCC.07]	Service Provider Configurable	
MESSAGE STORE AUTH	[RCC.07]	[RCC.07]	Service Provider Configurable	
DATA CONNECTION SYNC TIMER	[RCC.07]	[RCC.07]	Service Provider Configurable	
MESSAGE STORE SYNC TIMER	[RCC.07]	[RCC.07]	Service Provider Configurable	
MESSAGE STORE EVENT REPORTING	[RCC.07]	[RCC.07]	Service Provider Configurable	
MESSAGE STORE ARCHIVE AUTH	[RCC.07]	[RCC.07]	Service Provider Configurable	
SMS MESSAGE STORE	[RCC.07]	[RCC.07]	Service Provider Configurable	
MMS MESSAGE STORE	[RCC.07]	[RCC.07]	Service Provider Configurable	

Parameter	Functional Definition	Syntax Definition for transport using [RCC.14]	Client Configurability	Aligned Value for this profile
CHAT MESSAGING TECHNOLOGY	[RCC.07]	[RCC.07]	Fixed Value: 1	
CHAT REVOKE TIMER	[RCC.07]	[RCC.07]	Service Provider Configurable	300
MESSAGING UX	Section 5.3.7	Implemented in the profile defined in this document based on the definitions in section 5.3.7	Service Provider Configurable	
USER ALIAS AUTH	Section 5.3.7	Implemented in the profile defined in this document based on the definitions in section 5.3.7	Service Provider Configurable	
MESSAGING FALLBACK DEFAULT	Section 5.3.7	Implemented in the profile defined in this document based on the definitions in section 5.3.7	Service Provider Configurable	
RECONNECT GUARD TIMER	Section 5.3.7	Implemented in the profile defined in this document based on the definitions in section 5.3.7	Service Provider Configurable	
CFS TRIGGER	Section 5.3.7	Implemented in the profile defined in this document based on the definitions in section 5.3.7	Service Provider Configurable	
MAX 1 TO MANY RECIPIENTS	Section 5.3.7	Implemented in the profile defined in this document based on the definitions in section 5.3.7	Service Provider Configurable	

Parameter	Functional Definition	Syntax Definition for transport using [RCC.14]	Client Configurability	Aligned Value for this profile
1 TO MANY SELECTED TECHNOLOGY	Section 5.3.7	Implemented in the profile defined in this document based on the definitions in section 5.3.7	Service Provider Configurable	
DISPLAY NOTIFICATION SWITCH	Section 5.3.7	Implemented in the profile defined in this document based on the definitions in section 5.3.7	Service Provider Configurable	
File Transfer Parameters				
PROVIDE FT	[RCC.07]	[RCC.07]	Fixed Value: 0	
FT MAX SIZE	[RCC.07]	[RCC.07]	Service Provider Configurable	102400 (i.e. 100MB)
FT MAX SIZE INCOMING	[RCC.07]	[RCC.07]	Fixed Value: 0	
FT WARN SIZE	[RCC.07]	[RCC.07]	Service Provider Configurable	102400 (i.e. 100MB)
FT CAP ALWAYS ON	[RCC.07]	N/A	Not instantiated	
FT AUT ACCEPT	[RCC.07]	[RCC.07]	Service Provider Configurable	1

Parameter	Functional Definition	Syntax Definition for transport using [RCC.14]	Client Configurability	Aligned Value for this profile
FT HTTP CS URI	[RCC.07]	[RCC.07]	Service Provider Configurable Recommended value: *ftcontentserver.rcs.mnc<MNC>.mcc<MNC>.pub.3gppnetwork.org* Whereby <MNC> and <MCC> shall be replaced by the respective values of the home network in decimal format and with a 2-digit MNC padded out to 3 digits by inserting a 0 at the beginning (as defined in [PRD-IR.67]).	
FT HTTP CS USER	[RCC.07]	[RCC.07]	Service Provider Configurable	
FT HTTP CS PWD	[RCC.07]	[RCC.07]	Service Provider Configurable	
FT DEFAULT MECH	[RCC.07]	[RCC.07]	Fixed Value: HTTP	
FT HTTP FALLBACK	[RCC.07]	[RCC.07]	Service provider configurable	
FT MAX 1 TO MANY RECIPIENTS	Section 7.3.3	Implemented in the profile defined in this document based on the definitions in section 7.3.3	Service provider configurable	
FT FALLBACK DEFAULT	Section 7.3.3	Implemented in the profile defined in this document based on the definitions in section 7.3.3	Service provider configurable	
Enriched Calling Related Parameters				

Parameter	Functional Definition	Syntax Definition for transport using [RCC.14]	Client Configurability	Aligned Value for this profile
PROVIDE VS	[RCC.07]	[RCC.07]	Service Provider Configurable	
PROVIDE IS	[RCC.07]	[RCC.07]	Fixed Value: 0	
ALLOW VS SAVE	[RCC.07]	[RCC.07]	Fixed Value: 0	
VS MAX DURATION	[RCC.07]	[RCC.07]	Service Provider Configurable	
IS MAX SIZE	[RCC.07]	[RCC.07]	Not instantiated	
COMPOSER AUTH	[RCC.20]	Implemented in the profile defined in this document based on definitions in [RCC.20]	Service Provider Configurable	
SHARED MAP AUTH	[RCC.20]	Implemented in the profile defined in this document based on definitions in [RCC.20]	Service Provider Configurable	
SHARED SKETCH AUTH	[RCC.20]	Implemented in the profile defined in this document based on definitions in [RCC.20]	Service Provider Configurable	
POST CALL AUTH	[RCC.20]	Implemented in the profile defined in this document based on definitions in [RCC.20]	Service Provider Configurable	
CALL COMPOSER TIMER IDLE	[RCC.20]	Implemented in the profile defined in this document based on definitions in [RCC.20]	Service Provider Configurable	
Geolocation Parameters				
Addr	[SUPLMO]	N/A	Not instantiated	
AddrType	[SUPLMO]	N/A	Not instantiated	

Parameter	Functional Definition	Syntax Definition for transport using [RCC.14]	Client Configurability	Aligned Value for this profile
PROVIDE GEOLOC PUSH	[RCC.07]	[RCC.07]	Fixed Value: 1	
PROVIDE GEOLOC PULL	[RCC.07]	[RCC.07]	Fixed Value: 0	
GEOLOCATION TEXT MAX LENGTH	[RCC.07]	[RCC.07]	Service Provider Configurable	300
GEOLOCATION VALIDITY	[RCC.07]	N/A	Not instantiated	
GEOLOCATION PULL BLOCK TIMER	[RCC.07]	N/A	Not instantiated	
Capability Discovery parameters				
DISABLE INITIAL ADDRESS BOOK SCAN	[RCC.07]	[RCC.07]	Service Provider Configurable	
POLLING PERIOD	[RCC.07]	[RCC.07]	Service Provider Configurable	0 (i.e. capability discovery polling disabled)
POLLING RATE	[RCC.07]	[RCC.07]	Service Provider Configurable	0
POLLING RATE PERIOD	[RCC.07]	[RCC.07]	Service Provider Configurable	0
CAPABILITY INFO EXPIRY	section 3.3.2.2	[RCC.07]	Service Provider Configurable	
SERVICE AVAILABILITY INFO EXPIRY	Section 3.3.2.1	Section 3.3.2.1	Service Provider Configurable	
NON RCS CAPABILITY INFO EXPIRY	[RCC.07]	[RCC.07]	Service Provider Configurable	
CAPABILITY DISCOVERY MECHANISM	[RCC.07]	[RCC.07]	Service Provider Configurable	

Parameter	Functional Definition	Syntax Definition for transport using [RCC.14]	Client Configurability	Aligned Value for this profile
CAPABILITY DISCOVERY VIA COMMON STACK	[RCC.07]	[RCC.07]	Not instantiated if CAPABILITY DISCOVERY MECHANISM is set to OPTIONS, Service Provider Configurable otherwise	0, if instantiated
CAPABILITY DISCOVERY ALLOWED PREFIXES	[RCC.07]	[RCC.07]	Service Provider Configurable	
APN parameters				
NO MSRP SUPPORT	[RCC.07]	[RCC.07]	Service Provider Configurable	
End User Confirmation parameters				
END USER CONF REQ ID	[RCC.15]	[RCC.15]	Service Provider Configurable	
Multidevice configuration parameters				
uuid_Value	[RCC.15]	[RCC.15]	Service Provider Configurable and device dependent	
IP Voice and Video Call configuration				
PROVIDE IR94 VIDEO	[RCC.07]	[RCC.07]	Service Provider Configurable	
PROVIDE RCS IP VOICE CALL	[RCC.07]	[RCC.07]	Fixed Value: 0 for primary devices, Service Provider Configurable for secondary devices	
PROVIDE RCS IP VIDEO CALL	[RCC.07]	[RCC.07]	Service Provider Configurable	
PROVIDE IR51 VOICE	[RCC.07]	[RCC.07]	Service Provider Configurable	
PROVIDE IR51 VIDEO	[RCC.07]	[RCC.07]	Service Provider Configurable	

Parameter	Functional Definition	Syntax Definition for transport using [RCC.14]	Client Configurability	Aligned Value for this profile
VIDEO AND ENCALL UX	Section 3.3.2.1	Implemented in the profile defined in this document based on the definitions in Section 3.3.2.1	Service Provider Configurable	
IR51 SWITCH UX	Section 10.3	Implemented in the profile defined in this document based on the definitions in Section 10.3	Service Provider Configurable	
CALL LOGS BEARER DIFFERENTIATION	Section 10.3	Implemented in the profile defined in this document based on the definitions in Section 10.3	Service Provider Configurable	
DATA OFF parameters				
RCS MESSAGING DATA OFF	[RCC.07]	[RCC.07]	Service Provider Configurable	
FILE TRANSFER DATA OFF	[RCC.07]	[RCC.07]	Service Provider Configurable	
SMSOIP DATA OFF	[RCC.07]	[RCC.07]	Service Provider Configurable	
MMS DATA OFF	[RCC.07]	[RCC.07]	Service Provider Configurable	
CONTENT SHARE DATA OFF	[RCC.07]	[RCC.07]	Service Provider Configurable	
PRE AND POST CALL DATA OFF	[RCC.07]	[RCC.07]	Service Provider Configurable	
VOLTE DATA OFF	[RCC.07]	[RCC.07]	Service Provider Configurable	
IP VIDEO CALL DATA OFF	[RCC.07]	[RCC.07]	Service Provider Configurable	
EXTENSIONS DATA OFF	[RCC.07]	N/A	Not Instantiated	
PROVISIONING DATA OFF	[RCC.07]	[RCC.07]	Service Provider Configurable	
SYNC DATA OFF	[RCC.07]	[RCC.07]	Service Provider Configurable	
API Parameters				

Parameter	Functional Definition	Syntax Definition for transport using [RCC.14]	Client Configurability	Aligned Value for this profile
ALLOW RCS EXTENSIONS	[RCC.07]	N/A	Not instantiated	
EXTENSIONS MAX MSRP SIZE	[RCC.07]	N/A	Not instantiated	
EXTENSIONS POLICY	[RCC.55]	N/A	Not instantiated	

Table 50: Overview of the applicable configuration parameters

Annex D Document Management

D.1 Document History

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
1.0	November 16th 2016	Initial version approved by PSMC.	PSMC	Catherine Maguire / GSMA

D.2 Other Information

Type	Description
Document Owner	Network 2020 Programme, Global Functional Requirements Group
Editor / Company	Catherine Maguire / 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

Your comments or suggestions & questions are always welcome.