RCS Universal Profile Service Definition Document
Version 2.3
06 December 2018

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

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.

Table of Contents

1 Introduction

1.1 Purpose of the Universal Profile

The Rich Communication Services (RCS) Universal Profile 2.3 represents an update of globally shared RCS specifications. This Service Definition Document (SDD) lists all the User Stories and Feature Requirements, based on the Universal Profile 2.0 specification. 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 2.3 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 2.3 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 (14 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.

In addition to maintenance of the core features of RCS, this SDD starts support of 3rd party developer applications who use interfaces to deliver their services using RCS as an enabler (we call that "MaaP – Messaging as a Platform").

Any major changes in comparison to the Universal Profile 2.0 are listed in the introduction section of each chapter.

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-2-2US.

For requirements and parts of requirements that are in italics, no realisation is provided in this version of the document.

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
A2P	Application to Person (communication)
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.
AF	Anonymization Function

Term	Description (contains technical and functional terms)
Aggregation of device capabilities	All of a user's capabilities for their RCS services on all of their RCS-enabled devices will be combined into a single set of capabilities which is shared with other users. Other users will not be able to determine on exactly which device another user has a specific capability, nor will other users know whether the user has multiple RCS devices available to him at all (using this capability information shared).
AKA	Authentication and Key Agreement
AMR	Adaptive Multi-Rate
Anonymous Mode	A user has agreed not to share their MSISDN with a Chatbot.
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.
Chatbot	An RCS-based (fully or partly) automated service provided to users whose output is presented in a conversational form. Often a piece of software interfacing with one or more users aiming to simulate intelligent human conversation. Two types of Chatbots can be differentiated: • Generic Chatbots which are referenced as "Chatbot" in this document. (These Chatbots may or may not be verified by a Verification Authority.) • "Critical Chatbots" which have specific attributes assigned that provide them with special rights as defined in this document.
Chat Message	A single text message that was exchanged between two or more RCS communication end points (e.g. users or Chatbots).
Chatbot Platform	A system that provides a mechanism for Chatbot developers to create and register Chatbots, which can then be exposed to the users connected to the platform through a messaging system.

Term	Description (contains technical and functional terms)
Chatbot Profile Information	Additional information provided by the Chatbot to the user that allows the user to e.g. contact the Brand operating the Chatbot over other channels, or better understand what the purpose of the Chatbot is or what the Brand operating the Chatbot does.
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 that 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
Default Dialler	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 including Revocation (CFS) and Network Fallback to SMS (NFS).
Delivery Notification	Indication that a message was successfully received by the B-Party device.
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

Term	Description (contains technical and functional terms)
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.
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).
File Transfer Status Notification or File Transfer States Notifications	A visible information for the sender of a File Transfer in 1-to-1Messaging or Group Chat about the progress of the delivery.
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 Setting(s)	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
Group Chat	A conversation where the creator invites 2 or more participants to take part. All participants are aware of each other, and all content exchanged is shared with the entire participants list.
HOS	Home Operator Services
HTML	Hyper Text Markup Language
HTTP	Hyper Text Transfer Protocol

Term	Description (contains technical and functional terms)
IARI	IMS Application Reference Identifier
ICSI	IMS Communication Service Identifier
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.
Is Typing Notification	A visible information for participants in a 1-to-1 Messaging or Group Chat conversation that another participant in the conversation is in the process of creating a message. This message may or may not be sent by that 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
MaaP Application	A remote service that the user is able to communicate with from the Messaging Application on the device, e.g. a Chatbot.
MDV[2]	Multi device Voice and Video
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).
Message Status Notification or Message States Notifications	A visible information for the sender of a message in 1-to-1 Messaging or Group Chat about the progress of the delivery.
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.

Term	Description (contains technical and functional terms)
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).
New Incoming Event Notification	An audible and/ or visible information for the receiving user (B-Party) that a new message or file has been received.
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.
OIDC	Open ID Connect
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
P2A	Person to Application (communication)
P2P	Person to Person (communication)
P-CSCF	Proxy Call Session Control Function
Plug-in	A mini application that appears within messaging or voice / video calling applications to aesthetically and functionally enrich the content of the conversation.
Plug-in Consumer	RCS client that is able to use Plug-ins
Plug-in Provider	Any app that contains and exposes a Plug-in

Term	Description (contains technical and functional terms)
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).
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
Public Mode	A user has agreed to share their MSISDN with a Chatbot.
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.
RCS Service Provider	A company providing Rich Communications Services (RCS) to end customers. RCS Service Providers are Mobile Network Operators
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.
Recurring Payment	A predictable payment of a fixed amount which the user has agreed to pay on a regular schedule.
Seamless Messaging	An MNO messaging service whereby the user does not have to choose 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.
Suggested Chip List	A number of suggested replies and/or actions that a Chatbot can send to a user along with a message

Term	Description (contains technical and functional terms)
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
Trusted Wi-Fi	Trusted Wi-Fi" refers to a Wi-Fi connection offered by the RCS Service Provider or via a third party trusted by the RCS Service Provider.
UE	User Equipment
UI	User Interface
Universal Profile	Specification that describes a profile of the RCS Standard that has the ambition to work globally on any RCS enabled network.
URI	Uniform Resource Identifier
UX	User Experience
Verification Authority	A provider of verification for Chatbots. A Verification Authority could be, but not limited to, a commercial trusted business (e.g. verification companies from the internet world), an MNO or a governmental function.
Verified Chatbot	A Chatbot that was verified to represent the identity (e.g. name, brand or institution) that their name, brand icon and Chatbot Profile Information suggest.
Video Message	A UI implementation that allows the user to record a video and send it to a 1-to-1 Messaging conversation, in a similar manner to sending and recording an Audio Message. For maximum duration, Video message follows audio message and/or file transfer maximum size limits (whichever is reached first).
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)
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 23.040]	3GPP TS 23.040, release 10, Technical realization of the Short Message Service (SMS) http://www.3gpp.org/DynaReport/23040.htm
[2]	[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
[3]	[3GPP TS 24.167]	3GPP TS 24.167, release 12, 3rd Generation Partnership Project; Technical Specification Group

Ref	Doc Number	Title
		Core Network and Terminals; 3GPP IMS Management Object (MO) http://www.3gpp.org/DynaReport/24167.htm
[4]	[3GPP TS 24.368]	3GPP TS 24.368, 3rd Generation Partnership Project; Non-Access Stratum (NAS) configuration Management Object (MO) http://www.3gpp.org/ DynaReport/24368.htm
[5]	[NG.102]	IMS Profile for Converged IP Communications Version 5.0 29 June 2018 http://www.gsma.com/
[6]	[PRD-IR.51]	IMS Profile for Voice, Video and SMS over untrusted Wi-Fi access Version 6.0 01 May 2018 http://www.gsma.com/
[7]	[PRD-IR.67]	GSMA PRD IR.67 - “DNS/ENUM Guidelines for Service Providers & GRX and IPX Providers” Version 14.0 21 November 2016 http://www.gsma.com/
[8]	[PRD-IR.90]	GSMA PRD IR.90 - “RCS Interworking Guidelines” Version 14.0 13 October 2017 http://www.gsma.com/
[9]	[PRD-IR.92]	GSMA PRD IR.92 - “IMS Profile for Voice and SMS” Version 12.0 02 May 2018 http://www.gsma.com/
[10]	[PRD-IR.94]	GSMA PRD IR.94 - “IMS Profile for Conversational Video Service” Version 13 21 June 2018 http://www.gsma.com/
[11]	[RCC.07]	GSMA PRD RCC.07 version 10.0 - “Rich Communication Suite 9.0 Advanced Communications Services and Client Specification” 06 December 2018 http://www.gsma.com/
[12]	[RCC.08]	GSMA PRD RCC.08 RCS Endorsement of 3GPP TS 29.311 Service level Interworking for Messaging Services Version 8.0 06 December 2018 http://www.gsma.com/
[13]	[RCC.10]	GSMA PRD RCC.10 Rich Communication Suite Endorsement of OMA CPM 2.2 Interworking Version 8.0 06 December 2018 http://www.gsma.com/
[14]	[RCC.11]	GSMA PRD RCC.11 Rich Communication Suite Endorsement of OMA CPM 2.2 Conversation Functions Version 8.0 06 December 2018 http://www.gsma.com/
[15]	[RCC.14]	GSMA PRD RCC.14 Service Provider Device Configuration Version 6.0 06 December 2018 http://www.gsma.com/
[16]	[RCC.15]	GSMA PRD RCC.15 IMS Device Configuration and Supporting Services Version 6.0 06 December 2018

Ref	Doc Number	Title
		http://www.gsma.com/
[17]	[RCC.20]	GSMA PRD RCC.20 Enriched Calling Technical Specification Version 5.0 06 December 2018 http://www.gsma.com/
[18]	[PRESENCE2MO]	OMA Management Object for Presence SIMPLE 2.0, Approved Version 2.0, 10 July 2012 http://www.openmobilealliance.org
[19]	[OMA-MMS-CONF]	OMA MMS Conformance Document, Version 1.3 – 28 Jan 2008 http://www.openmobilealliance.org
[20]	[RFC3966]	IETF RFC The tel URI for Telephone Numbers http://tools.ietf.org/html/rfc3966
[21]	[CPM-MSGSTOR-REST]	OMA-TS-CPM_Message_Store_Using_RESTFul_API-V1_0-20170516-D http://www.openmobilealliance.org

2 Device Provisioning

2.1 Description

An RCS Service Provider 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.

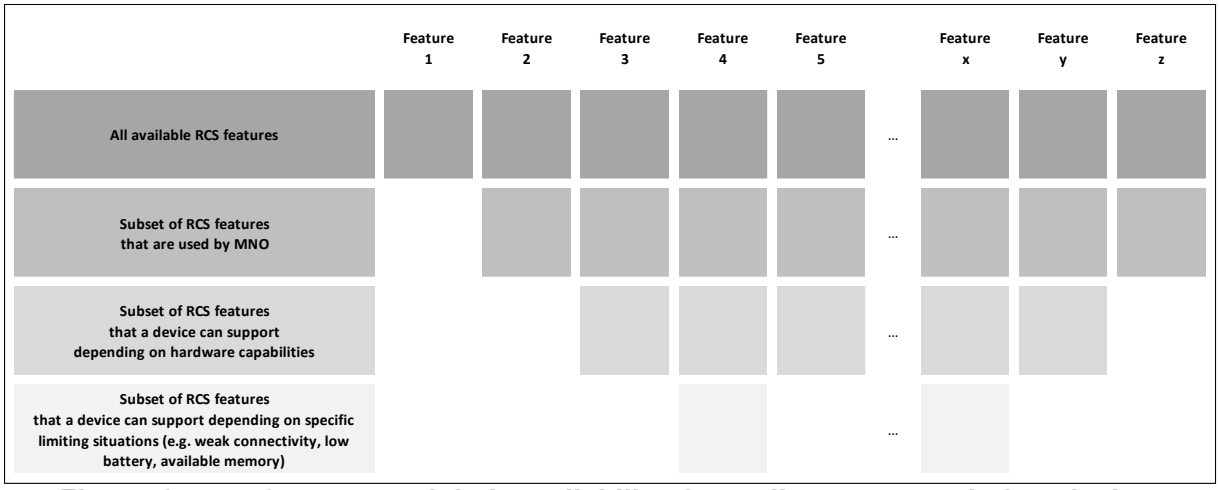


Figure 1: RCS features and their availability depending on MNO choice, device capability, and specific limiting situations.

Overview of major functional changes in this section compared to Universal Profile 2.0:

- Refinement of Dual SIM requirements.

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 a RCS Service Provider, 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 RCS Service Provider.

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

R2-1-3 It shall be made clear to the user what the effect of enabling / disabling RCS service is, e.g. enhanced messaging and enriched calling services will be disabled, but other services such as VoLTE are not affected by the Master switch.

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 and

R2-2-1-2 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 RCS Service Provider.

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

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

R2-3-1 The device shall attempt to be provisioned with the necessary RCS configuration without user interaction.

R2-3-2 If it should not be possible to provision the device within 7 days after the initial attempt to receive RCS configuration without user interaction (e.g. manual introduction of MSISDN), the device shall request the user’s support for configuration by asking for the device’s MSISDN

R2-3-3 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 (e.g. messaging app or dialler app).

R2-3-3-1 The user shall be informed why the device is asking him to provide his MSISDN.

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

NOTE: If the device has received a valid RCS configuration in the meanwhile, any user interaction is obviously obsolete.

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 clients

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 do not 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 RCS Service Provider, I want to be able to provide information and require consent BEFORE my users use the RCS service.**

R2-6-1 Upon RCS Service Provider 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).

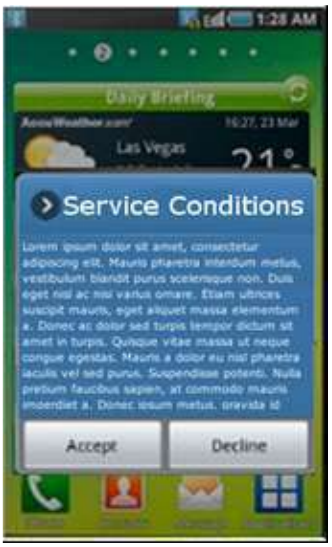


Figure 2: Example Terms & Conditions pop-up

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 RCS Service Provider, 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 RCS Service Provider 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 RCS Service Provider policies, additional messages may be displayed to the user.

US2-8 **As a RCS Service Provider, I want to request additional information from my users during first-time registration in order to fulfil specific security purposes.**

R2-8-1 Upon RCS Service Provider discretion, users may be requested to enter additional information during first-time registration in order to fulfil specific security requirements set by the RCS Service Provider.

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 A secondary device is linked to the identity of the primary device using the federation process.

NOTE: Any devices that are not the primary device are called secondary device(s).

R2-10-2 All devices I use shall use one identity for any incoming / outgoing calls or messages.

R2-10-2-1 The used identity shall be the MSISDN of the primary device.

NOTE: Any single connected device can be used as a secondary device for a number of different identities.

R2-10-3 If an MNO has deployed RCS Multi Device Messaging (MDM) and Multi Device Voice and Video (MDV^2) services, the federation process shall span both MDM and MDV^2 processes (from the user perspective).

R2-10-4 Secondary devices may use a SIM to authenticate to the data network or use a SIM-less data connection.

R2-10-5 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: Inclusion of individual Multi-SIM solutions is at the discretion of the individual MNO.

R2-10-6 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 RCS Service Provider, 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) 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.

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 RCS Service Provider does not want to provide RCS services to a particular subscription an RCS Service Provider 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 RCS Service Provider, I want to be able to push configuration settings in special cases.**

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

R2-12-1 The RCS Service Provider 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 RCS Service Provider shall be able to push configuration settings in case the network is upgraded to a new RCS release.

R2-12-3 The RCS Service Provider 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 have both SIMs active for RCS.**

R2-13-1 The device should try to activate RCS for both SIM cards when possible (i.e. when the associated MNOs both offer RCS services)..

R2-13-1-1 When both SIM cards' MNOs offer RCS services, both SIM cards should be active at the same time for RCS and shall be able to offer all supported RCS features (e.g. send / receive RCS Messages and File Transfers, reply to capability checks, provide Enriched Calling features etc.)

R2-13-1-2 When only one SIM card can offer RCS services then that identity should be activated for RCS no matter which SIM slot it is inserted into (slot 1 or 2).

R2-13-1-2-1 When only one SIM card can offer Enriched Calling features, Pre-Call features shall only be offered when the active RCS SIM card has been chosen to perform the call.

R2-13-1-3 When the user is requested to provide their MSISDN to provision the service, in addition to the single SIM scenario requirements, the device should clearly show the user for which SIM card the activation is required.

R2-13-1-4 The Master Switch and Settings implementations should follow the rules defined for a single SIM card device as far as possible. Additionally, an OEM can decide to apply a single configurable Master Switch and Settings that apply to both SIM cards or support separate Master Switch and Settings for each SIM card.

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

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

R2-14-1-1 The user shall not be able to perform Enriched Calling when a SIM other than an 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 an active RCS SIM, Enriched Calling (pre-call, in-call and post-call) shall be possible.

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

2.3 Technical Information

2.3.1 Overview

2.3.1.1 Provisioning

Provisioning shall be done as described in [RCC.07].

The RCS Service Provider may apply automatic authentication of a primary device based on the access described in, section 2.5 of [RCC.14] or automatic identification based on the SIM or based on the IMSI as specified in section 2.6 and 2.7 of [RCC.14].

If the RCS Service Provider is not able to identify the user automatically, they shall request the user for the MSISDN via the user interface, either based on OpenID Connect as defined in section mechanism defined in section 2.8.3.3 of [RCC.14] or via the client procedure defined in section 2.6 of [RCC.14]. Provisioning of secondary devices shall follow section 2.8 or 2.9 of [RCC.14].

Alternatively a generic approach for user authentication, authorisation and user consent is the application of OpenID Connect as defined in section 2.8 of [RCC.14]. Depending on the device capabilities, the provisioning client shall indicate support of authentication mechanisms for OpenID Connect as defined in [RCC.14] and [RCC.07].

The device shall assume that RCS is available on the user's network if the procedures for configuration server discovery as defined in section 2.2 of [RCC.14] and the supported service discovery defined in section 2.3 of [RCC.14] results in indications of the network to support RCS services.

The client shall indicate support of RCS services and related enablers via the “app” configuration request parameter defined in [RCC.14]. Depending on the support of RCS services and enablers, the client shall indicate the support of services for client configuration based on the definitions of [RCC.07], [RCC.15], [PRD-IR.51], [PRD-IR.92] and [PRD-IR.94].

The client shall indicate the support of the profile defined in this document via the “rcs_profile” configuration request parameter defined in [RCC.07] with a value set to "UP_2.3".

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 2.2.6), 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 2.4. and 4.2 of [RCC.14] or using End User Confirmation Requests (EUCR) as specified in section 3.1 of [RCC.15] or via OpenID Connect as specified in section 2.8.3.3 of [RCC.14]..

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 section B.1 apply.

2.3.2 Technical Implementation of User Stories and Service requirements

R2-15-1 The requirements in US2-1 and R2-2-1 and its sub requirements shall be realised locally on the device.

R2-15-2 R2-2-2 shall be realised as described in [RCC.07] section 2.3.2.

R2-15-3 R2-2-3 and R2-2-4 shall be realised locally on the device.

R2-15-4 For R2-2-5, shall set the rcs_state to -4 in the configuration request and follow client codes and procedures defined in section 2.3.2.2.1 of [RCC.07].

R2-15-5 Provisioning on networks with automatic identification (see requirement R2-3-1) 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 then depending on supported mechanisms, the RCS Service Provider may fall back to the SMS via the procedures defined in section 2.5 or 2.8 of [RCC.14].

R2-15-6 R2-3-2 shall be realised locally on the device if configuration without user interaction could not be concluded successfully.

R2-15-7 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 2.6 of [RCC.14] and its subsections or section 2.8 of [RCC.14].

R2-15-8 R2-3-3 and its sub requirements shall be realised locally on the device

R2-15-9 R2-3-4 and its sub requirements shall be realised locally on the device

R2-15-10 R2-3-5 shall be realised locally on the device

R2-15-11 R2-3-6 and its sub requirements shall be realised as described in section 2.6 or 2.8 of [RCC.14] using the SMS format being described in section 2.6.2 of [RCC.14] if the SMS should be handled silently.

R2-15-12 R2-3-7 shall be realised locally on the device

R2-15-13 R2-3-8 and R2-3-9 shall be realised locally on the device

R2-15-14 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™.

R2-15-15 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.

R2-15-16 On Android™ devices requirement R2-4-4 is implemented locally on the device with the Android setting related to the Default SMS app.

R2-15-17 On Android™ devices, R2-4-5 is implemented locally on the device with the Android™ setting related to the Default Dialler (or phone) application.

R2-15-18 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.

R2-15-19 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

R2-15-20 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 and Post-Call feature tags on the IMS network.
        - not announce support of Pre-Call, Shared Sketch, Shared Maps 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 and Post-Call feature tags on the IMS network.
        - announce support of Pre-Call, Shared Sketch, Shared Maps 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 and Post-call feature tags.
  - not announce support of Pre-Call, Shared Sketch, Shared Maps and Post-Call services during capability exchanges.

R2-15-21 R2-5-1 shall be realised locally on the device as described in section 4.3 of [RCC.14].

R2-15-22 As mention in section 2.3.1.1, configuration of additional devices shall be done as described in section 2.9 of [RCC.14] realising the requirements R2-10-1 to R2-10-6.

R2-15-23 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 2.4.2 and 4.2 of [RCC.14]. This mechanism shall be supported by the RCS clients and may be used upon the RCS Service Provider's discretion.

R2-15-24 As described in section 2.4.2 of [RCC.14] the User Message mechanism supports requirements R2-6-1 and R2-6-4.

R2-15-25 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.

R2-15-26 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.

R2-15-27 The RCS Service Provider is also able to implement the requirements of the user consent in user story US2-6 via the procedures for authorisation and consent via the procedure defined in section 2.8 of [RCC.14].

R2-15-28 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 RCS 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.

R2-15-29 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.

R2-15-30 Requirement R2-7-5 shall be implemented locally on the device

R2-15-31 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 R2-15-37 and R2-15-38 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 2.3.2.5 of [RCC.07].

R2-15-32 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.

R2-15-33 As described in section 2.5.3 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 2.6.3 and 2.6.4 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. Alternatively, the RCS Service Provider can use the mechanism for authorisation and user consent defined in section 2.8 of [RCC.14] to provide the functionality.

R2-15-34 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.

R2-15-35 If the subscriber cannot be provisioned due to MNO policy (i.e. a permanent unavailability as described in requirement R2-11-3), the RCS Service Provider can include a message as described in sections 2.4.2 and 4.2 of [RCC.14] in a response disabling the RCS client (i.e. RCS DISABLED STATE set to -1).

R2-15-36 As described in section 2.4.3 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 2.6.3 [RCC.14], for non-cellular networks, this situation shall be applicable only to that particular network however.

R2-15-37 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 R2-15-36 and R2-15-37 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.

R2-15-38 For the reconfiguration of primary and additional devices on which RCS is active already (required in R2-12-1 and 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].

R2-15-39 For User Story US2-13, an RCS enabled SIM shall be discovered by the client via the procedures for configuration server discovery and supported service discovery as defined in [RCC.14]. This should happen regardless of the type of network (Packet Switched (PS) network or Wi-Fi).

R2-15-40 After discovering a SIM to be supporting RCS as per the procedures in R2-15-39, 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

R2-15-41 The client should store the welcome message received from network against the corresponding SIM as additional information so that user could revisit the details at later point.

R2-15-42 For requirement R2-13-1-1, the client shall follow the discovery procedure as described in R2-15-39 and the activation procedure described in R2-15-40.

R2-15-43 Requirements R2-13-1-2 to R2-13-1-4 shall be implemented locally on the device.

R2-15-44 Requirements R2-14-1, R2-14-1-1 and R2-14-1-2, shall be realised locally on the device and when applicable enriched calling shall be provided as described in section 12.

R2-15-45 For requirement R2-14-1-3, a service discovery request targeted at the identity associated to a non-RCS enabled SIM will fail and as such, the caller will not be aware that enriched calling is possible and treat the call as a non-enriched call.

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 an RCS 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 RCS capability discovery and service availability is disabled on a given network and their devices, all RCS services 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 RCS 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 R12-51-1) 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 The initial contact list scan shall happen in the background without user impact. The timing of the contact list scan may be delayed or chunked to parts if negative user impact is likely to be expected (e.g., but not limited to, cases of low battery or slowing down the handset if the user replays a video).

R3-3-2-3 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. That shall include cases of adding an MSISDN to an existing contact or changing the MSISDN of an existing contact.

R3-3-3-1-1 If the device is configured by the RCS Service Provider for Integrated Messaging, the adding or modifying a contact as described in R3-3-3-1 in offline status shall result in a capability update once the device is online again.

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 Protocol (SIP) Options Exchange as specified in [RCC.07] Sections 2.6.1.1
- TE2: Presence Based Exchange as specified in [RCC.07] Sections 2.6.1.2

The two implementations are compatible through the co-existence solutions [RCC.07] Section 2.6.1.4.

In the profile defined in this document, Service Availability as defined in section 2.6.2 of [RCC.07] 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 once the call has been established successfully. This applies to the following services:

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

Capability information as defined in section 2.6.2 of [RCC.07] shall be used for determining whether the following services can be used with a contact:

- Chat when not “latched” (see section 5), or when a contact is identified as a Chatbot (see section 15.2)
- Group Chat (see section 6)
- File Transfer when not “latched” (see section 7) or when a contact is identified as a Chatbot (see section 15.2)
- File Transfer fall-back to SMS (see section 7)
- Geolocation Push (see section 5)
- Geolocation Push fall-back to SMS (see section 5)
- Plug-ins (see section 15.3)

To fulfil the requirements in section 3.2, Capability information and Service Availability information obtained through the capability exchange enablers will be cached on the device as specified in section 2.6.2 of [RCC.07].

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 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 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.	Optional Parameter

Configuration parameter	Description	Parameter usage
	In the case where based on the capability exchange the service is considered 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 colour 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	

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

These parameters are included in the UX tree defined in section 5.3.4.

Node: /<x>/UX/videoAndEncallUX

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”

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 when all of the following conditions are fulfilled:

- Capability Exchange is enabled (i.e. CAPABILITY DISCOVERY MECHANISM as defined in section A.1.9 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.1.9 of [RCC.07]) and
- Chat is enabled (i.e. CHAT AUTH as defined in section 5.3.4 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 A.1.9 of [RCC.07]).

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.1.9 [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 section 2.6.1.4.2 of [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 RCS 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 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.1.9 [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 be implemented locally on the device triggering the capability exchange using the capability discovery mechanism that was configured and taking into account the RCS Service Provider configuration described in section 2.6.2.1 of [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 be implemented locally on the device taking into account section 3.3.3 of this document and section 2.6.2.1 of [RCC.07] where applicable.

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 sections 2.6.2 and A.1.9 of [RCC.07] and section 3.3.1 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 A.1.9 of [RCC.07]

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 A.1.9 of [RCC.07].

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.1.9 of [RCC.07].

R3-4-9-4 For R3-3-5-4, the cache shall be managed as described in section 2.6.2 of [RCC.07]

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 2.6.1.1.2 of [RCC.07]) for TE1.

4 Operator Messaging

void

5 1-to-1 Messaging

5.1 Description

1-to-1 Messaging enables users to exchange conversational messages and locations with another party. This section describes the User Stories and Service Requirements for the core chat service, the Geolocation Push 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 do not 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

R5-1-2 with SMS (and MMS, if configured by the MNO) messages.

R5-1-3 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 Operator 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 fallback 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 manually changed again either 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 having to select 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 do not want my Messaging Application to show the Messaging Service being used when messages are displayed in my inbox unless the device is explicitly configured to do so during the device provisioning procedure.

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 By default, the RCS client will not show or visually indicate to the user the technology / service used to convey the message from / to the device. However, if explicitly configured during the device provisioning procedure, the RCS client will show or indicate to the user the technology / service. For example, the user may find the messaging technology / service by recognizing annotation of each message or different colours of message bubbles in the conversation history, or by clicking every message to check the message's detailed information, etc.

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 4: 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 rule set of Integrated Messaging or the rule set of Seamless Messaging.

R5-4-3-1 The RCS Service Provider shall be free to choose either Integrated Messaging or 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 successfully 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.

R5-5-1-3-2 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 to expect a Delivery Notification.

R5-5-1-4 Message Displayed: When the message has been displayed in the messaging thread on the receiving device

R5-5-1-4-1 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.

R5-5-1-4-2 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).

R5-5-1-4-3 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 to expect a Display Notification.

R5-5-1-5 Message sending failed: The expected outcome of the operation could not be confirmed by the network (in this case: Message 'Sent', 'Delivered' or 'Displayed' status has not been received) and the device does not attempt to send the message again. (Sending the message may be re-triggered manually by the user).

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

R5-5-3 Aggregation of 'Display' Sent Message States 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.

R5-5-4 The 'failed' Message Status shall never be aggregated but presented separately to the user.

R5-5-5 Message states only apply to messages to recipients that 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.2.

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 are temporarily offline (e.g. device switched off). I expect them to receive these Messages as soon as they can be terminated.

R5-8-1 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.

R5-8-1-1 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.

R5-8-2 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 do not 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 made aware with a New Incoming Event Notification if the user is not in the conversation in which the incoming event is received with the active device window.

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

R5-10-3 The visual New Incoming Event 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 New Incoming Event Notification in line with device settings.**

R5-11-1 For audio New Incoming Event 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 that contain unread messages to be differentiated from conversations that contain messages I have seen.**

NOTE: Unseen files or file download links or thumbnails cover events that use File Transfer as an enabler e.g. but not limited to Audio Messaging or vCard share.

R5-14-1 Conversations with unread messages or unseen files or file download links or thumbnails 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

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 RCS Service Provider configurable.

NOTE: For security reasons, the use of Alias in 1-to-1 Chat has been limited to 'display' (if an Alias is provided to the handset, it shall be displayed to the user) but not 'create' (handsets shall only offer to set an Alias for Group Chat, but not 1-to-1 Chat). In a future version, this limitation might be removed in conjunction with the introduction of additional security features, e.g. an "Alias Blacklist for 1-to-1 Chat"..

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 do not want to feel restricted by message size limits.**

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

NOTE: RCS Service Provider 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 share are covered in 'File Transfer', section 7.

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

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

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 in a trusted and safe environment.**

R5-19-1 The RCS Service Provider shall be able to store 1-to-1 Messaging conversations.

NOTE: Details of that storage are at the individual RCS Service Provider discretion.

R5-19-2 The RCS Service Provider shall be able to determine the storage duration for messages based on individual parameters.

R5-19-3 In case the RCS Service Provider deletes stored messages (e.g. for capacity limitation), these messages shall not be deleted from local user equipment.

R5-19-4 As a user, I want to restore my 1-to-1 Messaging conversations (e.g., but not limited to, after wiping the device or purchasing a new device).

R5-19-5 The user shall have the option to restore 1-to-1 Messaging conversations (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).

US5-20 **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.

R5-20-1 Any messages or entire conversations that have been deleted by the user shall no longer be available via the RCS Service Provider.

US5-21 **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.**

NOTE: During the Voice or Video Call, the user may make use of the 1-to-1 Messaging application.

R5-21-1 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.

R5-21-2 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.

US5-22 **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 specification.

R5-22-1 The 1-to-1 messaging conversation shall be a service entry point to initiate a Geolocation Push.

R5-22-2 There may be other service entry points available on the device to initiate a Geolocation Push (e.g. Contact Card, call log).

R5-22-3 The Geolocation Push Service shall 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.

R5-22-4 For Geolocation Push, the rules of Delivery Assurance as described in this section shall apply if the MNO supports Integrated Messaging.

R5-22-5 If Geolocation Push is delivered using SMS, the recipient's device shall be able to detect that it is a Geolocation Push and display that event as an icon.

R5-22-5-1 The icon shall make visible to the user that they received a location.

R5-22-5-2 If the user selects the icon, the service shall be performed as if the Geolocation Push would have been transferred as a RCS message.

US5-23 **As a user, I want to view an automatically detected position on map and have the ability to change this manually before sending.**

R5-23-1 If the current position is to be sent, the location shall be automatically detected and suggested to the end user.

R5-23-2 The user shall have the option to preview and correct the automatically detected position on a map view before sending.

R5-23-3 The Geolocation Push service shall support sending of a location from other applications (e.g. mapping apps).

US5-24 **As a user, I want to tag positions or locations with a text field.**

R5-24-1 The user shall have the option to tag a position or location with a free text field before sending.

US5-25 **As a user, I want to receive positions / locations in a map view.**

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

R5-25-1 When receiving a position or location, the RCS Geolocation Push user shall have the ability to see the position / location on a map.

R5-25-2 When receiving a position or location, the RCS Geolocation Push user shall be able to see any tags that were added by the sender.

US5-26 **As a user, I want to send many 1-to-1 messages and files by selecting multiple recipients.**

R5-26-1 The client shall make clear to the user the differences between multiple 1-to-1 message and a Group Chat.

R5-26-2 The user shall be able to create a distribution list for multiple 1-to-1 messages.

R5-26-2-1 The distribution list shall be available as a service entry point for multiple 1-to-1 messages.

R5-26-3 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.

R5-26-3-1 A distribution list shall be created in this case.

R5-26-3-2 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.

R5-26-3-3 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.

R5-26-4 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.

R5-26-5 Recipients of messages sent to a distribution list are not aware of the other recipients who are on the list and receive similar messages.

US5-27 **As an RCS Service Provider, I would like to control the use of multiple 1-to-1 messages.**

R5-27-1 To prevent Spam distribution, the RCS Service Provider shall be able to limit the list of recipients.

R5-27-2 The RCS Service Provider shall be able to determine the messaging service(s) that are used to convey multiple 1-to-1 message distribution.

R5-27-2-1 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 3.2.3 of [RCC.07]. In order for the RCS 1-to-1 Chat service to be used it shall be enabled by the RCS Service Provider via the configuration parameter CHAT AUTH as defined in section A.1.3 and A.2.4 of [RCC.07] and the client shall be registered in IMS. The client shall advertise the chat capability in accordance with the definitions of sections 2.6.1.3 of [RCC.07] based on the procedures specified in section 3.2.3 of [RCC.07]. RCS 1-to-1 Chat delivery is driven by Delivery assurance requirements described in section 5.2 that are realised as described in section 3.2.3.8 of [RCC.07].

  NOTE: As per [RCC.11], there is no message included in the SIP INVITE.

  - The RCS Standalone Messaging service as defined in section 3.2.2 of [RCC.07]. In order for the RCS Standalone messaging service to be used, it shall be enabled by the RCS Service Provider via the configuration parameter STANDALONE MSG AUTH as defined in sections A.1.3 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 RCS 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 RCS 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 RCS 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 3.2.6 of [RCC.07]. In order for the RCS Geolocation Push service to be used it shall be enabled by the RCS Service Provider via the configuration parameter PROVIDE GEOLOC PUSH as defined in sections A.1.7 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 A.1.3 and A.2.4 of [RCC.07] is present with a value other than "0".

5.3.2 Network Fallback Support Capability

Delivery Assurance in this profile is provided based on the procedures described in section 3.2.3.8 of [RCC.07].

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

The 1-to-1 Messaging technology selection rules defined in section 3.2.1 of [RCC.07] 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.

5.3.3 Chat Message revocation

Message Revocation shall be implemented as defined in section 3.2.3.8 of [RCC.07].

5.3.4 Configuration Parameters

5.3.4.1 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 3.2.1 of [RCC.07] 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
MSG TECH DISP SWITCH	This parameter is applicable only for Seamless messaging (when MESSAGING UX is set to 0). It controls whether RCS client will show or visually indicate to the user the technology / service used to convey the message from / to the device. 0 (Default Value), or absent. The RCS client shall not show or indicate to the user the underlying messaging technology / service 1, The RCS client shall show or indicate to the user the underlying messaging technology/service.	Optional parameter

Table 5: Additional Configuration Parameters to control 1-to-1 Messaging behaviour

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

Node: /<x>/UX

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 6: 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 7: 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 8: 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 9: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 the user has not toggled it before.
- Associated HTTP XML parameter ID: “msgFBDefault”

Node: /<x>/UX/msgTDSwitch

Leaf node that describes whether RCS client will show or visually indicate to the user the technology / service used to convey the message from/to the device.

When Integrated Messaging is used, this parameter should be ignored by RCS clients if it is present.

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

Table 10: UX MO sub tree addition parameters (msgTDSwitch)

- Values:
  0 (Default Value) or absent. The RCS client shall not show or indicate to the user the underlying messaging technology / service.

1, the RCS client shall show or indicate to the user the underlying messaging technology / service.

- Post-reconfiguration actions: Start using the provided value the next time when receiving / sending a message or xMS.
- Associated HTTP XML characteristic type: “msgTDSwitch”

Node: /<x>/UX/Ext

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

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	node	Get

Table 11: UX MO sub tree addition RCS Service Provider Extension Node

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

This lead to the following UX tree:

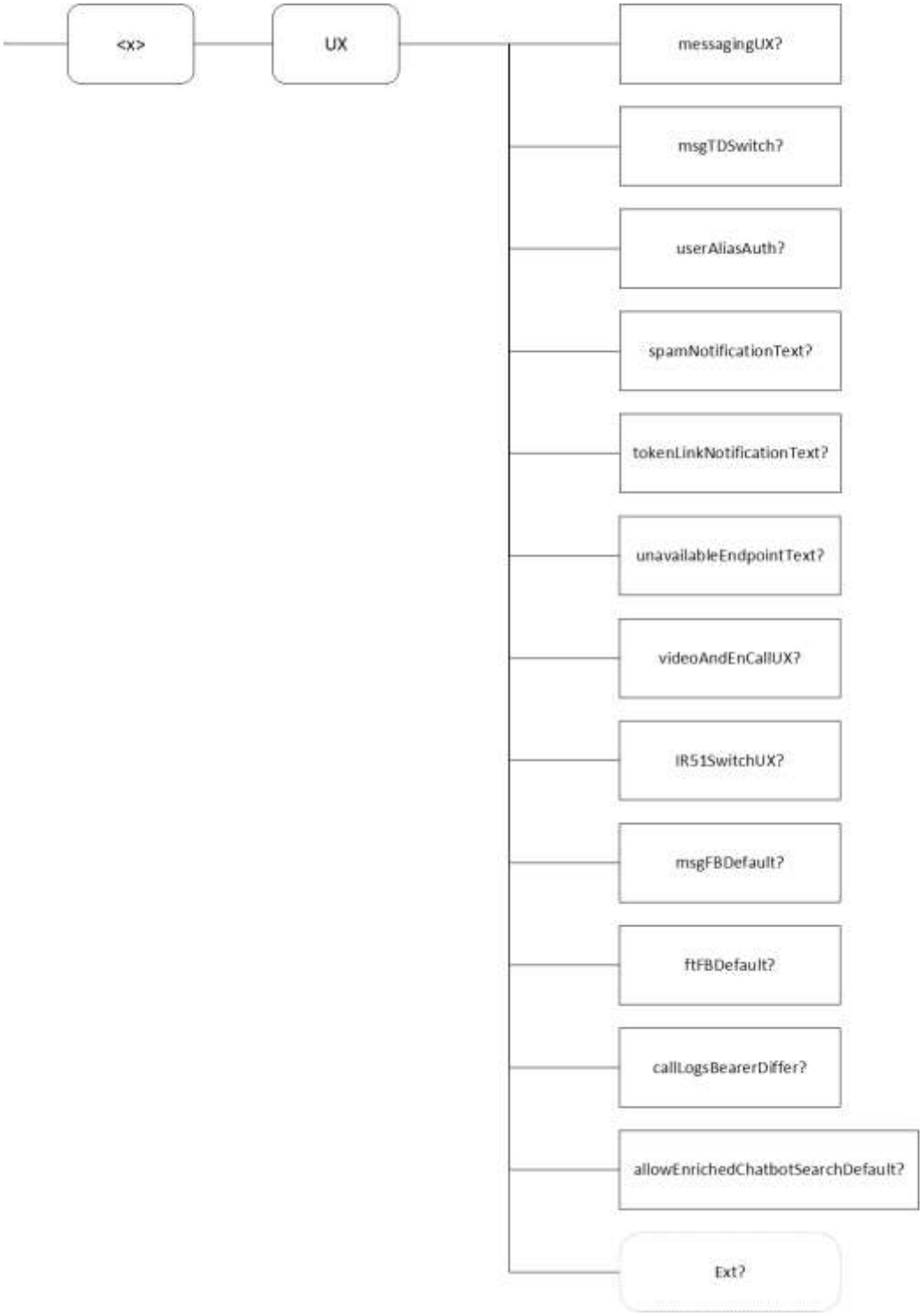


Figure 3: UX MO tree

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

```
<characteristic type="UX">
    <parm name="messagingUX" value="X"/>
    <parm name="msgTDSwitch" value="X"/>
    <parm name="userAliasAuth" value="X"/>
    <parm name="spamNotificationText" value="X"/>
    <parm name="tokenLinkNotificationText" value="X"/>
    <parm name="unavailableEndpointText" 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"/>
    <parm name="allowEnrichedChatbotSearchDefault" value="X"/>
    <characteristic type="Ext"/>
</characteristic>
```

Table 12: UX MO sub tree associated HTTP configuration XML structure

5.3.5 Technical Implementation of User Stories and Service Requirements

R5-28-1 Requirements R5-1-1 and R5-1-2 shall be implemented locally on the device.

R5-28-2 Requirement R5-2-1 shall be implemented locally on the device.

R5-28-3 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.

R5-28-4 Requirements R5-2-2-3, R5-2-2-4 and R5-2-2-5. shall be implemented locally on the device

R5-28-5 Requirement R5-2-3 shall be realised based on the interworking procedures in [RCC.07] and the applicable specifications it refers to.

R5-28-6 Requirement R5-2-3-1 shall be realised through the procedures in section 3.2.3.8.3 of [RCC.07].

R5-28-7 Requirement R5-2-4 shall be realised through the revocation procedures defined in section 3.2.3.8 of [RCC.07].

R5-28-8 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 3.2.3.8 of [RCC.07].

R5-28-9 Requirement R5-2-4-2 shall be implemented locally on the device.

R5-28-10 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.1.3 and A.2.4 of [RCC.07].

R5-28-11 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 5.3.4.

R5-28-12 Requirement R5-2-4-5 and its sub requirements shall be implemented on the device using the revocation procedures defined in section 3.2.3.8 of [RCC.07] 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 A.1.3 and A.2.4 of [RCC.07]. 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 A.1.3 and A.2.4 of [RCC.07] shall be set to zero.

R5-28-13 Requirement R5-2-4-6 shall be implemented locally on the device.

R5-28-14 Requirement R5-2-4-6-1 shall be implemented locally on the device. It is applicable when selected user settings resulting from RCS 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)

R5-28-15 Requirement R5-2-5 and its sub requirements shall be implemented locally on the device.

R5-28-16 Requirement R5-3-1 shall be implemented locally on the device.

R5-28-17 For requirement R5-3-2, the client shall rely on the value of the MSG TECH DISP SWITCH parameter which needs to be set by the MNO:

- For Integrated Messaging, this parameter shall be ignored by RCS clients if it is present.
- For Seamless messaging, if this parameter is absent, or is set 0, the RCS client shall not show or indicate to the user the underlying messaging technology / service; however, if this parameter is present and is set to 1, the RCS client shall show or indicate to the user the underlying messaging technology / service.

R5-28-18 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 3.2.3.4 and 3.2.3.8 of [RCC.07]. When RCS Standalone messaging is selected, originating or terminating fallback may be applied based on RCS Service Provider policies.

R5-28-19 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.

R5-28-20 Requirements R5-4-1 and R5-4-2 shall be implemented locally on the device.

R5-28-21 Requirement R5-4-3-1 shall be realised by configuring the MESSAGING UX parameter defined in section 5.3.4.

R5-28-22 Requirement R5-4-3-2 is realised as specified in section 18.3.

R5-28-23 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 R5-5-1-3-2 shall be realised based on the Interworking disposition notification as specified in section 3.2.3.1 of [RCC.07].

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 R5-5-1-4-1 shall be implemented locally on the device based on the setting for US18-7. Requirement R5-5-1-4-2 shall be implemented locally on the device. Requirement R5-5-1-4-3 shall be realised based on the Interworking disposition notification as specified in section 3.2.3.1 of [RCC.07]. Displayed status is not applicable if the client received an interworking notification but no delivery notification.

- **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.

R5-28-24 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 3.2.3.2 of [RCC.07].

R5-28-25 Requirements R5-5-3, R5-5-4 and R5-5-5 shall be implemented locally on the device.

R5-28-26 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.

R5-28-27 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 3.2.3.1 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.

R5-28-28 Requirement R5-8-1 is fulfilled based on sections 5.3.1 and 5.3.2 and section 3.2.3.8 of [RCC.07].

R5-28-29 Requirement R5-8-1-1 shall be implemented as defined in sections 3.2.3.2 and 3.2.3.3 of [RCC.07].

R5-28-30 Requirement R5-8-2 is fulfilled based on sections 5.3.1 to 5.3.3 and section 3.2.3.8 of [RCC.07].

R5-28-31 Requirement R5-9-1 shall be implemented as defined in sections 5.3.1 to 5.3.3 and section 3.2.3.8 of [RCC.07].

R5-28-32 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 RCS Service Provider to 1 to enforce the client to accept the session immediately.

R5-28-33 Requirement R5-9-3 and R5-9-4 shall be implemented locally on the device.

R5-28-34 The requirements of user stories US5-10 and US5-11 shall be implemented locally on the device.

R5-28-35 Requirement R5-12-1 shall be implemented locally on the device.

R5-28-36 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 Direction attribute defined in [CPM-MSGSTOR-REST].

R5-28-37 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.

R5-28-38 The requirements of user story US5-14 shall be implemented locally on the device.

R5-28-39 To satisfy the requirements of US5-15 the client shall apply the following procedure:

R5-28-40 If the configuration parameter USER ALIAS AUTH defined in section 5.3.4 is set to 0 then the client shall:

R5-28-41 Not offer the user to manage a user alias used for RCS communications.

R5-28-42 Not send a user alias for mobile originated chat sessions and

R5-28-43 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.

R5-28-44 If the configuration parameter USER ALIAS AUTH defined in section 5.3.4 is set to 1 or it is not present, then:

R5-28-45 The client shall offer the user to manage a user alias used for RCS communications.

R5-28-46 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].

R5-28-47 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.

R5-28-48 The client shall store the user alias in the local chat communication history.

R5-28-49 In addition, the client implementation shall respect the requirements of the post reconfiguration actions defined for the configuration parameter USER ALIAS AUTH in section 5.3.4.

R5-28-50 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.1.3 and A.2.4 of [RCC.07].

R5-28-51 For requirements R5-17-1 and R5-17-2 section 7.3 applies.

R5-28-52 Requirement R5-17-3 shall be implemented locally on the device.

R5-28-53 Requirement R5-18-1 shall be implemented locally on the device.

R5-28-54 Requirement R5-19-1 and R5-20-1 is fulfilled by deploying a Common Message Store as described in [RCC.07] and [RCC.11].

R5-28-55 Requirement R5-19-2 is fulfilled based on RCS Service Provider policies.

R5-28-56 Requirement R5-19-3 shall be implemented locally on the device.

R5-28-57 For requirement R5-19-5, a dedicated Message Store client shall be implemented on the device as defined in section 4.1 of [RCC.07] and [RCC.11].

R5-28-58 For requirement R5-20-1, the client shall delete messages and conversations in the Common Message Store after local deletion as defined in section 4.1.15.7 of [RCC.07].

R5-28-59 The requirements of US5-21 shall be implemented locally on the device.

R5-28-60 The requirements of the user stories US5-22 to US5-25 are implemented via the RCS Geolocation Push service defined in section 3.2.6 of [RCC.07].

R5-28-61 Requirements R5-26-1, R5-26-2, R5-26-3, R5-26-4 and R5-26-5 shall be implemented based on the 1-to-Many Messaging service procedures defined in section 3.2.2.8 of [RCC.07].

R5-28-62 For requirement R5-27-1, the MAX 1 TO MANY RECIPIENTS parameter defined in section A.1.3 and A.2.4 of [RCC.07] shall be configured.

R5-28-63 For R5-27-2, the 1 TO MANY SELECTED TECHNOLOGY parameter defined in section A.1.3 and A.2.4 of [RCC.07] shall be configured.

R5-28-64 Requirement R5-27-2-1 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 at the same time. All participants can see all other participants' activity within the group and replies are distributed to the entire group of participants.

Overview of major functional changes in this section compared to Universal Profile 2.0:

- Clarification that a Chatbot or MaaP Application cannot be a participant in a Group Chat.
- Differentiation between Group Chat and "Message a Chatbot" concepts as defined in section 15.

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.

R6-1-1-1 Any Chatbot or MaaP Application that is part of the user's contact list shall be considered as an incapable contact for Group Chat, i.e. these Chatbot contacts cannot be added to the participants list when creating a Group Chat conversation.

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. As a result of this operation, the existing 1-to-1 Messaging conversation window is closed and the conversation remains active and accessible. A new Group Chat is opened with an empty history in the foreground. The participants shall be the two participants from the 1-to-1 Messaging conversation plus the selected contact(s) from the extension.

R6-1-2-1 Any Chatbot or MaaP Application that is part of the user's contact list shall be considered as an incapable contact for Group Chat, i.e. these contacts cannot be added as participants to a Group Chat conversation.

R6-1-2-2 If a user is in an existing conversation with a Chatbot or MaaP Application, it shall not be possible to extend this conversation to a Group Chat by adding one or more capable (for this service) contact(s) from the contact list.

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).

R6-1-3-1 Any Chatbot or MaaP Application shall be considered as an incapable participant for Group Chat.

NOTE: When using "Message a Chatbot from a Group Chat conversation" the Chatbot will not appear as a regular participant in the Group Chat. In this case, the Chatbot or MaaP Application is not a participant to the Group Chat but just receives a message from one of the Group Chat participants and the answer provided by the Chatbot or MaaP Application is shared with all participants of the Group Chat.

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

NOTE: The feature "Message a Chatbot from a Group Chat conversation" can be used even if the maximum number of Group Chat participants is reached.

R6-1-5 When starting a new Group Chat, the inviting user or initiator shall invite at least two other Group Chat capable participants.

R6-1-5-1 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 invited participants never joined.

R6-1-6 When a user tries to create a new Group Chat with the same list of participants and the same Group Chat subject as an existing one, then the client shall jump to the existing Group Chat and not create a new one.

R6-1-7 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, then a new Group Chat shall be created.

R6-1-8 For any Group Chat conversations, the creator of a Group Chat shall be able to remove participants that have been added to the conversation (either when creating the Group Chat or later).

R6-1-8-1 In the case where a participant is removed, all participants shall be informed about a participant being removed from the Group Chat in the same way as when a participant leaves the Group Chat voluntarily.

R6-1-8-2 The removed user shall see a last update to the Group Chat thread politely indicating that they have been removed.

R6-1-8-3 The removed user shall not be able to create or send any further messages to that group (e.g. including the case when a user was offline during their removal from the group and messages were not sent).

R6-1-8-4 Once removed from a Group Chat, a user shall receive no further updates from the group.

R6-1-8-5 If the creator of a Group Chat leaves the conversation, then there shall be an option to pass on the right for removing participants from the Group Chat to another participant.

US6-2 **As a user, I want to add a Group Chat subject and icon to any Group Chat conversation.**

R6-2-1 When creating a Group Chat conversation, it shall be possible for the creator to define subject and an icon for that Group Chat

R6-2-2 If no subject has been defined, the application shall automatically generate a subject (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.

R6-2-2-1 The subject of a Group Chat shall be represented in the list of chat conversations similar to contact names for 1-to-1 Messaging conversations. In addition to the Group Chat subject, the number of Group Chat participants shall be indicated in brackets (e.g. “Group Chat Subject (4)” if the subject was set to ‘Group Chat Subject’ and the number of participants in the Group Chat is four).

R6-2-2-2 The subject of a Group Chat shall be visible as a ‘headline’ on top of the Group Chat window when the Group Chat conversation is displayed on the screen. The number of Group Chat participants shall be displayed in addition to the Group Chat Subject similar to the requirements in R6-2-2-1.

R6-2-2-3 If the Group Chat Subject is too long to be represented in the list of conversations or the headline of a Group Chat, the Group Chat Subject shall be truncated, and the user shall have the option to see the Group Chat Subject in full length on user interaction. The number of Group Chat participants shall however always be visible.

R6-2-2-4 The UI design shall allow the user to clearly differentiate Group Chat subjects from Chatbot names, to prevent that Group Chat is used as a tool for spoofing false identities.

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 subjects.

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.

R6-2-5-1 The change shall be visible for all Group Chat participants by an information in the Conversation History that subject and / or icon was changed, the person who made the change plus date and timestamp. (There is no need to log the content of the change). In case of offline devices, the change shall be visible once the device come online again).

R6-2-5-2 The user shall have the ability to see who has changed the icon or subject and when by browsing the message history of that Group Chat.

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.

R6-3-1-1 Additions of new participants shall be limited to user's contacts; it shall not be possible to add any Chatbot or MaaP Application to an existing Group Chat.

NOTE: When using "Message a Chatbot from a Group Chat conversation" the Chatbot will not appear as a regular participant in the Group Chat. In this case, the Chatbot or MaaP Application is not a participant to the Group Chat but just receives a message from one of the Group Chat participants and the answer provided by the Chatbot or MaaP Application is shared with all participants of the Group Chat.

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 RCS Service Provider (see R6-1-4).

NOTE: The feature "Message a Chatbot from a Group Chat conversation" can be used even if the maximum number of Group Chat participants is reached.

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 participating contacts whenever they wish.

R6-4-2 If the participants of a Group Chat Message is not in my contact list, they shall be represented by the RCS Alias name (if available), in addition to their MSISDN.

R6-4-2-1 Representation of Alias names in Group Chat conversations or list of Group Chat participants shall be visually differentiated from contact list matches, including clear wording that suggest the Alias name has not been verified, e.g. “+49171 1234567 (possibly “Alias”)”.

R6-4-3 If neither Contact name nor RCS Alias is available, a Group Chat participant shall be represented with their MSISDN in the Group Chat

R6-4-4 In the case where new Group Chat participants join the Group Chat, all other Group Chat participants shall be informed appropriately in the Conversation History

R6-4-5 In the case where Group Chat participants leave the conversation, all other Group Chat participants shall be informed appropriately in the Conversation History.

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

R6-5-1 The RCS Service Provider 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 RCS Service Provider configurable; if an RCS Service Provider decides to not support auto-accept, the invited user becomes participant in a Group Chat once the participation was manually accepted.

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 want to 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 confirmation of the message.

US6-8 **As a user, I want to send Group Chat messages to all Group Chat participants even when they are 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, all message(s) or updates to the list of Group Chat participants shall be delivered once the user is back online.

R6-8-2 The RCS Service Provider shall be able to set the storage duration for store & forward cases (deferred messaging) based on individual RCS Service Provider 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 Chat/Group Chat application.

NOTE: Standards for conversion of text strings to Emoji are described in the Annex "Emoticon conversion table", Annex A.2

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 do not 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: RCS Service Provider 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 and files.**

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

R6-11-1-1 Message or file 'Pending' - transfer of the message or file has been triggered but not actually started (e.g. queuing on device).

R6-11-1-2 File Transfer 'In Progress' – File Transfer started but not completed.

R6-11-1-2-1 The progress of sending the file shall be indicated to the user.

R6-11-1-3 File Transfer 'Cancelled' – the sender has cancelled the File Transfer during the File Transfer 'In Progress'.

R6-11-1-4 Message or file 'Sent' - confirmation that the message or file has been correctly handed over to the network successfully.

R6-11-1-5 Message or file 'Delivered' - the message or file has been successfully delivered to all recipient's devices.

NOTE: Networks may not support message or file 'Delivered' in Group Chat. In this case, there are no outgoing notifications generated and incoming message or file 'Delivered' notifications in Group Chat may be ignored.

R6-11-1-6 Message or file 'Displayed': the content of the message or file was brought to all recipients' attention.

R6-11-1-6-1 As per US18-7 and the related requirements, the user shall have the option to disable the feedback that the message or file was displayed.

R6-11-1-7 When the message or file 'Failed': The expected outcome of the operation could not be confirmed by the network (in this case: message or file 'Sent', 'Delivered' or 'Displayed' status has not been received and the device does not attempt to send the message or file again). Sending the message or file may be re-triggered manually by the user.

NOTE: For Message States and File Transfer States Notifications, restrictions e.g. in cases of legacy support as specified in sections 5 and 7 apply.

R6-11-2 If the sending device is offline at the time a message status is received, message states shall be stored on the network and forwarded once the sending device is online.

R6-11-3 In the messaging conversation, ‘Delivered’ and ‘Displayed’ states for messages and files shall only be indicated whenever all recipients devices have confirmed the status.

R6-11-4 The A-Party user shall be able to see detailed Message and File Transfer States Notifications per recipient when looking at details (triggered by A-Party user manual action).

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

R6-12-1 Any participant of the Group Chat shall be able to see when another Group Chat participant is in the process of creating a new message.

NOTE: Networks may not support “Is Typing” Notification. In this case, networks may ignore incoming “Is Typing” Notifications and may not send outgoing “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 or file transfer, the user shall be notified with a new incoming event notification.

R6-13-2 For audible new incoming event notifications, device audio related settings shall prevail.

US6-14 **As a user, I want New Incoming Event Notifications of rapidly sequenced incoming Group Chat Events intelligibly aggregated and counted.**

R6-14-1 Rapid sequence of incoming Group Chat Events 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 Group Chat subject and icon 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 that contain unread messages or unseen File Transfer events to be differentiated from conversations that contain messages I have seen.**

NOTE: 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 or unseen files 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 handshake 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 any files including 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 files including media that were exchanged in the selected Group Chat in an 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), any ongoing Group Chat shall stay active, i.e. 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 be made aware of this procedure.

R6-21-3 A Group Chat shall end permanently, which means that no further messages or files can be exchanged in this conversation,

R6-21-3-1 after an extended time of inactivity (no messages were exchanged, no participants were invited or removed) as defined by the RCS Service Provider.

R6-21-3-2 upon network configuration if the number of remaining users in a Group Chat equals one (1).

R6-21-4 Permanently closing the Group Chat shall be indicated to the last known remaining participants in the Conversation History similar to a Group Chat that was left by participant's intention.

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.

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.

NOTE: It is expected that the user is able to see the content of the Group Chat conversation irrespectively whether the user left intentionally or was removed from the list of participants as a result of a Group Chat creator action (see R6-1-8).

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 Group Chat 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 RCS Service Provider.

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.

R6-24-3 As a user, I want my Group Chat messages backed up in a trusted and safe environment.

R6-24-4 The RCS Service Provider shall be able to store Group Chat Conversations 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 RCS Service Provider discretion.

US6-25 **As a user, I want to restore my Group Chat Conversations (e.g. but not limited to, after wiping device or purchasing a new device).**

R6-25-1 The user shall have the option to restore Group Chat conversations with the entire content (messages and files) from the network (e.g. in case of handset replacement or factory reset of the users device).

US6-26 **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.**

R6-26-1 The user shall have the ability to share positions or locations with all participants of a Group Chat conversation.

R6-26-2 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 US5-25 detailing the service in addition to the above listed Group Chat specific requirements are valid accordingly.

US6-27 **As a user, I want to be made aware about creating multiple 1-to-1 messages or Group Chat messages.**

R6-27-1 The user shall be made aware of the difference of Group Chat versus multiple 1-to-1 messages as described in 1-to-1 Messaging section 5 in relevant places of the implementation.

6.3 Technical Information

6.3.1 Overview

The Group Chat service is provided based on the Group Chat technical enabler defined in section 3.2.4 of [RCC.07].

6.3.2 Technical Implementation of User Stories and Service requirements

R6-28-1 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 as defined in section 3.2.4.2 of [RCC.07].
- For requirement R6-1-1, the procedures for initiation of a group chat and the conditions for the client to select capable contacts are defined in section 3.2.4.3 of [RCC.07].
- R6-1-1-1 shall be realised locally on the device based on the Chatbot role capability indication defined in section 2.6.1.3 of [RCC.07].
- For requirement R6-1-2, in alignment with the UX procedures, a new Group Chat shall be created as a separate session as specified in section 3.2.4.4 of [RCC.07] without reference to the ongoing 1-to-1 Chat conversation.
- R6-1-2-1 shall be realised locally on the device based on the Chatbot role capability indication defined in section 2.6.1.3 of [RCC.07].
- R6-1-2-2 shall be realised locally on the device.

- For requirement R6-1-3, the procedures for a client to handle the invitation to a Group Chat as defined in section 3.2.4.4 of [RCC.07] apply.
- R6-1-3-1 shall be realised locally on the device based on the Chatbot role capability indication defined in section 2.6.1.3 of [RCC.07].
- For requirement R6-1-4, the procedures for the management of the maximum number of participants applies as defined in section 3.2.4.3 of [RCC.07] for the initiation of a Group Chat.
- Requirement R6-1-5 for the restriction upon Group Chat creation shall be implemented as defined in section 3.2.4.3 of [RCC.07].
- For requirement of R6-1-5-1, the RCS Service Provider's conforming to the profile defined in this document shall choose to set the value of the minimum number of participants allowed in a Group Chat as defined in section 3.2.4.9.2 of [RCC.07] to either "2" or "1". For the handling of a Group Chat invitation where no invited participant accepts the invitation, the procedures of [RCC.11] apply.
- Requirements R6-1-6 and R6-1-7 shall be implemented locally on the device.
- For the requirements in R6-1-8, the procedures described in
    - section 3.2.4.12 of [RCC.07] apply for the handling of removal requests. The conference focus of the Messaging Server shall set the "Participant Removal policy" described in section 3.2.4.14 of [RCC.07] to "administrator only". The client shall offer the option to remove a participant only if the client's own user is assigned with the "administrator" role.
    - section 3.2.4.8 of [RCC.07] applies for the information sent to other participants.
    - section 3.2.4.7 of [RCC.07] applies for the move of the administrator role to another participant. The Messaging Server shall set the "user role assignment policy" to "single administrator". If the "user role assignment policy" is set to "single administrator" and the client's own user is assigned with the "administrator" role and the user requests the client to leave the Group Chat, then the client shall first invoke the UX procedure to ask the user whether the role shall be moved to another participant. If the user selects another participant to become the "administrator", then the client shall invoke the procedure of the Group session data management to "move" the role to the selected participant. The client shall process the request to leave the Group Chat only after the request to move the "administrator" role has been finished. If the client is offline and the user is assigned to be the "administrator", then the

client shall not offer the user to leave the Group Chat, until it comes online again.

R6-28-2 For requirement R6-2-1, the "subject" shall be handled at the time of initiation of a Group Chat via the procedure described in section 3.2.4.3 of [RCC.07]. The "icon" shall be assigned to the Group Chat via the Group session data management for icon management described in section 3.2.4.7 of [RCC.07]. The client shall resize the Group Chat icon to have a maximum file size of 50 kBytes

R6-28-3 The requirements R6-2-2 to R6-2-4 shall be implemented locally on the device.

R6-28-4 The requirements of R6-2-5 shall be implemented via the Group session data management for subject and icon management described in section 3.2.4.7 of [RCC.07] for change of icon and via the procedures for receiving of Group Chat participant and meta information described in section 3.2.4.8 of [RCC.07] for the distribution to Group Chat members. The client shall resize the Group Chat icon to have a maximum file size of 50 kBytes.

R6-28-5 For requirement R6-3-1, to add participants, the procedure described in section 3.2.4.6 of [RCC.07] applies.

R6-28-6 For R6-3-1-1, this shall be realised locally on the device based on the Chatbot role capability indication defined in section 2.6.1.3 of [RCC.07].

R6-28-7 For requirement R6-3-2, the determination of the maximum number of participants applies as defined in section 3.2.4.6 of [RCC.07] for an existing Group Chat.

R6-28-8 For requirements R6-3-3 and R6-3-4, the recipient's capability to support the Chat service shall be treated as "service availability information" as defined in section 3.3.1 of this document.

R6-28-9 Requirement R6-3-5 shall be implemented locally on the device.

R6-28-10 For user story US6-4, the management of the Group Chat participants list shall be managed by the Messaging Server and the client using the procedure described in section 3.2.4.8 of [RCC.07].

The RCS Alias for Group Chat users described in requirements R6-4-3 and R6-4-4 shall be implemented as defined in section 2.5.3.4 of [RCC.07].

R6-28-11 For user story US6-5, the client handling for invitation to a new Group Chat as described in section 3.2.4.4 of [RCC.07] applies. A client being invited to a Group Chat via the procedure described in section 3.2.4.4 of [RCC.07], shall use the value of the SIP Referred-By header as per the definition of section 2.5.2.1 of [RCC.07], to indicate the originator of the invitation.

R6-28-12 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 3.2.4.10 of [RCC.07] and send the message to it.

R6-28-13 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.

R6-28-14 The requirements of user story US6-8, the Messaging Server shall implement the procedures for Store and Forward as described in section 3.2.4.15 of [RCC.07] with a duration of storage as per RCS Service Provider policy.

R6-28-15 The implementation of the graphics in a Group Chat conversation in the requirements of US6-9 shall be implemented locally on the device considering the definitions of defined in Annex A.2 and A.3.

R6-28-16 For the realization of the requirements R6-10-1, the client shall enforce the configured maximum message size of a Chat for sending messages as described in section 3.2.4.17 of [RCC.07].

R6-28-17 The requirement R6-10-2 shall be implemented locally on the device.

R6-28-18 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 3.2.4.17 of [RCC.07].

R6-28-19 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 3.2.4.15 of [RCC.07].

R6-28-20 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 3.2.3 of [RCC.07].

R6-28-21 The requirements for user stories US6-13 and US6-14 are implemented locally on the device.

R6-28-22 The requirement of user story US6-15 is implemented locally on the device in alignment with the requirements of user story US6-2.

R6-28-23 The requirement of user story US6-16 is implemented locally on the device.

R6-28-24 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. To meet the requirements R6-17-3 and R6-17-4 the implementation of the Messaging Server shall conform to definitions of section 3.2.4 of [RCC.07].

R6-28-25 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 in a Group Chat shall follow the procedures defined in section 3.2.4 and 3.2.5 of [RCC.07].

R6-28-26 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.

- For the interleaving of sent and delivered messages, the client shall respect the definitions of section 3.2.4.16 of [RCC.07] regarding support of direct delivery.

R6-28-27 The requirements of user story US6-20 shall be implemented locally on the device. The Messaging Server shall apply processing of the CPIM DateTime header as described in section 3.2.4.17 of [RCC.07].

R6-28-28 The requirements R6-21-1, R6-21-2 and R6-21-4 shall be implemented locally on the device based on the Group Chat life cycle described in section 3.2.4 of [RCC.07].

R6-28-29 The requirement R6-21-3 to terminate a Group Chat after inactivity shall be implemented on the Messaging Server based on the procedure described in section 3.2.4.9.2 of [RCC.07].

R6-28-30 The requirements of user story US6-22 shall be implemented locally on the device.

R6-28-31 The requirements of user story US6-23 shall be implemented as defined in section 3.2.4.11 of [RCC.07].

Subsequent invitations to a Group Chat which the user has left voluntarily shall be accepted by the client in accordance with the definitions for invitation to a new Group Chat, see user story US6-5.

R6-28-32 The client implementation shall ensure that the Group Chat handling as defined in R6-23-5 initiates a request to the network to leave the Group Chat.

R6-28-33 The requirement for automatic removal from the Group Chat defined in R6-23-7 shall be implemented via the procedure described in section 3.2.4.11 of [RCC.07].

R6-28-34 The requirements of user story US6-24 shall be implemented locally on the device.

R6-28-35 The requirements of user story US6-25 are implemented as defined in section 3.2.4.8 and 3.2.4.16 of [RCC.07] and based on the definitions in section 9 of this document.

R6-28-36 The implementation of user story US6-26 shall be based on Geolocation Push in a Group Chat as defined in section 3.2.6 of [RCC.07].

R6-28-37 The requirements of user story US6-27 shall be implemented locally on the device.

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.

R7-1-1-4 When the originating device is offline (i.e. not registered for RCS), but data connectivity is available, MMS should be used to send the file when the MMS service is enabled by the RCS Service Provider for that device.

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.

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.3).

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)

R7-1-5-7 Display of documents in pdf format

R7-1-6 Any RCS device may 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:

R7-1-7-1-1 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, will the client 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 and 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 should not 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 and an SMS link shall not 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 Profile 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 US5-27.

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 For A Party, the following File Transfer states shall be supported

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.

R7-4-1-2-1 The progress of sending the file shall be indicated to the user.

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 shall be 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 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.

R7-4-1-6-2 As per US18-7 and the related requirements, the user shall have the option to disable sending the feedback that the file was displayed.

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 do not want to perceive a restriction in file sizes that I want to transfer.**

R7-7-1 The RCS Service Provider shall set the File Transfer limit to 100MB.

R7-7-2 The RCS 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 RCS Service Provider shall be able to limit the list of recipients.

R7-10-2-1 The RCS Service Provider 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 RCS Service Provider 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

R7-10-4 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 are 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 an RCS Service Provider, I want to limit how long a file is available on the network for offline users.**

R7-12-1 The RCS Service Provider shall be able to define the network storage time for File Transfers that have not been downloaded yet.

NOTE: This requirement 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.

R7-13-4 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.

R7-13-5 The visual notification for an incoming File Transfer shall be permanently removed from the notification centre bar, once the thread with the file or thumbnail preview has been opened.

NOTE: Independently of whether the user has clicked the notification or has accessed the thread from the messaging application.

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 1-to-1 Messaging 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 '1-to-1 Messaging' and 'Group Chat', shall be applied to files.

R7-14-3 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).

R7-14-4 1-to-1 Messaging or Group Chat conversations with unread events (any event that is received within the 1 to 1 Messaging 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 their RCS Service Provider, 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 file is automatically downloaded in its entirety via cellular bearer if the file size is below a threshold defined by the RCS Service Provider and can be accessed from the Chat Conversation.

R7-15-3-2 If the file size is equal or above the threshold defined by the RCS Service Provider and the device is connected via cellular bearer, then the file shall not be automatically downloaded but manual confirmation as described in R7-15-1 and subsequent sub requirements shall apply.

R7-15-3-3 If the device is connected via Wi-Fi, then the file is always downloaded in its entirety without manual user interaction.

R7-15-4 The RCS Service Provider 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. (The user may be able to manually re-trigger File Transfer and resume from where the File Transfer failed).

US7-17 **As a user, I want to transfer one or multiple Contact's/Contacts' 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.

R7-17-2 When sending Contact Card(s) from service entry points listed in R7-3-1, the device shall include one or multiple contact cards in a single vcf-format file and send it to the destination recipient(s).

R7-17-3 Devices shall be capable to render vCard files in .vcf format and offer to store received Contacts in the device contact list.

R7-17-3-1 In case multiple contact cards are sent in one vcf-format file, the receiving device shall be capable to render all the contacts in that file, and permit the receiver user to select one or more of them to check details, edit, store, forward, delete or perform other operations.

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 RCS Service Provider storage time (as in R7-12-1) has not expired.

US7-19 **As an RCS 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 files backed up by the RCS Service Provider in a trusted and safe environment.**

R7-21-1 The RCS Service Provider shall be able to store files.

NOTE: Details of storage are at the individual RCS Service Provider discretion.

R7-21-2 In case the RCS Service Provider deletes stored files (e.g. for capacity limitation), these files shall not be deleted from local user equipment.

US7-22 **As a user, I want to restore my sent and received files.**

R7-22-1 The user shall have the option to restore transferred files from the network storage *(e.g. in case of handset replacement).*

7.3 Technical Information

7.3.1 Overview

The File Transfer service is provided based on the File Transfer Enabler defined in section 3.2.5 of [RCC.07].

The client shall advertise the capability for File Transfer in accordance with the definitions of section 3.2.5.2 of [RCC.07].

A RCS contact is considered File Transfer capable if the File Transfer capability is present.

7.3.2 Configuration Parameters

7.3.2.1 New Configuration Parameters

To provide operator control of the client's File Transfer behaviour the following new configuration parameter is defined for the profile defined in this document.

Configuration parameter	Description	RCS usage
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 13: Configuration Parameter for File Transfer Control

The FT FALLBACK DEFAULT configuration parameter is added to the UX tree defined in section 5.3.4.1 based on the following definition.

Node: /<x>/UX/ftFBDefault

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 14: 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 has not been toggled by the user before.

- Associated HTTP XML parameter ID: “ftFBDefault”

7.3.3 Technical Implementation of User Stories and Service requirements

R7-23-1 The requirements of R7-1-1 are implemented locally on the device.

R7-23-2 The requirement R7-1-2 is implemented locally on the device. For details of the technology selection for the transfer of a file to RCS and non-RCS contacts, refer to R7-1-7 and the corresponding technical implementation.

R7-23-3 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.

R7-23-4 The capability required in R7-1-4 is a basic function of the File Transfer enabler.

R7-23-5 The requirements of R7-1-5 and R7-1-6 are implemented locally on the device.

R7-23-6 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 A.1.4 of [RCC.07].

R7-23-7 The requirement R7-1-7-1 is applicable

- if the configuration parameter FT HTTP FALLBACK defined in section A.1.4 of [RCC.07] 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 A.1.4 of [RCC.07] 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 to the formats and codecs defined in [OMA-MMS-CONF].

The procedure defined in section 3.2.5.7.3 of [RCC.07] applies.

R7-23-8 The requirement R7-1-7-2 is applicable if the configuration parameter FT HTTP FALLBACK defined in section A.1.4 of [RCC.07] 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 3.2.5.7.3 of [RCC.07] applies.

R7-23-9 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 RCS Service Provider device provisioning, then the client shall ignore the value provided by the RCS Service Provider.

R7-23-10 The requirement R7-2-1 is implemented via the procedures for delivery assurance defined in section 5.3 of this document.

R7-23-11 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.

R7-23-12 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 7.3.2.1.

R7-23-13 The requirements of user story US7-3 shall be implemented locally on the device.

R7-23-14 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 (i.e. HTTP 204 NO CONTENT or HTTP 411 AUTHENTICATION REQUIRED as defined in [RCC.07]) 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 3.2.3.1 of [RCC.07], 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 3.2.3.1 of [RCC.07], 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 3.2.3.1 of [RCC.07], i.e. the client should indicate that the user should not expect a displayed status for the message in this case.
  The requirement R7-4-1-6-2 shall be realised locally on the device based on the setting defined for US18-7.

  For File Transfer Fallback, not applicable.

- **Failed:**
  The failed state applies whenever the processing to send the File Transfer fails and the client 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.

R7-23-15 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 3.2.3.2 of [RCC.07]
- SMS delivery status reports as specified in [3GPP TS 23.040].

R7-23-16 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

R7-23-17 For the requirement R7-6-1 of user story US7-6, videos shall be optimised and resized to facilitate a faster transfer experience during a call (i.e. “low file size” as the default selection).

The recommended approach is to resize the video by modifying the resolution:

- The default resolution shall be 480p encoded at 1200 kbps.
- The resulting size shall be compared to FT WARN SIZE and FT MAX SIZE. The UI shall act correspondingly if the values are reached.
- For a pre-recorded video:
  - If the resolution is higher than 480p but the file is smaller than FT WARN SIZE the UI warns the user about the resolution of the video.

- if the resolution is higher than 480p and the file is higher than FT WARN SIZE but smaller than FT_MAX_SIZE then the UI warns the user about the resolution and the size.

- if the resolution is higher than 480p and the file is higher than FT MAX SIZE then the UI warns the user about the size and forces the compression or aborts the transfer.

- For a live video recording:

  - Recording at the default resolution of480p encoded at 1200 kbps is done. When the FT WARN SIZE is reached, the recording is stopped automatically.

R7-23-18 The video resizing itself shall happen before the File Transfer to the recipient is initiated.

R7-23-19 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.1.4 of [RCC.07].

R7-23-20 The technical implementation of the requirements of user story US7-8 is defined in section 3.2.5 of [RCC.07] and the technical definitions for Group Chat defined in section 6.3 of this document.

R7-23-21 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.

R7-23-22 The requirements in use case US7-10 shall be implemented locally on the device based on the following mechanisms:

R7-23-22-1 For the requirement R7-10-1, 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 and 7.3.1 of this document.

R7-23-22-2 The 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 A.1.4 of [RCC.07].

R7-23-22-3 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 A.1.4 of [RCC.07] 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 A.1.4 of [RCC.07] 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.1.3 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.

R7-23-22-4 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 A.1.4 of [RCC.07] 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 A.1.4 of [RCC.07] 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.1.3 of [RCC.07].

R7-23-22-5 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 recipients does not exceed the value of the configuration parameter MAX_AD-HOC_GROUP_SIZE defined in section A.1.3 of [RCC.07]. For the implementation of File Transfer in a Group Chat, refer to section 6.3 of this document.

R7-23-23 The technical implementation of File Transfer Store and Forward of user story US7-11 is defined in sections 3.2.5 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 3.2.5.1 of [RCC.07] for File Transfer via HTTP or from the URL parameter defined in section 3.2.5.5 of [RCC.07] for File Transfer fallback. If the client attempts to download the file from the HTTP Content Server as defined in section 3.2.5.4.2 of [RCC.07] and it receives a HTTP 404 NOT FOUND error, then the client shall assume that the file has expired.

R7-23-24 The requirement of user story US7-12 is provided by the RCS Service Provider’s policy on the messaging server or the HTTP Content Server.

R7-23-25 The requirements of user stories US7-13 and US7-14 shall be implemented locally on the device.

R7-23-26 The requirements of user story US7-15 shall be implemented locally on the device with the threshold for the automatic File download being controlled by the FT WARN SIZE parameter defined in section A.1.4 of [RCC.07].

R7-23-26-1 The RCS Service Provider provides the default selection of auto download via the FT AUT ACCEPT parameter defined in section A.1.4 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.

R7-23-26-2 The client shall use the parameters of the file-info element of the HTTP message body content as defined in section 3.2.5.4.1 of [RCC.07] for File Transfer via HTTP or from the URL parameter defined in section 3.2.5.5 of [RCC.07] to support the user experience defined in US7-15.

R7-23-26-3 The thumbnail preview for File Transfer shall be implemented as defined in section 3.2.5 of [RCC.07].

R7-23-27 The requirements of R7-16-1 shall be implemented locally on the device based on the procedures defined in section 3.2.5.4.2 of [RCC.07] and the clarifications for the sub-requirements.

R7-23-27-1 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:

R7-23-27-2 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 3.2.5.4.2 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 3.2.5.7 of [RCC.07].

R7-23-27-3 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.

R7-23-27-4 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.

R7-23-27-5 For the implementation of requirement R7-16-1-5, the client shall take the definitions of section 3.2.5.4.2 of [RCC.07] into account.

R7-23-28 To implement the requirements of US7-17 refer to section 3.2.5.9.1 of [RCC.07].

R7-23-29 The requirement of US7-18 shall be implemented based on the procedures defined in

- section 3.2.5.4.1 of [RCC.07] for resume on the client when sending File Transfer or File Transfer fallback.
- section 3.2.5.4.2 of [RCC.07] for resume on the client when receiving File Transfer or File Transfer fallback.

R7-23-30 The file size limits defined in the user story US7-19 are configured via the FT MAX SIZE parameter defined in section A.1.4 of [RCC.07].

R7-23-31 The requirements of user story US7-20 shall be implemented locally on the device.

R7-23-32 For the implementation of user stories US7-21 through US7-22, refer to section 9 of this document.

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.

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 that 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.

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.

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 3.2.7.1 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 3.2.5.9.2 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 3.2.7.1 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 3.2.7.2.2. 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 3.2.7 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 section A.1.4 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 3.2.7.2.2. 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.

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 section 3.2.7.2.2 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 2 "Device Provisioning".

9.2 User Stories and Feature Requirements

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. For example when an MNO has deployed Multi Device Messaging, backup and restore may be provided to all its 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 RCS Service Provider offers me on all of my devices or interfaces.**

As an RCS user with multiple devices, I shall always receive communications on my primary device when connected to at least the cellular network regardless of the connectivity state of the secondary device(s) and interface(s).

NOTE: For some services this can mean only receiving notifications for the waiting content (e.g. notification of an 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.

R9-3-2 This store shall be used for RCS-enabled devices and interfaces to receive up-to-date message and conversation histories.

R9-3-3 All contents remotely stored shall be kept for an RCS Service Provider - 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

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, 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 nor navigation within the 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 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 sometimes apply when using multiple RCS identities on the same device or interface

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 18 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].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 OMA CPM 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 that 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 2.6.1.1.1 of [RCC.07]. A 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 2.10 of [RCC.07] and section 2.8 or 2.9 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 as in section 2.10.2 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, an 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:

R9-10-5-1 section 8.2.2.1 of [RCC.11] for CPM session invitation

R9-10-5-2 section 8.3.2.1 of [RCC.11] for handling CPM session responses and multiple MSRP media streams

R9-10-5-3 section 8.6.1 of [RCC.11] for procedures upon receiving MSRP

R9-10-5-4 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:

R9-10-6-1 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 of [RCC.07] in order to provide synchronisation capability for other connected and registered multi-device.

R9-10-6-2 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 of [RCC.07] and the synchronisation of multi-device as described in section 4.1.15.7 of [RCC.07]. The storage folder and objects for the RCS services and legacy messages can be technically realised as in section 4.1.6 of [RCC.07]. The RCS client and server procedures of CMS can be technically realised as described in section 6 and 7 of [CPM-MSGSTOR-REST].

R9-10-8 The quota size per user in the CMS is configured per operator policy.

R9-10-9 R9-3-5 shall be fulfilled as described for R9-3-1, R9-3-2, R9-3-3 and 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.

R9-10-10 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.

R9-10-11 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 and R9-3-4. The client shall use a notification channel for receiving updates on the status of messages in the Message Store and/or synchronisation triggers as specified in section 4.1.15.7 of [RCC.07]. When a user opens a conversation thread, the client shall give priority to synchronise that thread.

R9-10-12 R9-3-8 shall be realised based on section 4.1.15.7 of [RCC.07].

R9-10-13 R9-3-9 shall be realised using the client configuration parameter FT AUTO ACCEPT as mentioned in section 3.2.5.3.2.1 of [RCC.07]. A Common File

Store for File Transfer via HTTP in section 4.1.10 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.

R9-10-14 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.

R9-10-15 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 4.1.13 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.

R9-10-16 R9-4-3 shall be fulfilled based on R9-4-2.

R9-10-17 R9-4-4 is realised as described in the technical realisation for R9-4-3.

R9-10-18 R9-4-5 and R9-4-6 shall be realised by following section 3.2.5 of [RCC.07] and section 4.1.10 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.

R9-10-19 For 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.

R9-10-20 R9-5-1 is covered as described in section 3.2.4.2.3.1, section 3.2.4.2.3.2 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].

R9-10-21 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.

R9-10-22 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".

R9-10-23 R9-6-1 shall be realised per section 4.1.13 and 4.1.15.7 of [RCC.07].

R9-10-24 R9-6-1-1 shall be realised locally on the device (both primary and secondary device(s)).

R9-10-25 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 4.1.15.7 of [RCC.07].

R9-10-26 R9-6-3 shall be realised by the device not setting the '\Deleted' flag for messages that the user did not intend the delete.

R9-10-27 R9-7-1 shall be locally implemented in the secondary device.

R9-10-28 R9-7-2 shall be realised following the procedures specified in section 3.2.2, 3.2.4.2.6 and 3.2.4.2.7 of [RCC.07] and [RCC.11]. This requirement also has dependency on R9-1-2.

R9-10-29 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.

R9-10-30 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.

R9-10-31 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.

R9-10-32 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 If enabled by the service provider, 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 RCS Service Provider or via a third party trusted by the RCS 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 an RCS 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 an RCS 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 RCS 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 an RCS 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 an RCS 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 an RCS 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 an RCS 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 [PRD-IR.51], [PRD-IR.92], [PRD-IR.94], [RCC.07] 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 the configuration parameter Media_type_restriction_policy PROVIDE IR51 VOICE defined in section B.3 of [PRD-IR.51] enables Voice and/or Video over EPC-integrated Wi-Fi.
CALL LOGS BEARER DIFFERENTIATION	This parameter is applicable when the configuration parameter Media_type_restriction_policy defined in section B.3 of [PRD-IR.51] enables Voice over EPC-integrated Wi-Fi. 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 15: 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 5.3.4 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 16: 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
  1: Wi-Fi switch for IR.51 voice and conversational video services is visible to the user with default position set to OFF
  2: Wi-Fi switch for IR.51 voice and conversational video services is visible to the user with default position set to ON
- Post-reconfiguration actions: 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 17: 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 5.3.4.

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 RCS 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 RCS 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 configuration parameter Media_type_restriction_policy defined in section B.3 of [PRD-IR.51].

R10-15-8 Requirement R10-4-2 is fulfilled based on RCS Service Provider policy.

R10-15-9 Requirements R10-5-1, R10-5-2 and R10-5-3 shall be fulfilled based on the configuration parameters Media_type_restriction_policy defined in section B.3 of [PRD-IR.51] 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 R10-10-2, section 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 an RCS 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 If enabled by the service provider, IP Video Calls shall be possible through a Wi-Fi connection offered by the RCS Service Provider or via a third party trusted by the RCS Service Provider as well as any other Wi-Fi connection of the device.

US11-4 **As an RCS 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), IP video call continuity shall be maintained. If it is not possible to maintain the video call, the call shall continue as a Voice Call.

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 an RCS 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) the "live video" 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" view or downgrade the video call to audio only 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 an RCS 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 an RCS 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 3.5.2 of [RCC.07].

The three technical enablers shall co-exist based on procedures defined in section 3.5 of [RCC.07].

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 configuration parameter Media_type_restriction_policy defined in section C.3 of [PRD-IR.94]. RCS IP Video call is available in cellular access if Voice over LTE/Voice over Wi-Fi is not enabled on the device. The RCS 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.1.11 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 configuration parameter Media_type_restriction_policy defined in section B.3 of [PRD-IR.51].

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 the IR.94/IR.51 conversational video service, section 2.2.2 of [PRD IR.94] shall be considered. For the RCS IP Video call service, section 3.5 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.

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 3.5.2 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 3.5.2 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 3.5.2 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 the IR.51 conversational video service, section 2.4.4 of [PRD-IR.51] shall apply. For the RCS IP Video Call, section 3.5.2 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 3.5.2 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 Calling

12.1 Description

The Enriched Calling service evolves the current voice call experience throughout all phases of a voice call: before, during and after the voice call. For video calls, this section defines a pre-call experience.

Enriched Voice Calling covers the following functional areas:

- **Pre-call experience**: Enrichment of the voice or video call before the call is started. A calling user can “compose” and share content that the called party sees when receiving the 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 and with Video Services as described in “Green Button Promise for Video”, section 11 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 For the RCS Service Provider to enable the Enriched Calling Pre-Call features, they shall set the value of the COMPOSER AUTH configuration parameter (see sections 2.1.2 and 2.1.2.1 of [RCC.20] and sections A.1.5 and A.2.1 of [RCC.07]) to 1, 2 or 3, depending on the Call Composer services that are enabled.

R12-1-5 In order for the RCS 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 RCS 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 configuration parameter Media_type_restriction_policy defined in section C.3 of [PRD-IR.94] to enable Video over LTE. 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 configuration parameter Media_type_restriction_policy defined in section C.3 of [PRD-IR.94] and section B.3 of [PRD-IR.51] to enable Video over EPC-integrated Wi-Fi. This will enable both “Live Video” experience and initiating a Video Call “from scratch” experience.

R12-1-5-2 For sharing any file, in order the RCS 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.1.4. A.2.1 and A.2.4 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 RCS 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 RCS Service Provider to enable RCS Geolocation Push service it shall set the PROVIDE GEOLOC PUSH parameter (see sections A.1.7 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 RCS 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 RCS Service Provider to enable Shared Sketch service it shall set the SHARED SKETCH AUTH parameter (see sections A.1.5 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 RCS Service Provider to enable Shared Map service it shall set the SHARED MAP AUTH parameter (see sections A.1.5 and A.2.1 of [RCC.07]) to 1. This will enable in-call experience.

R12-1-6 In order for the RCS 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.1.5 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 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 or video call without the need for sharing pre-call content.**

R12-2-1 All voice or video call entry points remain the same (i.e. no additional enriched calling content sharing steps are required to make a non-enriched call).

US12-3 **As a user (B-Party), I want to receive and immediately accept or reject voice or video calls when Pre-Call content is available.**

R12-3-1 The incoming call entry point remain the same (i.e. no additional enriched 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 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 be available for 1-to-1 voice calls.

R12-4-3 The sharing of Pre-call content shall be available for 1-to-1 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 or video 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.2 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 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 void

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 call before answering the call.**

R12-5-1 All content shared by the A-Party when the 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 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 **void**

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 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 calls without the user having to expand the notification.

R12-7-2 If the B-Party incoming 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 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 3.3.2.1 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 3 and sections 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 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 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 that 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 voice call is not interrupted when enabling video.**

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.

NOTE: The term 'A-Party' references the initiator of the "live video", not the initiator of the voice call (i.e. any participant of the voice call can initiate a "live video" during a call).

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 Using "live video" shall be configurable by the MNO over supported bearers (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 in a voice call sharing “live video”, when I (i.e. A / B-Party) put the call in background, I want to have the ability to view the main video streamed.**

R12-16-1 When the call is in background and sharing two ways “live video”, then video received should be displayed in a non-intrusive way (i.e. small video frame in a corner of the screen).

R12-16-2 When the call is in background and only one way “live video” is shared, then the video shared shall be displayed in a non-intrusive way (i.e. small video frame in a corner of the screen).

R12-16-3 When “live video” in background, the user shall be able to place the video window to prevent be on top of other important parts of the UI from the app in foreground.

R12-16-4 It shall be possible to easily put the video from background to foreground again. (i.e. by clicking on the video window)

US12-17 **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.**

R12-17-1 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.

US12-18 **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.**

R12-18-1 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.

R12-18-2 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.

US12-19 **As a user sharing “live video”, I want my “live video” stream to continue in case of connectivity changes.**

R12-19-1 The terminal shall support continuity of the “live video” stream in a seamless manner when network conditions allow.

R12-19-2 If the “live video” needs to be suspended due to connectivity issues, the call shall continue as a Voice Call. “live video” shall automatically resume once sufficient connectivity is available (while the call is still ongoing).

R12-19-2-1 If the “live video” cannot resume despite improved (and sufficient) connectivity, the user shall be able to manually (re-) start “live video”.

NOTE: Once the call completely dropped (either by total connectivity loss or user interaction), no automatic re-establishment of “live video” or voice call is expected.

US12-20 **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.**

R12-20-1 Both A-Party and B-Party call logs should identify that a “live video” event occurred during the call.

R12-20-2 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.

US12-21 **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).

R12-21-1 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.

R12-21-2 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.

R12-21-3 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.

R12-21-4 The support of file types and file sizes shall follow the behaviour described in requirement R7-1-5.

R12-21-5 The default resize setting for picture sharing shall be “resized / reduced” to facilitate a quick transfer experience during a call.

R12-21-6 The default resize setting for video sharing shall be “resized / reduced” to facilitate a quick transfer experience during a call.

R12-21-7 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.

R12-21-8 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).

R12-21-9 For pictures, the same format supported in File Transfer shall be supported for display in the in-call screen.

R12-21-10 While a shared file is displayed, the user shall have easy access to standard in-call features (e.g. toggle loudspeaker, mute, etc.).

R12-21-11 Any file shared during a voice call shall be easily displayed to the B-Party, with no more than one click (i.e. receiving a video --> B-Party shows in in-call screen a badge in the sharing/messaging in-call icon --> one click is needed to access the messaging conversation with the A-party with the thumbnail displayed).

R12-21-12 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.).

US12-22 **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.**

R12-22-1 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.

R12-22-2 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.

R12-22-3 Sending messages to the other participant of the call shall be possible directly from the in-call screen.

R12-22-4 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.

US12-23 **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.**

R12-23-1 Location Push shall be possible during an ongoing voice call while the call shall continue seamlessly on the same bearer.

R12-23-2 When sending Location Push to the other participant in the call, the same logic as defined in US5-22 shall apply.

R12-23-3 Selecting and sending Location Push to the other participant of the call shall be possible without ending the call.

R12-23-4 Location Push received from the other participant of the call shall be automatically accepted (based on File Transfer configuration) by the B-Party.

R12-23-5 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.

R12-23-6 An audio signal played on the recipient's side may accompany any reception of an incoming Location Push / Location Push request.

R12-23-7 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

US12-24 **As a user, I want to use In-call Services even with contacts who are not Enriched Calling enabled.**

R12-24-1 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.

R12-24-2 When sending a Location Push to the other participant of the call, the same logic as defined in US5-22 shall apply when the B-Party is not Enriched Calling enabled.

R12-24-3 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 an 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].
- 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 3.2.7 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

R12-25-1 Requirements R12-10-1 shall be implemented locally on the device.

R12-25-2 For requirement R12-10-2, section 3.1.4 of [RCC.07] shall be taken into consideration. The client shall initiate in call services while being in a one to one call.

R12-25-3 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.

R12-25-4 Requirements R12-10-4 shall be implemented locally on the device.

12.7.2.2 Live Video

R12-25-5 Requirement R12-11-1 shall be implemented locally on the device based on clarifications provided in section 12.7.1 of this document.

R12-25-6 Requirement R12-11-2 shall be implemented locally on the device.

R12-25-7 For requirement R12-11-3, in case IR.94/IR.51 conversational video is added, section 2.4 of [PRD-IR.94] shall apply.

R12-25-8 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”.

R12-25-9 For requirement R12-11-5, IR.94/IR.51 conversational video service is available under Evolved UMTS (Universal Mobile Telecommunications System) Terrestrial Radio Access Network (E-UTRAN)/EPC-integrated Wi-Fi coverage and is enabled through the configuration parameter Media_type_restriction_policy defined in section C.3 of [PRD-IR.94].

R12-25-10 For requirement R12-11-6, IR.92/IR.51 voice call termination will result to video service termination.

R12-25-11 Requirements R12-11-7 and R12-11-8 shall be implemented locally on the device.

R12-25-12 For requirement R12-12-1, section 2.2.2 of [PRD-IR.94] shall apply.

R12-25-13 Requirement R12-12-2 shall be implemented locally on the device based on the SIP INVITE response.

R12-25-14 Requirements R12-12-3, R12-12-4 and R12-12-5 shall be implemented locally on the device.

R12-25-15 Requirement R12-13-1 shall be implemented locally on the device.

R12-25-16 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.

R12-25-17 Requirements R12-15-1 and R12-15-2 shall be implemented locally on the device.

R12-25-18 Requirement R12-16-1, R12-16-2, R12-16-3 and R12-16-4 shall be implemented locally on the device

R12-25-19 For requirement R12-17-1, section 2.2.2 of [PRD-IR.94] shall apply.

R12-25-20 For requirement R12-19-1 handover procedures defined in [PRD-IR.51], [PRD-IR.92] and [PRD-IR.94] shall be taken into consideration.

R12-25-21 Requirement R12-19-2 and its sub-requirement shall be implemented locally on the device.

R12-25-22 For requirement R12-19-2-1, in case of IR.94/IR.51 conversational video service loss section 2.4 of [PRD-IR.94] shall apply.

R12-25-23 Requirement R12-20-1 shall be implemented locally on the device.

R12-25-24 Requirement R12-20-2 shall be implemented locally on the device.

12.7.2.3 Share any file during call

R12-25-25 The realisation of requirement R12-21-1 shall be implemented as defined in section 12.7.1 of this document (sharing any file during a call bullet).

R12-25-26 Requirement R12-21-2 shall be implemented as defined in section 7.3.

R12-25-27 Requirement R12-21-3 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.

R12-25-28 Requirements R12-21-4 shall follow the procedures described in section 7.3.

R12-25-29 Requirement R12-21-5 and R12-21-6 shall be implemented locally on the device.

R12-25-30 Requirement R12-21-7 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.

R12-25-31 Requirements R12-21-8, R12-21-9, R12-21-10 and R12-21-11 shall be implemented locally on the device.

12.7.2.4 Exchanging messages

R12-25-32 Requirements R12-22-1 and R12-22-2 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.

R12-25-33 Requirements R12-22-3 and R12-22-4 shall be implemented locally on the device.

12.7.2.5 Location push

R12-25-34 Requirement R12-23-1 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).

R12-25-35 For requirement R12-23-2, as per section 3.2.6 of [RCC.07] an RCS Chat Message is used to convey the location information during a voice call, but next to that during a call it shall also be supported to receive location information using CPM File Transfer to provide backward compatibility to older clients. For Geolocation Push fallback scenarios during a voice call, the procedures described in section 5.3 shall apply.

R12-25-36 Requirements R12-23-3 to R12-23-7 shall be implemented locally on the device.

12.7.2.6 Enriched Calling In-Call Sharing with Non-Enriched Calling enabled contacts

R12-25-37 Requirement R12-24-1 shall be implemented as defined in section 7.3

R12-25-38 Requirement R12-24-2 shall be implemented as defined in sections 5.3 and 7.3.

R12-25-39 Requirement R12-24-3 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

US12-26 **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.**

R12-26-1 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.

R12-26-2 The on-going voice call shall continue seamlessly on the same bearer when a live sketch sharing is in progress.

US12-27 **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.**

R12-27-1 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.

R12-27-2 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.

R12-27-3 When a participant of the call puts the call On Hold, any entry point to Interactive In-call services shall be disabled.

US12-28 **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.**

R12-28-1 It shall be made clear to the A-Party that a request has been sent but is not yet accepted (or rejected).

R12-28-2 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.

R12-28-3 The A-Party shall be notified if the request to the live sketch sharing was rejected by the B-Party.

R12-28-4 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.

US12-29 **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.**

R12-29-1 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.

R12-29-2 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.

R12-29-3 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.

US12-30 **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.**

R12-30-1 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.

R12-30-2 Both parties shall be notified if the request to a live sketch sharing times out before the B-Party has accepted (or rejected) it.

US12-31 **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.**

R12-31-1 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.

R12-31-2 B-party can accept or reject a request to a live sketch sharing from A-Party.

R12-31-3 An audio signal played on the B-Party's device may accompany the incoming request to a live sketch sharing.

US12-32 **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.**

R12-32-1 The B-Party shall be able to accept the live sketch sharing directly from the live sketch sharing request.

R12-32-2 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.

US12-33 **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.**

R12-33-1 The B-Party shall be able to decline the request to the live sketch sharing.

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 edit the sketch.**

R12-34-1 During a live sketch sharing, both parties shall be able to edit the sketch, and view any edits they have made in real time.

R12-34-2 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.

R12-34-3 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.).

US12-35 **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.**

R12-35-1 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.

R12-35-2 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.

US12-36 **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.

R12-36-1 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).

US12-37 **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.**

R12-37-1 Either party shall be able to end the live sketch sharing at any time.

R12-37-2 Either party shall be able to end the live sketch sharing directly from their live sketch screen.

R12-37-3 Either party may be able to end the live sketch sharing directly from their in-call screen.

R12-37-4 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.

US12-38 **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.**

R12-38-1 Both parties shall be made aware when the live sketch sharing has ended.

US12-39 **As a user engaged in a shared sketch, I want the final sketch to be saved on my device.**

R12-39-1 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

US12-40 **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.**

R12-40-1 An entry point for a live sketch on an image should be provided on the in-call screen.

US12-41 **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.**

R12-41-1 Either party shall be able to change the live sketch background image and/or colour at any time during the live sketch.

R12-41-2 Any change to the live sketch background shall be shown in real-time on both parties' devices.

R12-41-3 Either party shall be able to select an existing image from the device gallery as the live sketch background.

R12-41-4 Either party shall be able to take a new picture from the device camera to use as the live sketch background.

R12-41-5 Either party should be able to select a live sketch background from a selection of pre-defined template backgrounds.

US12-42 **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.**

R12-42-1 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.

R12-42-2 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 not visible to the other party.

US12-43 **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.**

R12-43-1 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).

R12-43-2 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

US12-44 **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.**

R12-44-1 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).

R12-44-2 The A-Party's current location should be set as the default location for any new live sketch on a map for both parties.

US12-45 **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.**

R12-45-1 Both parties shall be able to change the scale of the map, independent of the map being viewed by the other party.

R12-45-2 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.

US12-46 **As a user (A-Party and B-Party) in an on-going voice call with an ongoing live sketch on a map, I want to know if the other party has made any edits that I cannot currently see on my map view.**

R12-46-1 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.

R12-46-2 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.

US12-47 **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.**

R12-47-1 Both parties should be able to see each other's locations on the map

R12-47-2 Both parties should be able to easily move the map to their location at any time.

R12-47-3 Both parties should be able to easily move the map to the other party location at any time.

R12-47-4 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.

R12-47-5 Both parties should be able to send a location marker to the other party, with this marker being visible on both parties' sketches.

R12-47-6 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

R12-48-1 Requirements R12-26-1, R12-27-1, R12-27-2, R12-28-2, R12-28-3, R12-28-4, R12-29-1, R12-29-2, R12-31-2, R12-32-2, R12-33-1, R12-34-1, R12-34-2 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.

R12-48-2 Requirements R12-26-2, R12-27-3, R12-28-1, R12-29-3, R12-30-1, R12-30-2, R12-31-1, R12-31-3, R12-32-1, R12-34-3, R12-35-1, R12-35-2, R12-36-1, R12-37-1 to R12-37-4, R12-38-1, R12-39-1 shall be implemented locally on the device.

12.9.3 Specific Shared Image Sketch Requirements

R12-48-3 Requirements R12-40-1 and R12-41-1 shall be implemented locally on the device.

R12-48-4 Requirement R12-41-2 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.

R12-48-5 Requirements R12-41-3, R12-41-4, R12-41-5 shall be implemented locally on the device.

R12-48-6 Requirements R12-42-1, R12-42-2, R12-43-1 and R12-43-2 shall be implemented locally on the device.

12.9.4 Specific Shared Map Sketch Requirements

R12-48-7 Requirements R12-44-2, R12-46-1, R12-46-2, R12-47-1 and R12-47-5 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.

R12-48-8 Requirements R12-44-1, R12-45-1, R12-45-2, R12-47-2, R12-47-3, R12-47-4 and R12-47-6 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.

US12-49 **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).

R12-49-1 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.

R12-49-2 Pre-defined Post-call Notes should be available for the user.

R12-49-3 The Pre-call Subject shall be presented as default Post-call Note.

R12-49-4 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.

R12-49-5 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.

US12-50 **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.**

R12-50-1 Post-call Notes or Voice Messages shall update the existing standard missed call indication on the B-Party's device.

R12-50-2 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.

R12-50-3 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.

R12-50-4 The B-Party shall be able to read the Post-call Note from the associated indication, either directly or by expanding the indication.

R12-50-5 The B-Party shall be able to play the Post-call Voice Message from the associated indication, either directly or by expanding the indication.

R12-50-6 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

US12-51 **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.**

R12-51-1 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

R12-52-1 Requirement R12-49-1 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].

R12-52-2 Requirements R12-49-2, R12-49-3 and R12-49-4 shall be implemented locally on the device.

R12-52-3 Requirement R12-49-5 shall be implemented as described in section 2.5.7 of [RCC.20].

R12-52-4 Requirements R12-50-1 to R12-50-6 shall be implemented locally on the device.

12.11.3 Enriched Calling Post-Call experience with Non-Enriched Calling enabled contacts

R12-52-5 Requirement R12-51-1 shall be implemented as described in section 2.5.7 of [RCC.20].

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.

US12-53 **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.**

R12-53-1 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

R12-53-2 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.

R12-53-3 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.

R12-53-4 Post-call enriched content shared with B-Party shall be notified to B-Party as a new 1-to-1 message.

R12-53-5 Pre-call and In-call enriched content shared with a B-Party shall not be notified to the B-Party as a new message, (if added to the messaging thread). The content shall be there but automatically flagged as "read" on the B-Party's device.

R12-53-6 The message thread shall identify content received from the B-party using Enriched Calling features as call content (in contrast to messaging content).

R12-53-7 Any Enriched Calling content shall be stored in the B-Party's message thread only if the associated content was presented on the device.

US12-54 **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.**

R12-54-1 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

R12-54-2 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

R12-54-3 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.

R12-54-4 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.

US12-55 **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.**

R12-55-1 Specific files shared or exchanged with a contact shall be available to both parties in a contact centric view (e.g. a gallery view).

R12-55-2 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	Shall(1)	Shall	Shall
In- Call	**Files**	Shall(1)	Shall	Shall
	Location	Shall(1)	Shall	
	Notes	Shall(1)	Shall	
	Sketches	Shall(1)	Shall	Shall
Post- Call	**Note**	Shall	Shall	
	Voice note	Shall	Shall	
Messaging	**Messages**		Shall	
	Files		Shall	Shall
	Location		Shall	

Table 18: 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

R12-56-1 Enriched content in Logs and media contact centric view shall be implemented locally on the device.

R12-56-2 For the Post-Call cases described in R12-49-5, the receiving client will not be able to distinguish whether the sender sent a Post-Call note or message and therefore the event will not be included in the call log.

R12-56-3 Additionally, the receiving client will not be able to distinguish whether the sender sent a Post-Call audio or file transfer audio message and therefore the event will not be included in the call log.

13 rcsVVM Service

void

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.

Network APIs can provide operators the ability to monetise xMS and RCS services. For example, Chatbots as defined in section 15 could use a Network APIs to deliver the service.

When Terminal or Network APIs are made available, implementations will offer the full range of messaging APIs (i.e. both SMS and RCS) so that the case when a developer has access to SMS APIs but not RCS APIs (and vice versa) is avoided.

NOTE: In this document “developer” means either OEM application developer, MNO application developer or third party developer

14.2 User Stories and Feature Requirements

US14-1 **As an MNO, I want to open up my RCS infrastructure to developers and third parties so that their applications can be enriched with these RCS 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.

R14-1-1 *APIs (either Terminal API or Network API) 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*

R14-1-1-4 *Geo-location,*

R14-1-1-5 *Audio Messaging,*

R14-1-1-6 *Enriched calling Pre-Call, Post Call and Interactive in-call services.*

R14-1-1-7 *All event types described in section 15.*

R14-1-1-8 *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, etc.).*

14.3 User Stories and Feature Requirements of Terminal API

US14-2 **As a user, I want to be able to use new applications (application installed on the devices or Chatbots) enriched with RCS services and enhanced with new innovative features.** *All the device or native RCS implementations (which support UP 2.0) shall provide APIs to expose the services listed above to third parties.*

R14-2-2 *When a user installs an application that uses Terminal APIs, the user shall be informed that the application will have access to his RCS services and features.*

R14-2-3 *Any application with access to the RCS services listed in R14-1-1-1 to R14-1-1-6 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.*

R14-2-4 *The device's RCS database containing the user's messages and RCS content shall be made available to third parties (already provided for SMS today).*

R14-2-5 *The device's call log information about the user's calls (including enriched call content associated with the calls where applicable) shall be made available to third parties (already provided for call logs today).*

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 Terminal APIs shall follow a permission verification process when it is installed on a device.*

R14-3-2 *During installation of an application that uses Terminal 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, I want to choose the default messaging client and default dialler that I prefer without my other messaging / dialler services suffering as a result.**

R14-4-1 *It shall be possible for a messaging app using Terminal APIs to operate as a default messaging client and to co-exist with a fully functioning native or embedded default dialler.*

R14-4-2 *It shall be possible for a dialler app using Terminal APIs to operate as a default dialler and to co-exist with a fully functioning native or embedded default messaging client.*

R14-4-3 *It shall be possible for an app using Terminal APIs to operate as both the default messaging client and default dialler.*

US14-5 **As a developer, I want my application to be able to send an Operator Message to a contact (with at least one MSISDN) without caring which messaging service is used (RCS or SMS) to transport the message.**

R14-5-1 *A generic Operator Message API shall be made available. When an application triggers the sending of an Operator Message in this way, either an RCS or SMS message is triggered for sending, depending on the capability and availability of the receiving user.*

R14-5-2 *Depending on operator configuration, the rules of Seamless or Integrated Messaging shall apply.*

US14-6 **As a developer, I want my application to be aware of the existence and RCS state of the SIMs currently in the device.**

R14-6-1 *Application(s) shall be able to identify which RCS identity is in use by the device at any time.*

R14-6-2 *Subscribing applications shall be notified by the device when the identity of the SIM that is active for RCS changes.*

R14-6-3 *Upon user approval, applications shall be able to assign the identity to be used for the RCS services on the device.*

14.4 User Stories and Feature Requirements of Network API

US14-7 **As an MNO, I want to be able to provide third parties with communication services as enablers.**

R14-7-1 *The MNO shall be able to offer APIs for RCS service features listed in R14-1-1 and further via network APIs.*

15 Messaging as a Platform: Chatbots and Plugins

15.1 Introduction

Offering RCS as a delivery channel for businesses to communicate with their staff, existing and potential customer base and M2M or IOT applications presents a huge opportunity to extend existing A2P (Application to Person) monetisation of operator messaging and add new revenue streams for mobile operators, Aggregators, application providers, Chatbot Platforms and businesses alike.

Messaging as a Platform (“MaaP”) will enable a variety of interactive services that can be categorised in different ways. A2P messaging is already available to businesses (using SMS) and represents a lucrative business for mobile operators and third party aggregators.

A major aspect in the evolution of Messaging as a Platform concerns providing an enhanced user experience and therefore business opportunity for the interaction between Businesses and their (potential) customers. Therefore, the present version of the Universal Profile focusses on two areas, Chatbots and Plugins, to describe requirements for such an enhanced interaction. These two areas describe the main ways innovation can be made available in the messaging client to support the exciting new types of services that customers want to use. The differentiation is important; the ’Chatbots‘ section covers

standards-compliant interactions between users and Chatbot or service-based conversation partners (i.e. A2P use cases) while the 'Plugins' section covers the enhancement of a Person to Person (P2P) and / or A2P conversation with new elements that go beyond the specified feature scope of the Universal Profile.

NOTE: In the wider technology industry the term 'Chatbot' is referred to a conversational entity as such while in this document the use of the term Chatbot specifically refers to a conversational entity interacted with via RCS-based services. xMS services might be supported by a Chatbot but these use cases are not in scope of this document.

Overview of major functional changes in this section compared to Universal Profile 2.0:

- Introduction of "Critical Chatbots" which cannot be removed or blocked by the user.
- Principle of one conversation with a Chatbot or Application using RCS or SMS messages.
- User information if a Chatbot or Application is (temporarily) unavailable.
- Refinement of anonymization
- Chatbot identity verification
- Incorporation of Static Rich Card definition into section 15.2.
- Introduction of finding a Chatbot in a directory.
- Deep Links to open a conversation with a Chatbot.
- Refined concept of "Report Spam"
- Chatbot capability to remove a message from the terminating Store & Forward server.

15.2 Chatbots

This section focusses on RCS-enabled Chatbots and sets the requirements that enable a frictionless journey for end-users. Chatbots that are not RCS enabled are out of scope.

US15-1 **As a user, I want to use secure and easy-to-use Chatbots that provide value-added services.**

R15-1-1 Users shall have the ability for a richer communication with Businesses (including 3rd parties and MNOs) through Chatbots beyond just plain voice calls and SMS/MMS.

R15-1-1-1 Users shall not be able to block "Critical Chatbots" which are verified by special MNO endorsement.

R15-1-2 Chatbots shall be identified by a Service ID which is globally unique across MNOs, RCS Service Providers and Chatbot Platforms.

R15-1-3 The namespace of these Service IDs shall be expandable to accommodate a potential growth of Chatbots and Chatbot platforms.

R15-1-4 Chatbots define and manage their Chatbot Profile Information accessible from within the messaging conversation view with that Chatbot. The Chatbot Profile Information shall consist of following elements:

R15-1-4-1 an alphanumeric Service Name that identifies the Chatbot in the list of conversations and within a conversation (mandatory).

R15-1-4-2 a non-animated thumbnail picture as Service Icon that identifies the Chatbot in the list of conversations and within a conversation (optional);

R15-1-4-3 an alphanumeric Service Description up to 500 characters to explain the purpose of the Chatbot (optional);

R15-1-4-4 a Call-back Phone Number e.g. for customer services(optional);

R15-1-4-5 a Theme Colour applied in the conversation view of the user with the Chatbot (e.g. colour for message bubbles and conversation header) (optional);

NOTE: Future specification are expected to include a more extended support of colour schemes.

R15-1-4-6 a Service Website (e.g. to provide user information and customer services detail) (optional);

R15-1-4-7 a link to Chatbot-specific Terms & Conditions (mandatory);

R15-1-4-8 a Service Email Address (e.g. for customer services) (optional).

R15-1-4-9 an SMS (long or short code) number (may or may not be filled by the Chatbot);

R15-1-4-10 a Background image applied in the Chatbot information page (optional).

NOTE: When both Theme Colour and Background Image are available or none of them is available, it is up to the device to decide how to handle it

R15-1-4-11 a Chatbot provider's name which is different from the Service Name (optional).

R15-1-4-12 an Address (e.g. for business location) (optional)

R15-1-4-13 a Category which can be used to filter the Chatbot list (optional)

R15-1-5 The Chatbot Profile Information shall be made accessible from within the messaging implementation.

R15-1-6 Updates to the Chatbot Profile Information by the Chatbot Provider shall become visible when the user opens the conversation with the Chatbot (or shortly after).

R15-1-7 *The user may be able to store the Chatbot Profile Information such as Service Name, the Service Icon and the Call-back Phone Number etc. in any available contacts application on their device.*

R15-1-7-1 *Storing and updating of Chatbot Profile Information in a contacts application may take place on user demand or automatically.*

R15-1-7-2 *A contacts application may limit editing of Chatbot Profile Information.*

R15-1-7-3 *Any user edits to Chatbot Profile Information within the contacts application shall not be reflected in the messaging implementation (i.e. the messaging*

implementation shall always reflect the current, up to date Chatbot Profile Information).

NOTE: Synchronisation of the Chatbot Profile Information with any potentially available cloud message store is not mandatory.

R15-1-8 Conversations with Chatbots shall be visually differentiated to the users from conversations with (personal) contacts.

R15-1-9 MNOs shall be able to manage Critical Chatbots for their subscribers.

R15-1-9-1 There shall be a specific verification indicator only used for Critical Chatbots that helps the user to understand that a Critical Chatbot cannot be blocked.

NOTE: This information is neither defined nor managed by the Chatbot itself

NOTE: It is expected that Critical Chatbots are always Verified Chatbots.

R15-1-10 If a Chatbot is temporarily unavailable, and the user attempts to contact that Chatbot, the user should be informed appropriately.

R15-1-10-1 There shall be technical means provided that prevent the message to be identified as spoofing (as the originator of the message indicated to the user is the Chatbot, but it comes from somewhere else).

R15-1-10-2 The message content shall be defined by each Chatbot individually for their users during onboarding procedures or later.

R15-1-11 If the Chatbot restricts its availability to customers of a given MNO, users to which the Chatbot is not available shall be notified with a message that is defined by their MNO whenever they try to access this Chatbot, e.g., but not limited to, after scanning a QR code with a deep link.

US15-2 **As a user, I want to use only secure Chatbot services that respect my data privacy needs.**

Anonymization Service Configuration and generic requirements

R15-2-1 The RCS Service Provider shall be able to configure the availability of the anonymization feature for their subscribers. If the RCS Service Provider decides to offer anonymization, by default, conversations with Chatbots are in ‘anonymous mode’ (i.e. the user’s MSISDN is not used as an identifier towards the Chatbot but instead the user is identified by a unique and anonymous ‘token’).

R15-2-1-1 The anonymization shall be performed either by the RCS Service Provider or by the Chatbot Platform, depending on commercial setup between the two.

R15-2-1-2 The ‘token’ shall be unique per Chatbot for any given conversation and not be re-used to represent that same user towards other Chatbots.

R15-2-1-3 No tokenizing shall be required when the user has agreed to share their MSISDN with the Chatbot ('public mode').

NOTE: In ‘anonymous mode’, the first message has to be sent by the user to the Chatbot (P2A, Person to Application). It is not possible to start a communication in anonymous mode with the Chatbot sending the very first anonymous message (A2P).

User Control of anonymization mode

R15-2-2 The user shall be able to control the sharing of the user’s identity (MSISDN) via explicit consent on a per Chatbot basis:

R15-2-2-1 The user shall be able to decide whether to share their MSISDN as the identifier for the communication with a Chatbot (‘public mode’) or an anonymous user identity (‘anonymous mode’). Either the anonymized token or the MSISDN is shared as an identifier for that user in their communication with a Chatbot.

R15-2-2-2 The UI implementation shall inform the user whether they are in ‘anonymous mode’ or in ‘public mode’ for the current communication with the Chatbot in each conversation.

Conversations in anonymous mode

R15-2-3 If the conversation between a user and any given Chatbot is in ‘anonymous mode’, then all messages sent by the user to the Chatbot shall not use the user’s MSISDN but the anonymous token to identify the user towards that Chatbot.

R15-2-3-1 The UI implementation shall inform the user that they are not sharing their MSISDN within the conversation view.

R15-2-3-2 The Chatbot shall be able to send messages to the user’s token, and the user shall be able to send messages to the Chatbot in which the token is used to represent the user towards the Chatbot.

R15-2-3-3 While in anonymous mode, Network Fallback to SMS (NFS) shall never be used.

R15-2-3-4 Re-send messages as SMS from the Chatbot to the user shall not be possible in ‘anonymous mode’.

R15-2-3-5 A user shall not be able to send SMS messages to the Chatbot while the communication is in anonymous mode, as anonymization for SMS is not available.

R15-2-3-5-1 The UI shall avoid (unintentional) sending of SMS messages from the user to the Chatbot.

R15-2-3-6 Message Status Notifications shall be shared with the Chatbot or MaaP Application as specified in section 5. In this case, the token shall be used as the identifier of the user towards the Chatbot.

R15-2-4 If the communication with a selected Chatbot is in 'anonymous mode', then the user shall have the option to reset the anonymous token on manual selection (similar to a “delete cookies” in the Internet ecosystem)

R15-2-4-1 The Chatbot shall not be able to identify that user or associate that user with any previous user activity, preferences or behaviour from the time before changing the anonymous user token.

R15-2-4-2 Potential messages from the Chatbot to the previous anonymized token shall not be delivered to the user and the Chatbot shall be informed about this (an 'unknown user error' message).

R15-2-4-3 When the user selects to reset the token, they shall have to confirm that selection of any previously received suggested actions and replies may no longer work as expected and potential leakage of privacy relevant user details.

NOTE: The expected Chatbot behaviour after a change of the anonymous user token is identical to the Chatbot behaviour when a new user starts a conversation with that Chatbot, including, but not limited to, any welcome messages or acceptance of terms and conditions.

Conversations in public mode

R15-2-5 If any given Chatbot conversation is in 'public mode', then the user's MSISDN shall be used as the identifier for that user towards the Chatbot

R15-2-5-1 The UI implementation shall inform the user that they are sharing their MSISDN within the conversation.

R15-2-5-2 Message Status Notifications shall be shared with the Chatbot or MaaP application as specified in section 5.

R15-2-5-3 Suggested actions, suggested chips and suggested replies shall be visible and selectable.

R15-2-5-4 *The Chatbot shall be able to configure outbound messages from the Chatbot to the user to allow NFS on a per message basis.*

R15-2-5-5 Messages sent and received from the Chatbot using the defined (long or short code) SMS number in R15-1-4-9 shall be displayed within the same conversation as messages exchanged with the Chatbot's Service ID.

R15-2-5-6 When using xMS as the messaging service to send messages from the user to a Chatbot, the communication shall be in public mode.

Transition from 'anonymous mode' to 'public mode'

R15-2-6 When the user selects to change from 'anonymous mode' to 'public mode', then the user shall be made aware that their MSISDN is shared from now on with the Chatbot.

R15-2-7 When a user leaves the 'anonymous mode', then the user's MSISDN shall be used to represent the user in that conversation.

R15-2-8 In any case, the user shall be informed appropriately and shall be requested to provide their explicit consent to share their MSISDN. If not agreed by the user, the conversation shall stay in anonymous mode.

R15-2-8-1 In some cases, it might be required by the Chatbot logic that the user needs to be known by their MSISDN. In that case, the user shall be able to link their MSISDN to the conversation history.

R15-2-8-1-1 If the last known anonymous identity is linked to the MSISDN, the user shall be appropriately informed and provide their explicit consent to link the conversation history (under the last 'token' that was used) with their MSISDN. If not agreed by the user, the history of the Chatbot conversation is not linked to the user's MSISDN.

R15-2-8-1-2 In order to fulfil local regulation, the information that explains to the user the impact of linking their MSISDN with their previous conversation shall be provided by the operator configuration.

R15-2-8-1-3 If the last known anonymous identity is linked to the MSISDN, then the anonymous identity shall be invalidated.

R15-2-9 The validity of any suggested actions, suggested replies or suggested chips from messages previously received in anonymous mode shall be up to the UI implementation; (see section "Representation of 'anonymous mode' and 'public mode' on UI level).

- Implementations using the single threaded view may grey out these suggested actions, replies or chips (not selectable).
- Implementations using the two-threaded view may want to keep these suggested actions, replies or chips active and selectable.

Transition from 'public mode' to 'anonymous mode'

R15-2-10 When a user changes a conversation with a Chatbot from 'public mode' to 'anonymous mode', then a 'token' shall be used to represent the user in all further messages or RCS events sent towards this Chatbot (until the user decides to share their MSISDN again). It shall not be possible for the third party (e.g. Chatbot) to derive the MSISDN from the token.

R15-2-10-1 The Chatbot shall consider the anonymous conversation as a new conversation without any link to the content of the previous conversation in public mode.

R15-2-10-2 The behaviour of any suggested actions, replies or chips from the previous conversation shall be defined by the UI implementation.

- Implementations using the single threaded view may grey out these suggested actions, replies or chips (not selectable).
- Implementations using the two-threaded view may want to keep these suggested actions, replies or chips active and selectable.

Control of sharing user data

R15-2-11 The user shall be able to control the sharing of the user's privacy relevant information as detailed below on a per Chatbot conversation basis:.

R15-2-11-1 Device Status (that includes device model, operating system version, messaging client identifier and version, and remaining battery charge in minutes). The user needs to agree for any one-time share.

R15-2-11-2 The user's location information. The user needs to agree for any one-time share.

R15-2-11-3 The sending of "Displayed" notifications for received messages from any given Chatbot conversation. At any point in time, either 'Displayed' Message Status Notifications are provided or not; (see US18-17 and subsequent requirements R18-17-5-3).

R15-2-11-3-1 To make changes on this setting, the user shall be guided to the setting for this Chatbot to allow sharing of the requested information with this Chatbot.

R15-2-11-3-2 The user shall be able to easily return to the conversation irrespectively of whether the privacy setting has been changed or not.

R15-2-11-4 If the user has restricted sharing of information (as described in R15-2-11 and subsequent requirements R15-2-11-1 to R15-2-11-3-2), but this information is essentially needed to perform a suggested or requested action / function, the Chatbot shall have the opportunity to ask the user to make a specific personal information available.

R15-2-11-4-1 For features delivered by a one-time information sending from the messaging application to the Chatbot (as described in R15-2-11-1 and R15-2-11-2), the user shall have the option to select sharing of that information by selection of a (by the Chatbot) suggested action or reply or by selection of the function from the device menu (if provided).

R15-2-12 At any point in time, the user shall be able to modify the sharing of each item of their personal data with permanent relevance on a per Chatbot conversation basis.

R15-2-12-1 The UI shall avoid the situation where preferences with permanent relevance are configured once and "hidden away" in obscure, easy to forget settings or 'Terms and Conditions' pages.

Anonymization in a Multi Device Setup

R15-2-13 If the user uses multiple devices (as described in section 9), then all messages and RCS events the user has exchanged with any given Chatbot shall appear on the primary and any secondary device.

R15-2-14 The user manages each device separately for sharing the MSISDN or anonymization. This means no alignment of this setting across devices is required.

Representation of 'anonymous mode' and 'public mode' on UI level

R15-2-15 It shall be up to the UI implementation to make the use of 'anonymous mode' and 'public mode' easy and straightforward for the user. This includes the

representation of the two modes in one combined conversation thread or two separated conversation threads with any given Chatbot.

R15-2-15-1 If an implementation uses one conversation thread for communication with any given Chatbot, then:

R15-2-15-1-1 The communication of the user with the Chatbot shall be set either to ‘anonymous mode’ or to ‘public mode’.

R15-2-15-1-2 If the conversation is currently in anonymous mode, and the Chatbot or MaaP Application sends a message to that user directed to their MSISDN, then

- the message shall be received within the conversation, and
- any suggested actions, suggested replies or suggested chips shall be displayed but cannot be selected (Suggested actions and / or replies shall be greyed out as they are not selectable), and
- Message Status Notifications shall be reported back to the Chatbot or MaaP Application, and
- the user shall be informed that if they want to answer to that message they should deactivate the ‘anonymous mode’ and share their MSISDN for privacy reasons.

R15-2-15-2 If an implementation uses two conversational threads to represent the communication between the Chatbot and the user, then

R15-2-15-2-1 one conversation thread for anonymous mode and one conversation thread for public mode shall be used (the UI may differentiate between the two conversation threads using tabs).

R15-2-15-2-2 the user may “switch between the two modes” implicitly by selection of the conversation.

R15-2-15-2-3 a given conversation thread shall only be in one mode - either anonymous or public, not both.

R15-2-15-2-4 two conversation threads with a Chatbot shall only be shown if the user has one anonymous conversation and one public conversation with that Chatbot.

R15-2-15-2-5 it shall be obvious for the user to be aware at any time in which conversation they are at any given point in time.

R15-2-15-2-6 changing from one mode to the other shall be performed by switching the conversation threads.

Chatbot identity verification

R15-2-16 It shall be possible to ensure users about the real identity of Chatbots, to avoid Chatbots spoofing an identity that they are not (e.g. by using a popular brand name or icon associated with a party they are not).

R15-2-16-1 It shall be possible for the user to communicate to a selection of verified and unverified Chatbots at any time.

NOTE: It is assumed that there is a high motivation for Chatbots to approach Verification Authorities to be verified.

R15-2-16-2 Chatbots with a valid Verification for subscribers of any given MNO shall be visually distinguished from unverified Chatbots so users can be certain whether they can trust that they are chatting with the party they intend.

R15-2-16-2-1 This visual differentiation shall be intuitive for the user and in a prominent position.

R15-2-16-2-2 The visual differentiation shall be visible at least in the following places:

- Chatbot directory or catalogue offered by MNOs

NOTE: there maybe 3rd parties not using the visual differentiation outside the circle of influence of this specification.

- List of conversations in the messaging application.
- Open conversation with a Chatbot.
- UI that displays the Chatbot's Profile Information

R15-2-16-2-3 On request (e.g. by clicking the visual identifier), the user may be able to see the Verification Authority that has verified the Chatbot.

R15-2-16-2-4 The Chatbot Verification shall ensure that the party in control of the Chatbot is eligible to use the chosen brand icon, Chatbot Service Name and Chatbot Service ID.

R15-2-16-2-5 Any change of the Chatbot brand icon, the Chatbot service name and the Chatbot Service ID shall require a renewal of the verification. Changes in other areas of the Chatbot Information shall not require renewal of the verification.

R15-2-16-2-6 The verification status shall have a validity period and shall have to be renewed after expiry if representation of the trust mark is still required.

R15-2-16-2-7 A user shall see a Chatbot as verified if at least one valid verification is available for that Chatbot. A verification shall be invalid for subscribers of a given MNO if:

- The validity of the verification of the Chatbot has expired.
- The Verification Authority that has verified the Chatbot is not accepted by that MNO.
- The verified content in the Chatbot info has been altered after verification.

- The verification mechanism appears to be corrupted or manipulated.

NOTE: The Verified Chatbot status of a Chatbot does not imply anything about the validity of any of the content that the Chatbot may send.

R15-2-16-3 The user shall be made aware by non-intrusive UI information whenever the Chatbot Profile Information of any given Chatbot has no valid verification for the subscribers of any given MNO.

NOTE: It is expected that the list of MNO trusted verification authorities does not frequently change (after a ramp-up period).

R15-2-16-3-1 Any update of the verification status in the Chatbot directory or search and the list of Chat conversations may not be visible before the Chatbot Information on the device has been updated.

R15-2-16-3-2 Updates on the Verification Status of a Chatbot, reflected by the trust mark, shall be performed when retrieving the Chatbot Information.

R15-2-16-3-3 A delay between removing the verified status by the operator and all clients no longer showing the trust mark is acceptable. If, for removal processes, timers are involved, then these timers shall be configurable by the RCS Service Provider.

NOTE: It is agreed to be acceptable that the removal of the trust mark is limited to screen refresh, i.e. if the client displays a UI with the trust mark on and the user does not interact with the UI, then the trust mark may be up on display for longer than the configured period.

NOTE: The requirements as described in R15-5-4 to R15-5-7 (blocking of selected Chatbots or Chatbot Platforms in cases of Spam) are applicable for situations of doubtful verifications as well.

NOTE: It will be very easy and straightforward for Chatbots to find a Verification Authority and go through the process of Chatbot Profile Information verification.

R15-2-16-4 It shall be possible that Chatbots are verified by multiple Verification Authorities.

R15-2-16-4-1 It shall be up to the MNO to specify a set of Verification Authorities to whom the MNO grants the authority to verify Chatbots for the MNO's subscribers.

R15-2-16-5 Critical Chatbots shall represent a specific verification indicator only used for Critical Chatbots that helps the user to understand that a Critical Chatbot cannot be blocked.

Recurring Payments

R15-2-17 *The user shall be able to see inside the Chat application the recurring payments that have been subscribed to with an option to cancel.*

US15-3 ***As a user, I want to be sure that a message I received from a Chatbot came from that Chatbot.***

R15-3-1 *Chatbot messages shall always be ensured to come from that Chatbot.*

R15-3-2 *Chatbot Messages that cannot be ensured to come from the declared source shall not be presented to the user.*

US15-4 **As a user, I want to discover and connect with a variety of relevant Chatbots that will help me complete tasks more efficiently than ever before, do more from my messaging application, and/or enrich my messaging conversations with others.**

R15-4-1 A Chatbot shall be able to limit its own discoverability and availability to specific operator network(s), language(s) and / or countries.

R15-4-2 A Chatbot Platform shall be able to limit the discoverability of its Chatbots towards users of specific operator network(s), language(s) and/or countries.

R15-4-3 The user shall be able to enhance the Chatbot search service by disclosing additional information during their search.

R15-4-3-1 The user shall have the option to enrich the search by disclosing additional information:

- preferred language(s) (default is the language the device is set to (e.g. for display of features and menus), the user shall be able to edit or add other languages they prefer for Chatbot search)
- current location of the device.

R15-4-3-2 If allowed by the user and RCS Service Provider, every search of the user shall be enriched by adding the MSISDN.

NOTE: If the RCS Service Provider has not enabled sharing the MSISDN, this enrichment is not available.

R15-4-4 All Chatbot Platforms shall maintain a published list of their available Chatbots that can be retrieved, parsed and displayed with their meta-data by any Chatbot discovery method.

R15-4-5 Messaging implementations shall support a Chatbot search for discovery of Chatbots.

R15-4-6 *The service shall allow an RCS Service Provider to configure the Chatbot Search Engine during the first-time provisioning or client re-provisioning for RCS.*

NOTE: Chatbot Search Engine specifics like parameters for ranking the results or consideration of user ratings, etc. are left to the implementation of the Chatbot Search Engine.

R15-4-7 The service shall allow RCS Service Providers to set an address of a managed Chatbot Directory that can offer access to selected Chatbots for their users.

R15-4-8 A Chatbot search shall be able to search based on Chatbot identifier (i.e. Service ID) and/or any of the Chatbot profile information listed in section US15-1.

R15-4-9 Chatbot search results or directory entries shall display at a minimum for each Chatbot found, the Chatbot identifier (Service ID), the service name and the service logo (if available).

R15-4-10 The user shall be able to initiate a conversation with a Chatbot from the results of any Chatbot search or from a list of Chatbots present in a directory by selecting the chosen Chatbot.

NOTE: All requirements for users starting a new conversation with a Chatbot apply.

R15-4-11 A Chatbot conversation shall be able to be invoked from (a) a link from a webpage displayed on a mobile browser, or (b) an application that is not the (native or downloaded) RCS enabled messaging application of the mobile device.

R15-4-11-1 If the user invokes a Chatbot from a deep link and the user already has an existing conversation with this Chatbot, then the ongoing conversation shall be opened within the currently active Operator Messaging application and the latest messages exchanged shall be displayed. Otherwise, if there is no existing conversation with that Chatbot on the user's device, then a new conversation shall be created and opened within the currently active RCS application.

R15-4-11-2 The webpage or mobile application from which the Chatbot is invoked shall be able to specify a suggested chip list consisting of suggested replies and actions. The website or application from which the Chatbot is invoked shall be able to supply context information to the resulting conversation whenever the user has selected one of the offered chips. When the conversation is opened within the currently active Operator Messaging application, this suggested chip list will be displayed without further user interaction.

NOTE: The ability to specify a suggested chip list along with Chatbot invocation allows the webpage or mobile application to provide the user with shortcuts for starting the conversation given the context of the invocation UI. For instance, if a user were looking at red shoes in a website, "Search for red shoes" can be a suggested reply included in the Chatbot conversation that is invoked. Additionally, these suggested replies and actions can carry invisible context from the invocation surface to the Chatbot via their corresponding postback data.

R15-4-11-3 The website or mobile application shall be able to specify an alternative communication mechanism if the link was not selected on a UP 2.2 (or higher) capable client. The user's Operator Messaging app may open an xMS conversation with the Chatbot if SMS integration has been implemented on the mobile network of the user.

R15-4-11-4 If a deep link is invoked from a device that is neither RCS nor SMS capable, the user may see an error message or a user-friendly message.

R15-4-12 It shall be possible for a Chatbot invocation link that could be displayed on a webpage to be embedded in a QR code, such that the Chatbot is invoked (with the same requirements as in R15-4-11) when the QR code is scanned and the link is opened.

R15-4-13 It shall be possible to start an RCS conversation by entering a unique Chatbot identifier in the 'to' field of the chat composer. Supported formats for the 'to' field shall be, but not limited to,:

- phone number (long or short format)
- email address format
- Service ID

R15-4-13-1 If the user enters anything else, a search function may be used to identify available Chatbots matching the user input.

R15-4-14 Any entry point for the Chatbot conversation shall be able to display two parameters. The parameters are text label and data which define a Suggested Reply (see R15-8-4-5) displayed to the user in the conversation with that Chatbot.

R15-4-15 When the user starts a new Chatbot conversation, the messaging implementation shall display a Chatbot-specific Introduction Screen.

R15-4-15-1 *The Introduction Screen may contain elements from the current Chatbot Profile Information.*

R15-4-15-2 The Introduction Screen shall contain a button which when being tapped by the user triggers the sending of the first message from the user to the Chatbot.

R15-4-15-3 *The Chatbot Introduction Screen shall be allowed to contain a list of suggested replies / suggested actions (max number of chips as defined in the standard chip list), e.g. for services that the Chatbot offers*

R15-4-16 In case the user wants to open a conversation with a Chatbot that is not available to the user, then the user shall be informed accordingly.

R15-4-17 A Chatbot shall be able to initiate conversations with mobile users directly, provided that the user has authorised the Chatbot to do so and the Chatbot is authorised to communicate with that specific user, e.g. via any 'offline channels' between businesses and customers they have a relationship with.

R15-4-18 *Users shall be able to share feedback on Chatbots to provide an overall rating of the Chatbot that indicates the quality of the Chatbot to other potential users.*

R15-4-19 *The user-provided feedback and aggregated rating shall be stored with the Chatbot Platform and published with the meta-data about available Chatbots.*

R15-4-20 *It shall be possible to make user rating information available to Chatbot Directories and Search features (e.g. to influence the finding algorithm and listing position).*

US15-5 **As a user, I want to avoid spam.**

R15-5-1 A user shall only receive messages from authorized Chatbots (i.e. Chatbots that have the user's consent to contact the user based on their MSISDN or have been contacted by the user in the first place).

R15-5-2 A user shall be able to block/unblock individual Chatbots locally on the device.

R15-5-2-1 The user shall not be able to block "Critical Chatbots".

R15-5-2-2 The blocking feature shall not be available to users on the UI in case of Critical Chatbots (it shall only be available for other Chatbots or contacts).

NOTE: Blocking a Chatbot is expected not to display any Operator Messages on the user's device, including RCS messages and xMS messages.

R15-5-3 A user shall be able to report a Chatbot for various types of inappropriate behaviour to the MNO/RCS Service Provider and Chatbot Platform from within the Chatbot conversation.

R15-5-3-1 A user shall be able to report a Chatbot for "Spam", e.g. in cases where the Chatbot continuously sends unsolicited messages.

R15-5-3-2 A user shall be able to report a Chatbot for "Fraud", e.g. in cases where the user has paid for goods which were not delivered.

R15-5-3-3 A user shall be able to report a Chatbot for "Inappropriate Content", e.g. in cases where the user has received inappropriate content from a Chatbot.

R15-5-3-4 A user shall be able to report a Chatbot for "Other" inappropriate behaviour for cases that are perceived inappropriate by the users but do not fall in one of the above-mentioned three categories.

R15-5-3-5 Users shall have the option to enter a reason for reporting inappropriate behaviour in a free text field and / or attach selected messages exchanged with that Chatbot for explanation.

R15-5-3-6 The implementation shall ensure that the user understands that the report function as described in R15-5-3-1 to R15-5-3-4 does not replace any complaints of the user towards the Chatbot, e.g. in cases where the user expects the Chatbot to reimburse payments of undelivered goods etc.

R15-5-4 The service shall facilitate an MNO and/or RCS Service Provider to block/unblock Chatbots that have been frequently reported for inappropriate behaviour on their network.

R15-5-5 The service shall facilitate an RCS Service Provider to block/unblock all Chatbots published by a specific Chatbot provider.

R15-5-6 Blocking a Chatbot by an MNO or RCS Service Provider shall prevent future discoverability of that Chatbot by the user and prevent the exchange (sending and receiving) of all messages, files etc. with that Chatbot.

NOTE: Blocking a Chatbot is expected not to display any Operator Messages on the user's device, including RCS messages and xMS messages.

R15-5-7 If a user tries to message a Chatbot that was blocked by an MNO or RCS Service Provider, an MNO / RCS Service Provider configurable user-friendly “error message” shall be displayed to indicate that the Chatbot is not available.

R15-5-8 The reported information shall be made available to the MNO and the Chatbot Platform Provider in a format that can easily be monitored in a database software so that the above-mentioned countermeasures can be triggered in an efficient and effective way.

R15-5-9 If a Chatbot has been blocked, users shall still be able to see the Chatbot Information that likely contains other ways to get in touch, e.g. phone number or email address.

US15-6 **As a user, I want to be able to pay for goods and services offered to me by Chatbots.**

R15-6-1 A Chatbot shall be able to propose one or more payment options to a user during a conversational exchange in order for the user to complete purchase of goods or services.

R15-6-2 The payment options proposed to the user shall include carrier billing (e.g. via add to bill API or RCS premium event charging) where available and other third party payment services that the Chatbot would like to offer.

R15-6-3 The Chatbot may also offer the option to complete payment within the conversational thread, in which case it shall be able to request specific payment information from the user (e.g. credit card details).

R15-6-4 Any payment information transmitted via the Chatbot conversation shall be adequately secured and in line with the current industry requirements for payment security (e.g. credit card numbers, cvv, etc.).

R15-6-5 Traffic associated with making payments (via carrier billing, third party service or direct settlement as described in R15-6-3) shall be labelled and identifiable as such.

US15-7 **As an MNO, I want to be able to monitor and track the interactions between my customers and the Chatbot services.**

R15-7-1 Technical means shall be provided that allow MNOs and Chatbot Platforms to measure all RCS-based events exchanged in each direction per Chatbot on a per user basis (i.e. completed with the Chatbot’s unique Service ID and the user’s MSISDN or identifier) per RCS Service (including 1-to-1 Messaging, *Group Chat*, Geo-Location Push, Audio Messaging, File Transfer).

R15-7-2 Technical means shall be provided to label and differentiate the traffic into the following categories

R15-7-2-1 Traffic that confirms a monetary transaction between user and Chatbot and its value (i.e. payment category of traffic). This category includes referrals to third-party websites for completion of transactions.

R15-7-2-2 Traffic that contains advertising (i.e. advertising category of traffic).

R15-7-2-3 Traffic that delivers premium value content (i.e. messages or files containing content that needs to be paid for by the user e.g. via his mobile bill) and its value.

R15-7-2-4 Traffic belonging to subscriptions

NOTE: Transmitting the monetary value is based on bi-lateral agreements between Chatbot provider and MNO.

NOTE: Carrier billing requirements are out of scope of this document.

US15-8 **As a user, I want to enjoy the benefits of rich Chatbot communication features.**

R15-8-1 The MNO shall have the ability to define and control the set of RCS services available to the Chatbot platform.

R15-8-1-1 If an operator doesn't offer certain RCS services to a Chatbot / Chatbot Platform, then that Chatbot / Chatbots on that platform shall not be able to offer those services to a user (e.g. if the MNO or RCS Service Provider does not allow "Geolocation Push" for that Chatbot Platform, any suggested reply would not contain an action to share location).

R15-8-2 xMS may be available in a conversation with a Chatbot in both directions when conditions allow and when the conversation is not in anonymous mode (i.e. the SMS number is known by each party) and shall be displayed in the same conversation window.

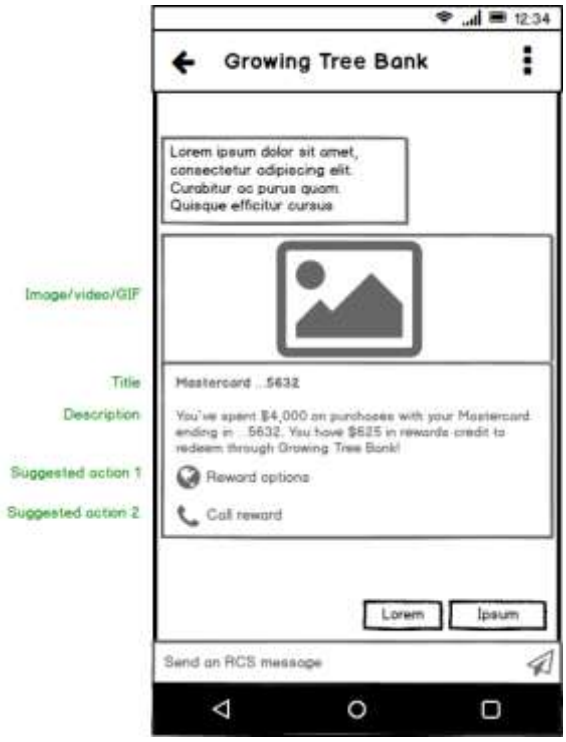


Figure 4: UX example for static Rich Card / Suggested Chip List

R15-8-3 A Chatbot shall be able to send a Static Rich Card that provides a single 'message bubble' with a static layout that integrates interactive content abilities.

NOTE: Static Rich Cards cannot be updated once sent by the Chatbot. Any later content update must be processed and sent as a new Static Rich Card.

R15-8-4 The static layout and interactive content abilities of the ‘message bubble’ shall be based on a set of defined templates as defined in R15-8-24 and following requirements supporting the following elements, each of which is optional to compose a Static Rich Card:

R15-8-4-1 Text field(s), such as title, sub-title, description;

NOTE: It is up to the client implementation how the text in each field is styled

R15-8-4-2 Image(s) (*animated or* not animated);

R15-8-4-3 Video(s);

R15-8-4-4 Audio(s);

NOTE: It is highly recommended that client implementations consider a (muted) auto-play experience for videos when the Static Rich Card is displayed in the conversation view.

R15-8-4-5 Suggested Replies which render with a non-empty text label and, when tapped, shall send a reply to the Chatbot consisting of the text as well as data if needed by the Chatbot – not seen by user – indicating which Suggested Reply was tapped;

NOTE: This data might be used by the Chatbot to differentiate between Suggested Replies with the same text but associated with different Chatbot messages.

R15-8-4-6 Suggested Actions, which shall render with an optional text label and, when tapped, shall be able to trigger one of the following:

R15-8-4-6-1 Open a web URL (which can also be used to open another app on the device if there is a default app handler for that URL registered with the operating system);

R15-8-4-6-2 Initiate a voice call to a defined destination (i.e. open dialler with number prefilled by the Chatbot). If the conversation is in anonymous mode, then the call shall be set up without presenting the user's MSISDN (i.e. CLIR active). If this cannot be ensured, the option to set up a call shall not be available if the conversation is in anonymous mode;

R15-8-4-6-3 Compose an Enriched Call to a defined destination (i.e. open Enriched Calling Call Composer with destination and call title, prefilled by the Chatbot). (This suggested action shall only be offered if the required capabilities are confirmed);

R15-8-4-6-4 Initiate a video call to a defined destination (i.e. open video dialler with destination prefilled by the Chatbot). (This suggested action shall only be offered if the required capabilities are confirmed);

R15-8-4-6-5 Initiate the recording and sending of an audio or video message to a defined destination (i.e. open audio or video message recording interface with number prefilled by the Chatbot);

R15-8-4-6-6 Send a message to a defined destination (i.e. open messaging interface to number prefilled by the Chatbot with content prefilled by the Chatbot but editable by the user);

R15-8-4-6-7 Send a geolocation push back to the Chatbot (i.e. open the location chooser UI);

R15-8-4-6-8 Open the user's default mapping app to a position indicated by either latitude-longitude coordinates or a mapping search query;

R15-8-4-6-9 Open the user's default calendar app to the new event page, with start time, end time, title, and description pre-filled;

R15-8-4-6-10 Send a response to a request to the user to grant a permission about sharing specific pieces of personal information with the Chatbot (according to R15-2-2, e.g. MSISDN, device specifics, user's location, enabling sending of "displayed" notifications etc.). The user shall be informed that such an acceptance of the request will change his privacy settings towards that Chatbot and have therefore an impact on his future sharing. The change will be permanent until further changes are made again by the user.

R15-8-4-6-11 When the user's MSISDN is not set to "share" with the Chatbot, then any suggested actions matching R15-8-4-6-3 to R15-8-4-6-6 shall not be presented to the user.

R15-8-4-6-12 When the user's location is not set to "share" with the Chatbot, then any suggested actions matching R15-8-4-6-7 shall not be presented to the user.

R15-8-5 When the user taps on a Suggested Action, an event shall be sent to the Chatbot indicating that the user has done so and exactly which Suggested Action was tapped.

R15-8-6 Static Rich Cards may be grouped together and displayed in scrollable "carousel" format containing up to ten Static Rich Cards.

R15-8-7 Limitations configured by the RCS Service Provider for automatic download of files shall be applied also when receiving a Static Rich Card.

R15-8-8 A Chatbot shall be able to send a Suggested Chip List that provides the user with quick interaction options.

R15-8-9 A Suggested Chip List shall be conceptually associated with a message from the Chatbot, and this association is specified by the Chatbot.

R15-8-9-1 A Suggested Chip List must not be shown by default unless the associated Chatbot message is the most recent message within the conversation.

NOTE: Suggested replies in the rich card are expected not to disappear after the next user input.

R15-8-9-2 A client implementation may offer the user a mechanism to view the Suggested Chip List associated with a message that is not the most recent within a conversation, but this must not be the default UI.

R15-8-9-3 A Chatbot shall not send a Suggested Chip List without an associated message.

R15-8-10 A Suggested Chip List may contain:

R15-8-10-1 Suggested Replies, as defined in R15-8-4-5;

R15-8-10-2 Suggested Actions, as defined in R15-8-4-6.

R15-8-11 A Suggested Chip List shall not contain more than eleven Suggested Replies and/or Suggested Actions combined.

R15-8-12 Suggested Replies shall always appear before Suggested Actions within the Suggested Chip List.

R15-8-13 *A Chatbot shall be able to specify a set of Suggested Replies (as per R15-8-4-5) and Suggested Actions (as per R15-8-4-6) that constitute a Persistent Menu.*

R15-8-13-1 *Persistent Menu shall be only used in a 1-to-1 conversation between a user and a Chatbot.*

R15-8-13-2 *Persistent Menu can contain up to three levels of hierarchy—i.e. top level, one level deep, two levels deep—which are specified by the Chatbot.*

R15-8-13-2-1 *While navigating the Persistent Menu, the user shall have a means to navigate to the previous level of hierarchy—e.g. from one level deep to top level—provided the user is not within the top level already.*

R15-8-13-3 *Each level of hierarchy shall contain at most five items, where each item is a Suggested Action or Reply, or a menu item to navigate to a deeper level of the hierarchy.*

R15-8-13-4 *At any point within a conversation with a Chatbot, the Persistent Menu shall be displayed on user action / request and the user is able to select one of the Suggested Actions or Replies, or a menu item to navigate to a deeper level of the hierarchy.*

R15-8-13-5 *If the Persistent Menu is presented to the user, the user shall have the option to make the Persistent Menu disappear.*

R15-8-13-6 *A Chatbot's Persistent Menu shall be the same for all users interacting with that Chatbot.*

R15-8-13-7 *Updates to the Persistent Menu shall be applied when changes were made by the Chatbot provider and the user opens the conversation with the Chatbot.*

R15-8-14 Both a Chatbot provider and the user shall receive the following states for their sent messages, file transfers, and Static Rich Cards:

R15-8-14-1 Pending;

R15-8-14-2 Sent;

R15-8-14-3 Delivered;

R15-8-14-4 Displayed (if enabled for that conversation);

NOTE: Displayed status might not be supported by all networks.

R15-8-14-5 Failed.

R15-8-15 If a Static Rich Card cannot be successfully delivered as the recipient is offline, the RCS Service Provider shall store the RCS event and deliver once the user is back online (i.e. 'Store & Forward').

R15-8-16 *For RCS events sent by a Chatbot to the user, NFS and CFS apply under certain conditions:*

R15-8-16-1 *If the Chatbot has allowed NFS and the terminating network supports NFS, then the network shall convert the RCS message (if not deliverable within the operator-defined time) in the most user-friendly way to SMS.*

- *Text elements shall be represented as text in SMS*
- *Pictures or other media elements shall use the procedures as defined in NFS for File Transfer.*
- *Chips (i.e. suggested actions and replies) shall not be represented unless they are available similar to media elements.*

R15-8-16-2 *If the Chatbot has not allowed NFS, then the RCS events shall be stored on the network until either delivered, or removed by the Chatbot or discarded on the network.*

R15-8-16-3 The Chatbot shall be able to remove any RCS event, including, but not limited to Rich Cards, that was previously sent by this Chatbot at any time before the RCS event has been delivered to the recipient's device.

NOTE: In contrast to P2P messaging, this is valid whether the terminating network supports NFS or not.

R15-8-16-4 The network shall notify the Chatbot of successful removal of RCS event from the network store & forward.

R15-8-16-5 CFS shall never be used to re-send messages via SMS in conversations with Chatbots.

R15-8-17 When a new message from a Chatbot is received and the conversation with the Chatbot is not in front view, a notification of this incoming event shall be displayed (same as for P2P events). The notification shall use the logo and service name from the Chatbot provider (as in the conversation thread), even if it is not stored within the Messaging implementation.

R15-8-18 The notification sound from an incoming Chatbot event should be configurable to distinguish it from P2P event notifications (see R18-6-3).

R15-8-19 A user should be able to mute notifications per individual Chatbot conversation (see R18-6-4).

R15-8-20 *Users shall be able to message a Chatbot from within an ongoing personal 1-to-1 (e.g. by adding '@chatbotXYZ' before the content of the message).*

R15-8-20-1 *When discovering the Chatbot that shall be messaged from the 1-to-1 conversation, the client shall propose results from the Chatbot search or Chatbot directory as defined in R15-4-5 and subsequent requirements*

R15-8-20-2 *Only messages explicitly directed to the Chatbot shall be received by the Chatbot.*

R15-8-20-3 *When a Chatbot is messaged, then the Chatbot shall be made aware of whether that message occurred in a conversation directly with it or in a conversation involving more than one user.*

R15-8-20-4 *If a Chatbot is messaged from within a personal 1-to-1 conversation, the conversation shall follow the requirements of 1-to-1 messaging (i.e. section 5) as far as possible.*

R15-8-20-5 *Only personal information from the sending user shall be shared with the Chatbot if this user has allowed sharing the identity with this particular Chatbot. In any other case, the Chatbot conversation shall be anonymized. No personal information from any other participant shall be shared with the Chatbot.*

R15-8-20-6 *CFS shall never be used to re-send messages via SMS in conversations with Chatbots.*

R15-8-21 *Users shall be able to message a Chatbot from within an ongoing Group Chat (e.g. by adding '@chatbotXYZ' before the content of the message.*

R15-8-21-1 *When discovering the Chatbot that shall be messaged from the Group Chat conversation, the client shall propose results from the Chatbot search or Chatbot directory as defined in R15-4-5 and subsequent requirements.*

R15-8-21-2 *Only messages explicitly directed to the Chatbot shall be received by the Chatbot.*

R15-8-21-3 *If a Chatbot was messaged from a Group conversation, then any messages from and to the Chatbot shall be seen by all participants in the conversation.*

R15-8-21-4 *The Chatbot who has been messaged from a Group Chat shall not be able to see who is participating in a Group Chat with the exception of the participant who messaged the Chatbot. User settings for sharing details apply, including the user settings for aliasing and anonymization and sharing Displayed notifications.*

R15-8-21-5 *The Chatbot shall be able to see Sent Message Status Notifications of the reply back to the Group Chat participant who originated the message to the Chatbot.*

R15-8-21-6 *Personal information from the sending user shall be shared with the Chatbot only if this user has allowed sharing the identity with this particular Chatbot. In any other case, the Chatbot conversation shall be anonymized.*

No personal information from any other participant shall be shared with the Chatbot

R15-8-21-7 *CFS shall never be used to re-send messages via SMS in conversations with Chatbots.*

R15-8-22 *Any Chatbot-generated events and user interaction with Chatbots shall be supported in a Multi Device Messaging environment (see section 9 for details).*

NOTE: Interaction with smart watches and in-car entertainment systems might be supported as a lightweight implementation because of hardware limitations of these devices.

R15-8-23 *A Chatbot shall be able to query the user's current location at any time.*

R15-8-23-1 *When the user's setting for sharing location information with the Chatbot is set to 'share' (R15-2-11-2), then the user's messaging client shall respond to any such request with its current location information automatically, without any user interaction.*

R15-8-23-2 *When the user's location information is set to 'share', it shall be made clear to the user exactly when the user's location has been shared with the Chatbot. The log of location shares shall be available for user information and could, for example, be presented in the conversation history.*

R15-8-23-3 *When the user's setting for sharing location information with the Chatbot is set to 'do not share' (R15-2-11-2), then no location information shall be shared automatically. Instead, on trigger of the Geolocation poll request the user shall be asked to share the geolocation once. If agreed, the device may offer the user selections such as "share once, always allow this Chatbot to poll without user interaction or never share". If the user has selected "never share" or a similar setting, the Geolocation poll of this Chatbot shall never lead to user interaction unless the user has manually changed the setting.*

NOTE: The rules as defined in R15-5-1 and subsequent requirements are especially important for this feature.

Static Rich Cards

R15-8-24 There shall be two types of static rich cards: domain-specific and general purpose.

R15-8-25 *Domain-specific static rich cards shall be specific to a use case. For example, a domain-specific static rich card for a boarding pass card could have boarding pass-specific fields—e.g. origin city, destination city, time of departure, gate, seat, etc. with a boarding pass-specific layout.*

NOTE: Domain-specific cards are not in scope of this Universal Profile. This document focuses exclusively on general purpose cards.

R15-8-26 General purpose cards shall be comprised of generic fields—e.g. image, title text, description text—with a generic layout.

Persistence

R15-8-27 General purpose cards shall be persistent. They do not disappear like Suggested Actions and Replies in a Suggested Chip List.

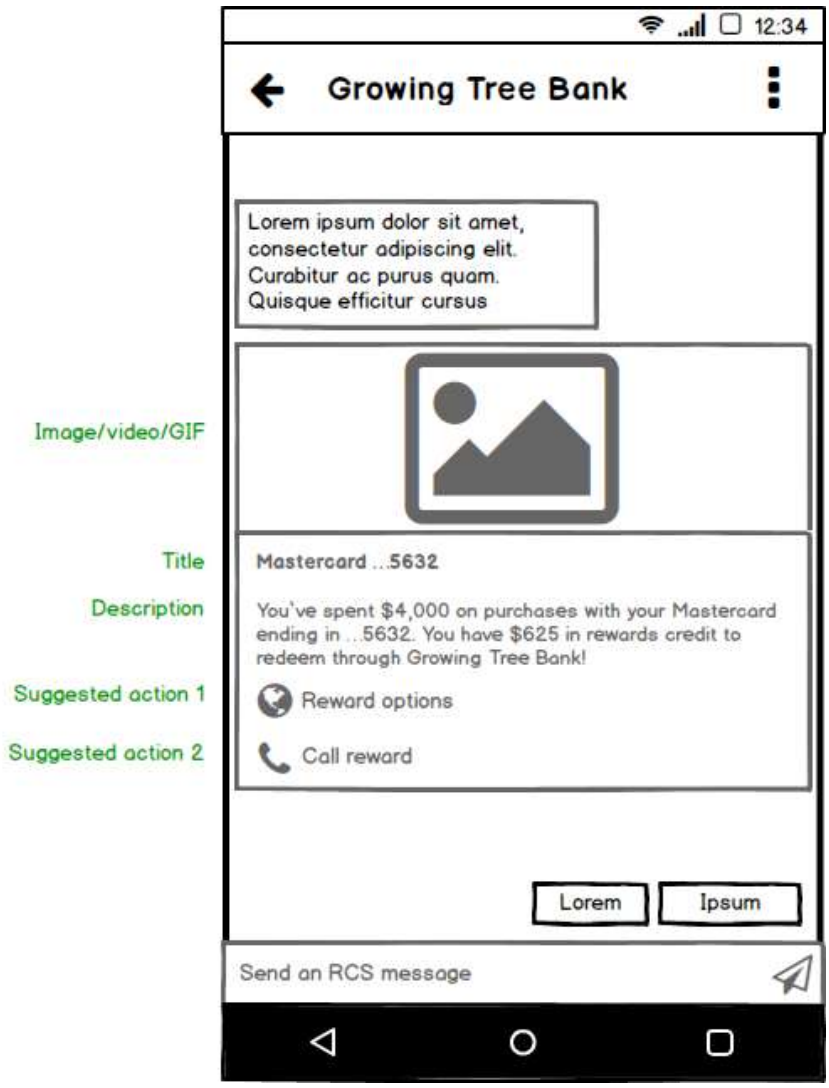
Fields

R15-8-28 A general purpose card shall contain the following generic fields, which should be laid out in this relative order:

1. Media: image, GIF, video, or audio file
2. Title text
3. Description text
4. List of suggested replies
5. List of suggested actions

R15-8-28-1 Each of these fields shall be optional, although at least one of fields 1-3 must be included to form a viable general purpose card. The layout order of the fields cannot be changed (with the exception of the horizontal standalone card, discussed below).

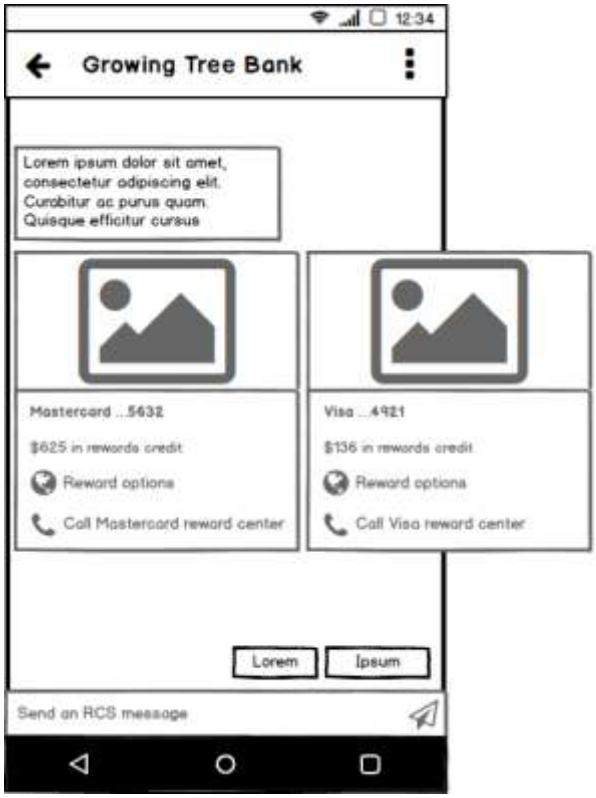
NOTE: Here is an example of a standalone general purpose card:



Carousels

R15-8-29 It shall be possible to send multiple general purpose cards as a carousel in a single message. (The max number is discussed below.)

R15-8-29-1 The cards are sent simultaneously—as part of the same message—and in the order that the client should render them in. The carousel can be scrolled horizontally.



Dimensions & Layout

- Standalone Card Width

R15-8-30 A general purpose card that is not part of a carousel should expand in width to the smaller of either:

- <width of the phone in portrait mode> - <width of the margins on either side of a card>
- MAX_STANDALONE_CARD_WIDTH

NOTE: The MAX_STANDALONE_CARD_WIDTH ensures that cards do not stretch too widely on tablets and desktop.
Recommendation: MAX_STANDALONE_CARD_WIDTH = 480 DP

NOTE: The width of a standalone card will always be the same in both portrait and landscape mode for a given device.

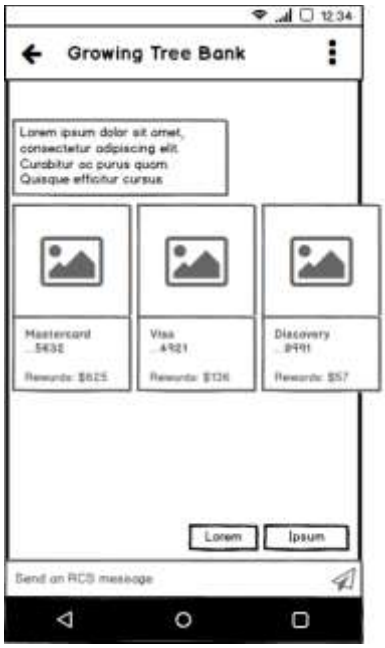
- Carousel Card Width

R15-8-31 For general purpose cards that are part of a carousel, the developer chooses whether the cards in that carousel should have SMALL_WIDTH: 120 DP or MEDIUM_WIDTH: 232 DP.

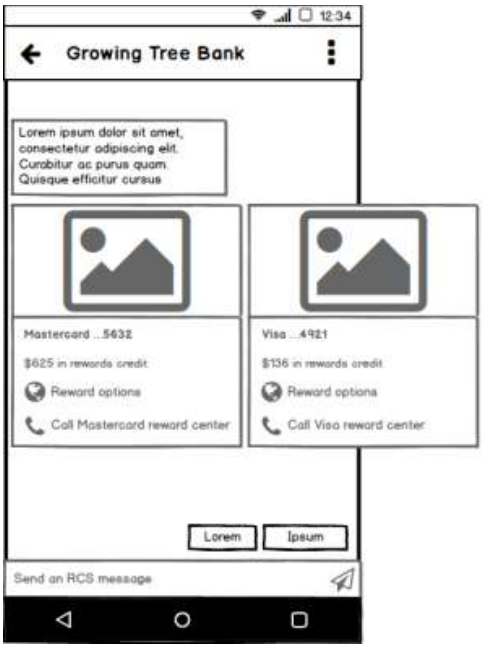
NOTE: **Recommendation**:

- SMALL_WIDTH: 120 DP
- MEDIUM_WIDTH: 232 DP

NOTE: For example:



SMALL_WIDTH



MEDIUM_WIDTH

- Height

R15-8-32 Standalone cards have a MIN_CARD_HEIGHT and MAX_CARD_HEIGHT.

NOTE: Recommendation:

- MIN_CARD_HEIGHT: 112 DP
- MAX_CARD_HEIGHT: 344 DP

MIN_CARD_HEIGHT

MAX_CARD_HEIGHT

R15-8-33 MEDIUM_WIDTH carousel cards shall have the same min and max heights as standalone cards. SMALL_WIDTH carousel cards have the same min height but a smaller max height: MAX_SMALL_WIDTH_CARD_HEIGHT.

NOTE: Recommendation*:* MAX_SMALL_WIDTH_CARD_HEIGHT = 224 DP.

R15-8-34 If the fields of a card are not large enough to fill the MIN_CARD_HEIGHT, then the card shall be expanded with white space at the bottom.

R15-8-35 If a card will exceed the MAX_CARD_HEIGHT, then the fields shall be truncated in the following order until it will not exceed MAX_CARD_HEIGHT: (3) description → (2) title → (5) suggested actions starting from the end of the list) → (4) suggested replies (starting from the end of the list).

Media

R15-8-36 A media file—image, GIF, video, or audio file —shall extend to the edges of the card on all sides, except for the bottom when there are other specified fields.

R15-8-37 If a card contains a media file and no other fields, then the media shall extend to all edges:

Media Heights

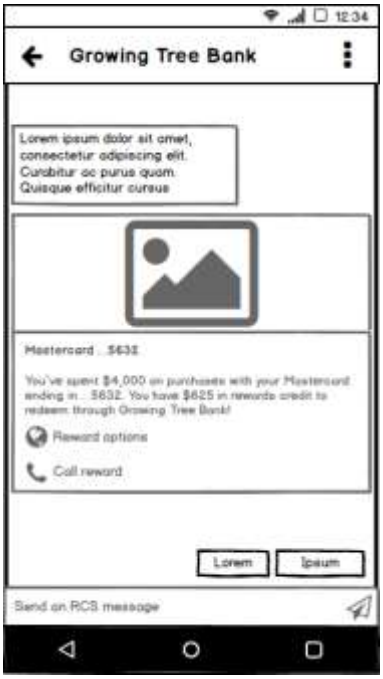
R15-8-38 For a standalone card or MEDIUM_WIDTH carousel card, the developer shall be able to choose one of three heights for the media:

1. SHORT_HEIGHT
2. MEDIUM_HEIGHT
3. TALL_HEIGHT

NOTE: Recommendation:

- SHORT_HEIGHT = 112 DP
- MEDIUM_HEIGHT = 168 DP
- TALL_HEIGHT= 264 DP

R15-8-39 For a SMALL_WIDTH carousel card, the developer shall be able to choose only SHORT_HEIGHT and MEDIUM_HEIGHT



SHORT_HEIGHT

MEDIUM_HEIGHT

TALL_HEIGHT

Title Text

R15-8-40 The title text shall wrap if it exceeds the width of the card. There shall not be any line or character limit for the title text, although it may be truncated due to max card height constraints.

Description Text

R15-8-41 The description text shall wrap if it exceeds the width of the card. There shall not be any limit to how many lines of description text. However, this is the first field to be truncated if the card exceeds the maximum total height.

Suggested Replies and Actions

R15-8-42 Suggested replies and actions shall be stacked, with all replies displayed first, then all actions. The text label for a given suggested reply or action is truncated after a maximum of 25 characters.

R15-8-42-1 At most 4 combined suggested replies and actions shall be possible to be included in a single card. However, it is highly unlikely that 4 suggested replies and actions can be rendered given max card height constraints and the truncation logic described above.

Horizontal Standalone Cards

R15-8-43 A standalone card can choose to have its media file on the right side (this is flipped to the left side for right-to-left languages):

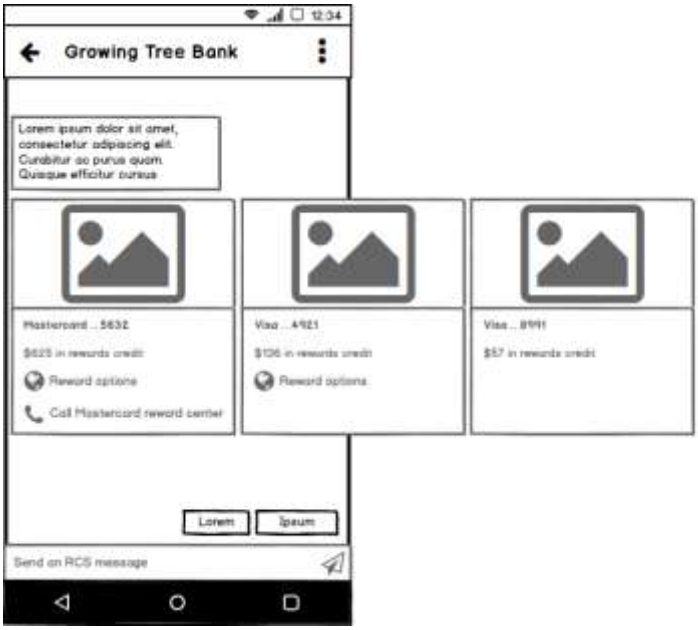
R15-8-43-1 In these cards, the displayed image should always be HORIZONTAL_LAYOUT_MEDIA_WIDTH.

NOTE: Recommendation: HORIZONTAL_LAYOUT_MEDIA_WIDTH = 128 DP.

Carousels

R15-8-44 There shall be at least 2 and up to 10 cards within a carousel. If more than 10 cards are sent within the same message, the client shall either ignore the additional cards or it can choose to load them on an asynchronous basis, e.g. when the user begins scrolling.

R15-8-44-1 Within a carousel, the fields within all cards must be vertically aligned. This is accomplished through the following rules:



R15-8-44-1-1 All media files within the cards shall have the same height

R15-8-44-1-2 All title fields within the cards shall have the same height, which is the height of the largest title text field. Title fields with fewer lines are padded with whitespace below the text to match the height of the largest title field.

R15-8-44-1-3 Description fields and suggested actions shall follow the same logic as title fields for height matching

Interactions

R15-8-45 Tapping a suggested action within a card shall have the same effect as tapping a suggested action within a Suggested Chip List, i.e. the action is taken and an interaction call-back is sent to the Chatbot for the purpose of analytics. There is no residual indication of selection in the UI.

R15-8-46 Tapping a suggested reply within a card shall have a similar but different effect as tapping a suggested reply within a Suggested Chip List. The similarity is that, when tapped, the user sends the suggested reply text to the conversation, and invisible postback data is sent to the Chatbot along with the text. The difference is that, once a suggested reply is tapped in a Suggested Chip List, the Suggested Chip List disappears because it is no longer associated with the last message in the conversation; whereas when a suggested reply is tapped in a rich card, the suggested replies and actions in the rich card do not disappear.

R15-8-47 Tapping an image/GIF in a rich card shall open the image/GIF in full-screen mode.

R15-8-48 Tapping a video or audio shall file play the file.

R15-8-48-1 A client may provide an affordance to play a video or audio file inline vs. full screen.

15.2.1 Technical Information for the realisation of Chatbots

15.2.1.1 Overview

The Chatbot functionality can be realised using 1-to-1 Chat as described in section 3.6 of [RCC.07]. The impact of Chatbots on addressing is defined in section 2.5.4 of [RCC.07].

It is an MNO choice to define a list of Chatbots requiring specific management. In order to do so, the MNO shall provide a Specific Chatbots List Server and configure the clients to access this server through the SPECIFIC CHATBOTS LIST client configuration parameter defined in section A.1.3 of [RCC.07].

15.2.1.2 Configuration Parameters

To provide the required MNO control of the Chatbot UX, the following parameter is added to those that are available in [RCC.07], [RCC.14] and [RCC.15]:

Configuration parameter	Description	RCS usage
SPAM NOTIFICATION TEXT	This parameter controls the notification text shown to the user when they try to access a Chatbot that is considered as Spam. If not provided, the text shown will be a default text determined by the client	Optional Parameter
TOKEN LINK NOTIFICATION TEXT	This parameter controls the notification text shown to the user when they indicate that they want to make a Chatbot aware of the link between the anonymous token used for communication with that Chatbot and their actual identity. If not provided, the text shown will be a default text determined by the client	Optional Parameter
UNAVAILABLE ENDPOINT TEXT	This parameter provides a message of type String that shall be displayed if an endpoint declines a conversation with a user as per section 3.6.8.2.3 of [RCC.07]	Optional Parameter
ALLOW ENRICHED CHATBOT SEARCH DEFAULT	This parameter controls the default position (ON or OFF) of the user setting to enrich the Chatbot search. If not provided, the setting default position will be set to ON i.e. the user setting to enrich the Chatbot search is enabled.	Optional Parameter

Table 19: Additional Configuration Parameters to control the Chatbot UX

The SPAM NOTIFICATION TEXT parameter is added to the UX tree defined in section 5.3.4 with the following formal definition:

Node: /<x>/UX/spamNotificationText

Leaf node that provides the notification text shown to the user when they try to access a Chatbot that is considered as Spam.

If not instantiated, the text shown shall be determined by the client implementation.

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

Table 20: UX MO sub tree addition parameters (spamNotificationText)

- Values: <string to be shown to the user>, minimum 10 characters long, maximum 200 Characters
- Post-reconfiguration actions: no specific actions.
- Associated HTTP XML characteristic type: “spamNotificationText”

Node: /<x>/UX/tokenLinkNotificationText

Leaf node that provides the notification text shown to the user when they indicate that they want to make a Chatbot aware of the link between the anonymous token used for communication with that Chatbot and their actual identity.

If not instantiated, the text shown shall be determined by the client implementation.

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

Table 21: UX MO sub tree addition parameters (tokenLinkNotificationText)

- Values: <string to be shown to the user>, minimum 10 characters long, maximum 200 Characters
- Post-reconfiguration actions: no specific actions.
- Associated HTTP XML characteristic type: “tokenLinkNotificationText”

Node: /<x>/UX/unavailableEndpointText

Leaf node that provides the notification text shown to the user when an endpoint declines a conversation with a user as per section 3.6.8.2.3 of [RCC.07].

If not instantiated, the text shown shall be determined by the client implementation.

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

Table 22: UX MO sub tree addition parameters (unavailableEndpointText)

- Values: <string to be shown to the user>, minimum 10 characters long, maximum 200 Characters
- Post-reconfiguration actions: no specific actions.
- Associated HTTP XML characteristic type: “unavailableEndpointText”

Node: /<x>/UX/allowEnrichedChatbotSearchDefault

Leaf node that provides the default position (ON or OFF) of the user setting to enrich the Chatbot search.

If not instantiated, the setting default position will be set to ON i.e. the user setting to enrich the Chatbot search is enabled.

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

Table 23: UX MO sub tree addition parameters (allowEnrichedChatbotSearchDefault)

- Values:
  0, user setting to enrich Chatbot search default position is set to OFF
  1, user setting to enrich Chatbot search default position is set to ON (default)
- Post-reconfiguration actions: no specific actions.
- Associated HTTP XML characteristic type: “allowEnrichedChatbotSearchDefault”

The representation of the parameters in the UX tree and the associated HTTP configuration XML structure with this parameter are shown in section 5.3.4.

15.2.1.3 Technical Implementation of User Stories and Service Requirements

R15-9-1 For the implementation of the requirements in user story US15-1 the following applies:

R15-9-1-1 For R15-1-1, refer to the RCS architecture in section 2.1 of [RCC.07] that allows for deployment of Chatbot Platforms.

R15-9-1-2 Requirement R15-1-1-1 shall be implemented locally on the device. The client shall consider as a critical Chatbot any Chatbot whose URI matches an URI of the list of critical Chatbots URIs as defined in section 3.6.11 of [RCC.07].

R15-9-1-3 For R15-1-2 and R15-1-3 for a globally unique Service ID that can accommodate a potential growth of Chatbots and Chatbot Platforms, refer to section 2.5.4.1 of [RCC.07].

R15-9-1-4 For requirement R15-1-4 and its sub-requirements, the information shared shall be provided during the Chatbot onboarding process. This procedure is out of the scope of this specification. The information provided shall be mapped to a JSON format as defined in section 3.6.4.1.1 of [RCC.07].

R15-9-1-5 Requirement R15-1-5 shall be realised on the client using the interface and procedure as described in section 3.6.4 of [RCC.07].

R15-9-1-6 For Requirement R15-1-6 shall be realised on the client using the interface and procedure as described in section 3.6.4 of [RCC.07].

R15-9-1-7 Requirement R15-1-8 shall be implemented locally on the device.

R15-9-1-8 Requirement R15-1-9 shall be realised using the procedures in section 3.6.11 of [RCC.07].

R15-9-1-9 Requirement R15-1-9-1 shall be implemented locally on the device. The client shall provide the indicator for Chatbots whose URI matches an URI of the list of critical Chatbots URIs as defined in section 3.6.11 of [RCC.07].

R15-9-1-10 Requirement R15-1-10 and its sub-requirement shall be implemented by the Chatbot Platform as per section 3.8.6.2.1 of [RCC.07].

R15-9-1-11 Requirement R15-1-11 shall be implemented on the Client using the procedure specified in section 3.8.6.2.2 of [RCC.07] and the configuration parameter UNAVAILABLE ENDPOINT TEXT in section 15.2.1.2

R15-9-2 For the implementation of the requirements in user story US15-2 the following applies:

R15-9-2-1 R15-2-1 is realized by the procedures of the Anonymization Function (AF) described in section 3.6.5.1.5.3 of [RCC.07] and by the fact that Clients are configured through the PRIVACY DISABLE parameter (as defined in section A.1.3 of [RCC.07]) to enable anonymization or not.

R15-9-2-2 Requirement R15-2-1-1 is handled by the fact that [RCC.07] allows the Anonymization Function to be deployed in the RCS Service Provider's network or as part of the Chatbot Platform.

R15-9-2-3 Section 2.5.4.2 of [RCC.07] mandates the uniqueness of the token, fulfilling R15-2-1-2.

R15-9-2-4 R15-2-1-3 is managed by the client in the following way: when the user agrees to share their MSISDN, the client shall follow the procedures of section 3.6.5.1.2.4 of [RCC.07].

R15-9-2-5 R15-2-2 and its sub-requirements are managed locally on the device and propagated on the network via the procedures defined in sections 3.2.1.2 and 3.6.8.3 of [RCC.07]

R15-9-2-6 R15-2-3 is managed locally on the device. The ‘anonymous mode’ is requested via the privacy header as defined in step 5 of section 3.6.8.3.1 of [RCC.07].

R15-9-2-7 R15-2-3-1 shall be implemented locally on the device.

R15-9-2-8 As in anonymous mode the token is the user’s identifier given to the Chatbot platform, the Chatbot is able to reuse it, fulfilling requirement R15-2-3-2.

R15-9-2-9 R15-2-3-3 is ensured by section 3.6.8.5.1 of [RCC.07] (see bullet 4).

R15-9-2-10 R15-2-3-4 shall be implemented locally on the Chatbot Platform or the Chatbot.

R15-9-2-11 R15-2-3-5 and its sub-requirement shall be implemented locally on the device.

R15-9-2-12 R15-2-3-6 is fulfilled because Notifications are not managed differently for an anonymous conversation than from any messaging conversation.

R15-9-2-13 R15-2-4 is fulfilled by the client through the procedures defined in section 3.6.5.1.2.3 of [RCC.07].

R15-9-2-14 The deletion of a token results in closing any potential active session established with the old token. In addition, a Chatbot trying to reuse a deleted token will receive an error as per section 3.6.5.1.3.2 of [RCC.07] for an MNO AF or via specific internal procedures for Chatbot Platform AF. Therefore, requirement R15-2-4-1 and R15-2-4-2 are fulfilled.

R15-9-2-15 Requirement R15-2-4-3 shall be implemented locally on the device.

R15-9-2-16 For R15-2-5 and its sub-requirements, the ‘public mode’ is requested when there is no use of the privacy header as defined in step 5 of section 3.6.8.3.1 of [RCC.07].

R15-9-2-17 Requirement R15-2-5-1 shall be implemented locally on the device.

R15-9-2-18 R15-2-5-2 is fulfilled because Notifications are not managed differently for a public conversation than from any messaging conversation.

R15-9-2-19 Requirement R15-2-5-3 shall be implemented locally on the device.

R15-9-2-20 Requirements R15-2-5-5 and R15-2-5-6 shall be implemented locally on the device.

R15-9-2-21 Requirements R15-2-6 and R15-2-7 shall be implemented locally on the device.

R15-9-2-22 Requirement R15-2-8-1-1 shall be implemented locally on the device.

R15-9-2-23 Requirement R15-2-8-1-2 shall be realised through the TOKEN LINK NOTIFICATION TEXT client configuration parameter defined in section 15.2.1.2.

R15-9-2-24 Requirement R15-2-8-1-3 is covered in sections 3.6.5.1.3.1 and 3.6.5.1.4.1 of [RCC.07] as the AF invalidates the token.

R15-9-2-25 Requirement R15-2-9 shall be implemented locally on the device.

R15-9-2-26 When a user changes a conversation with a Chatbot from 'public mode' to 'anonymous mode', a new Chatbot session is established, using a token as the user's identity. Therefore, for the Chatbot there is no link between this new session and the one using the user's identity. R15-2-10-1 is then fulfilled.

R15-9-2-27 Requirement R15-2-10-2 shall be implemented locally on the device.

R15-9-2-28 Requirements R15-2-11-1, R15-2-11-2 and R15-2-11-3 shall be implemented locally on the device. It is a device implementation to interact with the user with respect with the settings of the privacy relevant information.

R15-9-2-29 R15-2-11-4 is managed by the Suggested action defined in 3.6.10.6.1.2 of [RCC.07]. The device Status is requested by the Chatbot by sending the 'requestDeviceSpecifics' Suggested action defined in 3.6.10.6.1.2 of [RCC.07]. If the user agrees to the one-time share request, the client shall follow the procedures described in section 3.6.10.6.2 of [RCC.07]. The location information is requested by the Chatbot by sending the 'requestLocationPush' Suggested action defined in 3.6.10.6.1.2 of [RCC.07]. If the user agrees to the one-time share request, the client shall send response to the suggested action including postback data as per section 3.6.10.6.2.2 of [RCC.07]. The client shall send the user's location information following the 1-to-1 Geolocation Push service procedures described in section 3.2.6.2.1 of [RCC.07]. The sending of "Displayed" notification for received messages is requested by the Chatbot by sending the 'enableDisplayedNotifications' Suggested action defined in 3.6.10.6.1.2 of [RCC.07]. The change of the setting is managed locally on the device based on the related setting required by R18-17-5-3.

R15-9-2-30 Requirement R15-2-11-4-1 shall be implemented locally on the device.

R15-9-2-31 Requirement R15-2-12 and its sub-requirement shall be implemented locally on the device.

R15-9-2-32 Requirement R15-2-13 is fulfilled thanks to the multi-device message support as requested by section 9 of this document.

R15-9-2-33 Requirement R15-2-14 is fulfilled as the settings are managed locally on the device.

R15-9-2-34 Requirement R15-2-15 and its sub-requirements shall be implemented locally on the device.

R15-9-2-35 R15-2-16 shall be realised based on the procedures in section 3.6.4.2 of [RCC.07].

R15-9-2-36 R15-2-16-1 shall be implemented locally on the device.

R15-9-2-37 For R15-2-16-2, the identification of the Chatbot verification status shall be performed based on the procedures described in section 3.6.3.1, 3.6.3.2.1 and 3.6.4.2 of [RCC.07]. The visual differentiation shall be implemented locally on the device.

R15-9-2-38 For R15-2-16-2-3, the Verification authority shall be retrieved based on the procedures described in section 3.6.4.2 of [RCC.07]. The display of the Verification Authority shall be implemented locally on the device.

R15-9-2-39 R15-2-16-2-4 shall be implemented based on the procedures described in section 3.6.3.2.1 and 3.6.4.2 of [RCC.07].

R15-9-2-40 R15-2-16-2-5 is fulfilled by the complying with the procedures described in section 3.6.3.2.1 and 3.6.4.2 of [RCC.07].

R15-9-2-41 R15-2-16-2-6 is fulfilled by complying with steps 5 b) and c) of section 3.6.3.2.1 of [RCC.07] and steps 5 b) and c) of section 3.6.4.2.3.1 of [RCC.07].

R15-9-2-42 R15-2-16-2-7 shall be implemented based on the procedures described in section 3.6.3.1, 3.6.3.2.1 and 3.6.4.2 of [RCC.07].

R15-9-2-43 R15-2-16-3 shall be implemented locally on the device.

R15-9-2-44 R15-2-16-3-1 shall be implemented based on the policies the Directory to Directory interface HTTPS GET request is sent. The Directory to Directory interface is defined in section 3.6.3.2 of [RCC.07]. The procedures for the Chatbot Information retrieval shall be based on section 3.6.4 of [RCC.07] and they shall be based on client triggers.

R15-9-2-45 R15-2-16-3-2 shall be implemented based on the procedures described in section 3.6.4 of [RCC.07].

R15-9-2-46 For R15-2-16-3-3, the removal of the MNO trusted verification authorities is network internal. The retrieval of the Chatbot Verification Status shall be based on the procedures described in sections 3.6.3.1 3.6.4.1.3 and section 3.6.4.2.4 of [RCC.07].

R15-9-2-47 R15-2-16-4-1 shall be implemented based on network internal procedures.

R15-9-2-48 Requirement R15-2-16-5 shall be implemented locally on the device. The client shall provide the indicator for Chatbots whose URI matches an URI of the list of critical Chatbots URIs as defined in section 3.6.11 of [RCC.07].

R15-9-3 void

R15-9-4 For the implementation of the requirements in user story US15-4 the following applies:

R15-9-4-1 In order to support requirement R15-4-1, Chatbot developer/owner shall limit its own availability by specifying the MCC/MNC code(s) and the language(s) with which the Chatbot can be discovered. This can be done during the Chatbot onboarding process by the Chatbot Platform. The onboarding process procedure is out of the scope of this specification.

R15-9-4-2 For requirement R15-4-2, the Chatbot platform shall limit the Chatbot availability by specifying the MCC/MNC code(s) and language (s) with which the Chatbot can be discovered. This is based on the Chatbot Platform available interconnections and internal policies.

R15-9-4-3 Requirement R15-4-3 and its sub-requirements shall be implemented based on the procedures described in section 3.6.3.1 of [RCC.07].

R15-9-4-4 Requirement R15-4-4 shall be fulfilled based on the procedures described in section 3.6.3.2 of [RCC.07].

R15-9-4-5 Requirement R15-4-5 shall be implemented based on the procedures described in section 3.6.3.1 of [RCC.07].

R15-9-4-6 Requirements R15-4-6 and R15-4-7 shall be realised by the CHATBOT DIRECTORY parameter defined in Annex A.1.3 and A.2.4 of [RCC.07].

R15-9-4-7 For requirement R15-4-8, the client shall generate the query based on the procedures described in section 3.6.3.1 of [RCC.07]. The query entries are specified in the “q” query parameter. If the entry is a Chatbot identifier, the client does not need to trigger query against the Service Provider Chatbot directory to acquire the Chatbot Service ID because it already has the Chatbot Service ID.

R15-9-4-8 For requirement R15-4-9, the RCS client shall retrieve the Chatbot list by following the query procedures specified in section 3.6.3.1 of [RCC.07]. If the service logo is unavailable, a default service logo shall be displayed based on the client implementation.

R15-9-4-9 For R15-4-10 for a user initiating a conversation with a Chatbot, the procedures in sections 3.2.1.2 and 3.6.8.3 of [RCC.07] apply.

R15-9-4-10 Requirement R15-4-11, its sub-requirements and R15-4-12 shall be implemented locally on the device using the procedures for creating a new conversation or continuing an existing one as defined in R15-9-1, R15-9-2, R15-9-4 and their sub-requirements. The deep link format is specified in section 3.6.3.4 of [RCC.07].

R15-9-4-11 Requirement R15-4-13 and R15-4-14 shall be implemented locally on the device.

R15-9-4-12 For R15-4-13-1 and for the case where the user enters an email address in the "to" field of the Chat Composer, the client shall do a directory lookup as specified in section 3.6.3.1 of [RCC.07] using the provided string as value for the "q" parameter.

R15-9-4-13 Requirement R15-4-15 shall be realised locally on the device and may be based on the Chatbot Information retrieved according to the procedure in section 3.6.4 of [RCC.07].

R15-9-4-14 Requirement R15-4-15-2 shall be realised through the client offering in the introduction screen a UI element with a fixed label text that is implementation specific. When this UI element is tapped the client shall open the Messaging thread with the Chatbot, set up a session with the Chatbot as defined in sections 3.2.1.2 and 3.6.8.3 of [RCC.07] and send a Client Response for Suggested Replies content to the Chatbot (i.e. as defined in section 3.6.10 of [RCC.07]). In this response, the client shall provide a display text and set the displayText field to the text displayed in the tapped button. Therefore, it shall show the message in the Messaging thread. The client shall set the data field of the postback object to the fixed string *"new_bot_user_initiation"_hl* where hl is the value of the parameter defined in section 3.6.4.1 of [RCC.07].

R15-9-4-15 For R15-4-17 for a Chatbot initiating a conversation with a user, the procedures in section 3.6.8 of [RCC.07] apply.

R15-9-5 For the implementation of the requirements in user story US15-5 the following applies:

R15-9-5-1 Requirement R15-5-1 shall be realised through anonymization described for the realisation of US15-2. Requests addressed to the user's MSISDN will be considered as authorised and when addressing an anonymised identity, a mapping will have to exist to the user's IMPU before the user can be reached. Such a mapping would be created if the user contacted the Chatbot first.

R15-9-5-2 Requirement R15-5-2 shall be realised on the client as described in section 3.6.6 of [RCC.07].

R15-9-5-3 Requirements R15-5-2-1 and R15-5-2-2 shall be implemented locally on the device. The client shall not provide the blocking feature for Chatbots whose URI matches an URI of the list of critical Chatbots URIs as defined in section 3.6.11 of [RCC.07].

R15-9-5-4 For Requirement R15-5-3 and its sub-requirements shall be realised through the Spam Report and reporting of other inappropriate behaviour functionality described in section 3.6.6.2 of [RCC.07].

R15-9-5-5 Requirement R15-5-4 shall be realised

R15-9-5-5-1 in the network as described in section 3.6.6 of [RCC.07] whereby the means to provide this functionality are out of scope of this document and/or

R15-9-5-5-2 on the client based on an entry in the Blacklist provided by the MNO or RCS Service Provider as described in section 3.6.6.1 of [RCC.07].

R15-9-5-6 Requirement R15-5-5 shall be realised

R15-9-5-6-1 in the network, as described in section 3.6.6 of [RCC.07] whereby the means to provide this functionality are out of scope of this document and/or

R15-9-5-6-2 on the client, based on an entry using regular expressions in the blacklist provided by the MNO or RCS Service Provider as described in section 3.6.6.1 of [RCC.07].

R15-9-5-7 Requirement R15-5-6 shall be realised through

R15-9-5-7-1 the MNO or RCS Service Provider not including the Chatbot in the Chatbot Directory described in section 3.6.3.1 of [RCC.07] and/or

R15-9-5-7-2 the client removing the entry for the blocked Chatbot from the discovery result based on the Chatbot's address matching an entry in the list of Chatbots to which access must be prevented that is provided by the MNO or RCS Service Provider as described in section 3.6.6.1 of [RCC.07].

R15-9-5-8 Requirement R15-5-7 shall be realised locally on the device based on the Chatbot's address matching an entry in the list of Chatbots to which access must be prevented that is provided by the MNO or RCS Service Provider as described in section 3.6.6.1 of [RCC.07] or based on a SIP 403 Forbidden response that includes a Warning header including the warning text set to "206 Spam Sender" when setting up a session to the Chatbot as described in section 3.6.6 of [RCC.07]. The message displayed to the user shall be determined by the SPAM NOTIFICATION TEXT client configuration parameter defined in section 15.2.1.2.

R15-9-5-9 For R15-5-8, the format defined in section 3.6.6.2 of [RCC.07] shall be used.

R15-9-5-10 For R15-5-9, blocking a Chatbot shall not lead to the retrieval of the Chatbot Info being blocked as specified in section 3.6.6 of [RCC.07].

R15-9-6 For the implementation of the requirements in user story US15-6 the following applies:

R15-9-6-1 Requirement R15-6-1 can be realised through a Suggested Chip List as defined for R15-8-8 to R15-8-12 including the available payment methods as Suggested Replied (see R15-8-10-1). This Suggested Chip List can be associated to a message asking for the user's preferred payment method.

R15-9-6-2 For R15-6-2, if the Chatbot or Chatbot Platform have an agreement with the MNO serving the user to provide Carrier Billing, the Suggested Chip List may include Carrier Billing as a Suggested Reply.

R15-9-6-3 For R15-6-3, the use of a Suggested Chip List and regular messages allows completing the payment within the conversational thread and it is up to the Chatbot to determine whether it can make use of those methods.

R15-9-6-4 For R15-6-4, the RCS communication between Chatbot and User is secured according to what is described in section 2.12.1 of [RCC.07] for the path between Chatbot Platform and User in combination with what is described for the interface between Chatbot and Chatbot Platform which is

out of scope of this document. It is up to the Chatbot to determine whether that allows to exchange the information required from the user for payment in a sufficiently secure manner.

R15-9-6-5 Requirement R15-6-5 on labelling traffic associated with payments is provided via the setting of the CPIM header described in section 3.6.7 of [RCC.07].

R15-9-7 For the implementation of the requirements in user story US15-7 the following applies:

R15-9-7-1 Requirement R15-7-1 on measuring all RCS-based events exchanged in each direction per Chatbot on a per user basis is supported as per RCS Service Provider charging requirements, and by RCS service identification as described in [PRD-IR.90] for RCS services.

R15-9-7-2 Requirement R15-7-2 and its sub-requirements are supported by the new CPIM header as defined in section 3.6.7 of [RCC.07].

R15-9-8 For the implementation of the requirements in user story US15-8 the following applies:

R15-9-8-1 Requirement R15-8-1 shall be realised through the MNO removing the capabilities corresponding to services that are not available to the Chatbot Platform from the capabilities provided to the RCS Client and the Chatbot Platform as part of the Capability Exchange (i.e. removal in both directions). The way in which this removal is done is out of scope of this document.

NOTE: An MNO may also restrict access to these services as part of a commercial agreement with the Chatbot Platform. In which case the Chatbot Platform should not announce the corresponding capabilities as part of the capability exchange, should not include suggested actions related to services that are unavailable and should make the Chatbots that it hosts aware that those services are not available and cannot be used. Such commercial agreements are out of scope of this document.

R15-9-8-2 Requirement R15-8-1-1 shall be realised on

R15-9-8-2-1 the Chatbot Platform based on the absence of the corresponding capabilities towards the RCS user and

R15-9-8-2-2 locally on the RCS Client where, as towards regular users, services for which no capability is available should not be offered to the user and where suggested actions corresponding to capabilities that are not available should not be shown to the user. This would apply to

- Sending a Geolocation Push as specified in R15-8-4-6-7 if the Geolocation Push capability is not available

R15-9-8-3 For messages originating from the client requirement R15-8-2 shall be realised using the messaging technology selection defined in section 3.2.1.2 of [RCC.07]. For messages originating from the Chatbot, they can be sent if their content type can be mapped to xMS and the Chatbot is aware of the user's MSISDN.

R15-9-8-4 The requirements as specified in R15-8-3 to R15-8-6 as well as R15-8-8, R15-8-9, R15-8-9-3 and R15-8-10 to R15-8-11 shall be realised through section 3.6.10 in [RCC.07].

R15-9-8-5 The requirements as specified in R15-8-7, R15-8-9-1, R15-8-9-2 and R15-8-12 shall be implemented locally on the device.

R15-9-8-6 For the message transfer states of requirement R15-8-14, the technical realization described for messaging in R5-28-23 and for File Transfer in R7-23-15 applies, with the status of “Error” being equivalent to the status of “Failed”.

R15-9-8-7 Notifications on delivery status information as defined in R15-8-15 shall be stored and forwarded in the Store and Forward server shall be realised as specified in sections 3.2.3.3 and 3.6.9 of [RCC.07].

R15-9-8-8 The requirement R15-8-16-3 and R15-8-16-4 for a Chatbot to be able to remove an event before it is delivered through the procedures in section 3.2.3.8 of [RCC.07] and the requirement R15-8-16-5 for no fall-back to xMS shall be realised as specified in section 3.6.8 of [RCC.07] for messages sent by the Chatbot and locally on the device for replies from the user.

R15-9-8-9 Requirements R15-8-17, R15-8-18, and R15-8-19 shall be implemented locally on the device.

R15-9-8-10 For R15-8-24, R15-8-25 and R15-8-26, the realisation of the general purpose Rich Card is defined in section 3.6.10 of [RCC.07]. This version of the Universal Profile does not define domain-specific Rich Cards yet.

R15-9-8-11 R15-8-27 shall be realised locally on the device for a received Rich Card.

R15-9-8-12 R15-8-28 and R15-8-28-1 shall be realised through the definition of the General Purpose Card in section 3.6.10.4 and 3.6.10.5.1 of [RCC.07] whereby the layout shall be handled locally on the device.

R15-9-8-13 R15-8-29, R15-8-29-1 and R15-8-31 shall be realised through the definition of the General Purpose Card Carrousel in sections 3.6.10.4 and 3.6.10.5.2 of [RCC.07].

R15-9-8-14 R15-8-30, R15-8-32 to R15-8-37, R15-8-40 and R15-8-41 shall be realised locally on the device.

R15-9-8-15 R15-8-38 and R15-8-39 shall be realised through the definition of the cardMedia message fragment in section 3.6.10.4 of [RCC.07].

R15-9-8-16 The 25 character limit defined in R15-8-42 shall be realised through the definition of a suggestion in section 3.6.10.4 of [RCC.07]. The stacking of the provided Suggested replies and actions shall be realised locally on the device.

R15-9-8-17 R15-8-42-1 shall be realised through the definition of the General Purpose Card and General Purpose Card Carrousel in section 3.6.10.4 and 3.6.10.5 of [RCC.07].

R15-9-8-18 R15-8-43 and R15-8-43-1 shall be realised through the definition of the General Purpose Card in section 3.6.10.4 and 3.6.10.5.1 of [RCC.07] whereby the layout shall be handled locally on the device.

R15-9-8-19 R15-8-44 shall be realised through the definition of the General Purpose Card Carrousel in section 3.6.10.4 and 3.6.10.5.2 of [RCC.07].

R15-9-8-20 For R15-8-44-1-1, the client shall assume that the media height provided for the first card of the Carrousel applies to the media in all cards (i.e. the media height indicated in the further cards shall be ignored).

R15-9-8-21 R15-8-44-1, R15-8-44-1-2 and R15-8-44-1-3 and R15-8-45 to R15-8-48-1 shall be realised locally on the device.

15.3 Plugins

This section focusses on RCS enabled Plugins and sets the requirements for a plugin framework that ensures a harmonized discovery and installation process. This section also describes how plugins can be used to enhance the communication experience.

US15-10 **As a user, I want to use Plugins that make my RCS service experience rich and powerful.**

R15-10-1 It shall be possible to install plugins that make new, additional RCS event types available to a user for use in a Messaging conversation or a Voice or Video call.

NOTE: Although plugins can also be used within the context of a Voice or Video Call, this version of the specification focusses on Messaging-related plugins.

R15-10-2 *Two types of plugins shall be enabled:*

R15-10-2-1 Uni-directional: Only the sender needs to have the plugin installed for an end-to-end experience of plugin-enabled events and contents (e.g. Stickers offered via a plugin).

NOTE: The receiving user might be a legacy RCS user or a non-RCS user but restrictions might apply for non-RCS users. For example, an animated sticker might be conveyed to the recipient using MMS but the animation itself might not be supported in this case.

R15-10-2-2 *Bi-directional: Both sender and recipient are required to have the plugin installed for an end-to-end experience of plugin-enabled events and contents (e.g. collaboration or gaming plugins).*

R15-10-3 Each plugin (regardless whether uni-directional or bi-directional) shall use for their events a plugin-specific identifier so that RCS events initiated through a plugin can be clearly identified and their content displayed within the conversation view according to the specifics of the plugin.

R15-10-4 *A plugin shall work on any UP 2.0 (or higher) plug-in enabled client and network.*

NOTE: For plug-ins that need to obtain user identifiers in clear form and that are not privileged by the client to do so, the client might trigger UX procedures asking for the user's consent.

R15-10-5 Within a Messaging conversation, the user shall be able to trigger plugin-specific RCS events through a clearly identifiable entry point shown in the sharing options of a 1-to-1 and/or Group conversation. Each plugin shall have its own entry point which is labelled with the plugin's name and/or icon).

R15-10-5-1 It shall be possible for a plugin provider to define whether the plugin sharing entry point is displayed to the user within a 1-to-1 (Messaging) conversation and / or a Group (Messaging) conversation.

NOTE: The technical realisation is expected to foresee an option to distinguish in addition future plugins for Voice and Video calls.

R15-10-5-2 *A service entry point for a bi-directional plugin shall only be displayed in conversation-sharing options with other users when those users are also all using UP 2.0 (or higher) compliant networks and clients that support plugins.*

US15-11 **As a user, I want that uni-directional plugin content is directly displayed on the receivers' conversation view without them needing the particular plugin installed themselves.**

R15-11-1 If content of a uni-directional plugin is sent to a recipient who does not have that same uni-directional plugin installed, then the content shall be able to be displayed to the recipient.

NOTE: The receiving user might be a legacy RCS user or a non-RCS user but restrictions might apply for non-RCS users. For example, an animated sticker might be conveyed to the recipient using MMS but the animation will not be supported in this case.

R15-11-2 In addition, the Messaging implementation should offer to a receiving party who is UP2.0 (or higher) not equipped with the plugin a link to install the plugin from the 'store'. This shall be done in a non-intrusive way.

R15-11-3 *The messaging client shall support the ability to send plugin-protected content between bi-directional plugins.*

R15-11-4 *Certain identifiable protected content which is plugin-specific shall not be stored or forwarded by the recipient using a UP2.0 (or higher) plugin-enabled client (i.e. the recipient needs to install the plugin themselves and fulfil any payment requirements associated with the content to send that plugin-enabled content).*

US15-12 **As a user, I want to have a seamless flow to invite my contact(s) to use a particular plugin that they have not installed (yet).**

R15-12-1 *If content of a bi-directional plugin is sent to a recipient who does not have the bi-directional plugin installed, then a generic placeholder of the plugin shall be displayed to the recipient offering an invite/link to install the plugin from any 'store' that facilitates the installation of that plugin.*

NOTE: If the recipient has no access to that plugin or plugin 'store' an appropriate message is expected to be displayed to the recipient.

US15-13 **As a user, I want to be able to find Plugins for installation within my Messaging implementation.**

R15-13-1 Plugins shall be discoverable for a user via a plugin ‘store’ that is accessible from within the Messaging interface.

R15-13-2 The service shall allow the RCS Service Provider to set a default plugin ‘store’ with the first-time provisioning or client re-provisioning for RCS.

NOTE: The Plug-ins that can be used by the client are the ones that are included in a configurable list of Plug-ins and not the Plug-ins that can be discovered in the default plug-in store.

R15-13-3 *The RCS Service Provider shall be able to add more available plug-in ‘stores’ to that list remotely.*

R15-13-4 *The user shall be able to add further plugin ‘stores’ to the existing default plugin ‘store’ by adding the plugin ‘store’ address. This should typically be offered within the Settings of the Messaging interface (see R18-17-3).*

R15-13-5 *The Messaging interface shall be able to open a plugin ‘store’ view which layout and content is defined and managed by each plugin ‘store’ provider.*

R15-13-6 *The user shall be able to close easily the plugin ‘store’ view to go back to the Messaging view.*

NOTE 1: Plugin store-specifics like payments for premium plugins, user ratings for plugins, descriptions, configuration options like which countries and networks are supported by a Plugin etc. are left to the implementation of each plugin ‘store’ provider.

NOTE 2: In order to access and download plugins from the ‘store’, the user has to accept the store’s terms and conditions.

R15-13-7 Once a Plugin is installed an update of that Plugin shall be possible without the need for updating the full Messaging application.

R15-13-7-1 *Each Plugin ‘store’ shall be able to notify users about the availability of a new version of an installed Plugin and to provide a seamless way for the user to confirm the installation of the update.*

R15-13-7-2 *Any update of a Plugin should also include an update of its configuration as required (e.g. whether a plugin can be used in 1-to-1 and/or Group conversations).*

R15-13-7-3 *The user shall be able to allow automatic updates for installed plugins if available (see R18-17-4 and sub-requirements).*

R15-13-8 The user shall be able to delete / uninstall plugins via the Messaging interface.

US15-14 **As a user, I want to use easy-to-use quality-approved Plugins that provide value-added services and respect my data privacy needs.**

R15-14-1 *The service shall allow the RCS Service Provider to whitelist the set of available plugin ‘stores’ that a user can select and set as preferred stores.*

R15-14-2 *The service shall facilitate the RCS Service Provider to block events sent via a Plugin on their network.*

NOTE: In case an RCS Service Provider has blocked the usage of a Plugin on their network, it has to be clarified based on the potential commercial agreement between the owner of the Plugin 'store' and the RCS Service Provider that the concerned Plugin is not offered to users of their network.

US15-15 **As an MNO and / or RCS Service Provider, I want to be able to monitor and track Plugin usage of my customers so that I can monetise value and prevent system abuse appropriately.**

R15-15-1 The service shall allow the MNO and the Plugin 'store' provider to track basic Plugin usage.

R15-15-2 It shall be possible to record the following accounting information on a per user basis:

R15-15-2-1 Number of Plugin installations; <total, active>;

R15-15-2-2 Number of events created with a specified Plugin (sent and received);

R15-15-2-3 Data volume transferred with a specified Plugin (sent and received);

R15-15-2-4 Number and billing details of events / transactions monetised within a Plugin interaction (sent and received).

NOTE: Monetisation of installations and transactions within a Plugin interaction are assumed to be handled through the Plugin 'store' provider which is expected to support both 3rd party payment and MNO payment methods.

US15-16 **As a user, I want a rich content experience within the Messaging conversation view.**

R15-16-1-1 Plugins shall be able to send a Rich Content Bubble that provides a single 'message bubble' based on a layout and content capability described below which provides the ability to integrate the following elements, each of which is optional within a Rich Content Bubble:

R15-16-1-2 *Text field, such as title, sub-title, description, total text length of max. 80 characters;*

NOTE: It is up to the client implementation how the text is styled.

R15-16-1-3 Image (i.e. not animated), potentially with transparent background;

R15-16-1-4 Animated image (with the ability to define how often an animation loop shall be repeated until stopped on last frame);

R15-16-1-5 Clickable link, to enable user to download associated plugin;

R15-16-1-6 *Action to open a 'full screen' view (full flexible and animated): the 'full screen' view shall leave screen space for the underlying Messaging implementation to indicate information about the conversation party / parties and to allow the user to close that 'full screen' view and return to the conversation view.).*

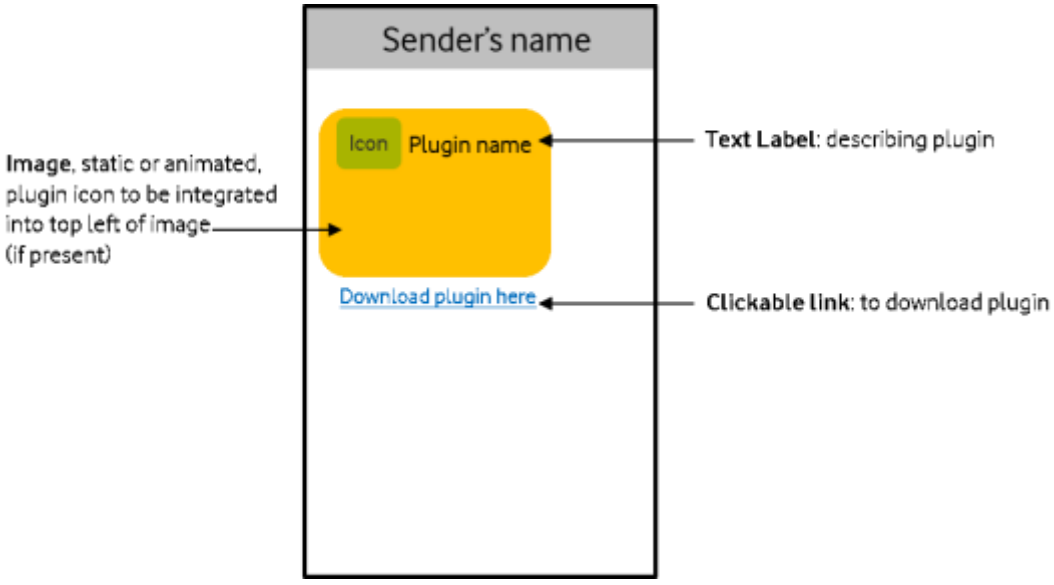


Figure 5: Example of a rich content bubble

R15-16-2 When plugin content contains an animation, the animation shall start automatically when visible within the conversation view and repeat until no longer visible within the view.

R15-16-3 RCS-specific delivery mechanisms shall apply to all Plugin-generated events (including new incoming event notifications, store and forward in case of recipient unavailability, sent message and file indications (for Chat and File Transfer related events), limitations configured by the RCS Service Provider for automatic file downloads, multi-device messaging).

R15-16-4 xMS fallback (NFS and CFS) for uni-directional plugin events should be made available.

R15-16-5 *xMS fallback (NFS and CFS) for bi-directional plugin events may be made available.*

R15-16-6 *xMS fallback content shall be determined by the plugin.*

15.3.1 Technical Realization

15.3.1.1 Overview

This section includes the technical procedures for Uni-directional Plug-ins.

Uni-directional Plug-ins shall generate content (or link to content) that can be retrieved and displayed by any client (RCS or non-RCS) regardless of the Plug-in being installed or not on the receiver. Depending on the Plug-in, the experience on the receiver may vary based on whether the Plug-in is installed or not.

The Uni-directional Plug-in service is provided based on the procedures described in section 3.2.8 of [RCC.07].

[RCC.07] allows Plug-ins to be discovered by retrieving a Catalog through a URL that is provided with the client configuration.

For the Uni-directional Plug-ins to be available, the CATALOG URI parameter defined in A.1.13 and A.2.4 of [RCC.07] shall be configured. The client can download Plug-ins that are listed in their Catalog using the store URL that is configured in their Catalog.

The generated Plug-ins content (or link to content) is transferred using Messaging services. The procedures for the Messaging service selection are covered in section 3.2.8.7.2 of [RCC.07]. Based on the selected Messaging service, the respective delivery procedures apply.

The procedures for bi-directional Plug-ins are not covered in this specification.

The solution involves device-local operations that are OS specific.

For Android™ devices, the procedures described in section B.3 apply.

15.3.1.2 Addresses Sharing Authorization

As part of the Plug-in to client communication, Plug-ins may receive addresses (e.g. for the Plug-in to identify the conversation). The addresses that the client can provide to the Plug-in vary depending on whether the Plug-in is eligible for receiving anonymised addresses or addresses in clear form.

15.3.1.2.1 Sharing anonymised addresses with the Plug-in

The Plug-ins that are included in the Catalog (see section 3.2.8.3.1 of [RCC.07]) are not authorized to receive any addresses in clear form from the client unless the conditions described in section 15.3.1.2.2 are met. The Plug-ins that are included in the Catalog are authorized to receive anonymised addresses. For the Plug-ins that are not authorized to receive addresses in clear form, the client shall only provide anonymised addresses. The anonymization function shall be implemented locally by the client.

15.3.1.2.2 Sharing addresses with the Plug-in in clear form

The client shall provide addresses in clear form towards Plug-ins that, when receiving addresses fall in one of the two categories described in the following sub-sections.

15.3.1.2.2.1 Asking the user consent for sharing addresses in clear form

For Plug-ins that need to acquire addresses in clear form by triggering client UX procedures asking for user consent, the client shall trigger the UX procedures upon detection of first Plug-in installation and once the user enters the client. The client shall provide to the Plug-in addresses in clear form only if the user provides their consent. The operations for requesting the user consent and sharing the addresses in clear form after the user has provided their consent (requested via client triggered UX procedures) are OS specific. For Android devices, the procedures are covered in section B.3.

15.3.1.2.2.2 Plug-in version(s) endorsed by the client

If the Plug-in does not indicate to the client to trigger UX procedures asking for user consent, the client shall provide the addresses in clear form for certain Plug-in versions only if they are endorsed to receive addresses in clear form by the client. The Plug-in endorsement procedures are OS specific. For Android devices, the procedures are covered in section B.3.

15.3.2 Technical Implementation of User Stories and Service Requirements

R15-17-1 Requirement R15-10-1 shall be implemented locally on the device.

R15-17-2 Requirement R15-10-2-1 shall be implemented based on the Plug-ins procedures defined in section 3.2.8 of [RCC.07]. For Android™ devices, the procedures defined in section B.3 shall be implemented.

R15-17-3 Requirement R15-10-3 shall be realised as described in section 3.2.8.6.2 of [RCC.07].

R15-17-4 Requirement R15-10-5 shall be implemented locally on the device based on OS specific procedures. For Android™ devices, it is based on the Plug-in descriptor described in section B.3.

R15-17-5 Requirement R15-10-5-1 shall be implemented locally on the device based on OS specific procedures. For Android™ devices, it is based on the value of the context of the CREATE_OBJECT action described in section B.2.

R15-17-6 Requirement R15-11-1 is fulfilled based on the sender procedures described in section 3.2.8.7 of [RCC.07]. For Android™ devices, the procedures described in B.3.7 also apply.

R15-17-7 Requirement R15-11-2 shall be implemented based on the procedures described in section 3.2.8.8 of [RCC.07]. For Android™ devices, the procedures described in B.3.7 also apply.

R15-17-8 For requirement R15-13-1, discoverable Plug-ins are based on a retrieved list of Plug-ins that is called Catalog. Plug-ins can be downloaded from the same or multiple stores based on the value of the store-url property set for each Plug-in.

R15-17-9 For requirement R15-13-2, the RCS Service Provider is able to configure the list of Plug-ins based on the procedures defined in 3.2.8.3 of [RCC.07].

R15-17-10 For requirement R15-13-7, the Plug-in updates are controlled by the applicable store.

R15-17-11 Requirement R15-13-8 is implemented locally on the device based on OS specific procedures. For Android™ devices, the procedures related to DELETE action described in Annex B.3.4 and B.3.6 apply.

R15-17-12 Requirement R15-15-1 is implemented based on the monitoring mechanisms implemented on the client and the applicable Plug-in store providers.

R15-17-13 Requirement R15-15-2-1 is implemented based on the monitoring mechanisms implemented on the client and the configured Plug-in stores.

R15-17-14 Requirements R15-15-2-2 and R15-15-2-3 is fulfilled for CPIM messages based on the new CPIM header Plug-Info defined in 3.2.8.6.2 of [RCC.07]. For Plug-in events transferred over SMS or MMS, they are based on monitoring mechanisms of the underlying technology.

R15-17-15 Requirement R15-15-2-4 is based on commercial agreements between the Plug-in provider, the RCS Service provider (i.e. Catalog provider) and the store

provider where the Plug-in is published. Technical procedures for billings and payments are outside of scope.

R15-17-16 Requirements R15-16-1-1, R15-16-1-3, R15-16-1-4 and R15-16-1-5 are implemented locally on the device based on OS specific procedures. For Android™ devices, Rich Content Bubble data are transferred using the messaging service (with a link) or file transfer service. The Rich Content bubble experience is possible between clients with the Plug-in installed. When the Plug-in is not installed, the user sees a link with text (when transferred using messaging service) or image (when transferred using file transfer).

NOTE: If the bubble contains a Plug-in specific view and the Plug-in supports the action VIEW, when the user clicks on the bubble the Plug-in will show a custom full screen view displaying the content (see Annex B.3.6.1.1).

R15-17-17 Requirement R15-16-2 is implemented locally on the device.

R15-17-18 Requirement R15-16-3 is fulfilled based on the Service selection and delivery procedures described in section 3.2.8.7.2 of [RCC.07].

R15-17-19 Requirement R15-16-4 is based on the xMS fallback procedures of the underlying selected Messaging service.

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, client verification, 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 Client authenticity verification

Section 2.11 of [RCC.14] describes generic procedures to allow a HTTP Configuration Server to verify the authenticity of the client requesting to be configured. This document defines the use of those procedures for verifying the client authenticity and the general trustworthiness of the platform on which the client is running for the following OS platforms:

- The Android™ OS using the procedures defined in section B.2.

Clients running on a platform for which these procedures have been defined shall support them. Networks receiving configuration requests from clients that support the procedures to verify the client authenticity should invoke them provided that they have sufficient information on the client to verify the results that are provided.

16.3.2 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 where client authenticity is not verified as defined in section 16.3.1).

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. RCS Service Providers 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.

16.3.3 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.

16.3.4 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.

16.3.5 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.

16.3.6 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.

In addition to interface specific authentication methods, the RCS Service Provider may extend a security context that has been generated by a common authentication endpoint to

interfaces using HTTP as access protocol using the single-sign on procedures of Open ID Connect, (OIDC) see section 2.12.2 of [RCC.07].

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 fallback 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. Support of OIDC single-sign-on is mandatory.	
Service Provider Client Configuration Configuration Over non 3GPP networks	Support of OTP based authentication is mandatory. Support of GBA authentication is mandatory. Support of OIDC single-sign-on 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. Support of OIDC single-sign-on is mandatory.	
Message Store Server Authentication	Support of plain password authentication is mandatory. Support of GBA based authentication is mandatory. Support of OIDC single-sign-on is mandatory	

Table 24: 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 as defined in [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 fallback to OTP based authentication is mandatory. Support of security configuration mechanism over PS and support of SMS port zero policy is mandatory. Support of OIDC single-sign-on 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. Support of OIDC single-sign-on 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. Support of OIDC single-sign-on is mandatory.
Message Store Server Authentication	Same as device that provides the terminal API	Support of plain password authentication is mandatory. Support of OIDC single-sign-on is mandatory.

Table 25: Authentication Mechanisms for non-embedded clients on primary device

16.3.7 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 2.7 and 2.5 of [RCC.14] respectively. The network based user authentication may be replaced or extended on RCS Service Provider request by the OTP based user authentication (see R16-4-4) as defined in section 2.5 and 2.6 of [RCC.14]. The authentication mechanism is negotiated between client and server as defined in [RCC.14]. In addition, single sign-on using the procedures of Open ID Connect is supported as defined in section 2.8 of [RCC.14].

R16-4-5-3 As defined in section 2.5.3 of [RCC.14] the RCS 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 RCS Service Provider by enforcing user input of the OTP as defined in section 2.6.4 of [RCC.14] or in section 2.8 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 2.5.3 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 2.6, 2,7, 2.8, 2.9 and 2.10 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 2.5.3 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 2.12.1.2 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 2.7 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 3.2.5.4.1 of [RCC.07]. In addition, single sign-on using the procedures of Open ID Connect is supported as defined in section 2.12.2

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 3.2.5.6 of [RCC.07].

R16-4-5-11 The authentication methods for the Common Message Store are described in section 2.12.3 of [RCC.07]. In addition, single-sign on using the procedures of Open ID connect is supported as defined in section 2.12.2 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 RESTful sessions are encrypted over HTTPS as defined in section 2.7 of [RCC.07].

R16-4-5-13 For MSRP transactions, 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 2.7 of [RCC.07] and 2.2.2.2 of [RCC.15].

R16-4-5-14 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.

R16-4-5-15 The encryption of RTP streams is determined by client configuration as defined in section 2.7 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 2.5 of [RCC.14] is transparent for the user if the RCS 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 2.6 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 RCS Service Provider policy to enforce user prompts for OTP as defined in section 2.6.2 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 2.6 of [RCC.14] requires user prompt for MSISDN and RCS Service Provider indication on the additional device. In addition, the user may need to enter an OTP or a PIN as defined in section 2.9.1 of [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 2.9.1 of [RCC.14] is "out-of-band".

The user interaction for the federation consent on a primary device via the external EUCR as defined in section 2.1.2 of [RCC.15] is "in-band".
The user interaction for the input of a PIN on the primary device as defined in section 2.1.2.2 of [RCC.15] is "in-band".

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 RCS Service Provider as defined in section 2.5.3 and 2.6 of [RCC.14].

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 RCS Service Provider responsibility to maintain this user identity and the related authentication, permission and preference data in synchronisation 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 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 26.

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’.

R17-1-5 Availability of technologies / bearers shall be configured by the RCS Service Provider independently whether the conversation is with another person / group of persons or a Chatbot.

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**
Interactive In-Call services	**Configurable**	**Configurable**
ViLTE (IR.94)	**Configurable**	**Configurable**
Provisioning	**Configurable**	**Configurable**
PS data/Internet Access	**Always off**	**Always off**

Table 26: 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 2.8.1.4 of [RCC.07] the complete behaviour is applicable via the Data Off functionality defined in section 2.8.1.5 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 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 RCS 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 26, 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 26 is implemented by the configuration parameters MMTEL_voice_exempt, MMTEL_voice_exempt_roaming, SS_ _config_exempt and SS_XCAP_config_exempt_roaming as defined in [PRD-IR.92] (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 SGs. In accordance with the requirement for SMS in Table 26, 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 26, the MNO capability to disable/enable SMS over IP is implemented by the configuration parameters SMSoIP_exempt and SMSoIP_roaming_exempt as defined [PRD-IR.92] (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 26, the MNO capability to disable/enable MMS is implemented by the configuration parameter MMS DATA OFF defined in section A.1.14 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 26 is implemented by the configuration parameter RCS MESSAGING DATA OFF defined in section A.1.14 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 26 is implemented by the configuration parameter FILE TRANSFER DATA OFF defined in section A.1.14 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 26 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 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 26 is implemented by the configuration parameter CONTENT SHARE DATA OFF defined in section A.1.14 of [RCC.07].

R17-2-11 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 26 is implemented by the configuration parameters MMTEL_video_exempt and MMTEL_video_exempt_roaming as defined in [PRD-IR.94] (covering R17-1-1-10).

R17-2-12 Operator Provisioning over 2G, 3G, 4G networks refers to the configuration procedures as defined in section 2.3 of [RCC.07], the initial catalog retrieval and refresh for Plug-ins as defined in section 3.2.8.3.2 of [RCC.07] and the configuration for Chatbots requiring specific management as defined in section 3.6.3.3 of [RCC.07]. The MNO capability to disable/enable Operator Provisioning as required in Table 26 is implemented by the configuration parameters "Device Management over PS data off exemption" and "Device Management over PS data off roaming exemption" as defined in section 6.2 of [RCC.14] and section A.1.14 of [RCC.07] (covering R17-1-1-11).

R17-2-13 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.1.14 of [RCC.07].

R17-2-14 For R17-1-2, this shall be realised through the use of the client configuration parameters defined in section A.1.14 of [RCC.07] and section 6.2 of [RCC.14] that provide separate settings to control the roaming and the on-net behaviour.

R17-2-15 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.1.14 of [RCC.07] and section 6.2 of [RCC.14].

18 RCS Settings

18.1 Description

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 RCS Service Provider 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: ‘An 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).

NOTE: The Master Switch is marked accordingly to inform the user what the effect of enabling / disabling RCS services is, e.g. enhanced messaging and call services, but other services such as VoLTE are not affected by the Master Switch.

US18-2 **As a user, I want to be able to set and change a Group Chat Alias.**

R18-2-1 The user shall have the option to customise the name label which is presented during RCS Group Chats to participants for whom the user is not in the contact list.

R18-2-2 The support of RCS Alias shall be configurable for the RCS Service Provider.

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 **As an Integrated Messaging 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 RCS Service Provider 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 sounds for incoming Chatbot events (that can be distinguished from Notifications in a P2P communication context)
- Notification preferences
- Customised ringtones (for Voice calls or IP Video)

- Visual customisation for chat (for example fonts, bubble styles, backgrounds etc.). NOTE: For Chatbot conversations, customization may be limited depending on the implementation.

R18-6-4 The user shall be able to mute selected conversations with Chatbot services so that these do not trigger notification sounds irrespectively of the settings in R18-6-3.

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 RCS Service Provider.

R18-7-2 The default for this setting shall be configurable by the operator.

R18-7-3 The user shall be able to change this setting on a per-conversation basis in a conversation specific setting. This shall be possible for any conversation, including conversations with persons and conversations with Chatbot services.

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.

R18-15-7 Exception: In case of any Critical Chatbots, the UI shall not offer the option to block this Chatbot.

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.

US18-17 **As a user, I want to control settings for Chatbots and Plugins.**

R18-17-1 void.

R18-17-2 void.

R18-17-3 *The user shall be able to add one or more Plugin Stores to the list of available Plugin Stores.*

R18-17-4 The user shall be able to allow automatic updates for installed Plugins.

R18-17-4-1 The default setting for cellular connectivity shall be 'off'.

R18-17-4-2 The default value for Wi-Fi connectivity shall be 'on'.

R18-17-5 The user shall be able to control the sharing or withholding (i.e. 'share' vs. 'do not share') of their personal information as detailed below on a per Chatbot basis. The user's personal information shall include:

R18-17-5-1 The user's MSISDN as the identifier for a conversation with a Chatbot. If the user does not share the MSISDN, then the conversation is anonymous. This setting shall be available per each Chatbot conversation. (Default setting: 'do not share')

R18-17-5-2 *The user's Geolocation information. (Default setting: 'do not share')*

R18-17-5-3 The sending of "Displayed" Message Status Notification in response to received Chatbot messages. This setting shall be available per each Chatbot conversation. (Default setting: as set in the related setting, see US18-7 and related requirements).

R18-17-6 *The user shall be able to maintain (including adding and removing) a list of Chatbots that are authorized to pro-actively contact the user (whitelisting) (see R15-5-1).*

R18-17-6-1 *The MNO or RCS Service Provider shall be able to pre-fill this list with Chatbots as part of the device configuration process.*

R18-17-7 The user shall be able to block/unblock Chatbots from a Chatbot blacklist setting.

R18-17-8 The user shall be able to maintain (including delete / uninstall) a list of installed Plugins on their device (see R15-13-8).

R18-17-9 *The user shall be able to maintain (including adding/removing) a list of preferred Plugin-Stores (see R15-14-1).*

R18-17-10 The user shall be able to allow "Enriched Chatbot search". The default setting for this shall be operator configurable. This setting shall impact the features described in R15-4-3-1 and R15-4-3-2.

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

R18-18-1 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.

R18-18-2 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 [RCC.07] 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 send a HTTP client configuration request only if the current configuration XML document includes settings for services that are not affected by the “Master Switch” (e.g. VoLTE). In such a HTTP client configuration request the client shall set the "rcs_state" parameter defined in [RCC.07] to "-4". If all services included in the current configuration XML document are affected by the “Master Switch”, the client shall not send a HTTP client configuration request. In all cases, the client shall keep the configuration data for services affected by the “Master Switch” 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 [RCC.07] to the version of the configuration XML document corresponding to the locally stored client configuration.

- If the user changes the value of the "Master Switch" from "ON" to "OFF" and the client is not registered for VoLTE/VoWiFi then it shall terminate existing sessions and cancel existing requests for RCS services. Otherwise, the client shall terminate existing sessions and cancel existing requests only for services other than IP Voice Calls and IP Video Call and SMS over IP (see also section 2.8.1.4 of [RCC.07]).

- If the user changes the value of the "Master Switch" from "ON" to "OFF" and the client is registered for VoLTE/VoWiFi and the client is configured to share a registration between RCS and Multimedia Telephony, then the client shall re-register in IMS with only the relevant ICSI and feature tags of [PRD-IR.92], [PRD-IR.94] respectively. Otherwise, the client shall de-register from the IMS for the registration related to the RCS services.

- 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 according to section 2.4.1 of [RCC.07] 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 4.1.11.8 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.

R18-18-3 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 2.5.3.4 of [RCC.07].

R18-18-4 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 RCS Service Provider has activated the IP Voice Call on the device via the configuration parameter Media_type_restriction_policy defined in section B.3 of [PRD-IR.51] to enable Voice over EPC-integrated Wi-Fi and the RCS 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 RCS Service Provider see section 10.3.

R18-18-5 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.

R18-18-6 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.

R18-18-6-1 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.

R18-18-6-2 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.

R18-18-7 The requirements for user story US18-6 shall be implemented locally on the device.

R18-18-8 Requirement R18-7-1 shall be implemented in accordance with the DISPLAY NOTIFICATION SWITCH client configuration parameter defined in section 5.3.4.1. When display notification is supported by the RCS 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”.

R18-18-9 When display notification is not supported by the RCS 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

R18-18-10 The configuration parameters for automatic acceptance of File Transfer of US18-8 shall be implemented locally on the device. The parameters shall overwrite the RCS 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.

R18-18-11 The requirements for user stories US18-9 to US18-12 shall be implemented locally on the device.

R18-18-12 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 5.3.4.1 shall be set.

R18-18-13 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 7.3.2.1 shall be set.

R18-18-14 The technical implementation of the requirements of user story US18-15 shall be implemented as follows:

R18-18-14-1 The client shall manage a client local list of originator addresses being subject to blacklisting. If the user adds a Chatbot to the client local list of originator addresses, then the Chatbot service identifier as defined in section 2.5.4.1 of [RCC.07] shall be used. The user shall only add a Chatbot whose URI does not match an URI of the list of critical Chatbots URIs as defined in section 3.6.11 of [RCC.07] (fulfilling R18-15-7).

R18-18-14-2 The client procedures for capability discovery are not impacted by blacklisting.

R18-18-14-3 The client shall reject an incoming SIP INVITE request with a SIP 486 Busy Here response, if the originator address matches a Chatbot service identifier contained in the client local blacklist. The user shall not be notified.

R18-18-14-4 Otherwise, for sessions and messages related to Standalone Messages as per section 3.2.2 of [RCC.07] or 1-to-1 Chat as per section 3.2.3 of [RCC.07], the client shall accept an incoming session request, if the originator address is contained in the client local blacklist. The client shall perform the procedures for reception of the message as defined for the corresponding service, including the procedures for delivery reporting. The client shall not notify the user and discard the incoming message. As a consequence, the client procedures for the processing display notification is not applicable for the relevant incoming messages.
For File Transfer, Audio Messaging and Geolocation Push received in a 1-to-1 Chat session or via Standalone Messaging, the client shall apply the procedure for the transport message as defined in R18-18-14-3. For File Transfer or Audio Messaging the client shall not invoke the file download procedure, i.e. not attempt to download the thumbnail or the file from the File Transfer content server.

R18-18-14-5 To satisfy the requirement R18-15-6 the client shall not screen received session invitations for Group Chat or chat messages received in a Group Chat session for originator addresses contained in the local client blacklist.

R18-18-14-6 To satisfy the requirements of R18-15-5, if the client receives an incoming call request for a voice or video call from an originator 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.

R18-18-14-7 For Enriched Pre-Call and Post call services; if the client receives a session invitation for an RCS Enriched Calling session from an originator 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 and discard the received elements.

R18-18-14-8 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.

R18-18-14-9 For MMS messages, if the client receives a MMS Notification from an originator address contained in the client local blacklist, the client shall confirm the MMS Notification, shall stop processing of the MMS transaction and shall not notify the user.

R18-18-14-10 The processing of client originated messaging and call handling is not impacted by the client local blacklist of originator addresses.

R18-18-15 The technical implementation of the user story US18-16 shall be implemented locally on the device.

R18-18-16 Requirement R18-17-3 shall be realised locally on the device

R18-18-17 For requirement R18-17-4 and its sub-requirements, the settings for Plug-in updates are those for applications provided by the applicable application store from which the plugin was obtained.

R18-18-18 For requirement R18-17-5, this shall be realised locally on the device

R18-18-19 For requirement R18-17-5-1, this shall be the setting to control the sharing of the MSISDN which shall trigger the sending of the Privacy Management commands described in section 3.6.5.1.2 of [RCC.07] as defined in section 15.2.1.

R18-18-20 Requirement R18-17-5-3 shall be realised locally on the device.

R18-18-21 Requirement R18-17-7 shall be realised through the client local blacklist as defined in section 3.6.6 of [RCC.07]

R18-18-22 Requirement R18-17-8 shall be realised locally on the device.

R18-18-23 Requirement R18-17-10 shall be implemented based on the procedures described in section 3.6.3.1 of [RCC.07]. The default setting shall be configured based on the ALLOW ENRICHED CHATBOT SEARCH DEFAULT parameter defined in section 15.2.1.2.

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 has the capability to make and / or receive phone calls under its own identity, this capability may or may not be affected by the federation with a primary device, depending on the individual operator implementation (using the native phone capability or a pre-installed / download app as the secondary interface on that 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) *and may be deployed by a Service Provider*:

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).*

R19-2-1-4 *It shall be at RCS Service Provider discretion to offer this configuration or not.*

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 should 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 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 *RCS Enriched calling services shall be available across all devices that are Enriched Calling capable for outgoing calls.*

R19-3-4 *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 MDV² settings.**

NOTE: *Any potential suspension of MDV² calling service does not affect any other calling service on a particular device*

R19-5-1 *It shall be possible to suspend the MDV² services on a secondary device for that particular secondary device.*

R19-5-2 *It shall be possible to remotely suspend MDV² 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).*

R19-5-6 *As a user, I want to transfer calls from one device to another federated device.*

R19-5-7 *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: To initiate the call transfer, the user shall be able to either 'push' the call from the device currently active in the call to another federated device or 'pull' the call from another federated device which is at that very moment not active in the call.

R19-5-8 *In-Call sharing content shall be accessible on the device that carries the call.*

R19-5-9 *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.*

R19-5-10 *As an MNO, I want my MDV² service to be in line with local regulations.*

R19-5-11 *All federated device shall support emergency calls (including actual calling device location).*

R19-5-12 *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 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
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

Emoticons	Character sequences	Examples describing graphical renditions
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
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.2 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 complies the latest Unicode Standard, available from

http://www.unicode.org.

A.3 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 6: Maximum zoom out (device in portrait mode)

Figure 7: 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 8: Navigation options when fully zoomed out

Figure 9: 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 OS/Platform Specific Functionality

B.1 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.1.1 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 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 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.1.2 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 27: Android™ RCS client Manifest meta-data properties

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 28: 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:

[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.

<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.

B.2 Android™ Client Authenticity Verification Procedure

NOTE: The procedure for Android™ is for further study.

B.3 Plug-ins on Android™ OS

B.3.1 Plug-ins manager

In order to properly encapsulate the Plug-ins logic and related implementation the concept of a **Plug-ins manager** component is introduced and used here. As good practice the RCS Client implementer should use an Android™ library module for this Plug-ins manager.

The Plug-ins manager contains the necessary primitives needed to discover, enumerate and interact with installed Plug-ins.

The same modularity concept can be applied on the android application that acts as a Plug-in: also in this case a Plug-in manager library is used to encapsulate the Plug-ins related logic and implementation.

B.3.2 Interaction model

On Android™ a Plug-in is always encapsulated in an Android application which uses the binary apk format. The Plug-in developer can build headless Plug-ins (no icon in the app drawer) or expand existing Android apps which become Plug-ins and do publish one or more entry points in the RCS Client.

An Android app can contain one or more Plug-ins. These are described in the Plug-in descriptor.

The interaction between the consumer (RCS Client) and an existing Plug-in-app is loosely coupled. A consumer triggers a certain action, which will be honoured by a Plug-in if installed. A Plug-in can serve more than one consumer.

The consumer and Plug-in applications are never bound to each other. For this reason the typical client/server model (AIDL in android™) is avoided.

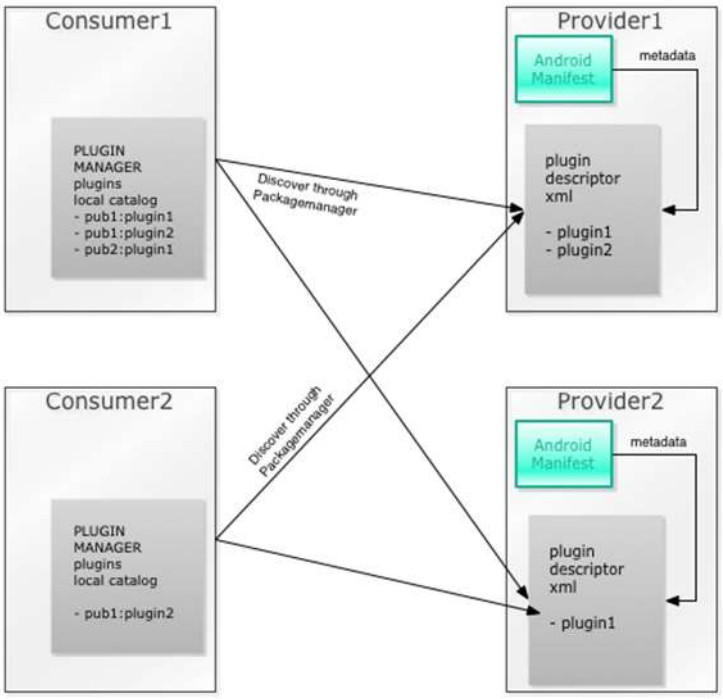


Figure 10: Plug-in model on Android™

B.3.3 Local Discovery

In the following procedures the term “Consumer” is used to indicate the Plug-ins implementation in the RCS Client while the term “Provider” is used to indicate the Plug-in implementation of the Android™ application containing a (or multiple) Plug-in.

B.3.3.1 Enumeration procedure for the consumer

The RCS Client shall perform an enumeration of all available Plug-ins. The result of this enumeration is the **local Plug-ins catalog** which contains and maintains the metadata of each Plug-in along with the supported actions.

The enumeration requires scanning all installed apps via the Android™ package manager and verifying if the app presents a Plug-ins descriptor resource.

In particular:

A consumer which is started on an Android™ device, shall next to the other client behaviour also perform following actions:

- Retrieve the list of installed applications from the PackageManager, and identify existing Plug-in-apps by looking for the meta-data property named "gsma.plugins.descriptor", as defined in the next section.
- For every Plug-in-apps that are found, the client shall open the descriptor xml indicated in the found meta-data property value.
- Each opened plugins-descriptor shall be parsed to verify the necessary conditions to become part of the local catalog.

- A descriptor shall be ignored and discarded if the Plug-in application version (xml element gsma:pluginappversion) is higher than the Plug-in application version of the client. The Plug-ins application version defined in this version is “1”
- The descriptor shall be ignored and discarded if it does not contain at least one Plug-in where the element gsma:type has value type “msgobjecthandler”.
- For each valid (type=”msgobjecthandler”) Plug-in xml section an entry shall be created in the local catalog.
- The client shall then parse each Plug-in section in the descriptor to populate each catalog entry.
- The catalog entry for each Plug-in shall maintain the meta-data information (label, icon, description) along with the supported actions.

B.3.3.1.1 Tracking un/installation of Plug-in-apps

The consumer shall setup a BroadcastReceiver that is listening to the Package manager installation events:

- the consumer shall react to the intent **ACTION_PACKAGE_ADDED** to detect if a new app is installed by the user (via the catalog configured store or side-loading). The consumer shall verify the new app for the presence of a descriptor. If a descriptor is present the procedure described above shall be repeated.
- The consumer shall listen and capture the event **ACTION_PACKAGE_REMOVED** to detect if an application is uninstalled by the user. In case the app had one or more entries in the local catalog then the consumer shall remove the corresponding entries in the local catalog and update the UI entry points to remove the entry-points (if any) belonging to the removed Plug-in-app.
- The consumer shall listen and capture the events **ACTION_PACKAGE_REPLACED** and **ACTION_PACKAGE_CHANGED** to detect if an application has been updated or reconfigured. In case the app had one or more entries in the local catalog then the consumer shall remove the corresponding entries in the local catalog and update the UI entry points to remove the entry-points (if any) belonging to the removed Plug-in-app. If the changed app has a valid plugin-descriptor then the parsing procedure described above shall be repeated for the updated application.

B.3.3.2 Local Catalog and Network Catalog whitelisting

The Client needs to maintain a local catalog of the enumerated Plug-ins already installed on the device. This local catalog shall keep all relevant Plug-in information (mime-types, actions etc.) but also a status if the Plug-in is enabled (usable by the user). The network catalog described in 3.2.8.3.1 of [RCC.07] acts as a whitelist over this local catalog. Only Plug-ins present in the catalog are allowed to function i.e. are enabled in the local catalog.

B.3.3.3 Enumeration discoverability for the provider

An application that wants to become a Plug-in shall have a specific metadata property in its manifest Manifest.xml:

Name	Resource	Description
gsma.plugin.descriptor	Pointer to Android™ resource	Points to the descriptor resource

The following example illustrates the meta-data that shall be added to the Manifest.xml file (manifest excerpt):

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

        <!-- the following meta-data is used to identify the plugin descriptor resource -->
        <meta-data android:name="gsma.plugin.descriptor" android:resource="@xml/gsma_plug-in"/>

…….
```

Table 29: Android descriptor pointer

The descriptor shall declare the Plug-ins that are available inside the application. Each Plug-in section shall also state the supported actions.

B.3.4 Plug-in descriptor

The Plug-in descriptor shall be embedded in every Android™ application in order to declare the presence one or more Plug-ins in the app.

The descriptor root structure is presented in the table below:

```
<?xml version="1.0" encoding="UTF-8"?>
<plug-in-provider xmlns:android="http://schemas.android.com/apk/res/android"
   xmlns:gsma=http://schemas.gsma.com/plug-ins>
   <gsma:pluginappversion value=”1”/>
   <plug-in
      gsma:pluginid=”com.example.package#exampleplugin"
      android:name="com.gsma.plugin.provider.MyPluginProviderService"
      android:label="@string/plugin_name"
      android:versionCode="100"
      android:versionName="1.0"
      android:icon="@drawable/plugin_icon
      gsma:description="@string/plugin_description"
      gsma:disclaimer="@string/plugin_disclaimer"
      gsma:type="msgobjecthandler" >
      <actions>
       ....
      </actions>
    </plug-in>
     ……
   <plug-in
   </plug-in>
   <endorsements>
      ……
   </endorsements>

</plug-ins-provider>
```

Table 30: Android Plug-in descriptor root structure

This subtree is formally defined as follows:

Node: /plug-in-provider

All Plug-ins are declared under this root node.

Status	Occurrence	Format
Required	One	node

Table 31: Android Plug-in descriptor root structure

- Values: N/A

Node: /plug-in-provider/gsma:pluginappversion

This leaf declares the Plug-in application version which the Plug-in app uses.

Status	Occurrence	Format
Required	One	Int

Table 32: Plug-in app version leaf node

- Values: 1 (Plug-in application version is “1” for this version of this document)

Node: /plug-in-provider/plug-in

This node is the declaration container for a single Plug-in

Status	Occurrence	Format
Required	OneOrMore	node

Table 33: Plug-in node

- Values: N/A
- Attributes:
    - **android:name** is the fully qualified name of the class that implements the Android™ service which receives the action intents.
    - **android:label** points to the localized label that is displayed to the user under this entry point.
    - **android:versionName** can be used by the Client to display a version in readable format.
    - **android:versionCode** is representing the version of the Plug-in as usual for Android executables.
    - **android:icon** OPTIONAL, can be used to override the icon. If defined it overrides the icon defined in the Android™ application icon.
    - **gsma:pluginid** is the unique ID of the Plug-in defined in section 3.2.8.4 of [RCC.07].
    - **gsma:description** OPTIONAL, can be used by the client to provide further readable information about the Plug-in.
    - **gsma:disclaimer** OPTIONAL, can be used to provide a human readable disclaimer.

- **gsma:type** this declared the Plug-in type. Only one type is currently defined. The mandatory value is “msgobjecthandler”.
- **gsma:addressesPrivacy** indicates if the Plug-in needs the user addresses in clear form i.e. not anonymized. If not indicated then the value is by default anonym. If set to “clear” and there is no endorsement document then the Client shall trigger the appropriate consent that grants the permission to receive addresses in clear form.

Node: /plug-in-provider/plug-in/actions

This node is the declaration container for all actions supported by the Plug-in.

Status	Occurrence	Format
Required	One	node

Table 34: Actions node

- Values: N/A

Node: /plug-in-provider/plug-in/actions/action

Node that declares a supported action

Status	Occurrence	Format
Required	OneOrMore	node

Table 35: Single Action node

- Values: N/A
- Attributes:
  - **android:name** OPTIONAL, can be used to override the class name of the service that receives the intent. If defined it overrides the class name specified in the “plugin” node.
  - **android:label** OPTIONAL, can be used to override the label. If defined it overrides the label specified in the “plugin” node.
  - **android:icon** OPTIONAL, can be used to override the icon. If defined it overrides the already defined icon.
  - **gsma:type** this is the actual declared action. Possible values are:
    - VIEW (optional)
    - GET_TEMPLATE_VIEWS (optional)
    - DELETE (optional)
    - OBJECT_RECEIVED
    - CREATE_OBJECT

Node: /plug-in-provider/plug-in/actions/action/mimetype

Leaf node that declares a mime-type. This node is applicable only to the CREATE_OBJECT action type.

The list of declared mime-type shall be in order of priority as desired by the Plug-in implementer.

At least the mime-type text/plain shall be declared among the list.

Status	Occurrence	Format
Required	OneOrMore	Empty Node

Table 36: mime-type for CREATE_OBJECT

- Values: N/A
- Attributes:
  - **gsma:mimetype** contains the definition of a mime-type that the Plug-in can produce when the action CREATE_OBJECT is invoked.

Node: /plug-in-provider/plug-in/actions/action/context

Leaf node that declares the UX context in which the action is applicable. This node is applicable only to the CREATE_OBJECT action type.

Status	Occurrence	Format
Required	ZeroOrMore	Empty Node

Table 37: context for CREATE_OBJECT

- Values: N/A
- Attributes:
  - **gsma:name** contains the name of the UX context. Can be “1to1” or “group”.

Node: /plug-in-provider/plug-in/actions/action/text-regexp

Leaf node that declares the UX context in which the action is applicable. This node is applicable only to the OBJECT_RECEIVED action type.

Status	Occurrence	Format
Required	ZeroOrMore	Empty Node

Table 38: text-regexp for OBJECT_RECEIVED

- Values: N/A
- Attributes:
  - **gsma:name** contains the regular expression (java syntax) that is used to parse a chat message and recognize it as belonging to the Plug-in.

Node: /plug-in-provider/endorsements

This node is the declaration container for all endorsements received by the Plug-in.

Status	Occurrence	Format
Required	ZeroOrOne	Node

Table 39: Endorsements node

Node: /plug-in-provider/endorsements/endorser

Leaf node that declares the signature of an endorser for the provided endorsement xml.

Status	Occurrence	Format
Required	ZeroOrMore	Empty Node

Table 40: Endorser leaf node

- Values: SHA256 based signature of the endorsement xml generated by the endorser using his private endorsement key. The Client shall have the public endorsement key of the endorser in order to proceed with the signature verification.
- Attributes:
  - **gsma:name** name of the endorser entity. Used by the Client to look for the public endorsement key.
  - **Hash** hashing algorithm used for the signature. Defined as “SHA256”.

B.3.4.1 Full descriptor example

```
<?xml version="1.0" encoding="UTF-8"?>

<plugin-provider xmlns:android="http://schemas.android.com/apk/res/android"
   xmlns:gsma="http://schemas.gsma.com/plugins" >

   <gsma:pluginappversion value="1"/>

   <plugin
      gsma:pluginid=”com.example.package#exampleplugin"
      android:name="com.gsma.plugin.sample.MyPluginService"
      android:label="@string/plugin_name"
      android:icon="@drawable/plugin_icon"
      android:versionCode="10100"
      android:versionName="1.1.0"
      gsma:description="@string/plugin_description"
      gsma:disclaimer="@string/plugin_disclaimer"
      gsma:type="msgobjecthandler"
      gsma:addressesPrivacy=”clear”>
      <actions>
         <action gsma:type="VIEW" />
         <action gsma:type="DELETE" />
         <!-- Sample of using an alternative Service for an action -->
         <action
            android:name="com.gsma.plugin.sample.MyPluginTemplateService"
            gsma:cacheExpirationTime="30"
            gsma:type="GET_TEMPLATE_VIEW" />
         <!-- Sample of using an alternative icon for an action -->
         <action
            android:icon="@drawable/plugin_create_object_icon"
            gsma:type="CREATE_OBJECT" >
            <!-- List of supported mimetypes -->
            <mimetype gsma:mimetype="image/png" />
            <mimetype gsma:mimetype="text/plain" />
            <!-- Plugin entry point shall be shown in single-user chats -->
            <context gsma:name="1to1"/>
            <!-- Plugin entry point shall be shown in multi-user chats -->
            <context gsma:name="group"/>
         </action>
         <action gsma:type="OBJECT_RECEIVED" >
            <!-- The following regex recognizes messages containing HTTP URLs from sampledomain.com -->
            <text-regexp gsma:name="^(.*):\\s+(http|https)\\:\\/\\/sampledomain.com\\/[^\\s]+$" />
         </action>
      </actions>

   </plugin>

   <!-- any other plugin could be declared here by adding a new plugin tag -->
   <endorsements>
      <endorser gsma:name=”Vodafone Group” hash=”sha256”>
a9993e364706816aba3e25717850c26c9cd0d89d</endorser>
   </endorsements>

</plugin-provider>
```

Table 41: Complete Android™ Plug-in Descriptor example

B.3.5 Communication between the Client and the Plug-ins

B.3.5.1 Client

The communication between the Client and the Plug-in is based on standard Android Intents.

In order to execute an action the Client shall prepare an Intent and call startService(), depending on the action type (see Actions).

The intent target component shall be the one declared in the android:name attribute of the action or if not present the android:name attribute of the plugin node.

In order to receive the result from the action execution the intent shall contain also a ResultReceiver with the extra key “action_extra_result_receiver”. The Plug-in will use this to provide a result related to the action.

```
public boolean createObject(Context context,
                String pluginPackageName,
                String pluginServiceName,
                String pluginID,
                final String clientObjectId,
                String[] supportedMimetypes,
                String senderId,
                String receiverId,
                Handler resultHandler) {
  //create an Intent with the desired action
  Intent intent = new Intent(ACTION_CREATE_OBJECT);
  //set Intent component to use the specific application and service to handle it
  intent.setComponent(new ComponentName(pluginPackageName, pluginServiceName));
  //set specific plugin id
  intent.putExtra(EXTRA_PLUGINID, pluginID);
  //create a result receiver here to prevent spoofing of createObjectId
  ResultReceiver resultReceiver = new ResultReceiver(resultHandler) {
    @Override
    protected void onReceiveResult(int resultCode,
                        Bundle resultData) {
      switch (resultCode) {
        case RESULT_OK:
          //create object completed succesfully, take resultData and send it
          //probably, the implementation will make use of the clientObjectId
          break;
        default:
          //a problem has occurred, notify the user
      }
    }
  };
  intent.putExtra(EXTRA_RESULT_RECEIVER, resultReceiver);
  //add sender and receiver
  if (senderId != null) {

    intent.putExtra(EXTRA_SENDER, senderId);

  }
  if (receiverId != null) {
    intent.putExtra(EXTRA_RECEIVER, receiverId);
  }
  //add the list of supported mimetypes
  intent.putExtra(EXTRA_SUPPORTED_MIMETYPES, supportedMimetypes);
  //data is not really used by the plugin, it's here just to be sure that the receiver service will always be called
  //type, instead, is used to retrieve the client packageName
  intent.setDataAndType(Uri.parse(ExtensionsManager.EXTENSION_PREFIX +
            ":" + pluginID + "/" + ACTION_CREATE_OBJECT + "/"
```

```
            + SystemClock.elapsedRealtime()),
        "package:" + context.getPackageName());

    //beware of any exception thrown by the system in the calling method
    return (context.startService(intent) != null);
}
```

Table 42: Android™ java snippet of the Action Intent

NOTE: Only actions supported (i.e. declared in its descriptor) by the plugin shall be executed by the Client.

B.3.5.2 Plug-in Application

The Plug-in application shall declare the Android Services components to reflect what has been declared in the Plug-in descriptor. Usually a single service is enough but the implementer can decide to have multiple services and override the used service per action by defining a new android:name leaf node in the action description.

```
<?xml version="1.0" encoding="utf-8"?>
<manifest xmlns:android="http://schemas.android.com/apk/res/android"
    [...] >

    [...]
    <application [...] >
        [...]
        <meta-data
            android:name="gsma.plugin.descriptor"
            android:resource="@xml/plugin_descriptor" />
        <service
            android:name=".MyPluginService"
            android:enabled="true"
            android:exported="true" />
    </application>
</manifest>
```

Table 43: Android™ service declaration example

If the Service receives an Action from the Client which is not supported (i.e. not declared by the descriptor) it should be silently ignored.

It is recommended to use the Android™ “IntentService” to free as soon as possible the invoking main-thread.

In case a ResultReceiver has been provided with the Action Intent then it should be used to provide a proper result (Action specific).

B.3.6 Actions

Action	Description	Intent Extra
VIEW	Used to request the Plug-in to show/display the object identified by the objectid passed with the intent.	String containing the objectid Intent Extra key: “objectid” Or Bundle with object payload (key = “objectbundle”)

Action	Description	Intent Extra
DELETE	By invoking this a consumer can request the deletion for a certain object or list of objects identified by the passed objectid/s.	String or Array of Strings containing the objectid/s Intent Extra key: “objectid” Or Bundle with object payload (key = “objectbundle”)
GET_TEMPLATE_VIEW	This allows a consumer to request the Template content that represents the object identified by the passed objectid. The received content is then used to populate a rich bubble.	String containing the objectid Intent Extra key: “objectid” Or Bundle with object payload (key = “objectbundle”)
OBJECT_RECEIVED	Indicates that the consumer has an object that belongs to the called Plug-in.	Bundle with object payload (key = “objectbundle”)
CREATE_OBJECT	Called by the consumer to ask the Plug-in for the creation of a new object. This usually raises an activity that allows the user to edit the creation of the object.	String or Array of Strings with key “accept-type” containing the mime-types the Plug-in can choose from to create the content. Sender and Receiver.

Table 44: Actions

B.3.6.1 Action procedures and parameters

B.3.6.1.1 Action VIEW

B.3.6.1.1.1 Conditions to be invoked by the client

The Client shall invoke this Action when the user taps on the message container of a message that is marked internally by the Client to belong to an installed Plug-in (see OBJECT RECEIVED in B.3.6.1.4). The Client shall not invoke it if the VIEW action is not declared by the Plug-in’s descriptor. If the message containers belongs to an installed Plug-in and an object_id has been received from the OBJECT_RECEIVED (or CREATE_OBJECT) action then the object_id shall be passed to the Plug-in with the action intent. Otherwise the Intent will contain a bundle with the message content see B.3.6.1.1.2.

B.3.6.1.1.2 Intent parameters and Extras

This node is the declaration container for all actions supported by the client.

Intent Parameter	Type	Value
action	String	“gsma.plugin.action.VIEW”
component	componentName	Package name + service class as defined in the Plug-in descriptor “android:name”. Note that this can be overridden in every action node.
data	URI	Shall contain a random and unique number. Recommended is pluginv1:// <pluginId>/view/<systemclock>.

Intent Parameter	Type	Value
		This is dummy and a workaround to ensure the OS will execute 2 subsequent view actions
type	URI	package:<client_packagename>

Table 45: VIEW Intent Parameters

Intent Extra	Type	Value
object_id	String	This is the object_id associated to the message as received from OBJECT_RECEIVED or CREATE_OBJECT. Not present if not received from OBJECT_RECEIVED or CREATE_OBJECT.
messageBundle	Bundle	Contains: String: receiver = <address of the recipient> String: sender = <address of the sender> String: msgmimetype=<the mime-type of the received message> String: message=<the actual received message> String: cpimheader=<cpim header value>

Table 46: VIEW Intent Extras

B.3.6.1.1.3 Results

N/A

B.3.6.1.1.4 Client operations after Action execution

N/A

B.3.6.1.1.5 Plug-in operations of the action execution

When the Plug-in receives the VIEW action intent it shall either:

- Take the passed object_id (if set) and use it to generate the Plug-in specific content in order to display to the user.
- Take the passed message_Bundle (if set) and use it to generate the Plug-in specific content in order to display to the user.

B.3.6.1.2 Action DELETE

B.3.6.1.2.1 Conditions to be invoked by the client

The Client shall invoke this Action when the user selects the delete function on a message container of a message that is marked internally by the Client to belong to an installed Plug-in (see OBJECT RECEIVED in B.3.6.1.4). The Client shall not invoke it if the DELETE action is not declared by the Plug-in's descriptor. If the message containers belongs to an installed Plug-in and an object_id has been received from the OBJECT_RECEIVED (or CREATE_OBJECT) action then the object_id shall be passed to the Plug-in with the action intent. Otherwise the Intent will contain a bundle with the message content see B.3.6.1.2.2.

In case of a complete conversation thread deletion this action shall be repeated for each message belonging to a Plug-in.

B.3.6.1.2.2 Intent parameters and Extras

This node is the declaration container for all actions supported by the client.

Intent Parameter	Type	Value
action	String	“gsma.plugin.action.DELETE”
component	componentName	Package name + service class as defined in the plugin descriptor “android:name”. Note that this can be overridden in every action node.
data	URI	Shall contain a random and unique number. Recommended is pluginv1:// <pluginId>/delete/<systemclock>. This is dummy and a workaround to ensure the OS will execute 2 subsequent view actions.
type	URI	package:<client_packagename>

Table 47: DELETE Intent Parameters

Intent Extra	Type	Value
object_id	String	This is the object_id associated to the message as received from OBJECT_RECEIVED or CREATE_OBJECT. Not present if not received from OBJECT_RECEIVED or CREATE_OBJECT.
messageBundle	Bundle	Contains: String: receiver = <address of the recipient> String: sender = <address of the sender> String: msgmimetype=<the mime-type of the received message> String: message=<the actual received message> String: cpimheader=<cpim header value>
resultReceiver	ResultReceiver	Can be optionally set by the Client if the Client wants to be informed about the action completion or failure.

Table 48: DELETE Intent Extras

B.3.6.1.2.3 Results

The resultReceiver (if set by the Client) shall receive a resultCode that is set to

- RESULT_OK: the action completed successfully
- error code higher than 1: action completed with error. The Client ignores the actual value.

B.3.6.1.2.4 Client operations after Action execution

After the Client invoked the delete action it can wait for its completion or simply go ahead with the deletion of the actual message that the user wants to delete.

B.3.6.1.2.5 Plug-in operations of the action execution

When the Plug-in receives the DELETE action intent it shall either:

- Take the passed object_id (if set) and use it to delete any information associated to the object_id or terminate any ongoing activity associated to the object_id.
- Take the passed messageBundle (if set) and use it to delete any information associated to the messageBundle or terminate any ongoing activity associated to the messageBundle.
- Do nothing if there is no information or activity associated.

NOTE: Plug-ins which do not have these associations should not declare the DELETE action in the descriptor.

If the Client passed a resultReceiver then the Plug-in shall return a resultCode of the operation.

B.3.6.1.3 Action GET_TEMPLATE_VIEW

B.3.6.1.3.1 Conditions to be invoked by the client

Used to transform a Plug-in generated message into a rich Bubble that is based on the templates as defined for General Purpose Card in section 3.6.10 of [RCC.07]. The client shall not send any response or SharedData to the Plug-in. From the suggestions, it shall support the Suggested actions.

The Client shall invoke this Action once per message if the message is marked internally by the Client to belong to an installed Plug-in (see OBJECT RECEIVED in B.3.6.1.4).

The Client shall not invoke it if the GET_TEMPLATE_VIEW action is not declared by the Plug-in's descriptor.

If the message containers belongs to an installed Plug-in and an object_id has been received from the OBJECT_RECEIVED (or CREATE_OBJECT) action then the object_id shall be passed to the Plug-in with the action intent. Otherwise the Intent will contain a bundle with the message content see B.3.6.1.3.2.

B.3.6.1.3.2 Intent parameters and Extras

This node is the declaration container for all actions supported by the client.

Intent Parameter	Type	Value
action	String	"gsma.plugin.action.GET_TEMPLATE_VIEW"
component	componentName	Package name + service class as defined in the plugin descriptor "android:name". Note that this can be overridden in every action node.
data	URI	Shall contain a random and unique number. Recommended is pluginv1:// <pluginId>/gettemplateview/<systemclock>. This is dummy and a workaround to ensure the OS will execute 2 subsequent get_template_view actions.
type	URI	package:<client_packagename>

Table 49: GET_TEMPLATE_VIEW Intent Parameters

Intent Extra	Type	Value
object_id	String	This is the object_id associated to the message as received from OBJECT_RECEIVED or CREATE_OBJECT. Not present if not received from OBJECT_RECEIVED or CREATE_OBJECT.
templateMimeType	String[]	List of the mime-type of the templates supported by the Client. For the Plug-in version 1 this shall be set to ""
messageBundle	Bundle	Contains: String: receiver = <address of the recipient> String: sender = <address of the sender> String: msgmimetype=<the mime-type of the received message> String: message=<the actual received message> String: cpimheader=<cpim header value>
resultReceiver	ResultReceiver	Shall be set by the Client to receive the template JSON.

Table 50: GET_TEMPLATE_VIEW Intent Extras

B.3.6.1.3.3 Results

The resultReceiver (if set by the Client) shall receive a resultCode that is set to

- RESULT_OK: the action completed successfully. The bundle contains a Template JSON as defined in General Purpose Card in section 3.6.10 of [RCC.07].
- error code higher than 1: action completed with error. The Client ignores the actual error value and will not try to render any rich Bubble.

In case of RESULT_OK the resultData bundle shall contain key called “templateview” with the value containing the populated template JSON.

B.3.6.1.3.4 Client operations after Action execution

After the Client invoked the get_template_view it shall take the resulting template JSON, store it for that message and render it as a rich Bubble.

Any content retrieved through the media URLs included in the General purpose cards is hosted on webservers managed by the Plug-in provider and it is made available on the internet. The Client shall apply the same retrieval procedures as for the Chatbot content hosted on webservers available on the internet.

B.3.6.1.3.5 Plug-in operations of the action execution

When the Plug-in receives the GET_TEMPLATE_VIEW action intent is shall either:

Take the passed object_id (if set) and use it to populate a proper template JSON that will be passed back to the Client.

Take the passed messageBundle (if set) and use it to populate a proper template JSON that will be passed back to the Client.

The received ResultReceiver shall be invoked passing the resultCode and the generated template JSON.

B.3.6.1.4 Action OBJECT_RECEIVED

B.3.6.1.4.1 Conditions to be invoked by the client

Used to notify a Plug-in about a received message that belongs to the Plug-in.

The Client shall invoke this Action after receiving a message that results to belong to the target Plug-in.

The Client shall not invoke it if the OBJECT_RECEIVED action is not declared by the Plug-in's descriptor.

The action Intent shall contain a bundle with the message content see B.3.6.1.4.2.

B.3.6.1.4.2 Intent parameters and Extras

This node is the declaration container for all actions supported by the client.

Intent Parameter	Type	Value
action	String	"gsma.plugin.action.OBJECT_RECEIVED"
component	componentName	Package name + service class as defined in the Plug-in descriptor "android:name". Note that this can be overridden in every action node.
data	URI	Shall contain a random and unique number. Recommended is pluginv1:// <pluginId>/objectreceived/<systemclock>. This is dummy and a workaround to ensure the OS will execute 2 subsequent object_received actions.
type	URI	package:<client_packagename>

Table 51: OBJECT_RECEIVED Intent Parameters

Intent Extra	Type	Value
messageBundle	Bundle	Contains: String: receiver = <address of the recipient> String: sender = <address of the sender> String: msgmimetype=<the mime-type of the received message> String: message=<the actual received message> String: cpimheader=<cpim header value>
resultReceiver	ResultReceiver	Shall be set by the Client to receive an optional object_id.

Table 52: OBJECT_RECEIVED Intent Extras

B.3.6.1.4.3 Results

The resultReceiver shall receive a resultCode that is set to

- RESULT_OK: the action completed successfully. The bundle could contain an object_id
- error code higher than 1: action completed with error. The Client ignores the bundle and renders the message as a normal chat message

In case of RESULT_OK the resultData bundle can contain a key called “object_id” with the value of the generated object_id.

B.3.6.1.4.4 Client operations after Action execution

After the Client invoked the object received action it shall take the object_id (if any), and store it associated to the related message. This object_id (if returned) is used in all subsequent action executions.

If GET_TEMPLATE_VIEW is defined by the Plug-in then the Plug-in can use it to render the message bubble as a rich message bubble (see GET_TEMPLATE_VIEW).

B.3.6.1.4.5 Plug-in operations of the action execution

When the Plug-in receives the OBJECT_RECEIVED action intent is should either:

- Create an object_id that is associated to the actual content represented by the passed message
- Do nothing.

NOTE: In case the Plug-ins never generates any object_id it shall not declare the OBJECT_RECEIVED action in its descriptor.

In either case the Plug-in shall take the passed message in order to fulfil and implement the specific Plug-in use case.

The received ResultReceiver shall be invoked passing the resultCode and, if generated, the object_id.

B.3.6.1.5 Action CREATE_OBJECT

B.3.6.1.5.1 Conditions to be invoked by the client

This action is used to create new Plug-in generated content.

When the user selects a Plug-in entry point then the Client shall invoke this action towards the selected Plug-in.

The CREATE_OBJECT action shall be declared in the Plug-in’s descriptor.

B.3.6.1.5.2 Intent parameters and Extras

This node is the declaration container for all actions supported by the client.

Intent Parameter	Type	Value
action	String	“gsma.plugin.action.CREATE_OBJECT”
component	componentName	Package name + service class as defined in the Plug-in descriptor “android:name”. Note that this can be overridden in every action node.

Intent Parameter	Type	Value
data	URI	Shall contain a random and unique number. Recommended is pluginv1:// <pluginId>/createobject/<systemclock>. This is dummy and a workaround to ensure the OS will execute 2 subsequent get_template_view actions.
type	URI	package:<client_packagename>

Table 53: CREATE_OBJECT Intent Parameters

Intent Extra	Type	Value
sender	String	Address of the sender
receiver	String	Address of the recipient
supportedMimetypes	String[]	List of mime-types the Plug-in can use to generate the content. This is a subset of the types declared by the Plug-in descriptors and what the recipient Client is able to receive.
resultReceiver	ResultReceiver	Shall be set by the Client to receive the result code, actual content and optionally an object_id and/or content_id.

Table 54: CREATE_OBJECT Intent Extras

B.3.6.1.5.3 Results

The resultReceiver (if set by the Client) shall receive a resultCode that is set to

- RESULT_OK: the action completed successfully. See below for the content of the bundle returned with the ResultReceiver.
- RESULT_CANCELED: the user cancelled the action. The Client shall ignore the transaction.
- error code higher than 1: action completed with error. The Client can inform the user about a generic creation error and shall ignore the transaction.

In case of RESULT_OK the resultData bundle shall contain:

Bundle Key	Type	Value
content	String	Depending on the generated mime-type this can be either a textual content (text and/or link pointing to the content resource) or a URI pointing to a FileProvider hosted in the Plug-in that the Client can use to retrieve the resource.
mimeType	String	Mime-type of the generated content.
objectId	String	OPTIONAL: can be generated by the Plug-in to track the content in the context of the Client->Plug-in interactions. This depends on the implemented Plug-in use case.

Bundle Key	Type	Value
contentId	String	OPTIONAL: shall be generated by the Plug-in to tag the returned content if the content is a repeatable content resource.

Table 55: CREATE_OBJECT resultData bundle

B.3.6.1.5.4 Client operations after Action execution

After the Client invoked the create_object action returns with valid content the Client shall retrieve the content from the ResultReceiver bundle:

- Use the content string as text if the mimeType is text/*.
- Use the content string as a FileProvider URI and fetch the content blob from the indicated URI if the mimeType is not a text/* content type.

In any case the Client shall only accept a content type that can be received by the B party either using the technology selection procedures described in 3.2.8.7.2 of [RCC.07].

If GET_TEMPLATE_VIEW is defined by the Plug-in then the Plug-in can use it to render the message bubble as a rich message bubble (see GET_TEMPLATE_VIEW).

If an objectId has been returned with the content then it shall be stored in association with the actual generated message container and used in further operations. (GET_TEMPLATE_VIEW, DELETE, etc.).

If a contentId has been returned with the content then it shall be stored in association with the actual generated message container and used during the transmission of the content in the CPIM header as described in 3.2.8.6.2 of [RCC.07].

B.3.6.1.5.5 Plug-in operations of the action execution

When the Plug-in receives the CREATE_OBJECT action intent it shall:

- Render the Plug-in use-case specific user experience that allows the user to pick, select or create the resource and or session that is represented by the content to return. If there are no options for the user and the content can be created immediately then the Plug-in can skip any interaction with the user.
- Return a RESULT_CANCELED in case the user cancels the content creation.
- The received ResultReceiver shall be invoked passing the resultCode. In case of successful content generation the returned bundle shall content either the text message or an URI that points to an Android™ FileProvider hosted by the Plug-in and which serves the actual binary content (image, audio, etc.). If the resulting content is associated to an internal state or object of the Plug-in then the Plug-in call also returns an object_id. If the returned content is a repeatable resource (e.g. a Sticker) then the Plug-in shall return also a content_id that identifies uniquely the content resource.

B.3.6.2 Clarification on the usage of IDs

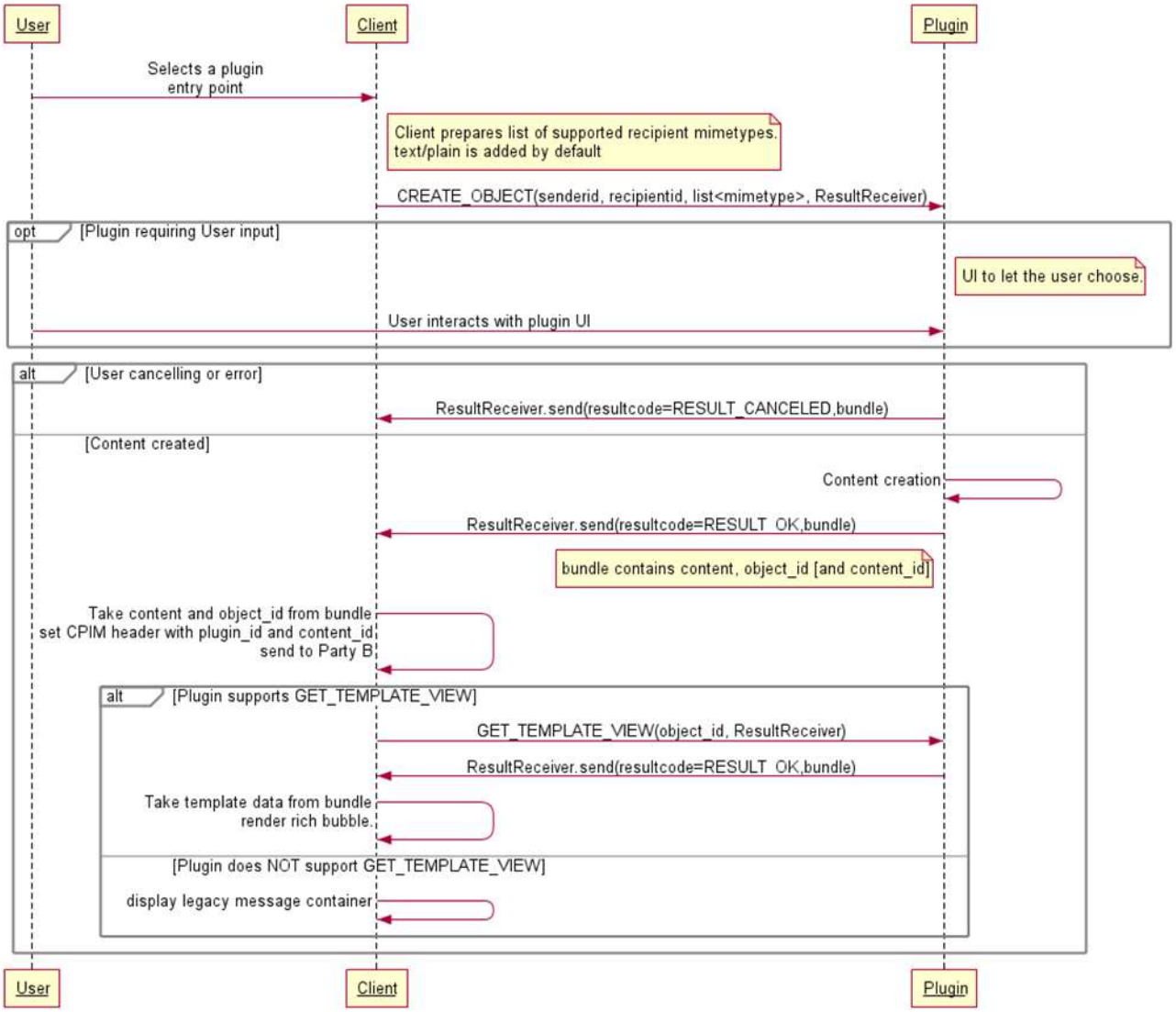
- objectId: The scope of this ID is limited on the device and the communication between the Client and Plug-in. It can be used (if generated by the Plug-in with the

content) to refer to the message/content so that the Plug-in can associate it to some internal state or object. The objectId shall not exceed 256 alphanumeric characters.

- pluginId: This is a unique identifier that is used to identify a Plug-in inside a Plug-in application. It is transmitted within the specific Plug-in CPIM header and used for tracking/monitoring purposes but also to route an incoming message to the relevant Plug-in if available (see sections 3.2.8.6 and 3.2.8.8.3 of [RCC.07]. In case the Plug-in is not installed it is used to identify the Plug-in in the network catalog and allow the user to install it. In order to ensure unicity on the pluginId (declared in the descriptor and the network catalog) shall be formed as defined in section 3.2.8.4 of [RCC.07]. Example: com.example.package#nicestickers.
- contentId: This identifies a certain repeatable content in the context of a Plug-in. It shall be returned by a Plug-in that generates a repeatable resource as content. The contentId is used for tracking/monitoring purposes and sent with the pluginId in the value of the Plug-in defined CPIM header (see section 3.2.8.6.1 of [RCC.07]).

B.3.7 Procedures for Client and Plug-in

B.3.7.1 User creating and sending Plug-in content

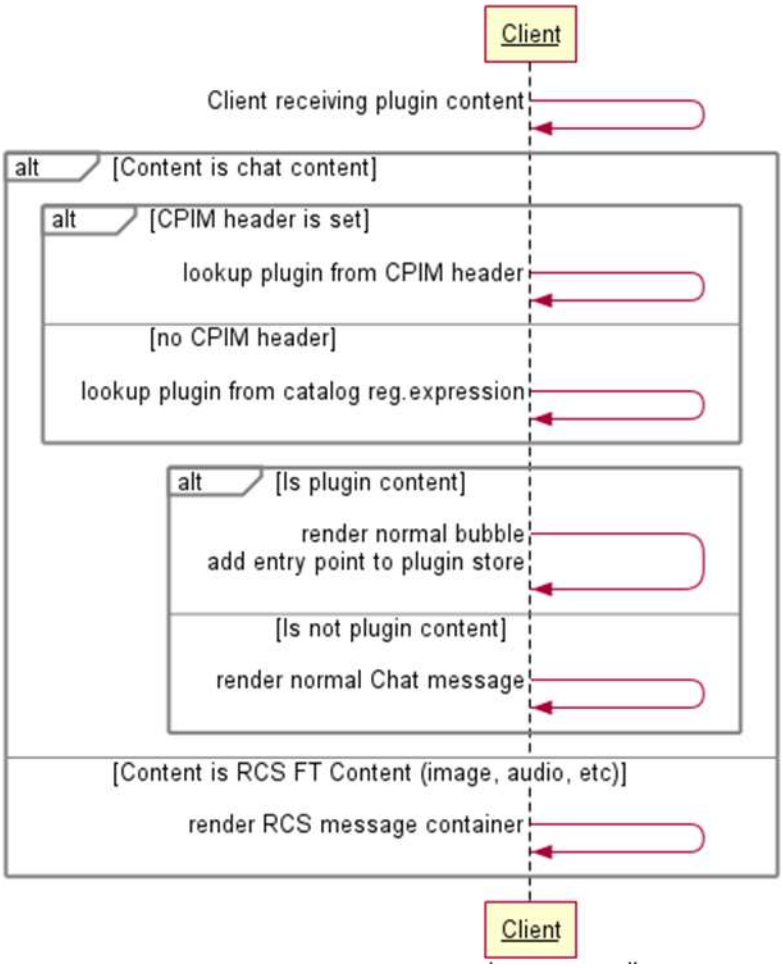


B.3.7.2 Client receiving Plug-in generated content

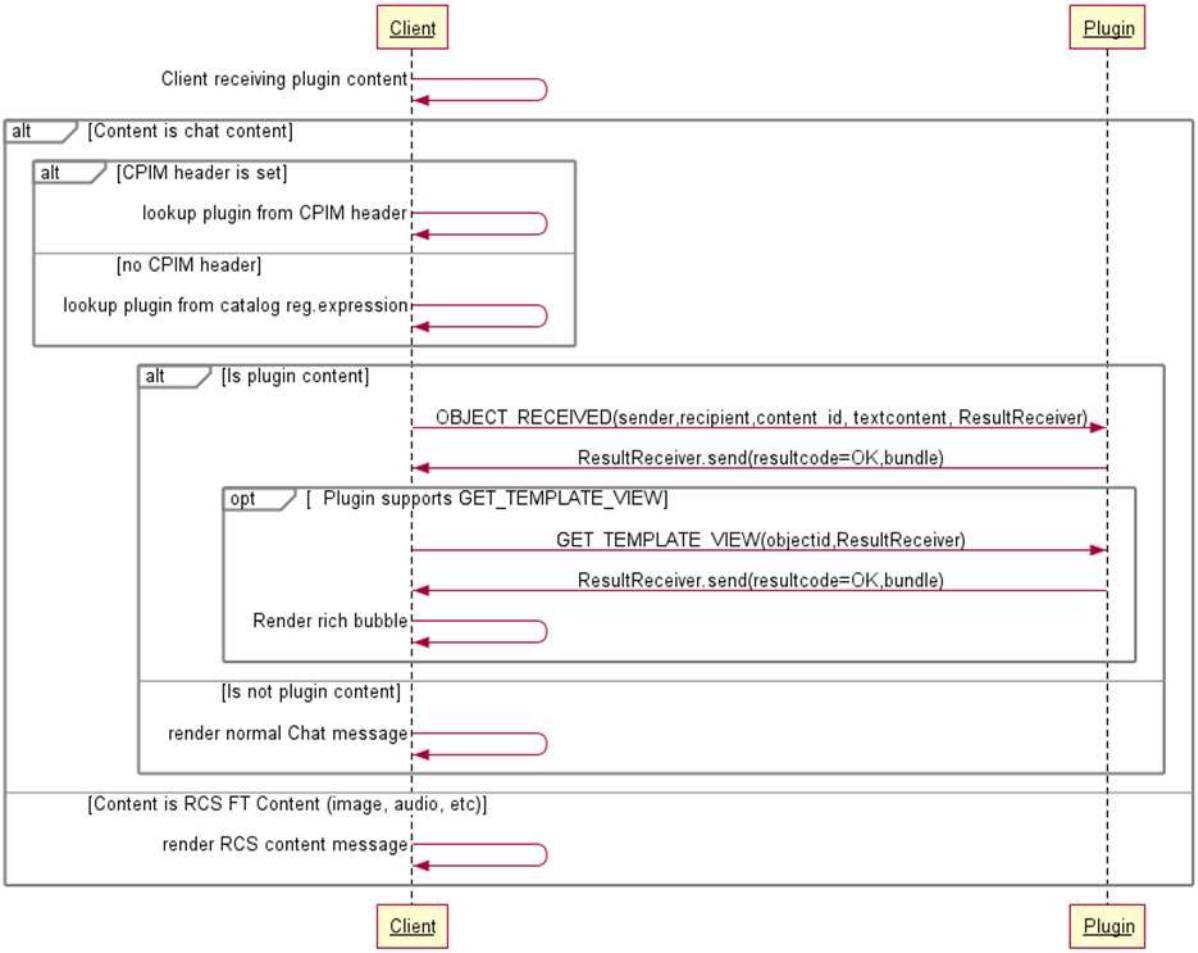
Plug-in generated content should be recognized as Plug-in content following the procedures described in section 3.2.8.8.3 of [RCC.07].

If the recognized Plug-in is available but not installed then the procedures defined in section 3.2.8.8.3 of [RCC.07] apply.

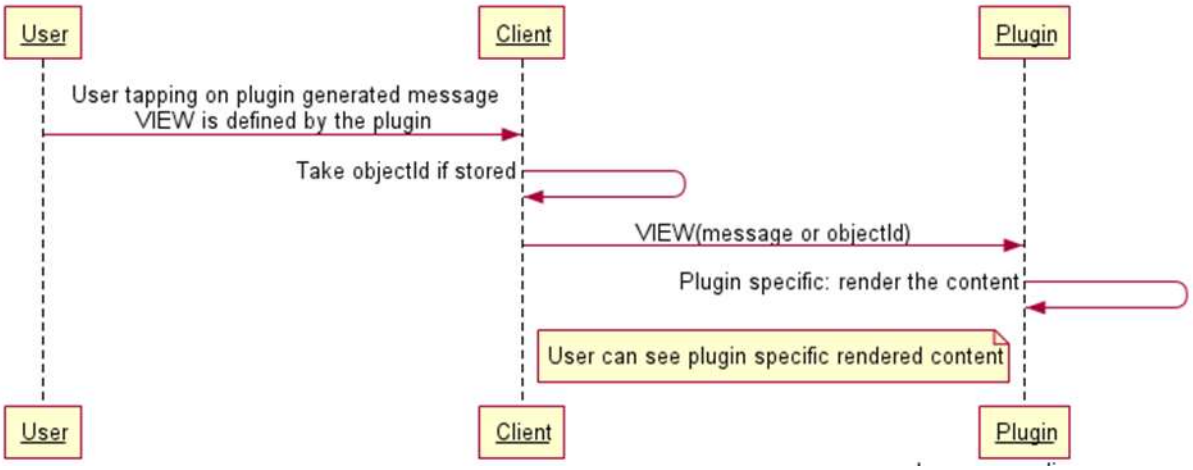
B.3.7.2.1 Content received when Plug-in is NOT installed



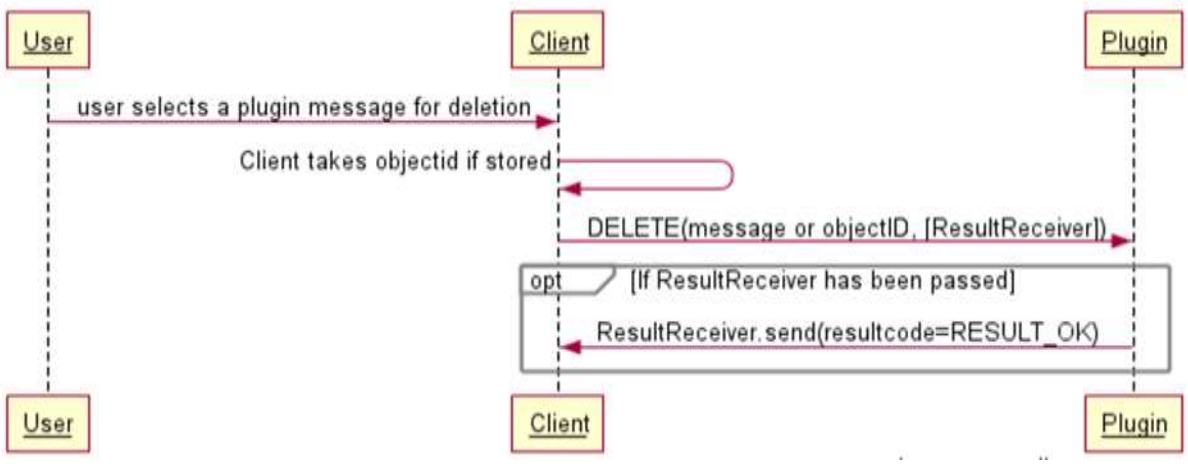
B.3.7.2.2 Content received when Plug-in is already installed



B.3.7.2.3 User tapping on Plug-in generated Bubble and VIEW declared



B.3.7.2.4 User deleting a Plug-in generated Message/Bubble



B.3.8 Sender/Recipient address format & Anonymization

With the Actions CREATE_OBJECT and OBJECT_RECEIVED the sender and recipient addresses, either in anonymous or clear form, are also passed to the Plug-in.

B.3.8.1 Format of SenderId and RecipientID

The format of these are defined as following:

A single user is represented using a tel URI as specified in [RFC3966], so:

tel:<telephone_number in E164 format>?<parameters>

Name	Type	Description
Alias	Optional String	Alias or nickname of the contact

Table 56: Addresses parameters

Example:

tel:%2B39123456789?alias=Robert%20Redford
Which specify that the user has +39123456789 as phone number and “Robert Redford” as his alias.

B.3.8.1.1 Address format case for group chat

In case of group chat the address is a special address that contains an id identifying the group chat but also a list of addresses belonging to the group of participants.

In case of CREATE_OBJECT and OBJECT_RECEIVED the recipient shall be the group address.

The group address has only Client and Plug-in scope i.e. shall never be transmitted outside the device.

The format of this address is defined as follows:

```
rcs-chat:<groupid>?users=<encoded list of users separated by comma>
```

If the list of users contains the current user, it has to be marked with a special parameter “self=true”.

The groupid shall identify uniquely the group. It is generated by the client. It is recommended to use the value of the contribution-id header.

For example, if user A is `tel:123456?alias=my%20name`, on user A phone the “users” parameter will contain `tel:123456?alias=my%20name&self=true`.

B.3.8.1.2 Anonymization

If the User didn’t granted consent to the client to provide addresses to the Plug-in in clear form and the Plug-in is not endorsed to receive addresses in clear form then the Client shall anonymise the addresses. This applies to both the sender but also the recipient(s) addresses.

Anonymization shall be performed by using a hashing algorithm which takes into account the package name of the Client, the package name of the Plug-in (to generate Plug-in specific IDs) and a secret salt that belongs to the Client.

The anonymization replaces the address with an apparently random uid. In order to have a global valid uid which identifies the same address in clear form for that particular Plug-in on all devices a hash function is used. The uid is the result of hashing the string resulting from the concatenation of the original address with the package name of the Plug-in app, the package name of the consumer app and an arbitrary salt. The salt is decided by the consumer and shall remain stable in all future versions of the consumer.

```
Uid = Hash(“<clearaddress>:<publisher-packagename>:<consumer-packagename>:<secretsalt>”)
```

NOTE: When anonymizing a URI, the client shall take care of anonymizing any URI parameter containing personal user data and of NOT anonymizing any plugin needed parameter, such as alias and self.
The anonymization applies also in case an address is part of a group chat address.

Example of an anonymized address:

```
tel:%2B123456789?alias=Goofy&self=true
```

becomes

```
tel:<AonymID>?alias=Goofy&self=true
```

When anonymizing a Group Chat URI, any single user in the group shall be anonymized.

Example of an anonymized group address:

```
rcs-chat:12345?users=tel%3A%252B123456789%3Falias%3DGoofy%26self%3Dtrue,tel%3A%252B123456788%3Falias%3DSpooky,tel%3A%252B123456787%3Falias%3Wooky
```

becomes

```
rcs-
chat:12345?users=tel%3A<HASH>%3Falias%3DGoofy%26self%3Dtrue,tel%3A<HASH>%3F
alias%3DSpooky,tel%3A<HASH>%3Falias%3Wooky
```

B.3.8.1.3 Anonymized addresses store

The Client shall store a table where all anonymous addresses are stored along with their addresses in clear form. This is needed to have a quick look up from anonymous ID to the addresses/identifiers in clear form.

B.3.9 Endorsement

A Plug-in provider can be endorsed by one or more endorser entities which are trustful to the Client. If a Plug-in is endorsed then the metadata declared in the endorsement xml documented are automatically granted and accepted by the Client. It is up to the endorser to decide if it wants to endorse a range of versions or all versions.

B.3.9.1 Endorsement verification procedure

In order to properly assign the right privileges to a certain Plug-in the Plug-in manager embedded in the consumer executes the following authorization check procedure.

- If the fingerprint of the Android™ package containing the Plug-in matches the consumer fingerprint then the Plug-in has all privileges (typically when the Plug-in is published by the Client producer)
- If the fingerprint is not known then the signatures and endorsers present inside the descriptor are loaded.
- If the endorser is unknown then the Plug-in is ignored i.e. shall not be enabled in the Plug-in local catalogue.
- If the endorser is known then the content of endorsement.xml is collated with the package information available in the OS via the package manager.
- If the content of the endorsement.xml does not match then the Plug-in is ignored i.e. shall not be enabled in the Plug-in local catalogue.
- If the content match then the signature is calculated and verified using the public certificate of the endorser embedded in the consumer application.
- If the signature is verified then all privileges are assigned to the Plug-in for the applicable versions
- If the signature does not match then the Plug-in is ignored i.e. shall not be enabled in the Plug-in local catalogue.

B.3.9.2 Endorsement XML Manifest metadata

A Plug-in app that needs to be endorsed shall contain a text file called endorsement.xml. This file is pointed to by a proper meta-data tag in the android Manifest.xml:

Name	Resource	Description
gsma.plugin.endorsement	Pointer to android resource	Points to the descriptor resource

The following example illustrates the meta-data that shall be added to the Manifest.xml file (manifest excerpt):

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

      <!-- the following meta-data is used to identify the plugin endorsment resource -->
      <meta-data android:name="gsma.plugin.endorsement" android:resource="@xml/gsma_endorsement"/>

.....
```

Table 57: Android endorsement pointer

The endorsement xml file shall be signed by the endorser (MNO) and the signature shall be included as an “endorser” element inside the “endorsement” tag included into the extension descriptor.

B.3.9.3 Endorsement XML document

This document is used by the Plug-in publisher to declare what is endorsed by the endorser. The package name, version (and version range), signature and the need for clear addresses are all declared and subject to be signed by an endorser.

The endorser provides its signature for the given endorsement xml (after appropriate audit and verification). This signature provided by the endorser shall then be included into the Plug-in descriptor.

NOTE: a Plug-in publisher can have multiple endorser. All endorsements are inserted into the Plug-in descriptor.

```
<?xml version="1.0" encoding="UTF-8"?>
<plugin-publisher>
  <entity>Vendor Ltd</entity>
  <application>SecretPhoto</application>
  <versioncode>1004</versioncode>
   <versioncodemax>1010</versioncodemax>
  <packagename>com.vendor.secretphoto</packagename>
  <publisherfingerprint hash="sha1">
EA:68:F9:04:FA:1B:8D:AA:BA:CE:77:37:CF:67:6C:D2:C9:42:3F:1C
</publisherfingerprint>
<privacy addresses=”clear”/>
</plugin-publisher>
```

Table 58: Android endorsement xml example

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				
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]	RCS Service Provider configurable	
Timer_T2	[3GPP TS 24.167]	[RCC.15]	RCS Service Provider configurable	
Timer_T4	[3GPP TS 24.167]	[RCC.15]	RCS Service Provider configurable	
Private_user_identity	[3GPP TS 24.167]	[RCC.15]	RCS Service Provider configurable	
Public_user_identity	[3GPP TS 24.167]	[RCC.15]	RCS Service Provider configurable	
Home_network_domain_name	[3GPP TS 24.167]	[RCC.15]	RCS 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.	

Parameter	Functional Definition	Syntax Definition for transport using [RCC.14]	Client Configurability	Aligned Value for this profile
LBO_P-CSCF_Address	[3GPP TS 24.167]	[RCC.15]	Tree is instantiated	
Address (LBO_P-CSCF_Address)	[3GPP TS 24.167]	[RCC.15]	RCS Service Provider configurable	
AddressType (LBO_P-CSCF_Address)	[3GPP TS 24.167]	[RCC.15]	RCS 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]	RCS Service Provider Configurable	
SMS_Over_IP_Networks_Indication	[3GPP TS 24.167]	[RCC.15]	RCS Service Provider Configurable	
Keep_Alive_Enabled	[3GPP TS 24.167]	[RCC.15]	RCS 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]	RCS Service Provider Configurable	
RegRetryBaseTime	[3GPP TS 24.167]	[RCC.15]	RCS Service Provider Configurable	
RegRetryMaxTime	[3GPP TS 24.167]	[RCC.15]	RCS Service Provider Configurable	
PhoneContext_List	[3GPP TS 24.167]	N/A	Tree not instantiated	
SS_domain_setting	[3GPP TS 24.167]	[RCC.15]	RCS Service Provider Configurable	
PS_domain_IMS_SS_control_preference	[3GPP TS 24.167]	[RCC.15]	RCS Service Provider Configurable	
Media_type_restriction_policy	[3GPP TS 24.167]	[RCC.15]	RCS Service Provider Configurable	
IMS Mode Authentication Type	[RCC.15]	[RCC.15]	RCS Service Provider Configurable	

Parameter	Functional Definition	Syntax Definition for transport using [RCC.14]	Client Configurability	Aligned Value for this profile
Realm	[RCC.15]	[RCC.15]	RCS Service Provider Configurable	
Realm User Name	[RCC.15]	[RCC.15]	RCS Service Provider Configurable	
Realm User Password	[RCC.15]	[RCC.15]	RCS Service Provider Configurable	
Transport Protocols: Signalling Cellular	[RCC.15]	[RCC.15]	RCS Service Provider Configurable Recommended Value: SIPoTCP or SIPoTLS (to avoid constant switchover to TCP)	
Transport Protocols: Signalling Roaming	[RCC.15]	[RCC.15]	RCS Service Provider Configurable Recommended Value: SIPoTCP or SIPoTLS (to avoid constant switchover to TCP)	
Transport Protocols: Signalling Wi-Fi	[RCC.15]	[RCC.15]	RCS Service Provider Configurable	Not instantiated, if authentication different from IMS AKA is used and thus IPsec is not enabled
Transport Protocols: Real Time Media Cellular	[RCC.15]	[RCC.15]	RCS Service Provider Configurable Recommended Value: Not instantiated	
Transport Protocols: Real Time Media Roaming	[RCC.15]	[RCC.15]	RCS Service Provider Configurable Recommended Value: Not instantiated	
Transport Protocols: Real Time Media Wi-Fi	[RCC.15]	[RCC.15]	RCS Service Provider Configurable	Not instantiated

Parameter	Functional Definition	Syntax Definition for transport using [RCC.14]	Client Configurability	Aligned Value for this profile
Transport Protocols: Discrete Media Cellular	[RCC.15]	[RCC.15]	RCS Service Provider Configurable Recommended Value: Not instantiated	
Transport Protocols: Discrete Media Roaming	[RCC.15]	[RCC.15]	RCS Service Provider Configurable Recommended Value: Not instantiated	
Transport Protocols: Discrete Media Wi-Fi	[RCC.15]	[RCC.15]	RCS Service Provider Configurable	Not instantiated
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]	RCS Service Provider Configurable	
RCS State Parameters				
RCS DISABLED STATE	[RCC.07]	[RCC.07]	RCS Service Provider Configurable	
SUPPORTED RCS VERSIONS	[RCC.07]	[RCC.07]	Fixed Value: 7.0,8.0, 8.1	
SUPPORTED RCS PROFILE VERSIONS	[RCC.07]	[RCC.07]	Fixed Value: UP_2.0,UP_2.2,UP_2.3	
Presence Parameters				

Parameter	Functional Definition	Syntax Definition for transport using [RCC.14]	Client Configurability	Aligned Value for this profile
CLIENT-OBJ-DATA-LIMIT	[PRESENCE2MO]	[RCC.07]	524288 (i.e. 512KB) if CAPABILITY DISCOVERY MECHANISM is set to 1. Not instantiated otherwise.	
CONTENT-SERVER-URI	[PRESENCE2MO]	N/A	Not instantiated	
SOURCE-THROTTLE-PUBLISH	[PRESENCE2MO]	[RCC.07]	RCS Service Provider Configurable if CAPABILITY DISCOVERY MECHANISM is set to 1. Not instantiated otherwise.	
MAX-NUMBER-OF-SUBSCRIPTIONS-IN-PRESENCE-LIST	[PRESENCE2MO]	[RCC.07]	RCS 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]	RCS Service Provider Configurable if CAPABILITY DISCOVERY MECHANISM is set to 1. Not instantiated otherwise. Recommended Value: Not instantiated	
Messaging parameters				
MAX_AD-HOC_GROUP_SIZE	[RCC.07]	[RCC.07]	RCS Service Provider Configurable	100
CONF-FCTY-URI	[RCC.07]	[RCC.07]	RCS Service Provider Configurable Recommended value: Not instantiated	

Parameter	Functional Definition	Syntax Definition for transport using [RCC.14]	Client Configurability	Aligned Value for this profile
EXPLODER-URI	[RCC.07]	[RCC.07]	Fixed dummy value: *sip:foo@bar* if STANDALONE MSG AUTH is set to 0, RCS Service Provider Configurable otherwise. Recommended Value: Not instantiated	
CHAT AUTH	[RCC.07]	[RCC.07]	RCS Service Provider Configurable	
GROUP CHAT AUTH	[RCC.07]	[RCC.07]	RCS Service Provider Configurable	
STANDALONE MSG AUTH	[RCC.07]	[RCC.07]	RCS Service Provider Configurable	
IM SESSION AUTO ACCEPT	[RCC.07]	[RCC.07]	RCS Service Provider Configurable	1
IM SESSION AUTO ACCEPT GROUP CHAT	[RCC.07]	[RCC.07]	RCS Service Provider Configurable	
IM SESSION TIMER	[RCC.07]	[RCC.07]	RCS Service Provider Configurable	
MAX SIZE IM	[RCC.07]	[RCC.07]	RCS Service Provider Configurable	8192 (bytes as defined in [RCC.07] section A.2.5)
MAX SIZE STANDALONE	[RCC.07]	[RCC.07]	RCS Service Provider Configurable	1048576 (i.e. 1MB)
MESSAGE STORE URL	[RCC.07]	[RCC.07]	RCS Service Provider Configurable	
MESSAGE STORE NOTIFICATION URL	[RCC.07]	[RCC.07]	RCS Service Provider Configurable	
MESSAGE STORE USERNAME	[RCC.07]	[RCC.07]	RCS Service Provider Configurable	
MESSAGE STORE PASSWORD	[RCC.07]	[RCC.07]	RCS Service Provider Configurable	

Parameter	Functional Definition	Syntax Definition for transport using [RCC.14]	Client Configurability	Aligned Value for this profile
MESSAGE STORE AUTH	[RCC.07]	[RCC.07]	RCS Service Provider Configurable	
MESSAGE STORE EVENT REPORTING	[RCC.07]	[RCC.07]	RCS Service Provider Configurable	
MESSAGE STORE ARCHIVE AUTH	[RCC.07]	[RCC.07]	RCS Service Provider Configurable	
SMS MESSAGE STORE	[RCC.07]	[RCC.07]	RCS Service Provider Configurable	
MMS MESSAGE STORE	[RCC.07]	[RCC.07]	RCS Service Provider Configurable	
CHAT REVOKE TIMER	[RCC.07]	[RCC.07]	RCS Service Provider Configurable	300
MESSAGING UX	Section 5.3.4	Implemented in the profile defined in this document based on the definitions in section 5.3.4	RCS Service Provider Configurable	
MSG TECH DISP SWITCH	Section 5.3.4	Implemented in the profile defined in this document based on the definitions in section 5.3.4	RCS Service Provider Configurable	
USER ALIAS AUTH	Section 5.3.4	Implemented in the profile defined in this document based on the definitions in section 5.3.4	RCS Service Provider Configurable	
MESSAGING FALLBACK DEFAULT	Section 5.3.4	Implemented in the profile defined in this document based on the definitions in section 5.3.4	RCS Service Provider Configurable	
RECONNECT GUARD TIMER	[RCC.07]	[RCC.07]	RCS Service Provider Configurable	

Parameter	Functional Definition	Syntax Definition for transport using [RCC.14]	Client Configurability	Aligned Value for this profile
CFS TRIGGER	[RCC.07]	[RCC.07]	RCS Service Provider Configurable	
MAX 1 TO MANY RECIPIENTS	[RCC.07]	[RCC.07]	RCS Service Provider Configurable	
1 TO MANY SELECTED TECHNOLOGY	[RCC.07]	[RCC.07]	RCS Service Provider Configurable	
DISPLAY NOTIFICATION SWITCH	[RCC.07]	[RCC.07]	RCS Service Provider Configurable	
SPAM NOTIFICATION TEXT	Section 15.2.1.2	Section 5.3.4.1	RCS Service Provider Configurable	
TOKEN LINK NOTIFICATION TEXT	Section 15.2.1.2	Section 5.3.4.1	RCS Service Provider Configurable	
UNAVAILABLE ENDPOINT TEXT	Section 15.2.1.2	Section 5.3.4.1	RCS Service Provider Configurable	
ALLOW ENRICHED CHATBOT SEARCH DEFAULT	Section 15.2.1.2	Section 5.3.4.1	RCS Service Provider Configurable	
CHATBOT DIRECTORY	[RCC.07]	[RCC.07]	RCS Service Provider Configurable	
BOTINFO FQDN ROOT	[RCC.07]	[RCC.07]	RCS Service Provider Configurable	
SPECIFIC CHATBOTS LIST	[RCC.07]	[RCC.07]	RCS Service Provider Configurable	
IDENTITY IN ENRICHED SEARCH	[RCC.07]	[RCC.07]	RCS Service Provider Configurable	
PRIVACY DISABLE	[RCC.07]	[RCC.07]	RCS Service Provider Configurable	
CHATBOT MSG TECH	[RCC.07]	[RCC.07]	RCS Service Provider Configurable	
File Transfer Parameters				
FT AUTH	[RCC.07]	[RCC.07]	RCS Service Provider Configurable	

Parameter	Functional Definition	Syntax Definition for transport using [RCC.14]	Client Configurability	Aligned Value for this profile
FT MAX SIZE	[RCC.07]	[RCC.07]	RCS Service Provider Configurable	102400 (i.e. 100MB)
FT WARN SIZE	[RCC.07]	[RCC.07]	RCS Service Provider Configurable	
FT AUT ACCEPT	[RCC.07]	[RCC.07]	RCS Service Provider Configurable	1
FT HTTP CS URI	[RCC.07]	[RCC.07]	RCS Service Provider Configurable Recommended value: Not instantiated	
FT HTTP DL URI	[RCC.07]	[RCC.07]	RCS Service Provider Configurable Recommended value: dl.rcs.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 (as defined in [PRD-IR.67]).	
FT HTTP CS USER	[RCC.07]	[RCC.07]	RCS Service Provider Configurable	
FT HTTP CS PWD	[RCC.07]	[RCC.07]	RCS Service Provider Configurable	
FT HTTP FALLBACK	[RCC.07]	[RCC.07]	RCS Service provider configurable	
FT MAX 1 TO MANY RECIPIENTS	[RCC.07]	[RCC.07]	RCS Service provider configurable	
FT FALLBACK DEFAULT	Section 7.3.2	Implemented in the profile defined in this document based on the definitions in section 7.3.2	RCS Service provider configurable	
Enriched Calling Related Parameters				

Parameter	Functional Definition	Syntax Definition for transport using [RCC.14]	Client Configurability	Aligned Value for this profile
COMPOSER AUTH	[RCC.20]	Implemented in the profile defined in this document based on definitions in [RCC.20]	RCS Service Provider Configurable	
SHARED MAP AUTH	[RCC.20]	Implemented in the profile defined in this document based on definitions in [RCC.20]	RCS Service Provider Configurable	
SHARED SKETCH AUTH	[RCC.20]	Implemented in the profile defined in this document based on definitions in [RCC.20]	RCS Service Provider Configurable	
POST CALL AUTH	[RCC.20]	Implemented in the profile defined in this document based on definitions in [RCC.20]	RCS Service Provider Configurable	
Geolocation Parameters				
PROVIDE GEOLOC PUSH	[RCC.07]	[RCC.07]	RCS Service Provider Configurable	1
Capability Discovery parameters				
DISABLE INITIAL ADDRESS BOOK SCAN	[RCC.07]	[RCC.07]	RCS Service Provider Configurable	
CAPABILITY INFO EXPIRY	[RCC.07]	[RCC.07]	RCS Service Provider Configurable	
SERVICE AVAILABILITY INFO EXPIRY	[RCC.07]	[RCC.07]	RCS Service Provider Configurable	
NON RCS CAPABILITY INFO EXPIRY	[RCC.07]	[RCC.07]	RCS Service Provider Configurable	
CAPABILITY DISCOVERY MECHANISM	[RCC.07]	[RCC.07]	RCS Service Provider Configurable	

Parameter	Functional Definition	Syntax Definition for transport using [RCC.14]	Client Configurability	Aligned Value for this profile
CAPABILITY DISCOVERY ALLOWED PREFIXES	[RCC.07]	[RCC.07]	RCS Service Provider Configurable	
End User Confirmation parameters				
END USER CONF REQ ID	[RCC.15]	[RCC.15]	RCS Service Provider Configurable	
Multidevice configuration parameters				
uuid_Value	[RCC.15]	[RCC.15]	RCS Service Provider Configurable and device dependent	
IP Voice and Video Call configuration				
PROVIDE RCS IP VOICE CALL	[RCC.07]	[RCC.07]	Fixed Value: 0 for primary devices, RCS Service Provider Configurable for secondary devices	
PROVIDE RCS IP VIDEO CALL	[RCC.07]	[RCC.07]	RCS Service Provider Configurable	
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	RCS 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	RCS 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	RCS Service Provider Configurable	
DATA OFF parameters				
RCS MESSAGING DATA OFF	[RCC.07]	[RCC.07]	RCS Service Provider Configurable	

Parameter	Functional Definition	Syntax Definition for transport using [RCC.14]	Client Configurability	Aligned Value for this profile
FILE TRANSFER DATA OFF	[RCC.07]	[RCC.07]	RCS Service Provider Configurable	
SMSoIP_exempt	[PRD-IR.92]	[RCC.15]	RCS Service Provider Configurable	
SMSoIP_exempt_roaming	[PRD-IR.92]	[RCC.15]	RCS Service Provider Configurable	
MMS DATA OFF	[RCC.07]	[RCC.07]	RCS Service Provider Configurable	
CONTENT SHARE DATA OFF	[RCC.07]	[RCC.07]	RCS Service Provider Configurable	
PRE AND POST CALL DATA OFF	[RCC.07]	[RCC.07]	RCS Service Provider Configurable	
MMTEL_voice_exempt	[PRD-IR.92]	Annex A of [RCC.14]	RCS Service Provider Configurable	
MMTEL_voice_exempt_roaming	[PRD-IR.92]	Annex A of [RCC.14]	RCS Service Provider Configurable	
SS_XCAP_config_exempt	[PRD-IR.92]	Annex A of [RCC.14]	RCS Service Provider Configurable	
SS_XCAP_config_exempt_roaming	[PRD-IR.92]	Annex A of [RCC.14]	RCS Service Provider Configurable	
MMTEL_video_exempt	[PRD-IR.94]	Annex A of [RCC.14]	RCS Service Provider Configurable	
MMTEL_video_exempt_roaming	[PRD-IR.94]	Annex A of [RCC.14]	RCS Service Provider Configurable	
Device Management over PS data off exemption	[3GPP TS 24.368]	[RCC.07] and [RCC.14]	RCS Service Provider Configurable	
Device Management over PS data off roaming exemption	[3GPP TS 24.368]	[RCC.07] and [RCC.14]	RCS Service Provider Configurable	
SYNC DATA OFF	[RCC.07]	[RCC.07]	RCS Service Provider Configurable	

Parameter	Functional Definition	Syntax Definition for transport using [RCC.14]	Client Configurability	Aligned Value for this profile
Plug-ins				
CATALOG-URI	[RCC.07]	[RCC.07]	RCS Service Provider Configurable	

Table 59: 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	16 November 2016	Initial version approved by PSMC.	PSMC	Catherine Maguire / GSMA
2.0	28 June 2017	Universal Profile 2.0: includes approved CR1002	TG	Tom Van Pelt / GSMA
2.1	21 December 2017	Add modularisation of Universal Profile 2.0 as Annex D, Approved as CR1004	TG	Tom Van Pelt / GSMA
2.2	16 May 2018	Universal Profile 2.2: includes approved CR1003	TG	Tom Van Pelt / GSMA
2.3	16 May 2018	Universal Profile 2.3: includes approved CR1004	TG	Tom Van Pelt / GSMA

D.2 Other Information

Type	Description
Document Owner	Future Networks Programme, Global Functional Requirements Group / Network Group, Global Specification Group
Editor / Company	Tom Van Pelt / 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.