Rich Communication Suite 5.0 Advanced Communications Services and Client Specification

Version 1.0

19 April 2012

This is a ***Non Binding*** *Permanent Reference Document of the GSMA.*

Security Classification – NON CONFIDENTIAL GSMA MATERIAL

Copyright 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 RCS 5 Principles and Vision

RCS (Rich Communication Suite) 5.0 provides a framework for discoverable and interoperable advanced communication services and detailed specifications for a basic set of advanced communication services. RCS 5.0 builds on the fundamentals from RCS Release 1 to 4 and RCS-e (RCS-enhanced) 1.2 (see [RCSe12]) that are succeeded by this specification.

As indicated in Figure 1, the set of services specified in RCS 5.0 includes all services from RCS-e 1.2 as well as most of the functionality from RCS Release 1-4. RCS 5.0 extends this basis with new services (indicated in **bold** in Figure 1) and provides enhancements for existing services (indicated in *italics* in Figure 1). All these services can be deployed using a variety of clients on access networks that can be Service Provider controlled or not.

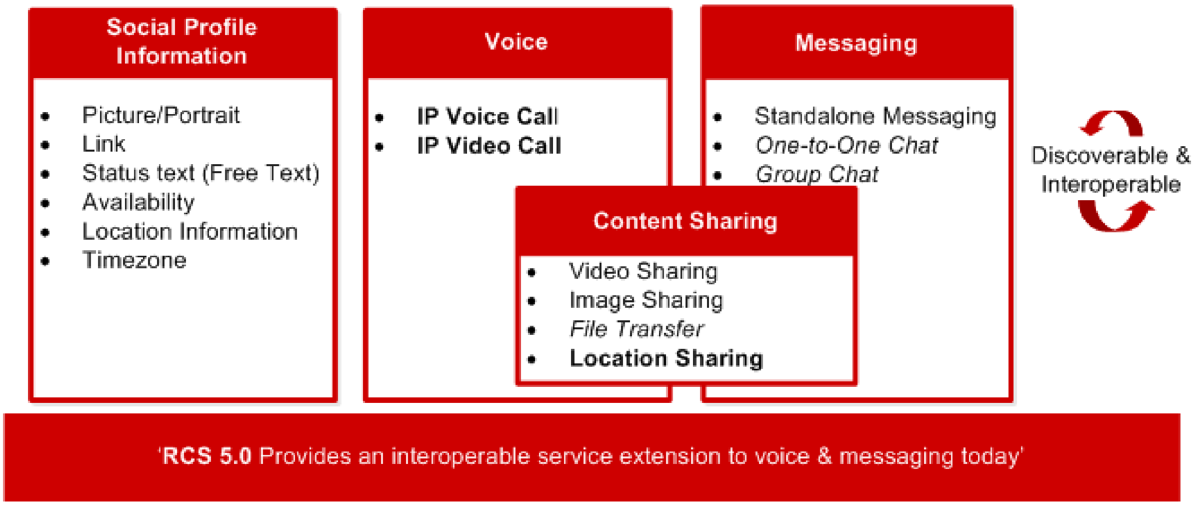


Figure 1: RCS 5.0 Positioning

As a headline, RCS provides an “interoperable extension to voice and messaging today”. The services are designed to run over data and can stand alone (e.g. share a picture from the media gallery) or be used in combination with a voice call (e.g. see-what-I-see video).

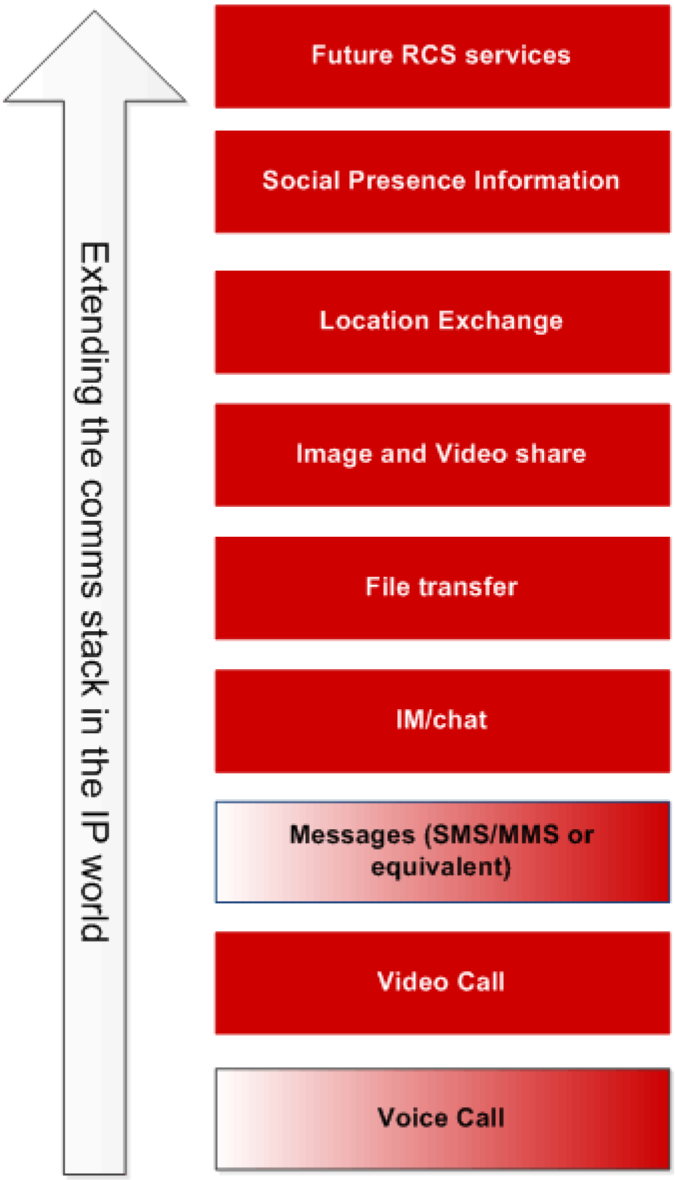

Extending the comms stack in the IP world
Future RCS services
Social Presence Information
Location Exchange
Image and Video share
File transfer
IM/chat
Messages (SMS/MMS or equivalent)
Video Call
Voice Call

Figure 2: RCS 5.0 Industry Proposition

As indicated in section 1.2.2, a Service Provider may choose not to deploy all services defined as part of RCS 5.0; however when deploying an individual RCS 5.0 service it will be interoperable with other Service Providers deploying the same service. This also means that even if this specification offers different deployment options to accommodate for different market realities, full interoperability between those deployments is provided for each corresponding service and for the RCS 5.0 discovery framework. As a consequence of the choices in this specification, RCS-e 1.2 is itself a subset of the RCS 5.0 functionality.

The cornerstone mechanism that enables RCS is a service or capability discovery framework. For example, when a user scrolls through their Address Book, they will see their contacts with the RCS services that are available to communicate.

This mechanism is implemented either using the Session Initiation Protocol's (SIP) OPTIONS request or using a Presence-based solution defined in RCS Release 1-4. Both will result in one of three types of response:

1. The contact is registered for service resulting in the contact's current service capabilities being received and logged by User A, or,
2. The contact is not registered (they are provisioned but not registered)
3. The contact is not found (they are not provisioned for service).

This discovery mechanism is important since it ensures User A can determine what services are available before communicating and allows Service Providers to roll-out new agreed services based on their own deployment schedule or market requirements. These same mechanisms can be used to initially discover (and/or periodically check) the service capabilities of all the contacts within an address book when the user first registers for the service.

1.2 Scope

This document extends the core principles and services framework from the initial set of functionalities defined in RCS-e 1.2 and RCS Release 1 to 4. The framework is designed to be extensible and to support new services going forward.

This document focuses mainly on the User Network Interface (UNI) which to a large extent also determines the Network-Network Interface (NNI). This document also specifies how networks who may choose a different set of deployment options (from the ones described) can work with each other. The interconnect-specific aspects of the NNI are described in a separate document (see [PRD-IR.90]).

It should be noted that the aim of this document is to only specify functionality that can be validated in standard compliant Internet Protocol (IP) Multimedia Subsystem (IMS) pre-production and production environments without major customisation or changes. Service Providers can still introduce customizations and changes to optimise or differentiate their networks however.

It should be noted that all text describing the User Experience (UX), pictures and flow diagrams are for informative purposes only, with the exception of those in Annex B.

1.2.1 Original Equipment Manufacturer (OEM) Integration

This specification is independent from any specific device operating system and is not intended to prescribe the supplier user experience. However, where appropriate key service logic is illustrated through wireframes to aid the reader. It is expected that each device or client supplier will map the basic service principles defined in this document within their own products and drive innovative and differentiated experiences.

1.2.2 Conformance

For terminals, the minimum conformance to the RCS 5.0 specification can be achieved by a terminal providing the necessary functionality to support the RCS framework, including the capability and new user discovery mechanism (covered in detail in section 2) and one or more of the services specified in detail in section 3. Support for multiple services is optional, however is highly recommended. These conformance criteria ensure that RCS can target low-end devices and therefore boost the market penetration curve.

For networks, the conformance criteria are similar. The framework should be supported including the measures to provide compatibility with all other deployed networks and at a minimum one of the services should be supported. Also, the network should prevent non-compliant clients from connecting to the network or affecting the UNI to a compliant client or the NNI to a compliant network.

1.3 Definition of Terms

Term	Description
2G	2nd Generation of Global System for Mobile Communications (GSM)
ACK	Acknowledgement
ACL	Access Control List
ADSL	Asymmetric Digital Subscriber Line
ALG	Application Layer Gateway
APN	Access Point Name
AP	Authentication Proxy
AS	Application Server
ASAP	As Soon As Possible
AVC	Advanced Video Codec
BA	Broadband Access
bool	Boolean
BP	Baseline Profile
bps	Bits per second (used with Mbps: Mega-, kbps: kilo-)
CA	Certification Authority
CAB	Converged Address Book
CPIM	Common Profile for Instant Messaging
CPM	Converged IP Messaging
CRLF	Carriage Return Line Feed
CS	Circuit Switched
CSFB	Circuit Switched FallBack
DNS	Domain Name System
DNS SRV	Domain Name System Service record
DRX	Discontinuous Reception
DTM	Dual Transfer Mode
DTX	Discontinuous Transmission
e2ae	end-to-access edge
e2e	end-to-end
EAB	Enhanced Address Book
EOF	End Of File
EUCR	End User Confirmation Request
FIFO	First IN First Out
FQDN	Fully Qualified Domain Name
FTTH	Fibre To The Home
GAA	Generic Authentication Architecture
GBA	Generic Bootstrapping Architecture
GBR	Guaranteed Bitrate
GGSN	Gateway General Packet Radio Service Support Node
GIBA	General Packet Radio Service -IMS-Bundled Authentication
GIF	Graphics Interchange Format
GML	Geography Markup Language
GMLC	Gateway Mobile Location Centre
GPRS	General Packet Radio Service
GPS	Global Positioning System
GRUU	Globally Routable User agent URI
GSM	Global System for Mobile Communications
GSMA	GSM Association
HPLMN	Home Public Land Mobile Network
H-SLP	Home SUPL Location Platform
HSPA	High Speed Packet Access
HSS	Home Subscriber Server
HTTP	Hyper-Text Transfer Protocol
HTTPS	Hyper-Text Transfer Protocol Secure

HW	HardWare
IARI	IMS Application Reference Identifier
ICSI	IMS Communication Service Identifier
IETF	Internet Engineering Task Force
IM	Instant Messaging. The term chat is also applied in this document to the same concept.
IMAP	Internet Mail Access Protocol
IM-AS	Instant Messaging Application Server Note: This equivalent terminology for Messaging Server is used in some of the figures
IMDN	Instant Message Disposition Notification
IMEI	International Mobile Station Equipment Identity
IMPI	Internet Protocol Multimedia Subsystem Private Identity
IMPU	Internet Protocol Multimedia Subsystem PUblic identity
IMS	Internet Protocol Multimedia Subsystem
IMSI	International Mobile Subscriber Identity
IMS AKA	IMS Authentication and Key Agreement
Int	Integer
IP	Internet Protocol
IPsec	Internet Protocol Security
IP-SM-GW	Internet Protocol Short Message Gateway
IPX	Internet Protocol Packet eXchange
ISIM	Internet Protocol Multimedia Services SIM
ISF	Interworking Selection Function
IWF	InterWorking Function
JPEG	Joint Photographic Experts Group
KB	KiloByte
LBS	Location Based Services
LTE	Long Term Evolution
MAP	Mobile Application Part
Messaging Server	A server providing support for the standalone messaging service (see section 3.2) according to [RCS5-CPM-CONVFUNC-ENDORS] and/or Chat (see sections 3.3 and 3.4) according to [RCS5-SIMPLEIM-ENDORS] or [RCS5-CPM-CONVFUNC-ENDORS]
MIME	Multipurpose Internet Mail Extensions
MLP	Mobile Location Protocol
MMS	Multimedia Message Service
MMS-C	Multimedia Messaging Service Centre
MMTEL	MultiMedia TELephony
MNO	Mobile Network Operator
MO	Management Object
MO-SMS	Mobile Originated Short Message Service
MPEG	Moving Pictures Experts Group
MSISDN	Mobile Subscriber Integrated Services Digital Network Number
MSRP	Message Session Relay Protocol
MSRPoTLS	Message Session Relay Protocol over Transport Layer Security
MTU	Maximum Transmission Unit
NAT	Network Address Translation
NGBR	Non-Guaranteed Bitrate
NNI	Network Network Interface
NW	NetWork
OEM	Original Equipment Manufacturer
OMA	Open Mobile Alliance
OMA-CP	Open Mobile Alliance Client Provisioning
OMA-DM	Open Mobile Alliance Device Management
OS	Operating System
OTP	One Time Password
PCO	Protocol Configuration Options
P-CSCF	Proxy-Call Session Control Function

PC	Personal Computer
PCC	Personal Contact Card
PDP	Packet Data Protocol
PDF	Portable Document Format
PIDF	Presence Information Data Format
PKI	Public Key Infrastructure
PNG	Portable Network Graphics
PRD	Permanent Reference Document
PS	Packet Switched
PSTN	Public Switched Telephone Network
QCI	Quality of Service Class Identifier
QoS	Quality of Service
RADIUS	Remote Authentication Dial In User Service
RAN	Radio Access Network
RCS	Rich Communication Suite
RCS-e	RCS enhanced
RCS User	An end user that has device or client (and the corresponding Service Provider subscription) supporting the RCS capability exchange framework and at least one of the services defined in the current specification.
RFC	Request For Comments
RLC	Radio Link Control
RLS	Resource List Server
RR	Receiver Report
RTCP	Real-time Transport Control Protocol
RTP	Real-time Transport Protocol
SASL	Simple Authentication and Security Layer
S-CSCF	Serving Call Session Control Function
SDP	Session Description Protocol
SDES	Session Description Protocol Security Descriptions for Media Streams
SET	Secure User Plane Location Enabled Terminal
SGs interface	3GPP defined reference point between the Mobility Management Entity and the Mobile Switching Centre
SIM	Subscriber Identity Module
SIMPLE	Session Initiation Protocol for Instant Messaging and Presence Leveraging Extensions
SIP	Session Initiation Protocol
SIPoTLS	Session Initiation Protocol over Transport Layer Security
SLA	Service Level Agreement
SMPP	Short Message Peer-to-Peer
SMS	Short Message Service
SMS-C	Short Message Service Centre
SMSoIP	Short Message Service over Internet Protocol
SP	Service Provider
SPI	Social Presence Information
SR	Sender Report
SRTP	Secure Real-time Transport Protocol
SSO	Single Sign On
STUN	Simple Traversal of User Datagram Protocol through Network Address Translations
SUPL	Secure User Plane Location
SW	SoftWare
TCP	Transmission Control Protocol
tel URI	telephone Uniform Resource Identifier
TLS	Transport Layer Security
UA	User Agent
UC	Use Case
UDP	User Datagram Protocol
UE	User Equipment
UI	User Interface
UMTS	Universal Mobile Telecommunications System

UNI	User Network Interface
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
USIM	Universal Subscriber Identity Module
UTC	Coordinated Universal Time
UUID	Universally Unique IDentifier
UX	User Experience
vCard	A format for electronic business cards
VIP	Very Important Person
VoHSPA	Voice over High Speed Packet Access
VoLTE	Voice over Long Term Evolution
W-CDMA	Wideband Code Division Multiple Access
Wi-Fi	Trademark of Industry Consortium "Wi-Fi Alliance" used as synonym for WLAN (Wireless Local Area Network)
WLAN	Wireless Local Area Network
XCAP	XML Configuration Access Protocol
XDM	XML Document Management
XDMC	XML Document Management Client
XDMS	XML Document Management Server
XML	Extensible Markup Language
XSD	XML Schema Definition
xSIM	Generic reference to different types of SIMs (e.g. USIM, ISIM, etc.)

1.4 Document Cross-References

Ref	Document Number	Title
1	[3GPP TS 23.221]	3GPP TS 23.221 Release 10, 3rd Generation Partnership Project; Architectural requirements http://www.3gpp.org
2	[3GPP TS 24.167]	3GPP TS 24.167 Release 10, 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; 3GPP IMS Management Object (MO) http://www.3gpp.org
3	[3GPP TS 24.229]	3GPP TS 24.229 Release 10, 3rd Generation Partnership IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP) http://www.3gpp.org
4	[3GPP TS 24.341]	3GPP TS 24.341 Release 10, 3rd Generation Partnership Support of SMS over IP networks; Stage 3 http://www.3gpp.org
5	[3GPP TS 26.141]	3GPP TS 26.141 Release 10, 3rd Generation Partnership IP Multimedia System (IMS) Messaging and Presence; Media formats and codecs http://www.3gpp.org
6	[3GPP TS 33.203]	3GPP TS 33.203 Release 10, 3rd Generation Partnership 3G security; Access security for IP-based services http://www.3gpp.org
7	[3GPP TS 33.222]	3GPP TS 33.222 Release 10, 3rd Generation Partnership Generic Authentication Architecture (GAA); Access to network application functions using Hypertext Transfer Protocol over Transport Layer Security (HTTPS) http://www.3gpp.org
8	[3GPP TS 33.328]	3GPP TS 33.328 Release 10, 3rd Generation Partnership IP Multimedia Subsystem (IMS) media plane security http://www.3gpp.org

9	[3GPP TR 33.978]	3GPP TR 33.978 Release 10, 3rd Generation Partnership Security aspects of early IP Multimedia Subsystem (IMS) http://www.3gpp.org
10	[IETF-DRAFT-SIPREC-PROTOCOL]	Session Recording Protocol, Version 02, http://tools.ietf.org/html/draft-ietf-siprec-protocol-02
11	[PRD-AA.60]	GSMA PRD AA.60 - “Template Agreement for Interworking” Version 8.1 4 December 2009 http://www.gsma.com/
12	[PRD-IR.33]	GSMA PRD IR.33 - “GPRS Roaming Guidelines” Version 6.0 25 May 2011 http://www.gsma.com/
13	[PRD-IR.58]	GSMA PRD IR.58 - “IMS Profile for Voice over HSPA” Version 1.0 28 December 2011 http://www.gsma.com/
14	[PRD-IR.65]	GSMA PRD IR.65 - “IMS Roaming and Interworking Guidelines” Version 6.0 30 August 2011 http://www.gsma.com/
15	[PRD-IR.67]	GSMA PRD IR.67 - “DNS/ENUM Guidelines for Service Providers & GRX/IPX Providers” Version 6.0 01 December 2011 Note: version to be updated once update containing RCS domain is available http://www.gsma.com/
16	[PRD-IR.74]	GSMA PRD IR.74 - “Video Share Interoperability Specification” 1.4 20 December 2010 http://www.gsma.com/
17	[PRD-IR.79]	GSMA PRD IR.79 - “Image Share Interoperability Specification” 1.4 29 March 2011 http://www.gsma.com/
18	[PRD-IR.84]	GSMA PRD IR.84 - “Video Share Phase 2 Interoperability Specification” 2.2 30 December 2010 http://www.gsma.com/
19	[PRD-IR.88]	GSMA PRD IR.88 - “LTE Roaming Guidelines” 6.0 31 August 2011 http://www.gsma.com/
20	[PRD-IR.90]	GSMA PRD IR.90 - “RCS Interworking Guidelines” 2.1 21 October 2010 http://www.gsma.com/
21	[PRD-IR.92]	GSMA PRD IR.92 - “IMS Profile for Voice and SMS” 4.0 22 March 2011 http://www.gsma.com/
22	[PRD-IR.94]	GSMA PRD IR.94 - “IMS Profile for Conversational Video Service” Version 1.0 28 December 2011 http://www.gsma.com/
23	[RCSe12]	GSMA RCS-e - Advanced Communications: Services and Client Specification version 1.2.1 http://www.gsma.com/
24	[RCS5-SIMPLEIM-ENDORS]	GSMA RCS 5.0 Endorsement of OMA SIP/SIMPLE IM 1.0, Version 1.0 19 April 2012 http://www.gsma.com/
25	[RCS5-CPM-CONVFUNC-ENDORS]	GSMA RCS 5.0 Endorsement of OMA CPM 1.0 Conversation Functions, Version 1.0 19 April 2012 http://www.gsma.com/
26	[RCS5-CPM-IW-ENDORS]	GSMA RCS 5.0 Endorsement of OMA CPM 1.0 Interworking, Version 1.0 19 April 2012 http://www.gsma.com/

27	[RCS5-3GPP-SMSIW-ENDORS]	GSMA RCS 5.0 Endorsement of 3GPP TS 29.311 Service level Interworking for Messaging Services, Version 1.0 19 April 2012 http://www.gsma.com/
28	[RCS5-CPM-MSGSTOR-ENDORS]	GSMA RCS 5.0 Endorsement of OMA CPM 1.0 Message Storage, Version 1.0 19 April 2012 http://www.gsma.com/
29	[PRIVACY-API]	GSMA Canadian OneAPI Pilot, Privacy Service Developer Guide v1.7 – November 2011 https://canada.oneapi.gsmworld.com
30	[RFC2396]	Uniform Resource Identifiers (URI): Generic Syntax IETF RFC http://tools.ietf.org/html/rfc2396
31	[RFC2425]	A MIME Content-Type for Directory Information IETF RFC http://tools.ietf.org/html/rfc2425
32	[RFC2426]	vCard MIME Directory Profile IETF RFC http://tools.ietf.org/html/rfc2426
33	[RFC2595]	Using TLS with IMAP, POP3 and ACAP IETF RFC http://tools.ietf.org/html/rfc2595
34	[RFC2617]	HTTP Authentication: Basic and Digest Access Authentication IETF RFC http://tools.ietf.org/html/rfc2617
35	[RFC3261]	SIP (Session Initiation Protocol) IETF RFC http://tools.ietf.org/html/rfc3261
36	[RFC3264]	An Offer/Answer Model Session Description Protocol IETF RFC http://tools.ietf.org/html/rfc3264
37	[RFC3329]	Security Mechanism Agreement for the Session Initiation Protocol (SIP) IETF RFC http://tools.ietf.org/html/rfc3329
38	[RFC3428]	Session Initiation Protocol (SIP) Extension for Instant Messaging IETF RFC http://tools.ietf.org/html/rfc3428
39	[RFC3501]	INTERNET MESSAGE ACCESS PROTOCOL - VERSION 4rev1 IETF RFC http://tools.ietf.org/html/rfc3501
40	[RFC3711]	The Secure Real-time Transport Protocol (SRTP) IETF RFC http://tools.ietf.org/html/rfc3711
41	[RFC3840]	Indicating User Agent Capabilities in the Session Initiation Protocol (SIP), IETF RFC http://tools.ietf.org/html/rfc3840
42	[RFC3858]	An Extensible Markup Language (XML) Based Format for Watcher Information, IETF RFC http://tools.ietf.org/html/rfc3858
43	[RFC3862]	Common Presence and Instant Messaging (CPIM): Message Format IETF RFC http://tools.ietf.org/html/rfc3862
44	[RFC3863]	Presence Information Data Format (PIDF) IETF RFC http://tools.ietf.org/html/rfc3863
45	[RFC3903]	Session Initiation Protocol (SIP) Extension for Event State Publication IETF RFC http://tools.ietf.org/html/rfc3903
46	[RFC3966]	The tel URI for Telephone Numbers IETF RFC http://tools.ietf.org/html/rfc3966
47	[RFC3994]	Indication of Message Composition for Instant Messaging IETF RFC http://tools.ietf.org/html/rfc3994
48	[RFC4028]	The Session Timers in the Session Initiation Protocol (SIP) IETF RFC http://tools.ietf.org/html/rfc4028
49	[RFC4122]	The Universally Unique IDentifier (UUID) URN Namespace IETF RFC http://tools.ietf.org/html/rfc4122
50	[RFC4479]	A Data Model for Presence, IETF RFC http://tools.ietf.org/html/rfc4479

51	[RFC4480]	RPID: Rich Presence Extensions to the Presence Information Data Format (PIDF), IETF RFC http://tools.ietf.org/html/rfc4480
52	[RFC4483]	A Mechanism for Content Indirection in Session Initiation Protocol (SIP) Messages IETF RFC http://tools.ietf.org/html/rfc4483
53	[RFC4568]	Session Description Protocol (SDP) Security Descriptions for Media Streams, IETF RFC http://tools.ietf.org/html/rfc4568
54	[RFC4572]	Connection-Oriented Media Transport over the Transport Layer Security (TLS) Protocol in the Session Description Protocol (SDP), IETF RFC http://tools.ietf.org/html/rfc4572
55	[RFC4589]	Location Types Registry, IETF RFC http://tools.ietf.org/html/rfc4589
56	[RFC4825]	The Extensible Markup Language (XML) Configuration Access Protocol (XCAP) IETF RFC http://tools.ietf.org/html/rfc4825
57	[RFC4961]	Symmetric RTP / RTP Control Protocol (RTCP) IETF RFC http://tools.ietf.org/html/rfc4961
58	[RFC4975]	The Message Session Relay Protocol (MSRP) IETF RFC http://tools.ietf.org/html/rfc4975
59	[RFC5196]	Session Initiation Protocol (SIP) User Agent Capability Extension to Presence Information Data Format (PIDF) IETF RFC http://tools.ietf.org/html/rfc5196
60	[RFC5438]	Instant Message Disposition Notification (IMDN) IETF RFC http://tools.ietf.org/html/rfc5438
61	[RFC5438Errata]	Instant Message Disposition Notification (IMDN) IETF RFC 5438 Errata ID 3013 http://www.rfc-editor.org/errata_search.php?rfc=5438 (see also section C.2)
62	[RFC5491]	GEOPRIV Presence Information Data Format Location Object (PIDF-LO) Usage Clarification, Considerations, and Recommendations IETF RFC http://tools.ietf.org/html/rfc5491
63	[RFC5547]	A Session Description Protocol (SDP) Offer/Answer Mechanism to Enable File Transfer IETF RFC http://tools.ietf.org/html/rfc5547
64	[RFC5626]	Managing Client-Initiated Connections in the Session Initiation Protocol (SIP) IETF RFC http://tools.ietf.org/html/rfc5626
65	[RFC5627]	Using Globally Routable User Agent URIs (GRUUs) in the Session Initiation Protocol (SIP) IETF RFC http://tools.ietf.org/html/rfc5627
66	[RFC6135]	Alternative Connection Model for the Message Session Relay Protocol (MSRP) IETF RFC http://tools.ietf.org/html/rfc6135
67	[RFC6223]	Indication of Support for Keep-Alive IETF RFC http://tools.ietf.org/html/rfc6223
68	[GML3.1.1]	OpenGIS® Geography Markup Language (GML) Implementation Specification, Version 3.1.1, OGC 03-105r1 http://www.opengeospatial.org/
69	[CAB_TS]	OMA Converged Address Book (CAB) Specification, Candidate Version 1.0, 19 October 2010 http://www.openmobilealliance.org
70	[CONNMO]	OMA Standardized Connectivity Management Objects for use with OMA Device Management, Approved Version 1.0 – 07 Nov 2008 http://www.openmobilealliance.org
71	[CONNMOHTTP]	Standardized Connectivity Management Objects HTTP Proxy Parameters for use with OMA Device Management, Approved Version 1.0 – 24 Oct 2008 http://www.openmobilealliance.org

72	[CPM-SYS_DESC]	OMA Converged IP Messaging System Description, Candidate Version 1.0 – 12 Oct 2010 http://www.openmobilealliance.org
73	[OMA-DM]	OMA Device Management, Approved Version 1.2.1 – 17 Jun 2008 http://www.openmobilealliance.org
74	[MMSMO]	OMA Management Object for MMS, Candidate Version 1.3 – 28 Jan 2008 http://www.openmobilealliance.org
75	[Location_API]	RESTful bindings for Parlay X Web Services – Terminal Location, Candidate Version 1.1 – 11 Jan 2011 http://www.openmobilealliance.org
76	[Presence]	OMA Presence SIMPLE Specification, 1.1, http://www.openmobilealliance.org/
77	[Presence2.0_DDS]	Presence SIMPLE Data Specification, Approved Version 2.0, 29 September 2009 http://www.openmobilealliance.org/
78	[Presence2.1_DDS]	Presence SIMPLE Data Specification, Approved Version 2.1, 02 October 2010 http://www.openmobilealliance.org/
79	[Presence2.0_TS]	Presence SIMPLE Specification, Candidate Version 2.0, 02 December 2010 http://www.openmobilealliance.org/
80	[Presence2.0_RLS_TS]	Resource List Server (RLS) Specification, Candidate version 2.0, 02 December 2010 http://www.openmobilealliance.org/
81	[Presence_Content]	Presence Content XDM Specification, Candidate Version 1.0, 23 December 2008 http://www.openmobilealliance.org/
82	[PRESENCEIG]	Implementation Guidelines for OMA Presence SIMPLE v1.1 Presence http://www.openmobilealliance.org/
83	[PRESENCEMO]	OMA Management Object for Presence SIMPLE, Approved Version 1.0, 25 February 2010 http://www.openmobilealliance.org
84	[PRESENCE2MO]	OMA Management Object for Presence SIMPLE 2.0, Candidate version 2.0, 17 September 2009 http://www.openmobilealliance.org
85	[PresenceXDM]	Presence XDM Specification, Approved Version 1.1 – 27 Jun 2008 http://www.openmobilealliance.org/
86	[RLSXDM]	Resource List Server (RLS) XDM Specification Approved Version 1.1 – 27 Jun 2008, http://www.openmobilealliance.org/
87	[SHARED-XDM]	Shared XDM Specification, Approved Version 1.1 – 27 Jun 2008 http://www.openmobilealliance.org/
88	[SUPL]	Secure User Plane Location, Candidate Version 2.0 – 27 May 2011 http://www.openmobilealliance.org/
89	[SUPLMO]	OMA Management Object for SUPL, Candidate Version 2.0 – 27 Jan 2011 http://www.openmobilealliance.org/
90	[XDM1.1_AD]	XML Document Management Architecture, Approved Version 1.1, 27 June 2008 http://www.openmobilealliance.org/
91	[XDM2.0_AD]	XML Document Management Architecture, Candidate Version 2.0, 16 September 2008 http://www.openmobilealliance.org/
92	[XDM1.1_Core]	XML Document Management (XDM) Specification, Approved Version 1.1, 27 June 2008 http://www.openmobilealliance.org/
93	[XDM2.0_Core]	XML Document Management (XDM) Specification, Candidate Version 2.0, 16 September 2008 http://www.openmobilealliance.org/
94	[XDMIG]	Implementation Guidelines for OMA XDM v1.1, http://www.openmobilealliance.org/

95	[XDMMO]	OMA Management Object for XML Document Management 1.1, http://www.openmobilealliance.org
96	[vCard21]	vCard, The Electronic Business Card, A versit Consortium Specification, 18 Sep 1996 http://www.imc.org/pdi/vcard-21.doc

1.5 Differences to previous specifications

RCS 5.0 takes its input from both RCS Release 4 and RCS-e 1.2. The following table lists the major differences

Area	Differences From RCS Release 4	Differences From RCS-e
General	• All services are optional Note: The capability discovery framework described in section 2 is mandatory though	• All services are optional Note: The capability discovery framework described in section 2 is mandatory though
Provisioning (See section 2.3)	• Support for optional HTTP(S)-based provisioning in addition to the Open Mobile Alliance's (OMA) Device Management (OMA-DM) • Description of provisioning triggers • Additional parameters	• OMA Client Provisioning (CP) no longer supported • Additional parameters
Registration (see section 2.4)	• Better alignment with Voice over Long Term Evolution (VoLTE) • Authentication described • New tags	• Better alignment with VoLTE including support for IMS AKA (IMS Authentication and Key Agreement) • New tags
Addressing (See section 2.5)	• Support for generic SIP Uniform Resource Identifiers (URIs)	No major differences
Capability and new user discovery (See section 2.6)	• Support for SIP OPTIONS based discovery • Support for fallback from Presence-based discovery to SIP OPTIONS • Support for interworking between presence and SIP OPTIONS • Description of the actions that trigger a capability discovery	• Support for fallback from Presence-based discovery to SIP OPTIONS • Support for interworking between presence and SIP OPTIONS
Capability values and status (See section 2.7)	• New capabilities • Description of the network coverage required for providing capabilities	• New capabilities
Protocol support (See section 2.8)	• Better support for Network Address Translation (NAT) Traversal • Support for secured protocols	• Support for Internet Mail Access Protocol (IMAP) and Secure User Plane Location (SUPL)
Cellular access (See section 2.9.1)	• Better description of what Access Point Name (APN) to use • Support for switchover to Wi-Fi • Improved Long Term Evolution (LTE) support: support for devices also supporting VoLTE	• Improved LTE support: support for devices also supporting VoLTE
Broadband Access (See section 2.9.2)	No major differences	No major differences
Multidevice (See section 2.11)	• Generic support for individual device addressing using sip.instance in addition to the existing Globally Routable User	No major differences

	agent URIs (GRUUs) which is used for messaging	
Security (See section 2.13)	• Authentication and security mechanisms specified in detail • Support for Transport Layer Security (TLS) enabled protocols including negotiation	• Support for IMS AKA in scope
NNI (See section 2.12)	• Compatibility mechanisms employed	• Compatibility mechanisms employed
End user confirmation requests (See section 2.10)	New functionality: not available in RCS Release 4	• New method and parameters
Standalone messaging (See section 3.2)	• Support for routing to device based on sip.instance	New functionality: not available in RCS-e 1.2
1-to-1 chat (See section 3.3)	• Support for both OMA SIMPLE (SIP for Instant Messaging and Presence Leveraging Extensions) IM (Instant Messaging) and OMA CPM (Converged IP Messaging) • Improved interworking between SIMPLE IM and CPM • Support for Store and forward when destination user is offline • Support for delivery and display notifications • Improved multidevice handling • Support for blacklist in the device	• Support for both SIMPLE IM and CPM • Interworking between SIMPLE IM and CPM
Group Chat (See section 3.4)	• Support for both SIMPLE IM and CPM • Interworking between SIMPLE IM and CPM • Support for delivery and display notifications • Support for blacklist in the device	• Support for both SIMPLE IM and CPM • Interworking between SIMPLE IM and CPM • Support for delivery and display notifications
File Transfer (See section 3.5)	• Support for both SIMPLE IM and CPM • Interworking between SIMPLE IM and CPM • Support for resumption, blacklist in the device, thumbnail and contact card push	• Support for both SIMPLE IM and CPM • Interworking between SIMPLE IM and CPM • Support for resumption, thumbnail and contact card push
Content sharing (See section 3.6)	• No support for image sharing with real-time interactions anymore • No support for network value added services • H.264 baseline profile level 1b is now the mandatory video codec • Video sharing inside a voice call can be bi-directional	• Support for video sharing outside of a voice call
Social Presence Information (See section 3.7)	No major differences	• Support for VIP (Very Important Person) and non-VIP groups • Support for inclusion of geolocation information

IP Voice Call (See section 3.8)	• Is now fully supported on mobile devices	• Is now fully supported on mobile devices
IP Video Call (See section 3.9)	**New functionality: not available in RCS Release 4**	**New functionality: not available in RCS-e 1.2**
Geolocation sharing (See section 3.10)	**New functionality: not available in RCS Release 4**	**New functionality: not available in RCS-e 1.2**

Table 1: Overview of differences with RCS Release 4 and RCS-e

2 RCS 5 General Procedures

2.1 RCS 5 architecture

For RCS 5.0, the one mandatory network element is the IMS core system which enables peer-to-peer communication between RCS clients. Other network nodes can be deployed by the Service Provider to provide additional parts of the RCS feature set. Figure 3 illustrates a simplified example of the RCS architecture; a Service Provider may choose a different approach to implement a function within the Service Provider domain not influencing the interoperable NNI aspects.

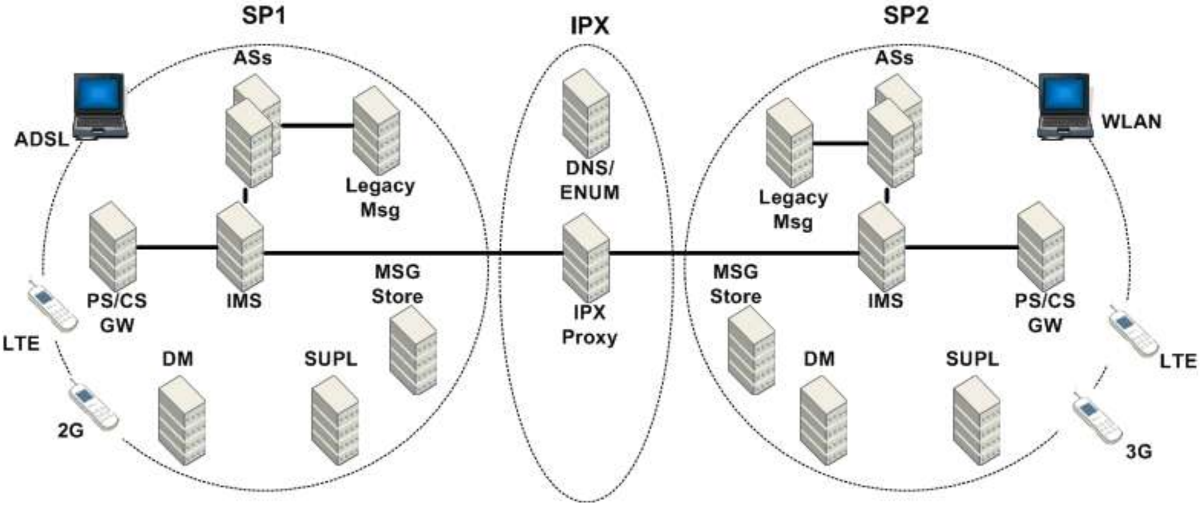


Figure 3: Simplified Example of RCS Architecture

The PS/CS gateway (GW) is used for interworking between Circuit Switched (CS) and Packet Switched (PS) voice, for example Voice over Long Term Evolution (VoLTE). SUPL indicates the Secure User Plane Location element as documented in [SUPL] to support exchanging geolocation information as part of Social Presence Information (SPI) and Geolocation PUSH and PULL. Msg Store relates to the CPM (Converged IP Messaging) Message Storage Server as illustrated in section 3.2. Legacy Msg refers to the Short Message Service (SMS)/Multimedia Message Service (MMS) services that may be utilized via an IWF (Interworking Function) located in the group of Application Servers (ASs) which in addition to these IWF node(s) may also include various other nodes used by the RCS services, for example:

- Presence Server
- Messaging Server
- XML (Extensible Markup Language) Document Management (XDM) Server (XDMS)
- Multimedia Telephony (MMTEL) Application Server
- Video Share Application Server, as utilized in [PRD-IR.84]

Figure 3 shows examples of two RCS Service Providers exchanging traffic with each other using the standard Network-to-Network Interface (NNI) mechanisms (IPX, IP Packet Exchange) as documented in [PRD-IR.90]. RCS is offered as an intra-Service Provider service however this example shows an inter-Service Provider scenario.

RCS compliant access networks include, but are not limited to, those illustrated in the Figure 3. Thus, deploying the RCS service does not indicate a 3G network should always be deployed. Further details of RCS services relating to particular access networks are found in section 2.6.4.1.

2.2 RCS Device Types

RCS defines these types of devices for voice service:

- RCS IP Voice Call capable (and CS capable) device with LTE (Long Term Evolution) access control (RCS-LTE, e.g., LTE smartphone with VoLTE support). An RCS-LTE device is configured for VoLTE unless otherwise stated;
- RCS IP Voice Call capable (and CS capable) device with HSPA access control (RCS-HSPA, e.g., 3G smartphone). An RCS-HSPA device is configured for VoHSPA unless otherwise stated;
- Access agnostic RCS IP Voice Call capable device with no LTE or HSPA access control (RCS-AA, e.g., a PC notebook with an LTE stick or another type of broadband access, or a tablet);
- Access agnostic RCS non-IP Voice Call capable device with CS voice (RCS-CS, e.g., a 3G smartphone without VoHSPA support).

Device enabled for VoLTE/VoHSPA: This is an RCS-LTE or RCS-HSPA device which is configured to use VoLTE/VoHSPA as described in section 2.9.1 in this document.

An RCS-LTE or RCS-HSPA device which is not enabled for VoLTE/VoHSPA (e.g. no subscription supporting these services) is considered as an RCS-CS device.

An RCS–AA device shall take into account the handling defined for RTP and RTCP NAT Traversal defined in section 2.6.1.

2.3 Configuration Procedures

RCS services can only be initiated once the client is configured and the user (uniquely identified by the relevant IMS Unique Resource Identifier [URI]; that is a tel URI and/or a SIP URI) is correctly provisioned to access the RCS services.

Both processes should be performed automatically. This gives the end user the impression that the new services are working out of the box and also minimises the operational impact on Service Providers.

A mobile network implementing RCS should be able to detect when a user connects to the network with an RCS capable device for the first time. This event triggers two processes:

1. Service provisioning: The relevant configuration is performed on the network to make the RCS services available to the user (e.g. provisioning an account on the IMS core and relevant application servers).
   Note: In addition to this autoprovisoning on first usage, the service may be provisioned in advance by the Service Provider.
2. Client configuration: The network provides the client configuration using one of the mechanisms described in section 2.3.3. The configuration document comprises of a set of configuration parameters, some required to operate and others to configure the client behaviour.

2.3.1 First-time Registration

The assumption in this scenario is that User A is entitled to access the RCS services (because for example the tariff includes the service) however they have never used an RCS enabled device previously.

Prior to the registration, it is necessary to provision the user on the network (e.g. by autoprovisioning) and to configure the client with the correct settings as described further in section 2.3. When the provisioning and client configuration is completed, the first-time registration procedure takes place. The first step is to register (as described in section 2.4) and to find the subset among the existing contacts (if any) who are also RCS users (as described in section 2.6.2).

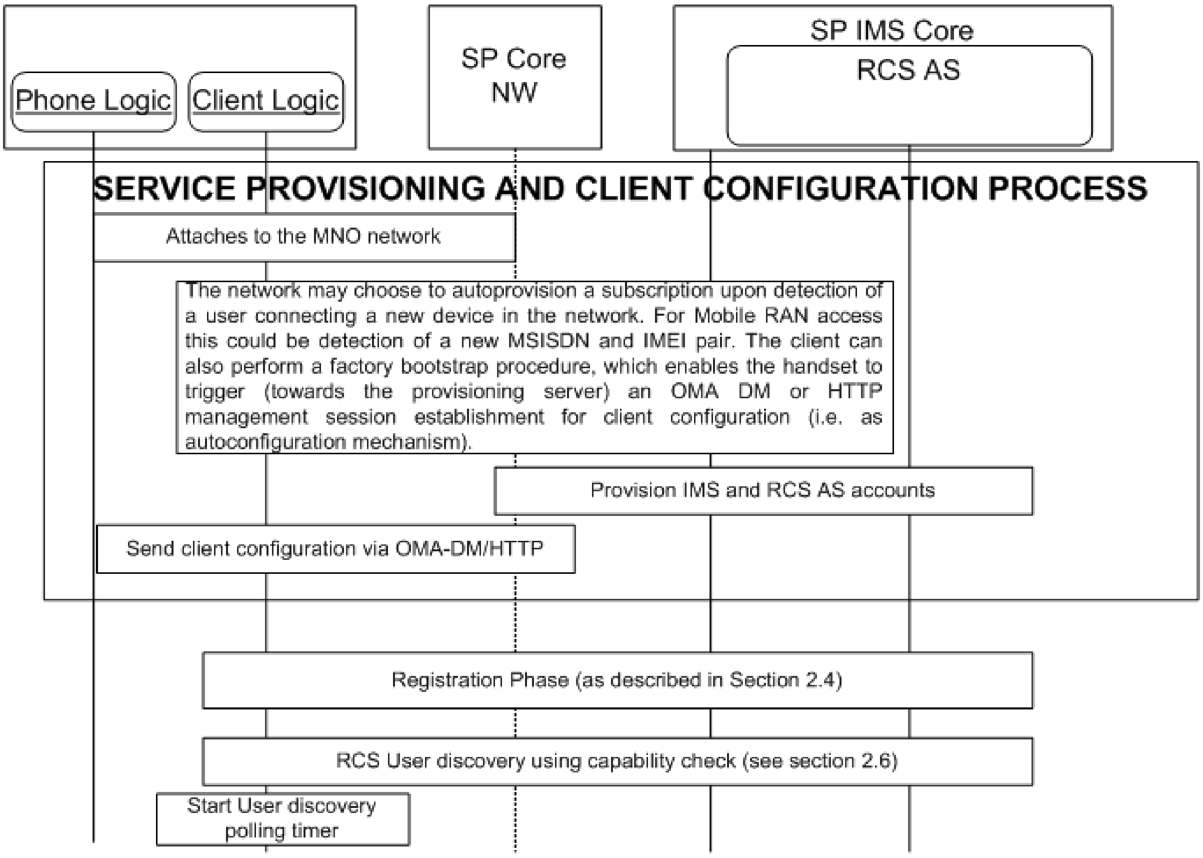

Phone Logic
Client Logic
SP Core NW
SP IMS Core
RCS AS
SERVICE PROVISIONING AND CLIENT CONFIGURATION PROCESS
Attaches to the MNO network
The network may choose to autoprovision a subscription upon detection of a user connecting a new device in the network. For Mobile RAN access this could be detection of a new MSISDN and IMEI pair. The client can also perform a factory bootstrap procedure, which enables the handset to trigger (towards the provisioning server) an OMA DM or HTTP management session establishment for client configuration (i.e. as autoconfiguration mechanism).
Provision IMS and RCS AS accounts
Send client configuration via OMA-DM/HTTP
Registration Phase (as described in Section 2.4)
RCS User discovery using capability check (see section 2.6)
Start User discovery polling timer

Figure 4: First-Time Start Sequence Diagram

As shown in the Figure 4, the first activity before an RCS device can be used is service provisioning and configuration, which can be triggered in a variety of ways. When the device is powered on, the network may be able to identify that the user/device pair can use RCS services and, as a consequence, trigger the relevant device configuration described in more detail later in this section. This triggering process is network specific and outside the scope of this specification. The device may also be able to perform a customized bootstrap (also named factory bootstrap) operation to trigger a client-initiated Open Mobile Alliance Device Management (OMA-DM) session towards the OMA-DM server for client configuration purposes.

An alternative to this automated mechanism could be a manually triggered configuration (e.g. requested by an operator in a store).

2.3.1.1 Additional first-time configuration scenarios

In addition to the scenario described in the section 2.3.1 (first time the user registers with the IMS network), there are several additional scenarios where the same sequence applies:

- When the customer changes to another RCS enabled device: In this case, the sequence is identical however the IMS provisioning (i.e. provision IMS and RCS AS accounts) is not required as it was performed previously.
- When the customer changes the Subscriber Identity Module (SIM) card: In this case, the sequence is identical to the one described in the section 2.3.1.
- A configuration update is required that implies changes in the user’s IMS identity (that is tel URI and/or SIP URI).
- A configuration update is required that implies changes in the capability discovery mechanism: As described in section 2.6, switching the capability discovery mechanism parameter automatically triggers the same process. This parameter is described in Annex A (section A.1.10).

2.3.2 Client configuration parameters

The set of client settings is presented in Annex A: Managed objects and configuration parameters.

All the parameters describing the configuration can only be modified by the Service Provider (via Service Provider customization settings or one of the procedures described in section 2.3.3) and are not accessible to the terminal user.

In a device enabled for Voice over LTE (VoLTE)/Voice over High Speed Packet Access (VoHSPA, see section 2.2), the default IMS settings as defined in [PRD-IR.92]/[PRD-IR.58] are expected to be used. Therefore as stated in section A.1.6.1 the parameters referred to from section A.1.6.2 and those in Table 55 are not used in this case.

After configuration, the client is ready to register with the network for the first time. Once this registration is completed, the user is able to access the RCS services. These configuration options could also be updated later by the Service Provider pushing new configuration documents using the OMA-DM enabler or the other configuration mechanisms defined in section 2.3.3.

2.3.3 RCS Client autoconfiguration mechanisms

2.3.3.1 Overview

This specification contemplates two alternative mechanisms to perform the autoconfiguration of the RCS functionality in terminals carrying the SIM associated with the user’s main identity:

1. [OMA-DM]: This is the same mechanism as the one proposed for RCS based on the managed object configuration proposed in Annex A, section A.2. All RCS capable devices (including open-market devices) shall support the following requirements for OMA-DM:

    - Multiple management authorities where Service Provider Device Management accounts are persistent, not editable and not visible to the user (e.g. Software (SW) updates do not delete/overwrite DM accounts) and accessible by the respective active Service Provider DM account only (protected by the OMA-DM Access Control List (ACL) mechanism).

    - The active Service Provider’s DM account needs to be selected and activated on SIM card change.

    - The settings are protected against non-Service Provider authorities (by the OMA-DM ACL mechanism).

    - Each Service Provider should have its own RCS management sub-tree and the OMA-DM account does have access to the device settings (e.g. for the purpose of access settings configuration if needed).

    - The active Service Provider’s RCS management sub-tree needs to be visible, selected and activated on SIM card changes.

    - The provided settings are active/updated and used on RCS client after successful configuration.

    - The device shall support the customized bootstrap (also named factory bootstrap, that is the Service Provider OMA-DM account, including OMA-DM server address, is loaded in the device at factory phase) procedure (as specified in section 5.1.2.1 of OMA Device Management Bootstrap, see [OMA-DM]) to trigger a client-initiated management session towards the OMA-DM server (operated by the Service Provider which the device is subscribing to, the Home Public Land Mobile Network (HPLMN)) allowing the OMA-DM client to initiate and perform a client configuration procedure for RCS configuration parameters.

    - The device shall be able to perform the factory bootstrap procedure[1]:
        - When a device is switched on for the first time
        - When the user changes the SIM card on the device if no stored configuration is available for the new SIM (see section 2.3.4)
    - After successfully processing the bootstrap, the DM client of the device shall automatically initiate a management session to the DM server configured in the bootstrap at the next practical opportunity[2] (that is when network connectivity and other factors would allow such a connection).

2. An optional mechanism defined further in section 2.3.3.2 based on the (Secure) Hypertext Transfer Protocol (HTTP/HTTPS) which can be requested by a Service Provider (i.e. during customization) with the following main goals:
    - Enabling a configuration procedure transparent to the user
    - Reducing the auto-detection mechanism complexity on a network infrastructure

For the configuration of additional devices (i.e. not carrying the SIM associated to the subscriber's main identity), the HTTP(S) mechanism shall be used as described in section 2.3.3.2.6.

Note: Although RCS provides different mechanisms to perform the auto-configuration, the configured parameters remain the same and are independent of the mechanism that is used. The used mechanism only determines the used protocol and the encoding of the parameters between the client and the network.

2.3.3.2 HTTP(S) based client configuration

The new mechanism is based on a HTTPS request made by the device to a configuration server to acquire the configuration data:

- Every time the device boots (or when the SIM is swapped without rebooting the terminal [hot swap]), there is an initial HTTP request to the RCS configuration server to acquire the current configuration settings version.
    - Note that in the case of a non-embedded mobile client or a PC client without SIM, this check should be performed every time the client is restarted.
- If the versions do not match, the server will include a configuration document in XML format with all the settings. This configuration document is covered in detail in Annex A, sections A.2 and A.3 and based on the OMA Client Provisioning (OMA-CP) syntax.
- If it is necessary to force a reconfiguration (e.g. SIM card swap), the device will reset the version value to 0 (the server configuration shall always have a value bigger than 0).
- If the Service Provider disables the RCS functionality from a device/client, the response will be an empty XML setting the version to 0 or -1.

The details on the exchanges (e.g. format employed for the requests) are covered in sections 2.3.3.2.1, 2.3.3.2.2, 2.3.3.2.3, 2.3.3.2.4, 2.3.3.2.5 and 2.3.3.2.6.

This alternative configuration mechanism works on the following pre-assumptions:

- As a security measure and to ensure the network can implement the necessary procedures to resolve the user's Mobile Subscriber Integrated Services Digital Network Number (MSISDN) (that is Remote Authentication Dial In User Service (RADIUS) requests, header enrichment and so on), the configuration of terminals carrying the SIM

[1] The Service Provider network may trigger an OMA-DM configuration when a configured SIM is used in a different device.

[2] This is an additional requirement compared to the OMA DM 1.2.1 specifications.

associated to the user's main identity can only occur if connected using a mobile PS[3] data network and, therefore, the device should have the necessary Access Point Name (APN) configuration to perform the connection.
Note: For other terminals the mechanisms defined in section 2.3.3.2.6 can be used.

- As some of the mechanisms presented in the previous paragraphs require an initial HTTP request, an HTTP request is performed first:
    - The device/client shall perform an HTTP request to the RCS autoconfiguration server's qualified domain name. In this initial request the GET parameters mentioned in Table 2 should not be included.
    - As a result of this request, the autoconfiguration server returns a HTTP 200 OK response. The client will then perform a second request towards the same Uniform Resource Locator (URL) with only the protocol change, this time using HTTPS. Note that the RCS configuration server should be able to correlate both HTTP and HTTPS requests on the server side. To achieve this, the server will provide a cookie in the response to the initial HTTP request (Set-Cookie header) and it will expect to receive that cookie in the subsequent HTTPS request (Cookie header).
- From the UX perspective, the customer is not aware of the configuration process (it is a background process with no pop-ups or notifications shown on the screen) unless the provisioned data includes a message for the end user.

It should also be noted that this mechanism also contributes to reduce the complexity of the auto-detection mechanism as the device will proactively request an update of the configuration settings every time the device is rebooted. However, for a non-embedded mobile client, an update on each client start is required.

2.3.3.2.1 *Initial Request*

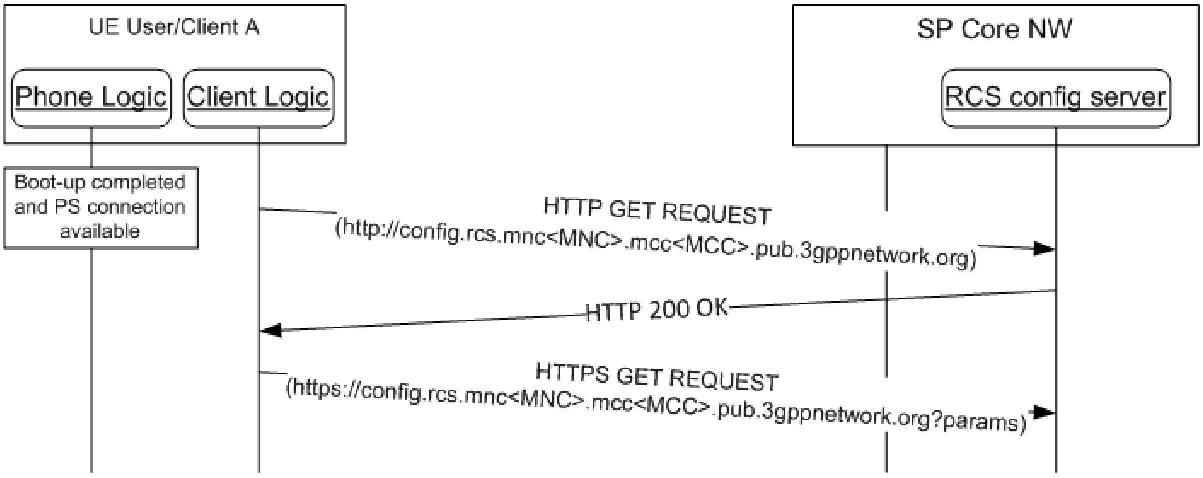

UE User/Client A
Phone Logic
Client Logic
SP Core NW
RCS config server
Boot-up completed and PS connection available
HTTP GET REQUEST (http://config.rcs.mnc<MNC>.mcc<MCC>.pub.3gppnetwork.org)
HTTP 200 OK
HTTPS GET REQUEST (https://config.rcs.mnc<MNC>.mcc<MCC>.pub.3gppnetwork.org?params)

Figure 5: RCS HTTP(S) configuration: Initial request

Parameters: The following information is passed as HTTP GET parameters using a query string:

[3] Please note that if a device does not have a Packet Switched (PS) connection, the autoconfiguration can also happen over Wi-Fi. The decision to implement this mechanism is up to the discretion of each Service Provider.

Parameter	Description	Mandatory	Format
vers	This is either -1, 0 or a positive integer. 0 indicates that the configuration must be updated (e.g. configuration is damaged, non-existent or follows a SIM change). A positive value indicates the version of the static parameters (those which are not subscriber dependent) so the server can evaluate whether an update is required. -1 indicates that the device/client must disable the RCS services including the autoconfiguration query performed at boot.	Y	Int (-1, 0 or a positive integer)
IMSI (International Mobile Subscriber Identity)	If available, the subscriber's IMSI should be sent as a parameter	N if the Operating System (OS) platform allows it, it shall be included	String (15 digits)
client_vendor	String that identifies the vendor providing the RCS solution.	Y	String (4), Case-Sensitive
client_version	String that identifies the RCS solution version.	Y	String (10 max), Case-Sensitive
terminal_vendor	String that identifies the terminal OEM.	Y	String (4), Case-Sensitive
terminal_model	String that identifies the terminal model.	Y	String (10 max), Case-Sensitive
terminal_sw_version	String that identifies the terminal software version.	Y	String (10 max), Case-Sensitive
IMEI (International Mobile Station Equipment Identity)	If available, the subscriber's IMEI should be sent as a parameter. The idea is that for those Service Providers supporting a comprehensive device database, the terminal_X parameters can be then ignored and the IMEI used instead, if available to the RCS implementation.	N if the OS platform allows it, it shall be included	String (15 digits)

Table 2: RCS alternative configuration: HTTPS request GET parameters

Please note that the client and terminal vendor, model and version parameters format and values should be agreed with the relevant Service Provider prior to any device or client commercialization or update.

- The configuration server URL will be composed based on the home Service Provider's MCC (Mobile Country Code) and MNC (Mobile Network Code) using a "*config*" subdomain of the domain reserved for RCS services in [PRD-IR.67]: *http://config.rcs.mnc<MNC>.mcc<MCC>.pub.3gppnetwork.org*
  where <MNC> and <MCC> have to 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])

- The application then will check the Mobile Country Code and the Mobile Network Code in the IMSI and complete the prior name depending on the Service Provider.
- If a device is employed by a Service Provider that does not support RCS, this domain will not be resolved. Therefore the application will handle it as a “client not valid” scenario.

2.3.3.2.2 *RCS configuration server response*

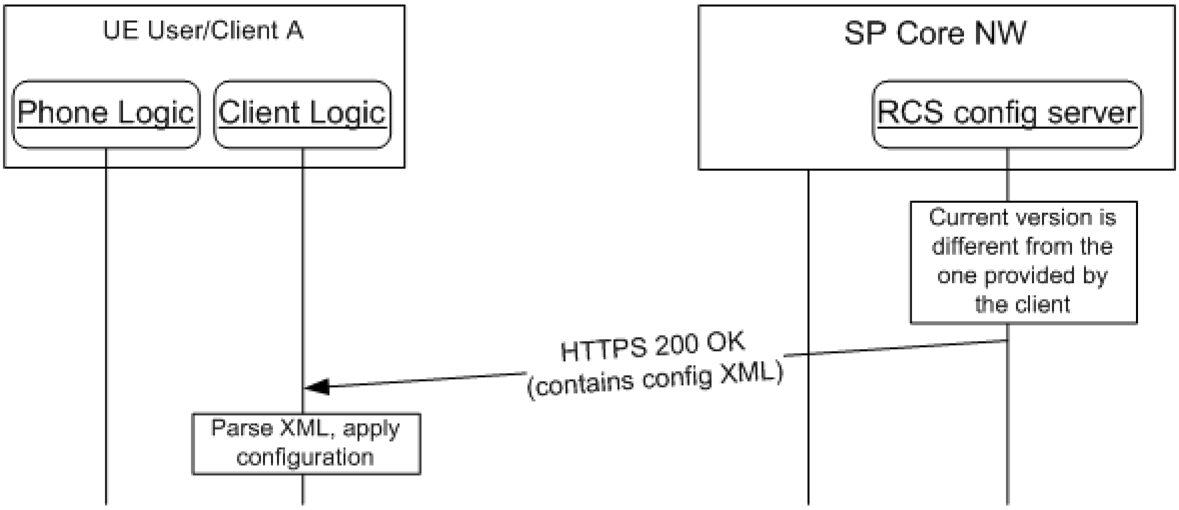

UE User/Client A
Phone Logic
Client Logic
SP Core NW
RCS config server
Current version is different from the one provided by the client
HTTPS 200 OK (contains config XML)
Parse XML, apply configuration

Figure 6: RCS HTTPS configuration: Server response

The server first validates the client and terminal parameters and then checks if the version provided by the client matches the latest version of the configuration available on the server.

The response will always contain two parameters:

1. The configuration version
2. The validity of the configuration in seconds

If the version matches (i.e. no new configuration settings required), the configuration XML document will be empty except for the version and the validity parameters:

- The version parameter will be set to the same value sent in the request
- The validity parameter will be reset to the server configured value

```
<?xml version="1.0"?>
<wap-provisioningdoc version="1.1">
        <characteristic type="VERS">
              <parm name=”version” value=”X”/>
              <parm name=”validity” value=”X”/>
        </characteristic>
</wap-provisioningdoc>
```

Table 3: RCS HTTPS configuration empty XML (no configuration changes required)

If the Service Provider wants to disable the RCS functionality from a device/client, the response will be an XML document containing only the version and validity, both set to 0:

```
<?xml version="1.0"?>
<wap-provisioningdoc version="1.1”>
        <characteristic type="VERS">
              <parm name=”version” value=”0”/>
              <parm name=”validity” value=”0”/>
        </characteristic>
</wap-provisioningdoc>
```

Table 4: RCS HTTPS configuration empty XML (reset RCS client)

Please note that if RCS is disabled on the device, the device should perform the autoconfiguration query every time it is booted up.

If the Service Provider wants to disable the RCS functionality from a device/client including the autoconfiguration query performed at boot, the response will be an XML document containing only the version and the validity, both set to -1:

```
<?xml version="1.0"?>
<wap-provisioningdoc version="1.1”>
        <characteristic type="VERS">
              <parm name=”version” value=”-1”/>
              <parm name=”validity” value=”-1”/>
        </characteristic>
</wap-provisioningdoc>
```

Table 5: RCS HTTPS configuration empty XML (reset RCS client and stop autoconfiguration query)

Note that if the SIM is swapped or the terminal reset, the terminal shall again query for configuration settings on every boot.

When the server has an updated configuration, the response will contain a configuration XML (i.e. content-type *text/xml*) document that the client needs to parse and apply:

The XML format of this document is based on the syntax used in OMA-CP (see Annex A, sections A.2 and A.3 for the details) with a new parameter to include the version, the validity and the message section. A sample of the complete autoconfiguration XML is provided for reference in section A.4.

Any other response different from those described in this section (i.e. an HTTP error) should trigger the device/client to try to retrieve the configuration settings the next time the device boots (or the client is started) and in the particular case of a 403 Forbidden error, the device/client implementation shall also remove the current configuration (as if a response with both validity and version set to 0 response was received).

Please note, that an "RCS Info" Management Object (MO) sub tree shall be included into the RCS management tree that contains the configuration parameter as described in Table 2, except for "*vers*" and "*IMEI*".

2.3.3.2.3 *User Messages*

As an option (that is the tag may not be present), the XML can be used to convey a user message associated with the result of an autoconfiguration server response. The additional XML section is displayed below:

```
<?xml version="1.0"?>
<wap-provisioningdoc version="1.1”>
        …
        <characteristic type="MSG">
              <parm name=”title” value=”Example”/>
              <parm name=”message” value=”Hello world”/>
              <parm name=”Accept_btn” value=”1”/>
              <parm name=”Reject_btn” value=”0”/>
        </characteristic>
        …
</wap-provisioningdoc>
```

Table 6: RCS alternative configuration: User notification/message sample

The meaning of the different parameters is the following:

- **Title**: The window title where the message is displayed.
- **Message**: This is the message that has to be displayed to the user. Please note the message may contain references to HTTP addresses (websites) that need to be highlighted and converted into links by the terminal/client.

- **Accept_btn**: This indicates whether the “Accept” button is shown underneath the message box. The action associated with the Accept button on the terminal/client side is always to clear the message box.
- **Reject_btn**: This indicates whether the “Decline” button is shown underneath the message box. The action associated with the Reject button on the terminal/client side is always to disable the RCS switch setting in the device.

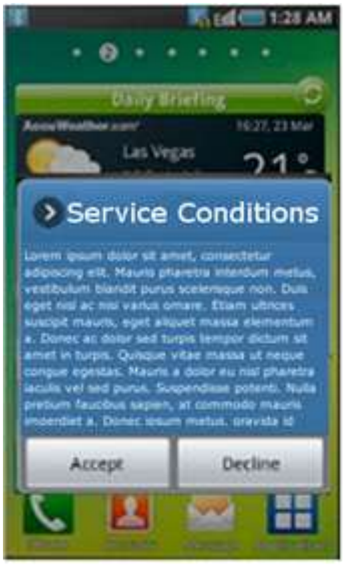
The MSG characteristic is optional and will be only present in two types of responses:

1. The response containing the full configuration settings.
2. The response disabling the RCS configuration on the device (version and validity set to 0).

The device should display the message and the relevant/configured buttons in the following scenarios:

- After receiving the full configuration settings, only if:
    - No working configuration was available previously
    - Following a terminal reset
    - Following a SIM swap no working configuration was available (backup) for that SIM
- After receiving the disabling RCS configuration response.

Finally, it should be noted that the RCS device/client is required to send the language locale settings to the server as the language in which the message is served depends on this parameter. To achieve this, the client should use the HTTP *Accept-Language* header in all the requests and set the value consistently with the device locale.



Service Conditions

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Mauris pharetra interdum metus, vestibulum blandit purus scelerisque non. Duis eget nisl ac nisi varius ornare. Etiam ultrices suscipit mauris, eget aliquet massa elementum a. Donec ac dolor sed turpis tempor dictum sit amet in turpis. Quisque vitae massa ut neque congue egestas. Mauris a dolor eu nisl pharetra iaculis vel sed purus. Suspendisse potenti. Nulla pretium faucibus sapien, at commodo mauris imperdiet a. Donec ipsum metus, gravida id

Figure 7 : Autoconfiguration server notification example

2.3.3.2.4 *Use Case Overview*

Although previously introduced, in this section we have compiled the different use cases to indicate what the device behaviour will be for each scenario:

1. **First detection**: This is the first time a user uses an RCS device. If the process is successful the device will receive the correct configuration XML. One of the parameters sent is the validity period. If the device has no issues in the registration process, it will not contact the server again until the validity has expired. As mentioned previously, this process could require some retries until the provisioning in IMS is performed.
   Please note that for those for devices not having successfully finished the

configuration yet, the device RCS related UX should remain disabled (i.e. vanilla behaviour) until a valid configuration is received.

2. **Version checking: no changes**. If the validity has expired, or the client has been asked to retry, the device will send a request to verify if it has the correct configuration. If the device already has the latest version, the client will receive an XML containing only the same version with the validity reset to the value specified in the server meaning that the configuration the device/client currently has is correct and, consequently, the validity is renewed.
3. **Version checking: new version available**. If the server has a new version of some of the fixed parameters (such as the registration IP address) or if the user has asked for a reconfiguration through Customer Care, the device/client will receive a new configuration XML the next time the device/client asks for a new version
4. **Validation process is not OK**. If either the RCS device/client or customers are not allowed to access the RCS service, the device will receive an XML with the version and validity set to 0.
   Consequently, the device/client must remove the existing configuration and remove the RCS-specific UX (that is vanilla behaviour).
5. **SIM change**: If the SIM changes, the previous configuration should be backed up and the device/client should behave as if no configuration is available (that is first-time configuration) and, therefore, the device implementation or client shall make a request for a new configuration. Please note that if there was already a configuration backup associated with the new SIM available on the device/client, the validity should be checked and, if still valid, it should be used instead of making a new request.
6. **User with different RCS devices**. If the client is using multiple RCS devices, the same configuration will be valid for all of them. The described process will ensure the device they currently use has the latest version.
7. **User asks Customer Care to disable the RCS service**. In this case the user will be un-provisioned on the IMS network, and when the application asks for a reconfiguration it will always receive an XML with the version and validity set to 0. This will remain disabled until the user requests Customer Care to be re-provisioned. **Consequently, the device/client must remove the existing configuration and remove the RCS-specific UX (that is vanilla behaviour).**

Please notice that all the scenarios described comply with one of the following behaviours of the application on the device:

- First time RCS device/client implementation: if it does not have the correct configuration (version 0 or it is not able to complete registration process), the device will send a request every time a boot sequence is completed (or when the client is restarted).
- If the device/client has received the proper configuration it will not ask for a new version unless:
  - The device/client is restarted, or,
  - The validity period has expired, or,
  - It is not able to complete registration to the IMS
- If the response of the server is 503 Retry-After, the device/client will retry the request after the time specified in the "Retry-After" header.
  - If any other error occurs (for example being unable to resolve the URL or getting an error from the autoconfiguration server) the device/client will retry the next time it reboots:
  - In the particular case of a 403 Forbidden, the existing configuration should be removed from the device implementation/client.

- In other error case scenarios (e.g. a 500 Internal Error is issued by the autoconfiguration server or the autoconfiguration server is not reachable), if there is valid configuration, the terminal/client should keep using it even if it has expired.
- The following notes apply to both 403 Forbidden and other errors:
  - Please note that to include those scenarios in which a device migrates to a network without RCS support, the maximum number of unsuccessful consecutive retries (this includes unsuccessful DNS lookup queries) is set to 5.
  - If the error persists, the RCS behaviour is disabled (both the general RCS behaviour if a valid configuration is still available and the autoconfiguration sequence performed at boot).
  - If the SIM is swapped or the terminal is reset, the terminal should again query for configuration settings on every boot.

Finally, (including error cases), please view all the possible responses below in Table 7:

Response	Use case	Client behaviour
200 OK	Initial HTTP request response	The client sends the HTTPS request including the cookie
503 Retry after	The server is processing the request/provision	Retry after the time specified in the “Retry-After” header
200 OK + XML with full configuration	New configuration sent to the terminal	Process configuration, try to register and if successful, not try reconfiguration until the validity period is expired, the device/client is restarted or SIM is swapped
200 OK + XML with version and validity period only	No update needed	Retry only after validity period, next restart or SIM swap
200 OK + XML with version and validity period only and both set to 0	Customer or device are not valid or the customer has been un-provisioned from RCS	Retry only after next restart or SIM swap If a configuration was available, it shall be removed from the client.
200 OK + XML with version and validity period only and both set to -1	Customer or device are not valid or the customer has been un-provisioned from RCS	The client shall no longer retry autoconfiguration until SIM is changed or a factory reset performed. If a configuration was available, it shall be removed from the client.
500 Internal Server error (or any other HTTP error except 403)	Internal error during configuration/provisioning	Retry on next reboot the next time the client starts
403 Forbidden	Invalid request (e.g. missing parameters, wrong format)	The configuration is removed in the device and version is set to 0. Retry on next reboot, the next time the client starts
The autoconfiguration server is not reachable	Autoconfiguration server missing or down	Retry on next reboot, the next time the client starts

Table 7: Summary of RCS autoconfiguration responses and scenarios

2.3.3.2.5 *Security considerations*

For terminals carrying the SIM associated to the user’s main identity the connection is done over the PS access network, therefore the current design ensures that it is impossible to perform a man-in-the-middle attack where a third party can impersonate the configuration server.

To secure interoperability between Service Providers and to reduce the complexity on the device/client implementation, the HTTP configuration server shall use public root certificates issued by a recognized Certification Authority (CA, similar to those used by standard webservers which are widely recognized by browsers and web-runtime implementations both in Personal Computers (PCs) and devices).

2.3.3.2.6 *Configuration of additional devices sharing the same identity*

This section describes the process of autoconfiguration authentication for the scenario in which the SIM associated with the IMS identity is not inserted in the device being provisioned.

In this case the device implementation/client will receive the credentials associated with the primary SIM card of the user whatever connection they are using (Wi-Fi, PS) to reach the server.

The process is the following:

1. As an option, the device implementation/client will offer the possibility to the user to perform manual provisioning
2. The user is prompted for the MSISDN or SIP URI of the primary device and the Service Provider associated with the primary SIM. The account created is always associated with this primary identity that the user has to enter in the application. Please note that as a precondition, the aforementioned identity already has to be provisioned using the mechanism described in the previous sections.
3. The device performs the HTTP configuration as presented in section 2.3.3.2.1, however, using the following GET parameters instead of the default ones:

Parameter	Description	Mandatory	Format
vers	This is either -1, 0 or a positive integer. 0 indicates that the configuration must be updated (e.g. configuration is damaged or non-existent). A positive value indicates the version of the static parameters (those which are not subscriber dependent) so the server can evaluate whether an update is required. -1 indicates that the client must disable the RCS services including the autoconfiguration query performed at boot.	Y	Int (-1, 0 or a positive integer)
msisdn	MSISDN in E.164 format of the primary SIM which is used to derive the identity	N, Mandatory if sip_uri not provided	E.164 (+44790000001)
sip_uri	SIP URI of the primary device	N, Mandatory if msisdn not provided	String (50 max), Case-insensitive
token	If this is the first time the additional device is being configured (or the validity of the token is expired), this should be an empty string. If not, the token obtained in the initial configuration process shall be reused here	Y	String (24 max), Case-Sensitive
client_vendor	String that identifies the vendor providing the RCS solution.	Y	String (4), Case-Sensitive
client_version	String that identifies the RCS solution version.	Y	String (10 max), Case-Sensitive
device_type	This indicates the type of device where the client is running.	Y	Possible values: - Tablet - PC - Other

Table 8: RCS alternative configuration for additional devices: Initial HTTPS request GET parameters

Please note that the initial HTTP request is not required in this case since the header enrichment requirement is not applicable. Therefore, the device implementation/client will directly perform the HTTPS request as presented in Figure 8.

4. At this stage the HTTP configuration server is able to identify whether this is a first time request:

   a) If the token value is empty, the request is then identified as a first time configuration. In this case, and provided the network allows for configuring additional devices using this mechanism, the HTTP server responds with a HTTP 200 OK response carrying a new cookie (Set-Cookie header) to be used in the subsequent HTTP request. The response will also contain a token to be used in subsequent and future requests:

```
<?xml version="1.0"?>
<wap-provisioningdoc version="1.1">
        <characteristic type="token">
                <parm name="token" value="X"/>
                <parm name="validity" value="Y"/>
        </characteristic>
</wap-provisioningdoc>
```

Table 9: RCS HTTPS configuration of additional devices: First time response to the initial HTTPS request

Please note if the validity is set to 0, the token will never expire. If there is an error of any kind, the server will provide a HTTP 403 response and the process would be concluded (the device is not configured as an end result).

b) If the token has a value, it is checked against the HTTP server database. If successful and from this point the procedure is identical to the one described in sections 2.3.3.2.2 and 2.3.3.2.3.

Note: There is no further authentication of the additional device or the user that starts the configuration process. Appropriate security measures to prevent malicious usage should be implemented on the configuration server.

5. If this is a first-time configuration, the user will receive an SMS message on the device with the MSISDN introduced in step 2. This SMS message will contain an OTP (One-Time Password).
6. The device performing the HTTP configuration prompts for the OTP. Therefore, the user should manually introduce the code ¨they received via SMS on their primary SIM device.
7. Once the user enters the OTP, the device performing the HTTP configuration makes a second HTTPS request using the following parameters in the GET request:

Parameter	Description	Mandatory	Format
OTP	This is the password received on the device carrying the SIM associated with the MSISDN introduced in step 1	Y	String (8 Max), Case-Sensitive
token	This is the token received in the initial HTTPS request response	Y	String (24 Max), Case-Sensitive

Table 10: RCS alternative configuration for additional devices: Second and final HTTPS request GET parameters

Please note this second HTTPS request shall carry the cookie obtained in step 4 (cookie header) therefore the HTTP configuration server can correlate the initial and final HTTPS requests.

8. From this point onwards the procedure is identical to the one described in sections 2.3.3.2.2 and 2.3.3.2.3. If the request is successful, one of the possible 200 OK responses described in section 2.3.3.2.2 is provided. If receiving a full XML and provided the network uses the sip.instance approach for multidevice handling as described in section 2.11, the response shall include the uuid_Value parameters (see Annex A sections A.1.13 and A.2.10 for further reference). If the request is not successful, the server replies with an HTTP 403 response and the process is concluded (the device is not configured as an end result).

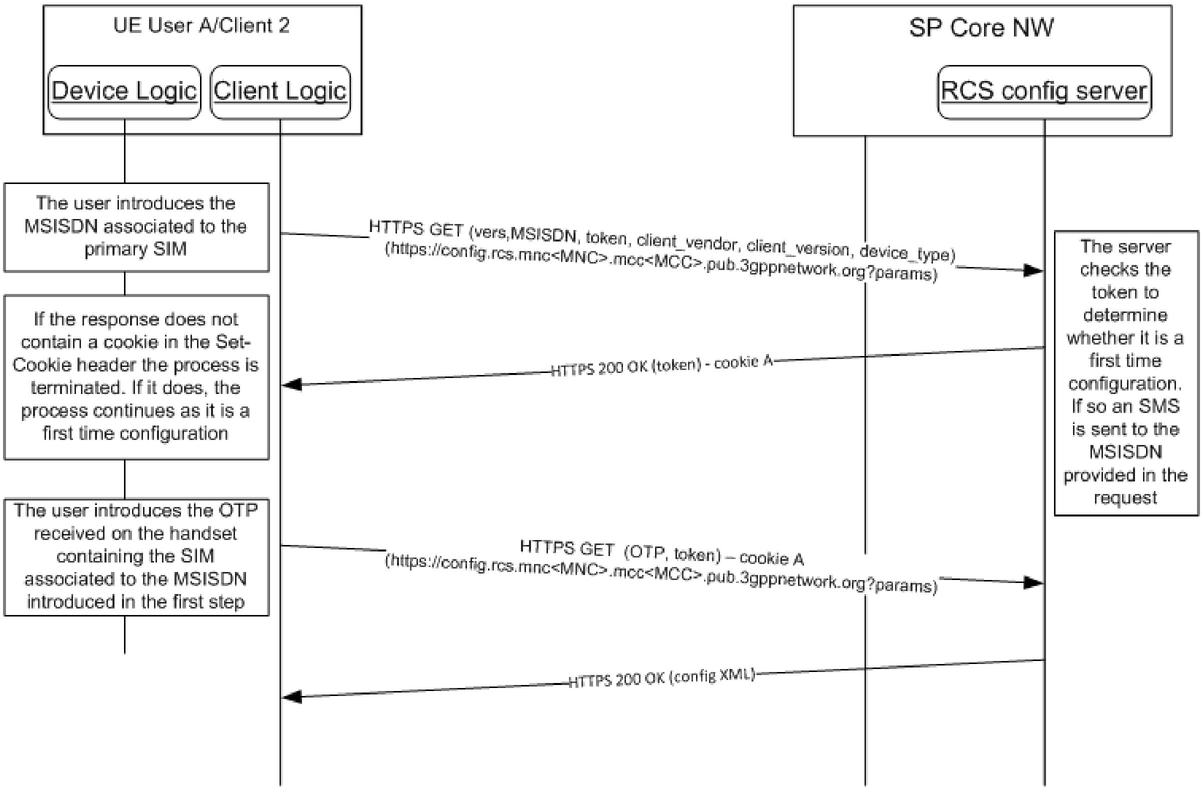

UE User A/Client 2
Device Logic
Client Logic
SP Core NW
RCS config server
The user introduces the MSISDN associated to the primary SIM
HTTPS GET (vers,MSISDN, token, client_vendor, client_version, device_type) (https://config.rcs.mnc<MNC>.mcc<MCC>.pub.3gppnetwork.org?params)
The server checks the token to determine whether it is a first time configuration. If so an SMS is sent to the MSISDN provided in the request
HTTPS 200 OK (token) - cookie A
If the response does not contain a cookie in the Set-Cookie header the process is terminated. If it does, the process continues as it is a first time configuration
The user introduces the OTP received on the handset containing the SIM associated to the MSISDN introduced in the first step
HTTPS GET (OTP, token) – cookie A (https://config.rcs.mnc<MNC>.mcc<MCC>.pub.3gppnetwork.org?params)
HTTPS 200 OK (config XML)

Figure 8: RCS alternative configuration for additional devices: First time configuration

Note: there is no further authentication of the additional device or the user that starts the configuration process (i.e. the initial HTTPS request). If misused via Internet, SMS messages could potentially be sent to all RCS users. Therefore, appropriate security measures to prevent such malicious usage should be implemented.

2.3.3.2.6.1 Subsequent configuration attempts and life cycle

Once the device has received the configuration for the first time, the device will employ the token provided during the initial configuration process:

- If the token is valid, the SMS procedure and the second HTTPS request will NOT be performed (i.e. a final configuration response will be provided to the initial HTTPS request). From this point the procedure is identical to the one described in sections 2.3.3.2.2 and 2.3.3.2.3.
- If the token is lost (e.g. device reset) or has expired, the device/client implementation shall keep the token empty so a first time configuration will take place again.
- If the client receives a 403 response to the HTTPS request, the token shall be removed and, therefore, the next time a first time configuration will take place.

2.3.3.2.6.2 Using End User Confirmation Request alternative

As an alternative to the use of SMS to confirm the identity of the user the Service Provider could choose to use the End User Confirmation Request (EUCR, see section 2.10).

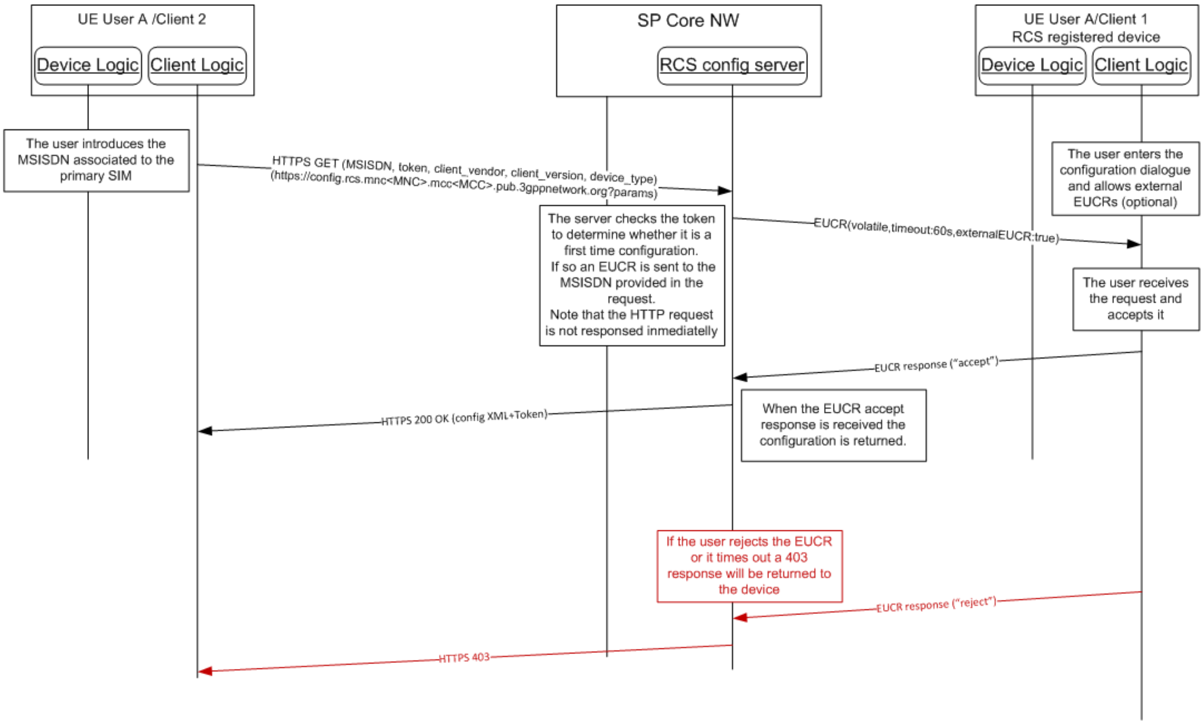

UE User A /Client 2
Device Logic
Client Logic
SP Core NW
RCS config server
UE User A/Client 1
RCS registered device
Device Logic
Client Logic
The user introduces the MSISDN associated to the primary SIM
HTTPS GET (MSISDN, token, client_vendor, client_version, device_type)
(https://config.rcs.mnc<MNC>.mcc<MCC>.pub.3gppnetwork.org?params)
The user enters the configuration dialogue and allows external EUCRs (optional)
The server checks the token to determine whether it is a first time configuration.
If so an EUCR is sent to the MSISDN provided in the request.
Note that the HTTP request is not responsed inmediatelly
EUCR(volatile,timeout:60s,externalEUCR:true)
The user receives the request and accepts it
EUCR response ("accept")
HTTPS 200 OK (config XML+Token)
When the EUCR accept response is received the configuration is returned.
If the user rejects the EUCR or it times out a 403 response will be returned to the device
EUCR response ("reject")
HTTPS 403

Figure 9: RCS alternative configuration for additional devices: First time configuration using EUCR

The process is very similar to the one described for SMS:

1. As an option, the device implementation/client will offer the possibility to the user to perform manual provisioning as in the SMS mechanism.
2. The user is prompted for the MSISDN or SIP URI of the primary device and the Service Provider associated with the primary SIM as in the SMS mechanism.
3. The device performs the HTTP configuration using the same GET parameters as in the SMS mechanism.
4. At this point the HTTP configuration server is able to identify whether this is a first time request:
    a) If the token value is empty, then the request is identified as a first time configuration.
    b) If the token has a value, it is checked against the HTTP server database. If successful, from this point the procedure is identical to the one described in sections 2.3.3.2.2 and 2.3.3.2.3.

    Note: There is no further authentication of the additional device or the user that starts the configuration process. Appropriate security measures to prevent malicious usage should be implemented on the configuration server.
5. An End User Confirmation Request flow starts for a first-time registration
    a) In case of malicious usage by other person via Internet, the End User Confirmation Request method may block the UI (by unwanted End User Confirmation Request popups) on the device registered for RCS. Therefore, the following optional user dialogue is recommended.
    If implemented on the RCS-registered mobile device, the user enters a UI dialogue to start the configuration of additional RCS devices. This dialogue sets the mobile device into a mode that allows End User Confirmation Requests initiated from an external source. This external source is in this case the user's additional device to configure.
    Note: If activation and de-activation of that mode is not implemented on the mobile device, all End User Confirmation Requests are allowed and shown to the user and

therefore also the End User Confirmation Requests related to the configuration of the device.

b) A volatile End User Confirmation Request is sent to the MSISDN or SIP URI provided in the HTTP request. The End User Confirmation Request includes the attribute externalEUCR set to true.
Note: The HTTP request is not answered immediately.

6. The End User Confirmation Request is received by the device and: will be shown in the user RCS device and:

a) If the device does allow external End User Confirmation Requests, it will be shown on the user's RCS device. The user may accept it, in which case a 200 OK response is sent as described in section 2.2.3.2.2. Please note that if receiving a full XML and provide the network uses the sip.instance approach for multidevice as described in section 2.11, the response shall include the uuid_Value parameters (see Annex A sections A.1.13 and A.2.10 for further reference). The response will also contain a token to be used in subsequent and future requests:

```
<?xml version="1.0"?>
<wap-provisioningdoc version="1.1">
        <characteristic type="token">
              <parm name=”token” value=”X”/>
              <parm name=”validity” value=”X”/>
        </characteristic>
        <characteristic type="VERS">
              <parm name=”version” value=”X”/>
              <parm name=”validity” value=”X”/>
        </characteristic>
        <characteristic type="APPLICATION">
              ….
        </characteristic>
</wap-provisioningdoc>
```

Table 11: RCS HTTPS configuration of additional devices using EUCR: First time response to the HTTPS request.

b) If the device does allow external End User Confirmation Requests but the user rejects the End User Confirmation Request or the timeouts expires, the server will reply with an HTTP 403 response and the process is concluded (the device is not configured as an end result).

c) If the device does not allow external End User Confirmation Requests, it shall ignore the request or reject it. As in b) the server will reply with an HTTP 403 response and the additional device is not configured.

Note: there is no further authentication of the additional device or the user that starts the configuration process (i.e. the initial HTTPS request). If misused via Internet, End User Confirmation Request may block an RCS user's UI (by unwanted popups) on the device associated with the primary SIM. Therefore, appropriate security measures to prevent such malicious usage should be implemented.

2.3.3.2.6.3 Using End User Confirmation request with PIN alternative

The Service Provider can add an extra layer of security by using the pin request feature in the End User Confirmation Request.

Using this alternative, the flow is similar as the SMS process described in section 2.3.3.2.6, except that instead of sending the One-Time Password in the SMS, the One-Time Password is chosen by the user and typed into both devices:

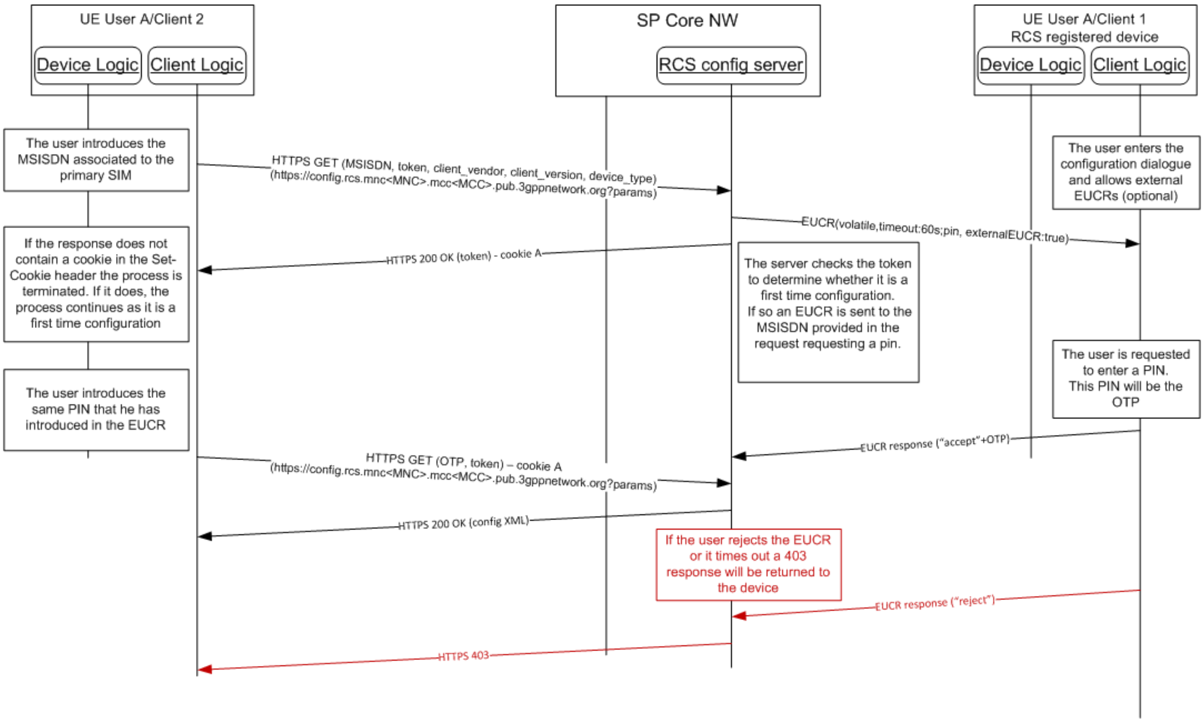

UE User A/Client 2
Device Logic
Client Logic
SP Core NW
RCS config server
UE User A/Client 1
RCS registered device
Device Logic
Client Logic
The user introduces the MSISDN associated to the primary SIM
HTTPS GET (MSISDN, token, client_vendor, client_version, device_type)
(https://config.rcs.mnc<MNC>.mcc<MCC>.pub.3gppnetwork.org?params)
The user enters the configuration dialogue and allows external EUCRs (optional)
EUCR(volatile,timeout:60s;pin, externalEUCR:true)
If the response does not contain a cookie in the Set-Cookie header the process is terminated. If it does, the process continues as it is a first time configuration
HTTPS 200 OK (token) - cookie A
The server checks the token to determine whether it is a first time configuration. If so an EUCR is sent to the MSISDN provided in the request requesting a pin.
The user is requested to enter a PIN. This PIN will be the OTP
The user introduces the same PIN that he has introduced in the EUCR
EUCR response ("accept"+OTP)
HTTPS GET (OTP, token) – cookie A
(https://config.rcs.mnc<MNC>.mcc<MCC>.pub.3gppnetwork.org?params)
HTTPS 200 OK (config XML)
If the user rejects the EUCR or it times out a 403 response will be returned to the device
EUCR response ("reject")
HTTPS 403

Figure 10: RCS alternative configuration for additional devices: First time configuration EUCR with PIN

Note: there is no further authentication of the additional device or the user that starts the configuration process (i.e. the initial HTTPS request). If misused via Internet, End User Confirmation Request may block an RCS user's UI (by unwanted popups) on the device associated with the primary SIM. Therefore, appropriate security measures to prevent such malicious usage should be implemented.

2.3.3.2.6.4 Use cases review

From the use cases presented in section 2.3.3.2.4, only the following scenarios apply to the configuration of additional devices sharing the same identity:

1. First detection
2. Version checking
3. Validation process is not OK
4. User asks Customer Care to disable the RCS service

2.3.4 Configuration storage on the RCS client

The RCS and, by extension, the IMS configuration should be stored securely on the device and should not be accessible to the user.

As indicated in section 2.4, it should be noted that a precondition to provide access to the RCS functionality is that all the mandatory parameters described in section A.1 must be configured correctly. If any of the required parameters are not configured or configured with an unexpected value, the RCS functionality should be disabled and not be presented or accessible to the user (that is the device behaves as a non-RCS enabled device). In this state, the RCS functionality can only be restored by completing the first-time registration procedure (see section 2.3.1; the first-time registration includes the RCS client configuration using one of the procedures described in section 2.3.3).

If an RCS configured device is reset, the RCS client should securely back up the configuration in the device together with the associated IMSI prior to the reset. Please note that this also applies in the event of swapping SIM cards. The configuration associated with the old SIM should then be securely backed up before triggering a first time registration.

The motivation behind the RCS configuration backup is to facilitate the scenario where following a reset or after a SIM swap, the original SIM card is re-introduced into the device. In that instance instead of triggering a first-time registration, the RCS configuration is restored.

In those terminals where as a consequence of the processes mentioned in the previous paragraphs (reset, SIM card swap) the terminal also deletes the contacts (for example a particular Service Provider is enforcing a policy where a SIM swap causes the deletion of the contacts), the associated RCS information (that is the cached capabilities per contact and the RCS contact list) should also be removed. In this case, the RCS information associated with the contacts is not backed up.

The number of configuration backups stored is left to the device's implementation, but shall be at least 2 (for the currently inserted and a previous SIM).

2.4 IMS registration

2.4.1 General

Prior to the registration, the device must be configured as described in section 2.3.

The device and IMS core network must follow the SIP registration procedures defined in [3GPP TS 24.229].

If the device is enabled for VoLTE/VoHSPA (i.e., an RCS-LTE or RCS-HSPA device as defined in section 2.2) then it must follow the procedures for registration specified in [PRD-IR.92]/[PRD-IR.58] with the changes and additions defined in this document (for example support for GRUU is not required in [PRD-IR.92]/[PRD-IR.58], but it is required for RCS devices). If the device uses the IMS based Conversational Video Service then it must in addition follow the procedures for registration specified in [PRD-IR.94].

If the device enabled for VoLTE/VoHSPA is also using RCS, a common IMS registration is shared by both RCS and VoLTE/VoHSPA applications.

If the device is access agnostic (i.e. an RCS-AA device as defined in section 2.2), it must fulfil the requirements as specified in [PRD-IR.92]/[PRD-IR.58], with the clarification that an RCS-AA device should always register in IMS. No requirements are provided for an RCS-AA device on when or whether it should register through cellular or non-cellular access.

When the domain selection has selected the IMS voice, an RCS-LTE or RCS-HSPA device shall not register in non-cellular networks (i.e. it shall not register on Wi-Fi).

When the domain selection does not use IMS voice, an RCS-LTE or RCS-HSPA device may de-register from IMS on the cellular network and register again through non-cellular access when that is available. It may only do this if it handles voice calls through CS access and it registers without IMS voice. This switch to non-cellular access will interrupt any ongoing RCS sessions.

As soon as the domain selection in an RCS-LTE device is again using IMS voice, it shall attempt to de-register from IMS through the non-cellular access and shall register again using IMS over the cellular network.

For a device not enabled for VoLTE/VoHSPA (see section 2.2), the client sends a SIP REGISTER message to the network using the configuration parameters (SIP proxy and other IMS parameters as presented in section A.1.6.2). If supported, the network shall authenticate the message using Single Sign-On (SSO)/General Packet Radio Service (GPRS) IMS Bundled Authentication (GIBA).

The device must use the authentication mechanisms as described in section 2.13.

Note: If the registration is not successful, the user should not be able to access any RCS services and all RCS contacts services/capabilities shall be reported to the user as not available independently of any setting (the IM CAP ALWAYS ON setting presented in Table 52 is ignored for example).

Finally note that a precondition to register is that all of the mandatory parameters presented in section A.1 are correctly configured. This includes those optional parameters that, due to their dependency on the configured value of a mandatory parameter, have become mandatory. If RCS is not the only IMS based functionality available on the device (that is other IMS services are incorporated) however, the precondition does not include having all of the mandatory parameters introduced by section A.1.6 correctly configured as in that scenario this configuration may have been obtained through other means.

2.4.2 Procedures for GRUU assignment

The device shall support using Globally Routable User agent URIs (GRUUs) to uniquely address each RCS client residing on different devices as specified in [3GPP TS 24.229] taking into account the clarifications given below.

When the user agent generates a REGISTER request (initial or refresh), it shall include the Supported header field in the request. The value of that header field shall include "*gruu*" as one of the option tags. This indicates to the registrar for the domain that the User Agent (UA) supports the GRUU mechanism.

In each contact included in the REGISTER request, the client shall include a "*sip.instance*" tag, whose value is the instance ID that identifies the user agent instance being registered. As network support for GRUU is not mandatory, sip.instance can be used instead.

If the client has access to the device IMEI, then sip.instance shall be the IMEI value as per [3GPP TS 24.229]. Otherwise, the value of sip.instance shall use either:

- The value provided as part of the device/client configuration (uuid_Value, as described in Annex A sections A.1.13 and A.2.10) shall be used. In this case, the network shall follow one of the algorithms described in [RFC4122], or,
- If the uuid_Value is not provided as part of the configuration (parameter not present in the configuration or present but with an empty value), the UUID (Universal Unique Identifier) shall be generated as per [RFC4122] section 4.2.

If the REGISTER response is a 2xx and the network supports GRUU, each Contact header field will contain a "pub-gruu" conveying the public GRUU for the user agent instance. The GRUU support is not mandatory for the Service Providers. Therefore user agents shall not always expect to receive a GRUU from the registrar.

2.4.3 Registration frequency optimization

An RCS client shall not send more register requests than what is needed to maintain the registration state in the network. When the IP connectivity is lost and restored with the same IP address, the RCS client shall:

- Only send a register refresh upon retrieval of IP connectivity if the duration for sending a register-refresh since the last REGISTER request has been exceeded, and,
- Only send an initial register upon retrieval of IP connectivity if the registration has expired

2.4.4 Registration flows

Prior to the first IMS registration, it is necessary to provision the user on the network (e.g. by autoprovisioning) and to configure the device with the required settings (see chapter 2.3). When the provisioning and device configuration phase is completed, the IMS registration takes place. Figure 11 shows the registration flow which applies for all authentication mechanisms covered in Section 2.13. After successful IMS registration, the device performs a capability and new user discovery procedure as described in Section 2.6.

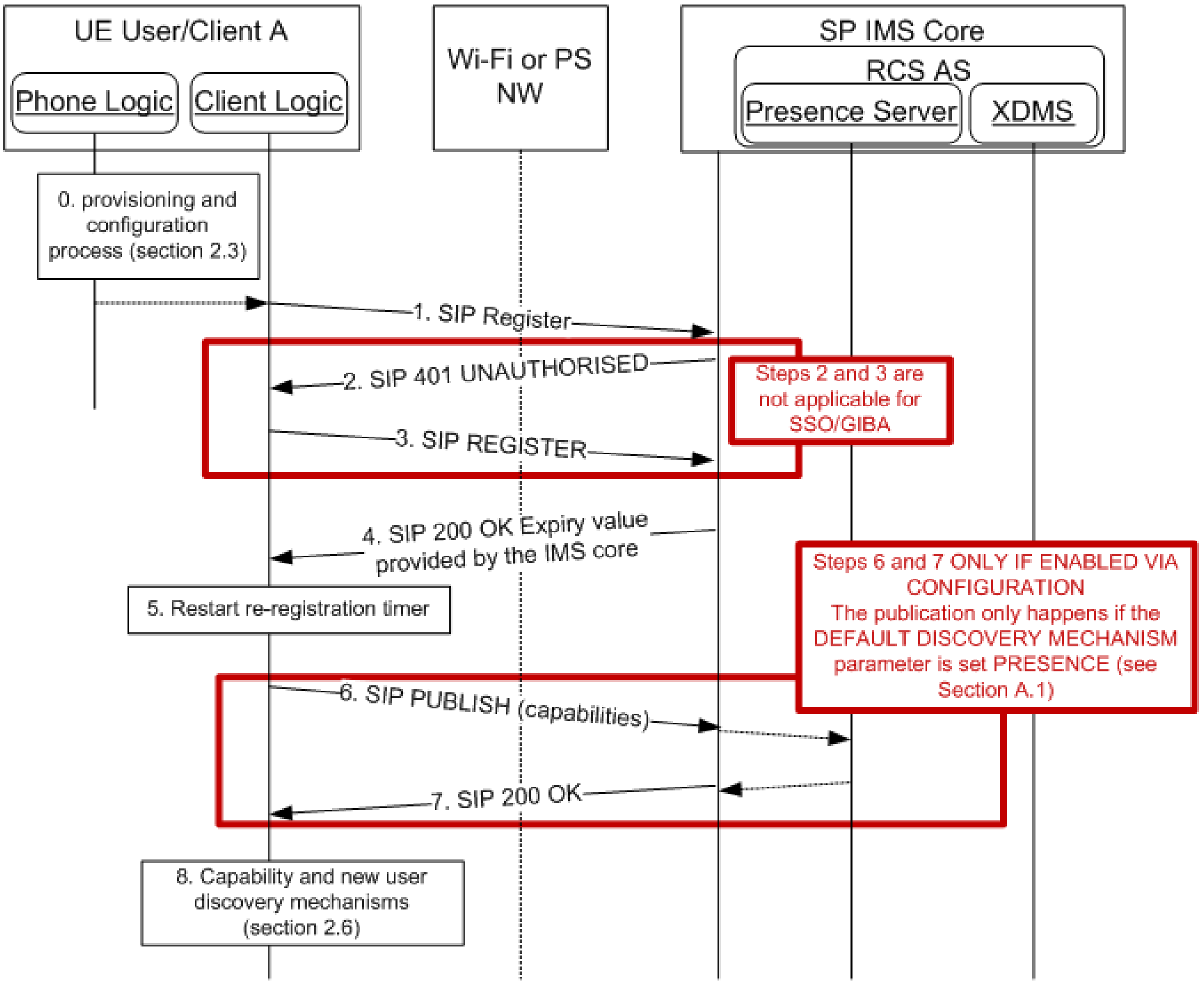

UE User/Client A
Phone Logic
Client Logic
Wi-Fi or PS NW
SP IMS Core
RCS AS
Presence Server
XDMS
0. provisioning and configuration process (section 2.3)
1. SIP Register
2. SIP 401 UNAUTHORISED
3. SIP REGISTER
Steps 2 and 3 are not applicable for SSO/GIBA
4. SIP 200 OK Expiry value provided by the IMS core
5. Restart re-registration timer
Steps 6 and 7 ONLY IF ENABLED VIA CONFIGURATION
The publication only happens if the DEFAULT DISCOVERY MECHANISM parameter is set PRESENCE (see Section A.1)
6. SIP PUBLISH (capabilities)
7. SIP 200 OK
8. Capability and new user discovery mechanisms (section 2.6)

Figure 11: IMS registration flow

Once registered the re-registration timer is initiated which is used to refresh the registration before it expires. If a presence based capability check is used (based on the DEFAULT DISCOVERY MECHANISM parameter specified in Table 58 in section A.1.10 see section 2.6), the device shall also publish its capabilities once it has registered.

Note: As stated in section 2.13, if SSO/GIBA authentication fails, Digest authentication shall be tried.

2.4.5 Procedures for Proxy-Call Session Control Function (P-CSCF) Fully Qualified Domain Name (FQDN) resolution

If the device or client is configured with a P-CSCF in FQDN format, the client shall perform the Domain Name System (DNS) resolution (IP address and port) as described in the GSMA [PRD-IR.67] section 4.5.2.

2.5 Addressing and identities

2.5.1 Overview

Telephone numbers in the legacy address book must be usable (regardless of whether RCS contacts have been enriched or not) for the identification of contacts of incoming and outgoing SIP requests.

Also, RCS users, especially in Enterprise segments, may be assigned a non MSISDN based identity. The RCS client would in that case be provisioned with only the appropriate SIP URI parameter as seen in section A.1.6.3, leaving the tel URI parameter empty.

Consequently, an RCS enabled terminal's address book should also be able to store alphanumeric SIP URIs as part of a contact's details.

NOTE: the handling of identities described in this section applies also to IP Voice Calls [PRD-IR.92] and [PRD-IR.58]. The functionality described here comes in addition to the functionality described in the related Permanent Reference Documents (PRDs), but not in conflict with them, e.g. the alias handling described in section 2.5.3.3.

2.5.2 Device Incoming SIP Request

2.5.2.1 From/P-Asserted-Identity

For device incoming SIP requests, the address(es) of the contact are, depending on the type of request, provided as a URI in the body of a request or contained in the *P-Asserted-Identity* and/or the *From* headers. If the *P-Asserted-Identity* header is present, the *From* header will be ignored. The only exception to this rule is when a request for Chat or Standalone Messaging includes a *Referred-By* header (it is initiated by Messaging Server for example in a store and forward use case as described in 3.3.4.1.4), thereby the *Referred-By* header should be used to retrieve the originating user instead.

The receiving client will try to extract the contact's phone number out of the following types of URIs:

- tel URIs (telephone URIs, for example *tel:+1234578901*, or *tel:2345678901;phone-context=<phonecontextvalue>*)
- SIP URIs with a "user=phone" parameter, the contact's phone number will be provided in the user part (for example *sip:+1234578901@operator.com;user=phone* or *sip:1234578901;phone-context=<phonecontextvalue>@operator.com;user=phone*)

Once the MSISDN is extracted it will be matched against the phone number of the contacts stored in the Address Book. If the received URI is a SIP URI but does not contain the "*user=phone*" parameter, the incoming identity should be checked against the SIP and tel URI address of the contacts in the address book instead.

If more than one *P-Asserted-Identity* is received in the message, all identities shall be processed until a matched contact is found.

2.5.3 Device Outgoing SIP Request

2.5.3.1 Identification of the target contact

If the target contact contains a SIP or tel URI the value shall be used by the RCS client when generating the outgoing request even if an MSISDN is also present for the contact. This applies to the SIP Request-URI and the "*To*" header (as defined in [3GPP TS 24.229]) for 1-to-1 communication, including the URIs used in the recipient list included in outgoing SIP requests for Group Chat.

If no SIP or tel URI is present the RCS client shall use the telephone number (in local format for example *0234578901* or international format *+1234578901*) set in the address book or a dial string entered by the user.

In the case of international-format telephone numbering, the device should support tel URI (for example "*tel:+12345678901*") as defined in [RFC3966] and SIP URI (for example *sip:+12345678901@domain;user=phone*) with the user parameter set to "phone" as defined in [RFC3261]. This should be configurable on the device according to the Service Provider's requirements or constraints related to national regulatory framework of SIP-SIP interconnection (the Service Provider will provide this choice during customization). If none of the above constraints apply, the use of tel URI is recommended as the domain name of the SIP URI is not significant.

In the case of non-international format telephone numbering, the RCS client should support tel URI and SIP URI (the user parameter should be set to "phone") with a phone-context value set as defined in [3GPP TS 24.229] for home local numbers (for example "*tel:0234578901;phone-context=<home-domain-name>*"). Similar to the international number case, whether a tel URI or a SIP URI is used, this should be configurable on the device according to the Service Provider's requirements or constraints related to national regulatory framework of SIP-SIP interconnection. If none of the above constraints apply, the use of tel URI is recommended.

2.5.3.2 Self-Identification to the network and the addressed contact

When generating an outgoing non-REGISTER request, the RCS client shall populate the *From* header field and may populate the *P-Preferred-Identity* header field with a SIP or tel URI which has been received in the *P-Associated-URI* header field returned in the 200 OK to the SIP REGISTER. If both a SIP URI and a tel URI are available, the tel URI should be used.

2.5.3.3 User alias

The user shall be able to specify an alias or a username for RCS services. This information will be sent when establishing a communication to another user so they can receive more information than just the MSISDN if the originating user is not in the receiver's Address Book. This scenario will probably be very common in Group Chat sessions.

This alias information will be set in the *From* header of the SIP request as the display name and also in the Common Profile for Instant Messaging (CPIM) *From* header as the formal name. On the receiving side, if there is no alias in the *From* header or *P-Asserted-Identity* headers of the SIP request, then the alias in the CPIM *From* header should be used.

When receiving a request, the RCS client device shall follow the rules explained in section 2.5.2.1 and extract the MSISDN or SIP URI. To avoid spam and identity manipulation, the receiver shall check the identity of the calling user against the address book. If the user is not in the address book, the alias information must then be used to provide more information about the calling user while clearly displaying in the User Interface (UI) that the identity is unchecked and it could be false. Otherwise the name of the contact in the address book shall be used instead.

2.6 Capability and new user discovery mechanisms

2.6.1 Capability discovery

The capability or service discovery mechanism is vital to RCS. The capability discovery is a process which enables a user to understand the subset of RCS services that is available to access and/or communicate with their contacts at certain points in time.
The RCS 5.0 specification provides two alternative mechanisms to perform the capability discovery:

- SIP OPTIONS exchange (section 2.6.1.1):
    - The SIP OPTIONS end-to-end message is used both to query the capabilities (services which the other user has available) of the target contact and to pass the information about which capabilities are supported by the requester. Using this method, both users get updated information in a single transaction.
    - This method requires a specific application server (Options-AS) in the network to provide multidevice support and, potentially, include optimizations.
- Presence (section 2.6.1.2):
    - In this case, instead of performing an end-to-end transaction, the capabilities are queried against a server using the standard OMA SIMPLE Presence procedures which are described in detail in section 2.6.1.2.
    - Consistent with the previous paragraph and the OMA SIMPLE Presence procedures, this method requires both a Presence and a XDM server in the network.

The default mechanism is configured in the device using the configuration parameter CAPABILITY DISCOVERY MECHANISM (see Annex A section A.1.10).

In accordance with the principle of interoperability between RCS 5.0 networks and devices, two mechanisms are provided to secure the interoperability between the mechanisms presented before:

- Coexistence based in a common device stack (section 2.6.1.3):
  - The interoperability is provided via a device implementation and, consequently, no additional network elements are required.
  - The principle of interoperability is that all devices support SIP OPTIONS exchange either as a default or a device fall-back mechanism (when the presence query fails for a particular user)
- Coexistence based in network interworking (section 2.6.1.3.3):
  - Network Interworking is required between Service Providers that do not support SIP OPTIONS exchange (as the default method or as a device fall-back mechanism) and those Service Providers that use SIP OPTIONS as the default discovery mechanism.
  - Interoperability is achieved by deploying a network based interworking function which translates requests and responses between the SIP OPTIONS and presence-based capability discovery mechanisms.

To secure that Service Providers choosing the network interworking approach do not experience situations where the device fall-back mechanism to SIP OPTIONS takes place, a new parameter (CAPABILITY DISCOVERY VIA COMMON STACK) is defined. The device fall-back mechanism only occurs if this parameter is set to 1 (see Annex A sections A.1.10 and A.2.8 for further reference).

2.6.1.1 Capability discovery process through SIP OPTIONS message

One of the available mechanisms for capability discovery is based on the exchange of a SIP OPTIONS request, a peer-to-peer message exchanged between clients.

When a SIP OPTIONS message is sent from User A to User B, User A will receive one of three types of response:

1. User B is Registered and the response from User B's client will include the CAPABILITY STATUS – the set of services currently available (using tags as described in section 2.6.1.1.1).
   - Note: the response must contain, at least, one of the tags assigned to the RCS 5.0 Services (see Table 24). If the response does not contain one of the mentioned tags, it will be equivalent to the case presented below in response type 3.
2. If User B is currently not registered (the device is off for instance), then the network will respond with one of the following error messages: 480 TEMPORARILY UNAVAILABLE (graceful deregistration took place) or 408 REQUEST TIMEOUT.
3. If User B is not provisioned for RCS the network will respond with an error message: 404 NOT FOUND[4].

[4] Please note that the response provided may depend on the network configuration. A useful approach for the terminal is to parse the response and if it is not either a 200 OK containing the capabilities as feature tags, a 480 TEMPORARILY UNAVAILABLE or a 408 REQUEST TIMEOUT, the target user should be considered as non-RCS. For simplicity, the present document assumes in the following sections that the response provided by the Service Provider core network is always 404 NOT FOUND, however, the previous statement should be taken into account.

From a user experience perspective, the handling of the responses provided in the cases 2[5] and 3 are the same and no RCS services will be shown as available.

In some cases sending an OPTIONS request is not required as the last SIP OPTIONS exchange took place just before the communication was set up (e.g. to send a SMS message, the user went to the address book, selected a user [SIP OPTIONS exchange takes place] and chooses to send a SMS message).

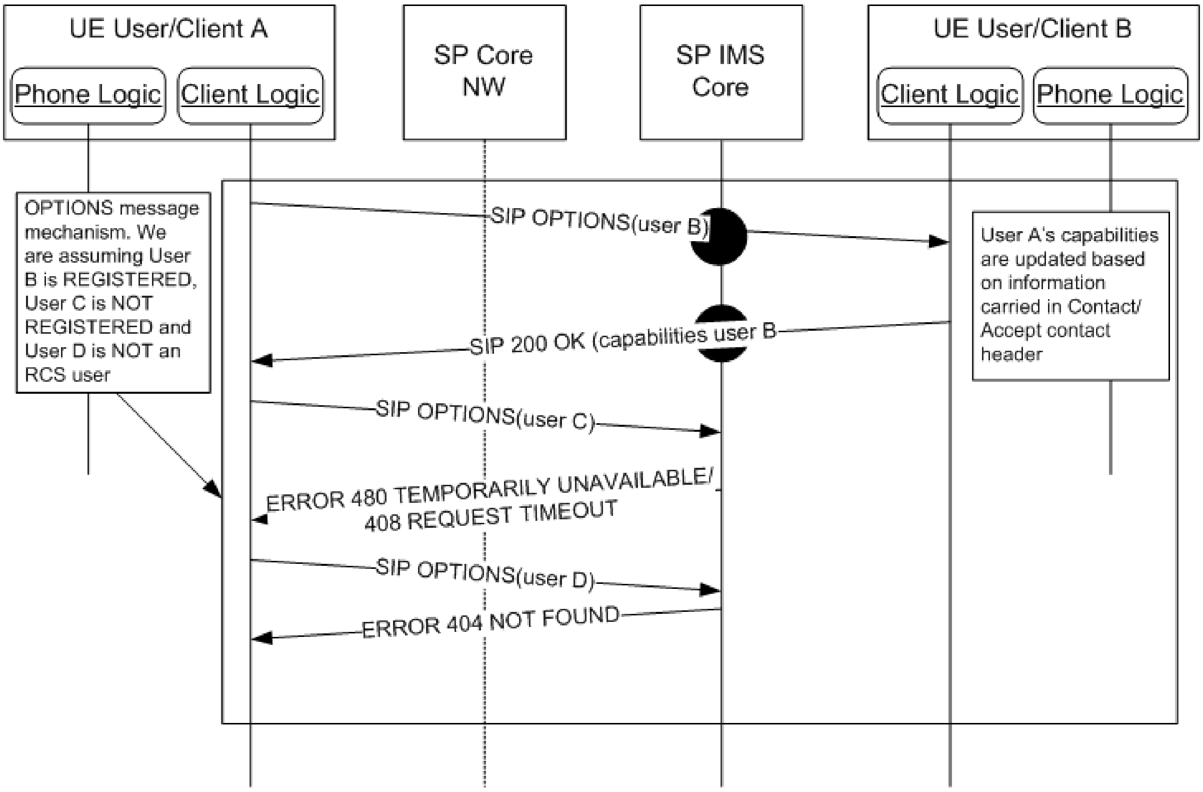

UE User/Client A
Phone Logic
Client Logic
SP Core NW
SP IMS Core
UE User/Client B
Client Logic
Phone Logic
OPTIONS message mechanism. We are assuming User B is REGISTERED, User C is NOT REGISTERED and User D is NOT an RCS user
SIP OPTIONS(user B)
User A's capabilities are updated based on information carried in Contact/ Accept contact header
SIP 200 OK (capabilities user B
SIP OPTIONS(user C)
ERROR 480 TEMPORARILY UNAVAILABLE/ 408 REQUEST TIMEOUT
SIP OPTIONS(user D)
ERROR 404 NOT FOUND

Figure 12: Capabilities discovery via SIP OPTIONS message

2.6.1.1.1 *SIP OPTIONS message extension to support capability discovery*

The RCS (Release 1 to 4) specifications only provide a mechanism to exchange the capability status (based on a SIP OPTIONS exchange) related to the Image and Video Share services during a call (associated with the capability query procedure described in [PRD-IR.74] and [PRD-IR.79]). This mechanism is based on the use of tags transported in the *Accept-Contact* and *Contact* headers for the SIP OPTIONS and its responses:

- The tags corresponding to the set of functionalities supported by the requesting terminal at the time this request is made are carried in both the *Contact* and *Accept-Contact* headers of the SIP OPTIONS message.
- The tags corresponding to the subset of the functionalities that are supported by the receiver are included in the *Contact* header of the 200 OK responses.

As described in [PRD-IR.74] and [PRD-IR.79], to have a Session Description Protocol (SDP) body in an OPTIONS request message is optional. It is not encouraged behaviour to insert it into this message. In RCS 5.0, the SIP OPTIONS request shall NOT contain an SDP body.

[5] Please note that in this case if IM CAP ALWAYS ON (see Annex A section A.1.3.3) is enabled, the Chat should still be reported to the user as available towards a known RCS user even the other end is not registered.

The mechanism described above is extended to be used not only for the exchange of capabilities for real-time services but also to query in real time to exchange the capabilities/services supported by both the requester and the receiver.

2.6.1.1.2 *Extensions to the existing tags*

Consequently with the RCS Release 1-4 specifications, the following tags can be employed to identify Image and Video Share service capabilities during a call:

RCS service	Tag
Image Share	+g.3gpp.iari-ref="urn%3Aurn-7%3A3gpp-application.ims.iari.gsma-is"
Video Share	+g.3gpp.cs-voice

Table 12: Standard RCS Release 1-4 SIP OPTIONS tags

These Image and Video Share capabilities can only be sent in SIP OPTIONS exchanges during an active call and are included only if the exchange takes place between the users in the active call. However Broadband Access devices should include these capabilities in an OPTIONS response even if they are not in an active call.

To support the full service discovery functionality presented in this document, it is necessary to extend the tag mechanism by adding the following service tags:

- As interoperability between the different technical implementations for Chat and File Transfer services is assumed, the following tags are employed for the Chat and File Transfer service:

RCS service	Tag
Chat	+g.3gpp.iari-ref="urn%3Aurn-7%3A3gpp-application.ims.iari.rcse.im"
File Transfer	+g.3gpp.iari-ref="urn%3Aurn-7%3A3gpp-application.ims.iari.rcse.ft"

Table 13: SIP OPTIONS tags for Chat and File Transfer

- Add a tag for IP based standalone text and multimedia messaging :

RCS service	Tag
IP Based Standalone messaging	+g.3gpp.icsi-ref="urn%3Aurn-7%3A3gpp-service.ims.icsi.oma.cpm.msg; urn%3Aurn-7%3A3gpp-service.ims.icsi.oma.cpm.largemsg"

Table 14: SIP OPTIONS tag for standalone messaging

- Add a tag for the video sharing outside of a call service:

RCS service	Tag
Video Share outside of a voice call	+g.3gpp.iari-ref=”urn:urn-7:3gpp-application.ims.iari.gsma-vs"

Table 15: SIP OPTIONS tag for video sharing outside a call

- Add a tag for Social Presence Information:

RCS service	Tag
Social presence information	+g.3gpp.iari-ref="urn%3Aurn-7%3A3gpp-application.ims.iari.rcse.sp"

Table 16: SIP OPTIONS tag for Social Presence Information

- Add tags for IP Voice and Video Call services:

RCS service	Tag
IP Voice Call	+g.3gpp.icsi-ref="urn%3Aurn-7%3A3gpp-service.ims.icsi.mmtel"
IP Video Call	+g.3gpp.icsi-ref="urn%3Aurn-7%3A3gpp-service.ims.icsi.mmtel";video

Table 17: SIP OPTIONS tags for IP Voice and Video Call

Note also that when a device supports both IP Voice Call and IP Video Call, the feature tag *+g.3gpp.icsi-ref="urn:urn-7:3gpp-service.ims.icsi.mmtel"* is only included once in the OPTIONS request/response.

Note: In case of interworking between two Service Providers, the validity of the IP Video Call capability tag highly depends on the end-to-end interconnection chain.

- Add tags for the Geolocation services:

RCS service	Tag
Geolocation PUSH	+g.3gpp.iari-ref="urn%3Aurn-7%3A3gpp-application.ims.iari.rcs.geopush"
Geolocation PULL	+g.3gpp.iari-ref="urn%3Aurn-7%3A3gpp-application.ims.iari.rcs.geopull"

Table 18: SIP OPTIONS tags for geolocation services

Please note that the new tags defined in this section are defined for SIP OPTIONS exchanges and that the standard tags defined in the supporting PRDs and endorsement documents shall be used to identify the services in the rest of relevant SIP transactions (e.g. *+g.oma.sip-im* for Chat implementation based on OMA SIMPLE IM as per [RCS5-SIMPLEIM-ENDORS]). It should also be noted that in some cases, the tags employed in the SIP OPTIONS exchange match the standard tags.

Note that for routing purposes, a device should also add to both the Contact and Accept-Contact header fields the same feature tags used at SIP Registration if not already included in the OPTIONS request/response for capability exchange. Finally, it should be taken into account that when several IMS Application Reference Identifier (IARI) tags or several IMS Communication Service Identifier (ICSI) tags are included in an OPTIONS request, consistently with [RFC3840], IARI tags or ICSI tags shall be concatenated using commas as described in the example below:

+g.3gpp.iari-ref="urn%3Aurn-7%3A3gpp-application.ims.iari.rcse.im,urn%3Aurn-7%3A3gpp-application.ims.iari.rcse.ft"

Table 19: IARI tag concatenation format example

2.6.1.1.3 *Future extensions to the mechanism*

In addition to the aforementioned additions and to allow a Service Provider (or group of Service Providers) to deploy additional services which can benefit from the RCS discovery mechanism, an additional tag format is defined:

- +g.3gpp.iari-ref="urn%3Aurn-7%3A3gpp-application.ims.iari.rcs.mnc<mnc>.mcc<mcc>.<service name>"
- Valid examples are:
  - +g.3gpp.iari-ref="urn%3Aurn-7%3A3gpp-application.ims.iari.rcs.mnc001.mcc214.serviceA"
  - +g.3gpp.iari-ref="urn%3Aurn-7%3A3gpp-application.ims.iari rcs.mnc680.mcc310.serviceB"

The service name is decided by the each Service Provider. The only requirement for a Service Provider following this approach is to include these tags in the relevant interoperability agreements with other Service Providers to avoid any interoperability issues.

RCS service	Tag
Service Provider specific service	+g.3gpp.iari-ref="urn%3Aurn-7%3A3gpp-application.ims.iari.rcs .mnc<mnc>.mcc<mcc>.<service name>"

Table 20: SIP OPTIONS tag proposal for future lines of work

2.6.1.1.4 *UI integration optimisations*

In addition to the optimizations to minimize the traffic generated by the SIP OPTIONS exchanges when possible, there are two additional optimizations related to the discovery mechanism integration on the UI that should be taken into account:

- The round trip time for a SIP OPTIONS exchange (send and receive response) is expected to range between under 1-2 seconds. Taking this into account, the UI has to be optimized to minimize the impact of this exchange delay.
- When sending the SIP OPTIONS messages to several users (for example during first time registration or when polling), it is recommended to employ a non-aggressive strategy and allow time between each exchange to:
    - Minimize potential network impact
    - Avoid any impact on the user experience (for example a slower UI, blockings and so on)

Please note that in this case this specification does not specify the specific mechanisms which should be implemented leaving space to Original Equipment Manufacturers (OEMs) and third parties to drive innovative and differentiated solutions, which distinguish their products from competitors.

2.6.1.1.5 *Multidevice support: Options-AS*

Ultimately, the choice of supporting multiple devices for a single user is decided by each Service Provider. The considerations contained in this section will only apply to those Service Providers willing to include RCS multidevice support in their networks.

In a multidevice scenario, when the user is registered to the IMS CORE with various devices using the same URI (that is the same implicit registration set), the OPTIONS exchange will return incomplete information:

- The capabilities contained in the OPTIONS message refer only to the originating device (that is the originating user may be logged in with the same URI in several devices).
- The IMS Core, depending on the configuration, either sends the OPTIONS message to the device that first registered to the IMS CORE or forks the OPTIONS to all of the registered devices. In any case, only the first response is passed back to the requester, discarding the others. In other words, the capabilities returned in the OPTIONS response will be from only one of the user's devices.

The preferred implementation for handling the OPTIONS in a multidevice environment is left to the Service Provider's discretion. The only requirement is that it should not impact the terminal side (that is there will be no changes on the client side). A possible solution for extending the OPTIONS mechanism to a multidevice scenario is to include a custom AS implementing the following logic:

- A trigger will be setup in the IMS CORE to send all of the OPTIONS from an RCS user to the AS.
- The AS will fork the OPTIONS request to all of the RCS user's registered devices and will aggregate all of the capabilities returned into one OPTIONS response if the forking is not already implemented by the IMS core network.
- Once the responses from the different devices are received, the AS will aggregate all the capabilities from the replies and send them back to the caller.

- Even if not all of the replies have been received in less than a configurable amount of time (note the recommendation is to set the value to optimise the UX on the terminal) the AS will return the aggregated information received so far.
- Capabilities shall be aggregated to provide the response to an incoming SIP OPTIONS request. For outgoing requests, it is up to the Service Provider's policy to aggregate the capabilities.

Note: Similar procedures may at the service provider's discretion also be applied at originating side to aggregate the capabilities of all the user's devices in the OPTIONS request.

To implement this feature, an application server should be able to uniquely identify each user device to perform the forking of the OPTIONS message and to intercept and process the responses. The mechanism to have these individual identities (a GRUU or sip.instance feature tag) is covered in section 2.11.3.

While multidevice support is an option for each Service Provider to decide whether or not it is supported, the RCS capability discovery mechanism based on the SIP OPTIONS message is a mandatory requirement and the behaviour will be the one specified previously to ensure seamless interworking between Service Providers.

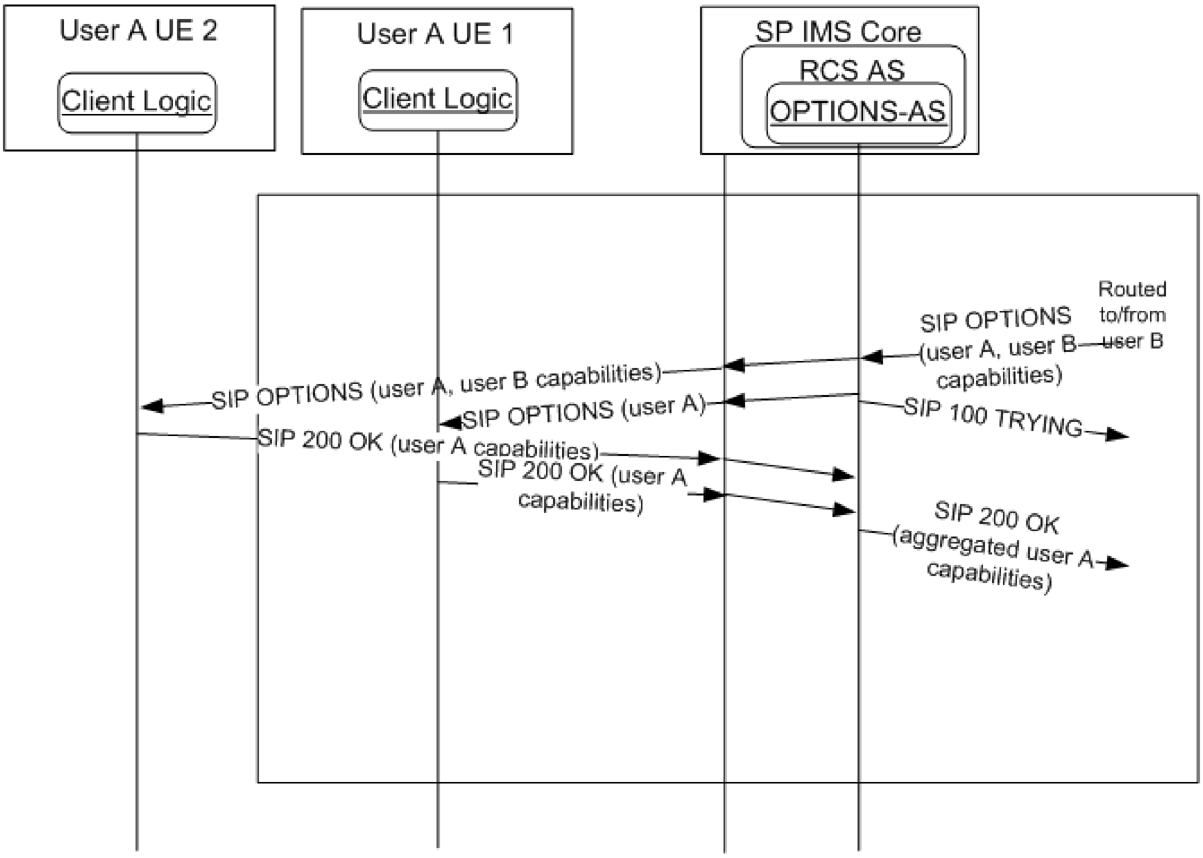

User A UE 2
Client Logic
User A UE 1
Client Logic
SP IMS Core
RCS AS
OPTIONS-AS
Routed to/from user B
SIP OPTIONS (user A, user B capabilities)
SIP OPTIONS (user A, user B capabilities)
SIP OPTIONS (user A)
SIP 100 TRYING
SIP 200 OK (user A capabilities)
SIP 200 OK (user A capabilities)
SIP 200 OK (aggregated user A capabilities)

Figure 13: Options application server: Capability aggregation on SIP OPTIONS request

2.6.1.2 Capability discovery via presence

2.6.1.2.1 *General Overview*

As an alternative to the SIP OPTIONS-based mechanism presented in the previous section, a Service Provider deploying a Presence Server may provide the capability discovery mechanism via presence. The service capabilities are then realized using the "*Service*" part of the Presence Data Model. This part is described in section 2.6.1.2.5.

2.6.1.2.2 *Publication of the Service Capabilities*

The capabilities are announced in a Presence document that is published by using the SIP PUBLISH method as defined in [Presence]. When the terminal is started, the client then sends a SIP PUBLISH request containing the capabilities (see section 2.6.1.2.5).

The publication is maintained in the Presence Server whenever the application is running by sending a refresh request before it expires.

If changes are required in the published capabilities (for example due to the behaviour specified in sections 2.6.2 and 2.6.3), a presence modify request is sent using the '*Sip-If-Match*' header according to [Presence]. When the client/device is switched off, it shall remove the published capabilities before unregistering according to the procedure defined in [RFC3903] (i.e. by sending a SIP PUBLISH request without a body including the '*Sip-If-Match*' header and an *Expires* header set to 0).

2.6.1.2.3 *Service Capabilities Retrieval*

Service capabilities of an RCS user can be retrieved by another RCS user via a presence subscription issued by their client, providing the pertaining Presence Authorization rules allow him to do so. The templates provided in section 3.7.4.5.2 allow this for the authorized users. An RCS user is therefore allowed to retrieve the service capabilities of contacts when they have an established Social Presence relationship.

RCS users may also retrieve the service capability information of contacts with whom they have not established a Social Presence relationship by means of Anonymous Fetch operations issued by their client (as described in section 7.1 of [PRESENCE]). This will result in a single NOTIFY request indicating the service capabilities of that contact. This information shall then be cached in the client as described in section 2.6.4. The Anonymous Fetch operation shall be supported in clients.

If an RLS-URI (Resource List Server URI, see Annex A section A.1.1.1) has been provisioned, a client shall use an Anonymous Fetch request using a request-contained list if the client has to query the capabilities of multiple users at once (e.g. during a poll). In this case it shall do so according to section 5.2.1.2.2 of [Presence2.0_TS].

If only a single contact needs to be queried, an individual fetch shall be done instead even if an RLS-URI has been configured.

2.6.1.2.3.1 General Processing Rules to Ensure Backwards Compatibility

To maintain enough flexibility and not to impose potentially sub-optimal technical choices on future RCS versions, the parsing of the capabilities in an RCS client should be sufficiently robust. First the watcher should apply the processing rules defined in [Presence2.0_DDS] and if then there are still multiple elements the watcher shall follow the guidelines in the RCS presence parsing presented below:

- Unknown or unsupported elements and tuples could be present in the document. In that case they should be ignored.
- Unknown service identifiers (Service-Id) could be present in the document. Tuples containing those should be ignored.
- Unknown service versions of known services could be present in the presence document. Tuples containing those should be ignored.
- The same service could occur multiple times in the presence document with different contact addresses. To cope with this case, the following behaviour shall be used for displaying and using the tuples:
  - If one of the tuples contains a contact address that corresponds to the presentity about which the presence document was received, all others shall be ignored.

  - Tuples that contain a contact (address) element which corresponds to another presentity (that is another contact in the contact-list of the user or another tel URI) shall be ignored.
  - Tuples containing contact elements with types of addresses that are not supported by the client for that service shall be ignored (for example messaging using an e-mail address while e-mail is not supported by the client)
  - If after applying the above rules, there are still multiple non-ignored tuples remaining for the service, all but the first shall be ignored.
  - If after applying the above rules there is a non-ignored tuple remaining, the service behaviour shall be as follows
    - The capability to use the service for communication with the contact shall be announced to the user
    - If the remaining tuple contained no contact address or it matched the one of the presentity, the presentity’s address will be used for setting up communication using that service
    - Otherwise the address contained in the contact element will be used for setting up the corresponding service
- The Watcher shall follow the procedures defined in section 6.2 "Default Watcher Processing" of [Presence2.0_DDS].

Regarding the use of the address provided in the contact, the communication addresses (contact) part of service tuples shall not be:

- Shown to the end-user, these addresses are handled locally by the terminal;
- Used to request presence subscription, an RCS client is NOT supposed to subscribe to the contact associated with a service capability tuple received in a presence document.

2.6.1.2.4 *Authorization for capabilities retrieval*

To provide authorization to retrieve the capabilities using an Anonymous Fetch request, an RCS client supporting the capability exchange using presence shall set the presence rules document in the presence XDMS as follows:

Presence XDMS:
AUID: org.openmobilealliance.pres-rules
Document name: pres-rules
Template

```
<?xml version="1.0" encoding="UTF-8"?>
<cr:ruleset
    xmlns:ocp="urn:oma:xml:xdm:common-policy"
    xmlns:op="urn:oma:xml:prs:pres-rules"
    xmlns:pr="urn:ietf:params:xml:ns:pres-rules"
    xmlns:cr="urn:ietf:params:xml:ns:common-policy">

    <! -- This rule allows all service capabilities to be sent for anonymous requests -->
    <! -- To realize the service capabilities to all requirement -->
    <! -- This rule replaces the default “wp_prs_block_anonymous” rule -->
    <! -- Note: May be modified to only allow RCS specified services -->
    <cr:rule id="rcs_allow_services_anonymous">
        <cr:conditions>
          <ocp:anonymous-request/>
        </cr:conditions>
        <cr:actions>
          <pr:sub-handling>allow</pr:sub-handling>
        </cr:actions>
        <cr:transformations>
          <pr:provide-services>
              <pr:all-services/>
          </pr:provide-services>
          <pr:provide-all-attributes/>
        </cr:transformations>
    </cr:rule>
</cr:ruleset>
```

Table 21: Presence XDMS template

If social presence is supported (see section 3.7), the *pres-rules* document should be set to contain both “*rcs_allow_services_anonymous*” described in this section and the rules provided in the template described in section 3.7.4.5.2.

Handling of this template shall be done as described in section 3.7.4.5.3.

2.6.1.2.5 *Service part of the presence Data Model*

A service capability is provided according to the model described in Table 22:

Attribute	Specification	Comment
Tuple: <presence> -> <tuple>	[RFC3863] and [Presence2.0_DDS]	According to the presence schema defined in the [Presence], services are presented with *tuple* elements.
Status <tuple> -> <status> -> <basic> -> Open	[RFC3863] and [Presence2.0_DDS]	Mandatory element in [RFC3863]. Once a tuple element is published the value 'open' will always be used. It does not have any particular meaning in RCS context.
Service-id <tuple> -> <service-description> -> <service-id>	[Presence2.0_DDS]	*Service-description* element identifies a service and is described by a *service-id* and *version*. *Service-id* element contains a string that identifies a single service.
Version <tuple> -> <service-description> -> <version>	[Presence2.0_DDS]	*Version* element contains the version number for the service, to identify different versions of the service (for example version number for specification number).
Media <tuple> -> <servcaps>	[RFC5196] and [Presence2.0_DDS]	Indicates the capabilities of the service. In RCS this is only used to provide media capabilities for some specific services (where mentioned below)
Contact <tuple> -> <contact>	[RFC3863] and [Presence2.0_DDS]	Contact element contains Presentity's communication address for the service. Contact address can be for example a tel or SIP URI, depending on the service used. The use of the Contact element is optional (if used it has to be a global routable URI) since the client may use the URI stored in the Address Book when initiating communication with the presentity. RCS Presentities either do not insert any contact element or insert a contact element for which the address matches the one used for identifying itself in communication (see Section 2.5)
Timestamp: <tuple> -> <timestamp>	[RFC3863] and [Presence2.0_DDS]	Timestamp when the presence information was published.

Table 22: Attributes of the Presence Service element

2.6.1.2.5.1 Service-descriptions for the Selected RCS Services

Registered Service-description values are listed in OMNA Presence <service-description> Registry:

http://www.openmobilealliance.org/Tech/omna/omna-prs-PidfSvcDesc-registry.aspx

Standalone Messaging
Service-id: *org.3gpp.urn:urn-7:3gpp-application.ims.iari.rcs.sm*
Version: 1.0
Contact address type: tel / SIP URI

Session Mode Messaging
Service-id: *org.openmobilealliance:IM-session*
Version : 1.0
Contact address type: tel / SIP URI

File Transfer
Service-id: *org.openmobilealliance:File-Transfer*
Version : 1.0
Contact address type: tel / SIP URI

Image Share
Service-id: org.gsma.imageshare

Version: 1.0
Contact address type: tel / SIP URI

Video Share during a call (Phase 1)
Service-id: *org.gsma.videoshare*
Version: 1.0
Contact address type: tel / SIP URI

Video Share outside of a voice call (Phase 2)
Service-id: *org.gsma.videoshare*
Version: 2.0
Contact address type: tel / SIP URI

Social presence information
Service-id: *org.3gpp.urn:urn-7:3gpp-application.ims.iari.rcse.sp*
Version: 1.0
Contact address type: tel / SIP URI

Capability discovery via presence
Service-id: *org.3gpp.urn:urn-7:3gpp-application.ims.iari.rcse.dp*
Version: 1.0
Contact address type: tel / SIP URI

IP Voice Call
Service-id: *org.3gpp.urn:urn-7:3gpp-service.ims.icsi.mmtel*
Version: 1.0
Media capabilities: audio, duplex
Contact address type: tel / SIP URI

IP Video Call
Service-id: *org.3gpp.urn:urn-7:3gpp-service.ims.icsi.mmtel*
Version: 1.0
Media capabilities: audio, video, duplex
Contact address type: tel/ SIP URI

Geolocation PUSH
Service-id: *org.3gpp.urn:urn-7:3gpp-application.ims.iari.rcs.geopush*
Version: 1.0
Contact address type: tel/ SIP URI

Geolocation PULL
Service-id: *org.3gpp.urn:urn-7:3gpp-application.ims.iari.rcs.geopull*
Version: 1.0
Contact address type: tel/ SIP URI

Note: This means that an RCS client shall include both the Video Share 2.0 and the Video Share 1.0 capabilities to indicate backwards compatibility.

The service capability information that is the object of a SIP PUBLISH by the RCS client (service tuple) corresponds to the services supported by the device. For example, an RCS-AA client (see section 2.2) can indicate its support for PS Voice according to section 3.8 with a service- and media description.

The set of services published may be further restricted by some Service Provider settings on the User Equipment (UE, on for example the services that are allowed by the Service Provider in the network).

2.6.1.2.6 *Future extensions to the mechanism*

Consistently with section 2.6.1.1.3, it is also possible to extend the capability discovery based in presence following the guideline presented in the table below to define new service-IDs:

RCS service	Tag
Service Provider specific service	Service-Id: org.3gpp.urn:urn-7:3gpp-application.ims.iari.rcs.mnc<mnc>.mcc<mcc>.<service name> Version: Service Provider choice

Table 23: Presence service tuple proposal for future lines of work

2.6.1.3 Coexistence between the discovery mechanisms

2.6.1.3.1 *Service/capability indicators*

The equivalence between presence Service-IDs and SIP OPTIONS tags are presented in the following table:

RCS service		Tag
Standalone Messaging	Tag	+g.3gpp.icsi-ref="urn%3Aurn-7%3A3gpp-service.ims.icsi.oma.cpm.msg; urn%3Aurn-7%3A3gpp-service.ims.icsi.oma.cpm.largemsg"
	Service Tuple	Service-id: org.3gpp.urn:urn-7:3gpp-application.ims.iari.rcs.sm Version: 1.0
Chat	Tag	+g.3gpp.iari-ref="urn%3Aurn-7%3A3gpp-application.ims.iari.rcse.im"
	Service Tuple	Service-id: org.openmobilealliance:IM-session Version : 1.0
File Transfer	Tag	+g.3gpp.iari-ref="urn%3Aurn-7%3A3gpp-application.ims.iari.rcse.ft"
	Service Tuple	Service-id: org.openmobilealliance:File-Transfer Version : 1.0
Image Share	Tag	+g.3gpp.iari-ref="urn%3Aurn-7%3A3gpp-application.ims.iari.gsma-is"
	Service Tuple	Service-id: org.gsma.imageshare Version: 1.0
Video Share during a call	Tag	+g.3gpp.cs-voice
	Service Tuple	Service-id: org.gsma.videoshare Version: 1.0
Video Share outside of a voice call	Tag	+g.3gpp.iari-ref=”urn:urn-7:3gpp-application.ims.iari.gsma-vs"
	Service Tuple	Service-id: org.gsma.videoshare Version: 2.0
Social presence information	Tag	+g.3gpp.iari-ref="urn%3Aurn-7%3A3gpp-application.ims.iari.rcse.sp"
	Service Tuple	Service-id: org.3gpp.urn:urn-7:3gpp-application.ims.iari.rcse.sp Version: 1.0
Capability discovery via presence	Tag	+g.3gpp.iari-ref="urn%3Aurn-7%3A3gpp-application.ims.iari.rcse.dp"
	Service Tuple	Service-id: org.3gpp.urn:urn-7:3gpp-application.ims.iari.rcse.dp Version: 1.0
IP voice call (IR.92/IR.58)	Tag	+g.3gpp.icsi-ref="urn%3Aurn-7%3A3gpp-service.ims.icsi.mmtel"
	Service Tuple	Service-id: org.3gpp.urn:urn-7:3gpp-service.ims.icsi.mmtel Version: 1.0 Media capabilities: audio, duplex
IP video call (IR.94)	Tag	+g.3gpp.icsi-ref="urn%3Aurn-7%3A3gpp-service.ims.icsi.mmtel”;video
	Service Tuple	Service-id: org.3gpp.urn:urn-7:3gpp-service.ims.icsi.mmtel Version: 1.0 Media capabilities: audio, video, duplex
Geolocation PULL	Tag	+g.3gpp.iari-ref="urn%3Aurn-7%3A3gpp-application.ims.iari.rcs.geopull"
	Service Tuple	Service-id: org.3gpp.urn:urn-7:3gpp-application.ims.iari.rcs.geopull Version: 1.0
Geolocation PUSH	Tag	+g.3gpp.iari-ref="urn%3Aurn-7%3A3gpp-application.ims.iari.rcs.geopush"
	Service Tuple	Service-id: org.3gpp.urn:urn-7:3gpp-application.ims.iari.rcs.geopush Version: 1.0

Table 24: Complete SIP OPTIONS tag and Presence Service ID usage for RCS 5.0

2.6.1.3.2 *Coexistence using a common device stack*

As mentioned in section 2.6.1, the principle for interoperability is to have a common stack on devices which is able to:

- Answer a SIP OPTIONS query as per the mechanism presented in section 2.6.1.1 independently on whether the device is configured to use SIP OPTIONS or presence as the default capability exchange mechanism.
- If the device is configured to use presence as the default capability exchange mechanism, implement the fallback to SIP OPTIONS procedure

2.6.1.3.2.1 Interworking when the request is originated in the Service Provider using presence as the default discovery mechanism

In this case, the initial capability exchange request is performed using presence (ANONYMOUS SUBSCRIBE), however either the originating or the terminating Service Provider Network detects that this method is not supported for that particular user and returns with one of the following errors:

- 405 METHOD NOT ALLOWED
- 501 NOT IMPLEMENTED

The RCS stack on the UE will then identify that the contact does not support this discovery mechanism and will mark it as such so from there on the OPTIONS-based mechanism (as presented in section 2.6.1.1) will be used to query that contact's capabilities.

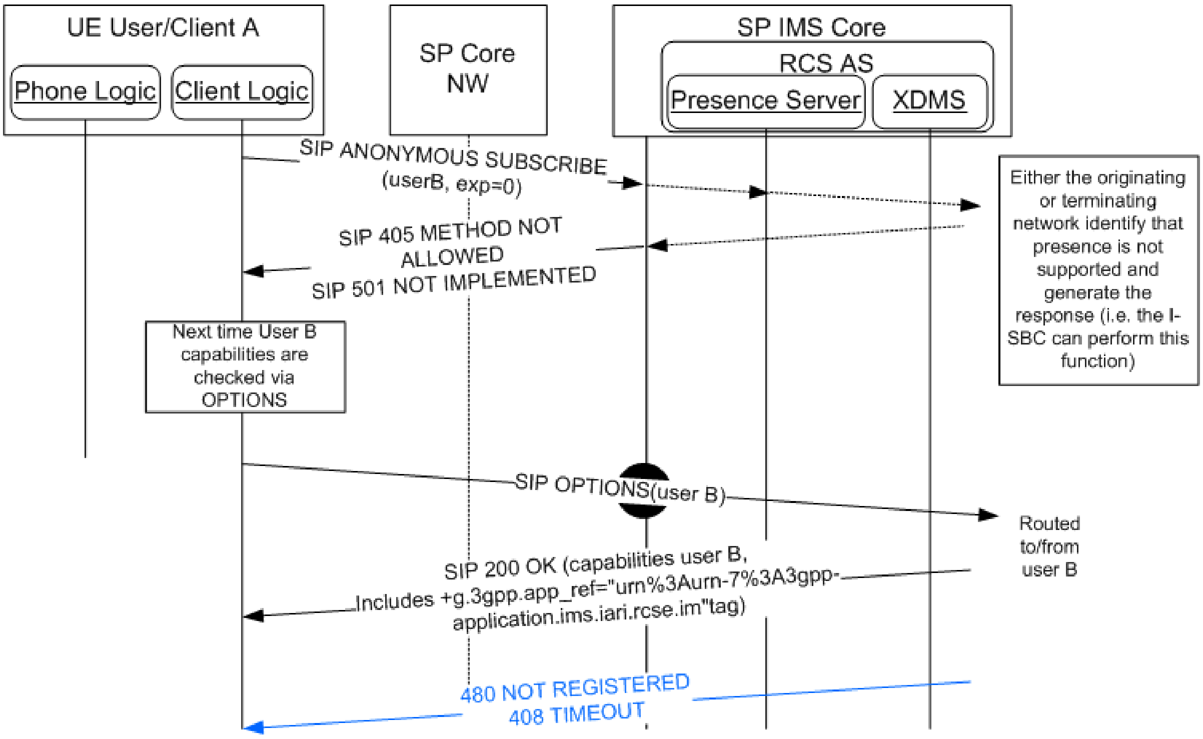

UE User/Client A
Phone Logic
Client Logic
SP Core NW
SP IMS Core
RCS AS
Presence Server
XDMS
SIP ANONYMOUS SUBSCRIBE (userB, exp=0)
SIP 405 METHOD NOT ALLOWED
SIP 501 NOT IMPLEMENTED
Either the originating or terminating network identify that presence is not supported and generate the response (i.e. the I-SBC can perform this function)
Next time User B capabilities are checked via OPTIONS
SIP OPTIONS(user B)
Routed to/from user B
SIP 200 OK (capabilities user B, Includes +g.3gpp.app_ref="urn%3Aurn-7%3A3gpp-application.ims.iari.rcse.im"tag)
480 NOT REGISTERED
408 TIMEOUT

Figure 14: Fallback to SIP-OPTIONS procedure

If in the future, the contact is again identified as supporting discovery via presence (i.e. the *+g.3gpp.iari-ref="urn%3Aurn-7%3A3gpp-application.ims.iari.rcse.dp"* tag was included either in the OPTIONS request or in its response), then capability discovery via presence (as described in section 2.6.1.2) will be used from there on for that contact.

2.6.1.3.2.2 Interworking when the request is originated in the Service Provider using SIP OPTIONS as the default discovery mechanism

In this case, the SIP OPTIONS message is exchanged end-to-end as described in section 2.6.1.1.1.

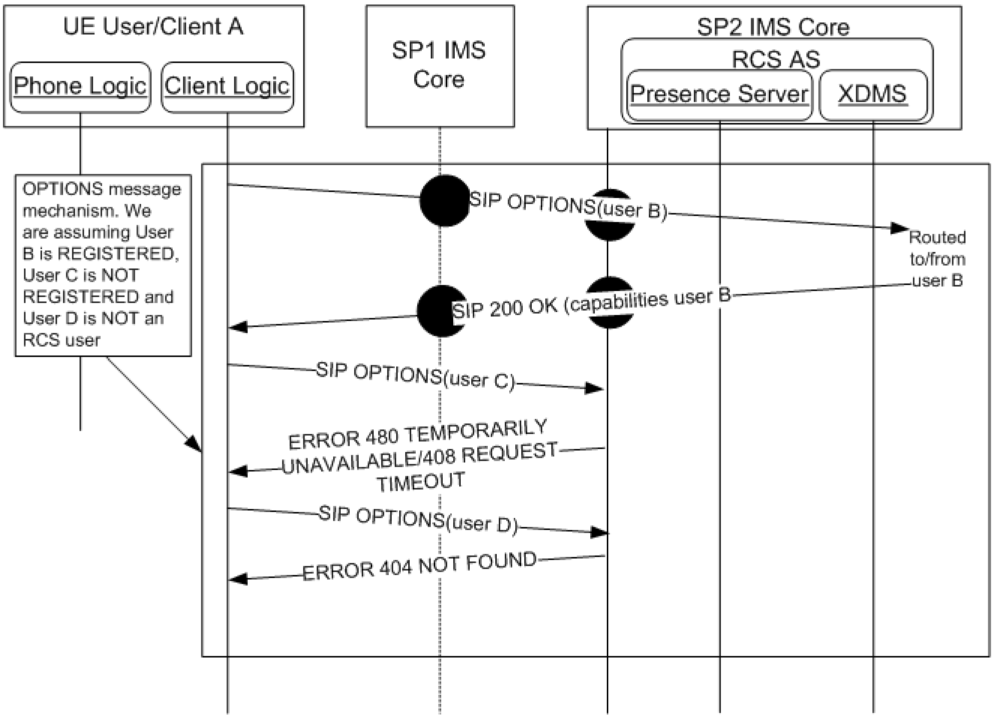

UE User/Client A
Phone Logic
Client Logic
SP1 IMS Core
SP2 IMS Core
RCS AS
Presence Server
XDMS
OPTIONS message mechanism. We are assuming User B is REGISTERED, User C is NOT REGISTERED and User D is NOT an RCS user
SIP OPTIONS(user B)
Routed to/from user B
SIP 200 OK (capabilities user B
SIP OPTIONS(user C)
ERROR 480 TEMPORARILY UNAVAILABLE/408 REQUEST TIMEOUT
SIP OPTIONS(user D)
ERROR 404 NOT FOUND

Figure 15: Inter-Service Provider SIP OPTIONS exchange for interworking

2.6.1.3.3 *Coexistence between the discovery mechanisms via network interworking*

When Service Providers use presence as the default discovery mechanism, there are two ways in which interoperability is achieved between such a Service Provider and those Service Providers who have selected SIP OPTIONS as the default discovery mechanism.

- Service Provider supports fallback to SIP OPTIONS: Interoperability leverages the common device stack as defined in 2.6.1.3.2 above. In this case, there is no requirement for network based interworking
- Service Provider does not support fallback to SIP OPTIONS: Interoperability is provided by network based interworking. Refer to the interworking table below to identify specific network based interworking requirements:

			Service Provider A			
			Default: SIP OPTIONS		**Default: Presence**	
			No Presence Server	**Presence Server**	**OPTIONS Fallback**	**No OPTIONS fallback**
Service Provider B	**Default: SIP OPTIONS**	**No Presence Server**	No Network Interworking Required[2]	No Network Interworking Required[2]	No Network Interworking Required[1]	**Bidirectional Interworking required[3]**
		Presence Server	No Network Interworking Required[2]	No Network Interworking Required[2]	No Network Interworking Required[1]	**Unidirectional Interworking required[4]**
	Default: Presence	**OPTIONS Fallback**	No Network Interworking Required[1]	No Network Interworking Required[1]	No Network Interworking Required[2]	No Network Interworking Required[2]
		No OPTIONS fallback	**Bidirectional Interworking required[3]**	**Unidirectional Interworking required[4]**	No Network Interworking Required[2]	No Network Interworking Required[2]

Table 25: Service Discovery network-based Interworking summary

Notes:

1. No interworking required; based on common stack approach
2. No interworking required; based on common default discovery mode
3. Interworking required for SIP OPTIONS conversion to SUBSCRIBE/NOTIFY and vice versa
4. Interworking required for SIP OPTIONS conversion to SUBSCRIBE/NOTIFY; requirement for conversion from SUBSCRIBE/NOTIFY to SIP OPTIONS contingent upon "SIP OPTIONS default" Service Provider support for Anonymous Fetch at PS

Note that Table 25 considers whether a service provider that uses SIP OPTIONS as the default discovery also supports presence or not:

- The Presence Server acts as a source for both SPI and capability information. This is addressed in 2.6.1.4 which states that capability exchanges are not required in the case where a social relationship is established.
- If a Service Provider uses SIP OPTIONS as the default discovery mechanism, and has deployed presence, the Service Provider may implement a policy that allows their Presence Server to respond to presence based discovery (anonymous) requests.
- Such a policy would impact the required interworking architecture; therefore it is addressed in Table 25 above.

Specific network interworking function requirements are contingent upon the service discovery modes and policies of each service provider. At the Service Provider's discretion, an interworking function can be implemented in the network to:

- Answer incoming SIP OPTIONS requests based on the Presence Server information (Figure 16).
- Convert SIP ANONYMOUS SUBSCRIBE requests into SIP OPTIONS requests (Figure 17).

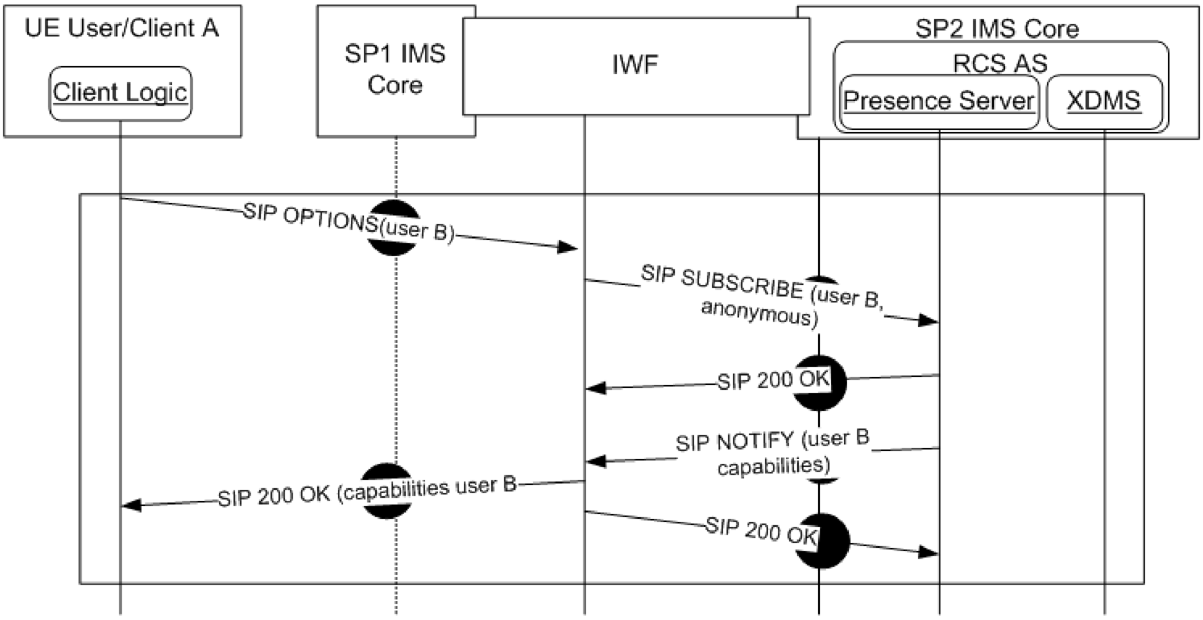


Figure 16: Capability interworking via network: Options request

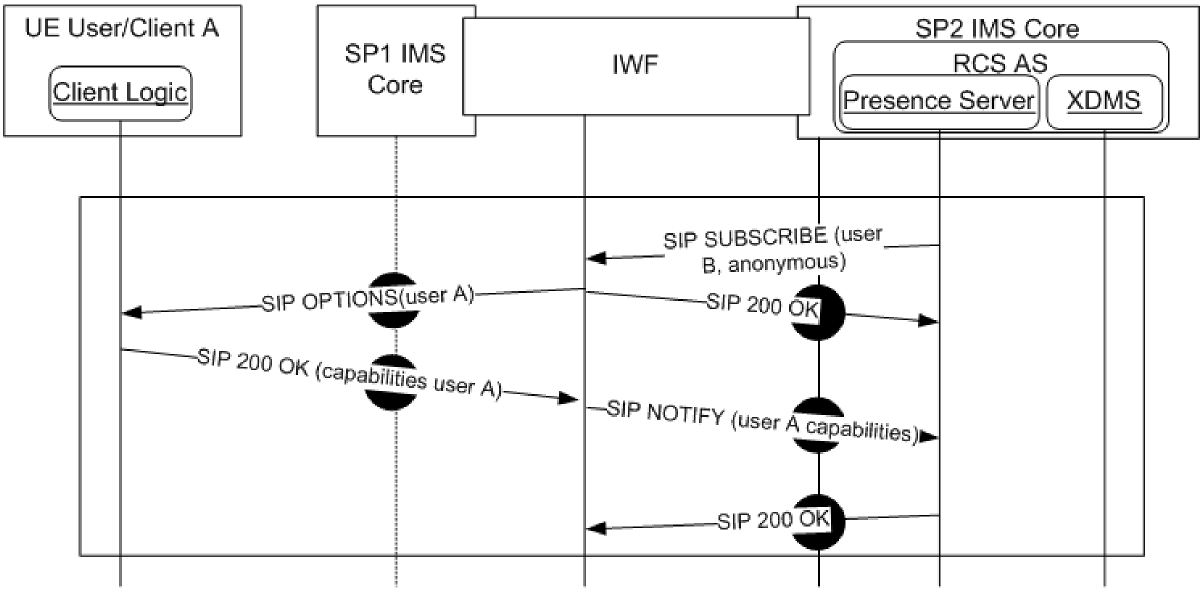


Figure 17: Capability interworking via network: Presence request

Note that Figure 16 and Figure 17 does not specify whether the IWF is deployed:

- In the Originating IMS network
- In the Terminating IMS network
- In the Inter-Network region

All of the above are valid architectural options. NNI impact is not uniform and is a function of the architecture selected. While the details surrounding the specific architecture and functionality of an IWF are left to the Service Provider, it is recommended that impact at the UNI should be minimal and as transparent as possible.

The successful deployment of network IWF capabilities must provide an environment where all RCS devices exchange capabilities information without requiring additional functionality or logic at the client (i.e. no UNI impact).

The following additional guidelines are provided regarding the implementation of an IWF function:

- If either Service Provider has a heterogeneous network from a capabilities discovery mode perspective, this must be factored into the IWF architecture.
- The Service Provider implementing an IWF must consider policy aspects of the functionality. This includes any decisions to filter or transform service capabilities across the IWF.
    - Domain/Service Provider based policies; i.e. specific services are configured to be exposed based on the destination domain.
    - Service level policies: specific services, including Service Provider proprietary or other specialized services that may be filtered from exposure to any external domains
    - User based policy; including privacy or other subscriber level policies

2.6.1.4 Capability discovery and social presence information coexistence

In the following two cases:

- The default mechanism for capability discovery is performed via SIP OPTIONS and the Service Provider has decided to deploy a Presence Server to provide the SPI service[6].
- The default discovery mechanism is based on presence

Then for those contacts who have a social presence relationship established with the sender, it is not necessary to perform a capability exchange because their capabilities will be updated automatically using the standard SPI mechanisms described in section 3.7.4.

2.6.1.5 Capability exchange optimisations

To avoid the overhead and increase the efficiency, the client may implement optimisation mechanisms as listed in section 2.6.4.

2.6.2 User discovery mechanism

With the main aim of optimising the UX and minimising the unnecessary traffic generated by an RCS client, a set of lists shall be generated and maintained by the UE or client:

- A list of the RCS enabled users as the list of users which support at least one RCS service and obviously the capability discovery framework. It should be noted that, the first view of the address book shall use this list to clearly identify the RCS capable contacts with a visual RCS flag.
- One individual list per RCS service of RCS contacts which are enabled to perform that particular service.

These lists should include both registered and non-registered contacts; in contrast, it does not include non-provisioned contacts.

To keep these lists up-to-date, the UE or client shall use one of the capability discovery mechanisms presented in section 2.6.1 in the following scenarios:

- When a new contact is added to the phonebook. The new contact may come from different sources and, therefore, the mechanism described in the following sections applies to all the scenarios presented below:
  - Contact added manually by the user
  - Synchronized via 3rd party servers or PC
  - Received via Bluetooth or handling a vCard file received, for example via e-mail
- The first time the user accesses the service from a new device, the whole address book needs to be polled.
- Periodically (frequency determined by the POLLING PERIOD parameter described in Annex A section A.1.10) to all the contacts in the phone address book whose capabilities are not available (e.g. non-RCS users) or are expired (see CAPABILITY INFO EXPIRY parameter in Annex A section A.1.10 for reference),
- When a contact’s details are edited thereby modifying the information which is used to identify the contact as RCS (as described further in section 2.6.2 e.g. the MSISDN is modified or a new MSISDN is added).

Additionally, it should be noted that if a client is NOT registered at the time the new contact(s) are added, the client should keep the necessary information on the device. In this case the capabilities shall be verified the next time the RCS client completes the registration process.

[6] It may be possible for a Service Provider to always perform service discovery via SIP OPTIONS, but have a policy allowing for remote domain (NNI) support for discovery via presence as discussed in 2.6.1.3.3. This would allow a remote Service Provider that does not support fallback to SIP OPTIONS to obtain capability information using anonymous SUBSCRIBE without traversing a network IWF.

2.6.2.1 Discovery via OPTIONS message

The SIP OPTIONS message can be employed not only to determine the capabilities but also to identify whether or not a contact is an RCS user; independently from whether the contact is registered at the time the query is performed.

When a SIP OPTIONS message is sent from User A to User B, User A will learn about user B's capabilities through one of 6 scenarios:

1. User B is registered and the response from User B's client will include the CAPABILITY STATUS – the set of services currently available (based on tags as described in section 2.6.1.1.2). Please note that regarding the list of RCS users, the contact shall be only considered as an RCS user, if the response (SIP 200 OK) includes any of the tags described in Table 24.
2. If User B is currently not registered (e.g. the device is switched off, out of coverage or roaming with data services disabled), then the network will respond with one of the following error messages: SIP 480 TEMPORARILY UNAVAILABLE (graceful deregistration took place) or SIP 408 REQUEST TIMEOUT. From the new user discovery point of view, this response is ignored because it is inconclusive:
   - It does not confirm whether the contact is an RCS user, and,
   - It does not provide any relevant update to the list of RCS contacts capable of a particular service
3. If User B is not provisioned for RCS the network will respond with a message error: SIP 404 NOT FOUND[7]. Therefore, if this message is received, the user is identified as a non-RCS user (removed from the list of RCS users and from the individual list of RCS users capable of a particular service)
4. If User B was previously identified as an RCS user and the response to the OPTIONS message indicates that User B is no longer supporting any RCS services, User B should be identified as a non-RCS user and, consequently, removed from the list of RCS enabled contacts
5. In addition to this and based on the fact the SIP OPTIONS request contain the list of services supported by the requester, the receiver shall use the SIP OPTIONS message to update both the RCS contact list and the relevant per service lists as per the criteria presented in the previous four scenarios .
6. Please note there is a possibility an RCS user who is not within the address book contacts may send OPTIONS messages or responses (e.g. when receiving a call or making a call using a MSISDN not included in the contacts). In this case the capabilities shall be stored temporarily in the terminal to:
   - Keep the service availability updated while a session (Chat, File Transfer, Video/Image Share, IP Voice or Video call, Geolocation PUSH) is still in place, and,
   - To add the information to the new contact (both the fact that it is an RCS user and the cached capabilities) if the user decides to add a new address book entry following a communication.

To illustrate the behaviour, the following example is provided. User A is registered and decides to add or modify a new contact which results in a new IMS identity for the contact (e.g. new MSISDN which implies a new tel URI). As a consequence, the client is required to

[7] Please note that the response provided may depend on the network configuration. A useful approach for the terminal is to parse the response and if it is not either a 200 OK containing the capabilities as feature tags, a 480 TEMPORARILY UNAVAILABLE or a 408 REQUEST TIMEOUT, the target user should be considered as non-RCS. For simplicity, the present document assumes in the following sections that the response provided by the Service Provider core network is always 404 NOT FOUND, however, the previous statement should be taken into account.

verify whether the contact is an RCS user and, therefore, add them to the list the terminal maintains.

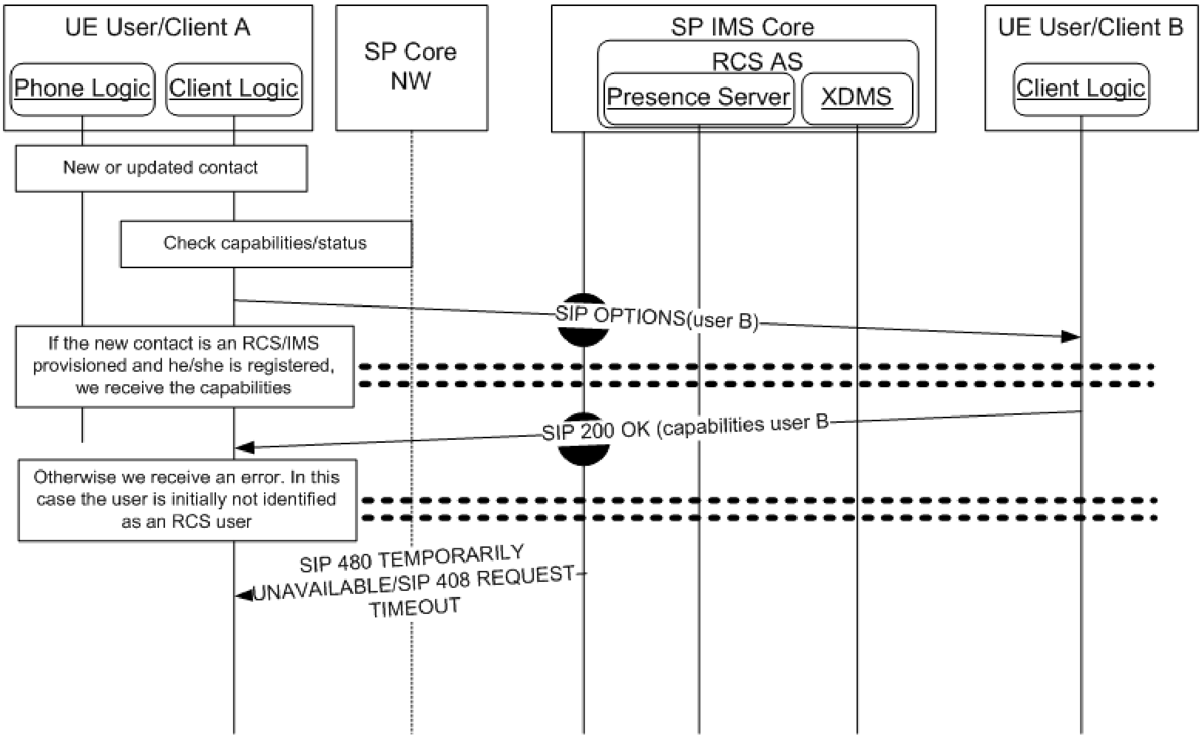

UE User/Client A
Phone Logic
Client Logic
SP Core NW
SP IMS Core
RCS AS
Presence Server
XDMS
UE User/Client B
Client Logic
New or updated contact
Check capabilities/status
SIP OPTIONS(user B)
If the new contact is an RCS/IMS provisioned and he/she is registered, we receive the capabilities
SIP 200 OK (capabilities user B
Otherwise we receive an error. In this case the user is initially not identified as an RCS user
SIP 480 TEMPORARILY UNAVAILABLE/SIP 408 REQUEST TIMEOUT

Figure 18: Adding/Editing a contact

2.6.2.2 Discovery via PRESENCE

The procedure for user discovery using presence is analogous to the capability discovery procedure using presence as described in section 2.6.1.2. However the following additional considerations shall be taken into account:

- When User A queries User B's capabilities, the response will include the CAPABILITY STATUS – the set of services currently available (based on the service-IDs presented in section 2.6.1.3.1). Please note that regarding the list of RCS users, the contact shall be considered as an RCS user, only if the response includes one of the tags described in Table 24.

2.6.2.3 Coexistence between user discovery mechanisms

Please note that the mechanisms described in sections 2.6.1.3 also apply to the user discovery mechanisms co-existence.

2.6.2.4 User discovery and social presence information coexistence

Please note that the considerations presented in section 2.6.1.4 also apply to the user discovery process.

2.6.2.5 Capability polling mechanism

To enhance the discovery of new users and, ultimately, keep the list of RCS contacts up to date, this specification provides a mechanism, capability polling, consisting of the polling of the status/capabilities of all the contacts in the address book whose capabilities are not available (such as non-RCS users) or have expired (see CAPABILITY INFO EXPIRY parameter in Annex A section A.1.10 for further reference).

It should be noted that the capability polling mechanism is optional and will be only performed if the related configuration settings have been provisioned (that is if the POLLING PERIOD parameter presented in Annex A section A.1.10 is set to 0, this polling mechanism will not be used).

Assuming the POLLING PERIOD is configured to be greater than 0 and after the polling timer expires, the client will use the following mechanism to update the list of RCS contacts and update their capabilities.

Please note the capability polling is only performed on:

- Those contacts without capability information (non-RCS users and RCS users with unknown capabilities), and,
- The rest of RCS contacts, provided the associated capability information is older than the CAPABILITY INFO EXPIRY parameter (see Annex A section A.1.10 for further reference)[8].

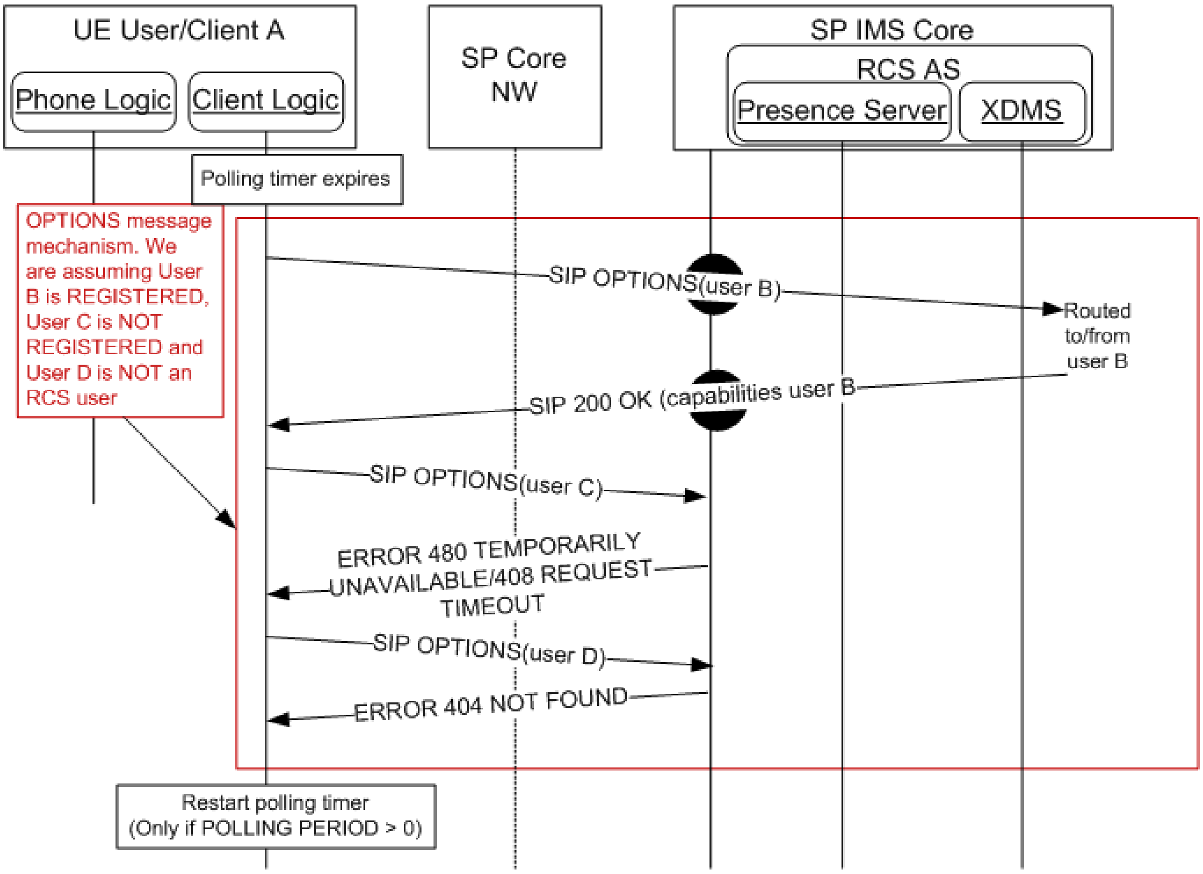

UE User/Client A
Phone Logic
Client Logic
SP Core NW
SP IMS Core
RCS AS
Presence Server
XDMS
Polling timer expires
OPTIONS message mechanism. We are assuming User B is REGISTERED, User C is NOT REGISTERED and User D is NOT an RCS user
SIP OPTIONS(user B)
Routed to/from user B
SIP 200 OK (capabilities user B
SIP OPTIONS(user C)
ERROR 480 TEMPORARILY UNAVAILABLE/408 REQUEST TIMEOUT
SIP OPTIONS(user D)
ERROR 404 NOT FOUND
Restart polling timer (Only if POLLING PERIOD > 0)

Figure 19: Capabilities polling via OPTIONS message

When CAPABILITY DISCOVERY MECHANISM is set to presence (see Annex A section A.1.10), the presence based discovery based in the use of SIP ANONYMOUS SUBSCRIBE requests are used for all the contacts except:

- If implementing co-existence based on a common device stack, those contacts which are identified as not supporting presence discovery (SIP OPTIONS will be used instead as per the fallback procedure presented in section 2.6.1.3.2.1).
- Those users with a SPI relationship in place because their capabilities will be updated automatically using the standard SPI mechanisms described in section 3.7.4.

[8] Please note this is a traffic optimization to reduce the amount of SIP OPTIONS messages generated by capability polling

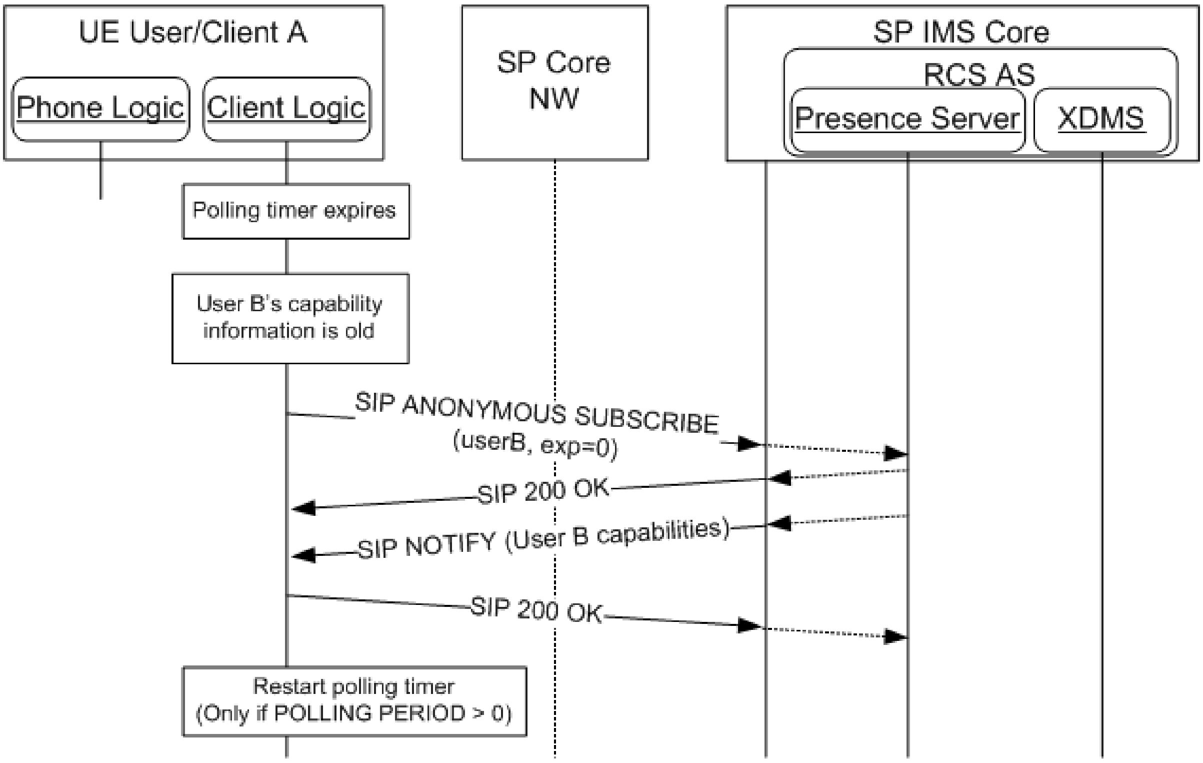

UE User/Client A
Phone Logic
Client Logic
SP Core NW
SP IMS Core
RCS AS
Presence Server
XDMS
Polling timer expires
User B's capability information is old
SIP ANONYMOUS SUBSCRIBE (userB, exp=0)
SIP 200 OK
SIP NOTIFY (User B capabilities)
SIP 200 OK
Restart polling timer (Only if POLLING PERIOD > 0)

Figure 20: Capabilities polling via anonymous fetch

Note that if an RLS-URI was provisioned (see Annex A Section A.1.1.1) and the capabilities of multiple contacts need to be queried, the capability query could be initiated by the device using a request contained list that is decomposed by the RLS service in the originating network (see section 2.6.1.2.3 for more details). In this case the SIP SUBSCRIBE request shown in Figure 20 would be a back end subscribe issued by the user's home RLS and should be forwarded to the correct destination Presence Server(s). The RLS will gather the notifications and send aggregated notifications to the device.

Finally, and as a summary of the capability and new user discovery mechanism composition the following diagram is provided.

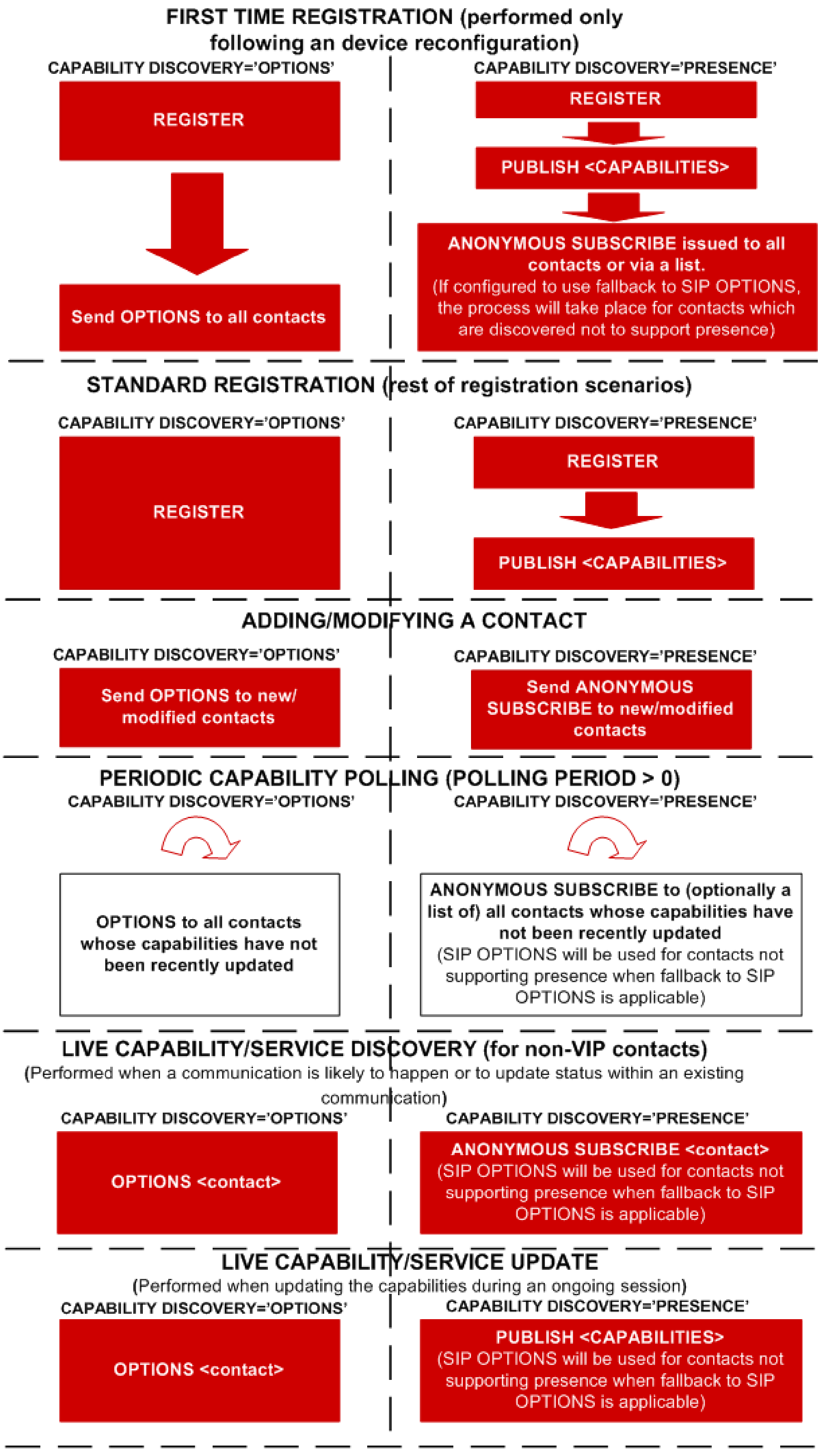

FIRST TIME REGISTRATION (performed only following an device reconfiguration)
CAPABILITY DISCOVERY='OPTIONS'
REGISTER
Send OPTIONS to all contacts
CAPABILITY DISCOVERY='PRESENCE'
REGISTER
PUBLISH <CAPABILITIES>
ANONYMOUS SUBSCRIBE issued to all contacts or via a list.
(If configured to use fallback to SIP OPTIONS, the process will take place for contacts which are discovered not to support presence)
STANDARD REGISTRATION (rest of registration scenarios)
CAPABILITY DISCOVERY='OPTIONS'
REGISTER
CAPABILITY DISCOVERY='PRESENCE'
REGISTER
PUBLISH <CAPABILITIES>
ADDING/MODIFYING A CONTACT
CAPABILITY DISCOVERY='OPTIONS'
Send OPTIONS to new/ modified contacts
CAPABILITY DISCOVERY='PRESENCE'
Send ANONYMOUS SUBSCRIBE to new/modified contacts
PERIODIC CAPABILITY POLLING (POLLING PERIOD > 0)
CAPABILITY DISCOVERY='OPTIONS'
OPTIONS to all contacts whose capabilities have not been recently updated
CAPABILITY DISCOVERY='PRESENCE'
ANONYMOUS SUBSCRIBE to (optionally a list of) all contacts whose capabilities have not been recently updated
(SIP OPTIONS will be used for contacts not supporting presence when fallback to SIP OPTIONS is applicable)
LIVE CAPABILITY/SERVICE DISCOVERY (for non-VIP contacts)
(Performed when a communication is likely to happen or to update status within an existing communication)
CAPABILITY DISCOVERY='OPTIONS'
OPTIONS <contact>
CAPABILITY DISCOVERY='PRESENCE'
ANONYMOUS SUBSCRIBE <contact>
(SIP OPTIONS will be used for contacts not supporting presence when fallback to SIP OPTIONS is applicable)
LIVE CAPABILITY/SERVICE UPDATE
(Performed when updating the capabilities during an ongoing session)
CAPABILITY DISCOVERY='OPTIONS'
OPTIONS <contact>
CAPABILITY DISCOVERY='PRESENCE'
PUBLISH <CAPABILITIES>
(SIP OPTIONS will be used for contacts not supporting presence when fallback to SIP OPTIONS is applicable)

Figure 21: RCS capability and new user discovery mechanisms[9]

[9] The red boxes represent mandatory procedures. Meanwhile the clear boxes represent optional procedures.

2.6.3 Capability update for services

2.6.3.1 User driven entry points for capability update

A capability update is triggered by one of the following activities:

- After first time registration to obtain the registration state and default set of capabilities for each contact in the device's address book (note one capability exchange takes place per IMS identity [that is tel URI/MSISDN or SIP URI] stored in the address book)[10],
- When checking the available RCS services/capabilities to communicate with another user (e.g. from the address book and call-log)
- After establishing voice call to obtain the real-time capabilities for the call or Chat session provided this has not been performed before (see previous bullet) or content sharing during a call is supported.
- After the call returns to an active state (e.g. returning from call wait, call on hold or multiparty call).
- When a communication is active with a user to provide an update when the relevant available capabilities change:
  - When a 1-2-1 Chat session is established and any of the following capabilities change:
    - File Transfer
    - Geolocation PUSH
    - Video Share without a call
  - When in an active call with an RCS user and any of the following capabilities change:
    - Chat
    - File Transfer
    - Geolocation PUSH
    - Geolocation PULL
    - Video Share
    - Image Share
    - IP Video Call
  - When an IP call or video call session is in place and any of the following capabilities change:
    - Chat
    - File Transfer
    - Geolocation PUSH
    - Geolocation PULL
    - Video Share
    - Image Share

[10] Please note a contact may have several MSISDNs or associated SIP URIs. The client will use ALL the MSISDNs/SIP URIs stored for that user to perform the capability exchange. If it is discovered that more than one of the associated tel URIs/SIP URIs are IMS provisioned, each will be treated as a separate RCS user. For example, if displaying the list of RCS contacts, two or more entries for a user will be shown ("John Smith mobile" and "John Smith home"), so the user can choose.

  - IP Video Call

- When there is a communications event (text, email, call or Chat) with another user in the address book, taking into account the optimizations presented in section 2.6.1.5.

2.6.3.1.1 *UX guidelines: Access to RCS services through address book and call-log interaction*

The address book (and by extension the call-log window as an alternative for users who have been recently phoned) is the centrepiece to access all RCS services. From it, the user is able to:

- Identify which services are available for each contact: When a contact is selected, the capabilities are updated using one of the mechanisms described in section 2.6 (SIP OPTIONS query or PRESENCE), and the result is presented to the user by showing the RCS services which are available to communicate with that particular contact
  - Please note for those contacts who have a social presence relationship established with the sender, it is not necessary to perform a capability exchange because their capabilities will be updated automatically using the standard SPI mechanisms described in section 3.7.4. Therefore and for those contacts, the capability exchange is not required
- If one or more RCS services are available[11], they can be started from the address book/call log entry. Please note the only exception is for those content sharing services that can be only accessed when during a call.

In addition to this, the first view of the address book may clearly identify the RCS capable contacts with an icon or flag.

2.6.3.1.1.1 General assumptions

The following sections describe the relevant chat message flows and reference UX. Please note that the following assumption has been made:

- For simplicity, the internal mobile network interactions are omitted in the diagrams shown in the following sections.

2.6.3.1.1.2 Capability update process

The capabilities update process is described in the following diagram. In this case the contact (User B) is an RCS contact which is registered.

[11] It should be noted that in this case if IM CAP ALWAYS ON (see Table 52) is enabled, the Chat should still be reported to the user as available even if the other end/user is not registered.

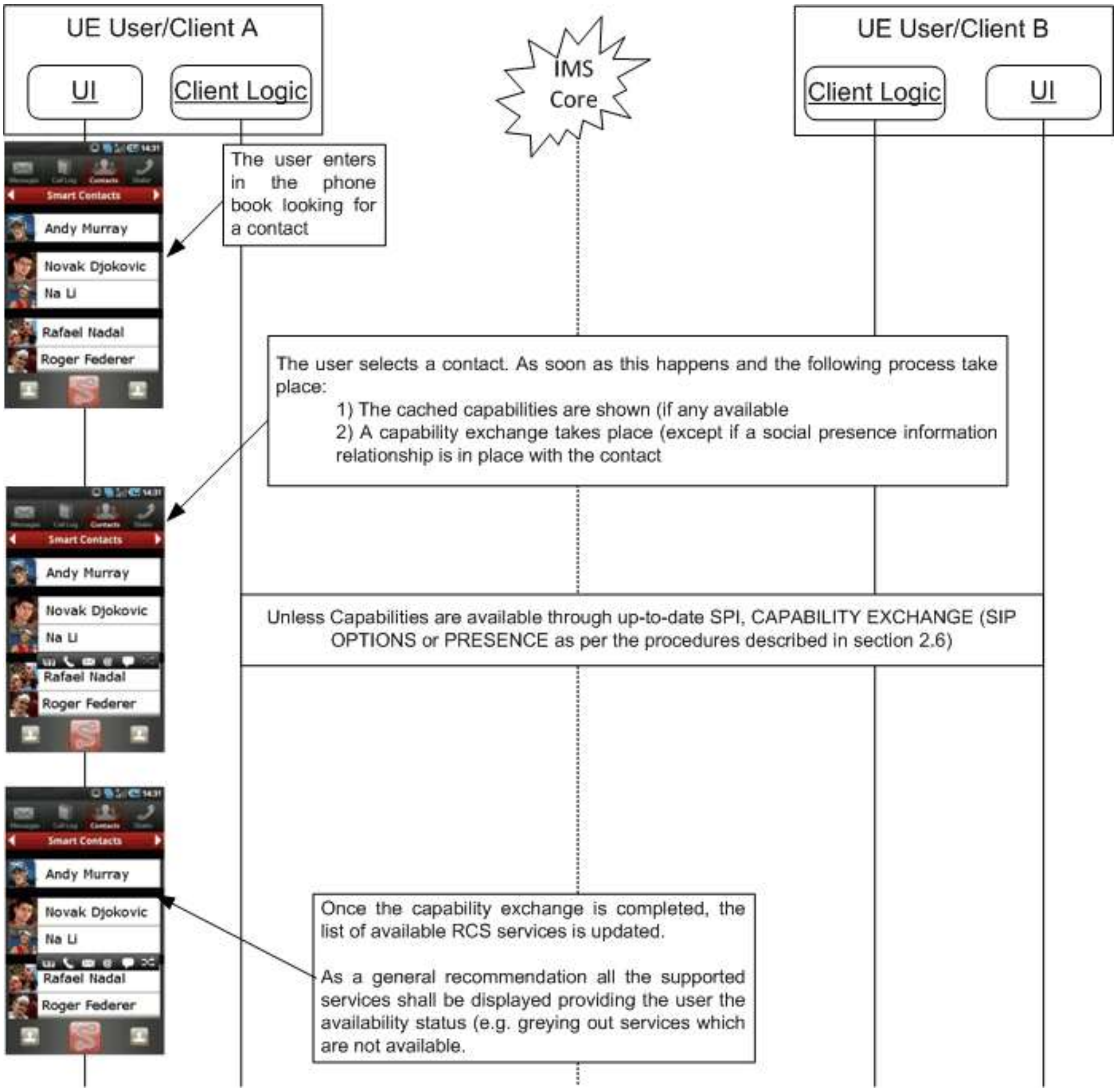

UE User/Client A
UI
Client Logic
IMS Core
UE User/Client B
Client Logic
UI
The user enters in the phone book looking for a contact
The user selects a contact. As soon as this happens and the following process take place:
1) The cached capabilities are shown (if any available
2) A capability exchange takes place (except if a social presence information relationship is in place with the contact
Unless Capabilities are available through up-to-date SPI, CAPABILITY EXCHANGE (SIP OPTIONS or PRESENCE as per the procedures described in section 2.6)
Once the capability exchange is completed, the list of available RCS services is updated.
As a general recommendation all the supported services shall be displayed providing the user the availability status (e.g. greying out services which are not available.
Smart Contacts
Andy Murray
Novak Djokovic
Na Li
Rafael Nadal
Roger Federer

Figure 22 : Address book and call-log service access: Capabilities update

If User B is either not an RCS user or they are not currently registered, User A's client will assume that no services are available to communicate with User B.

As a general recommendation all the supported RCS services shall be displayed providing the user the availability status (e.g. greying out services which are not available).

2.6.3.2 Standalone messaging: Text and multimedia messaging

The capability exchange is not required for this service.

2.6.3.3 1-to-1 Chat

In addition to the general user driven entry points and taking into account:

- The optimizations provided in section 2.6.1.5, and,
- The potential impact of having a SPI relationship with between sender and receiver as described in section 2.6.2.4.

The capability exchange shall take place (when the service capability query is supported by SIP OPTIONS or the contact is not a VIP Contact for SPI):

- Before the initial SIP INVITE is sent to initiate the service to verify if the receiver is ready for the service (unless an exchange of capabilities has just been made based on one of the criteria listed in section 2.6.3.1, as described in section 2.6.4)
- If an error takes place:
  - After the Chat session is abruptly terminated or irregular signalling behaviour during the establishment of the service is detected
  - When there is an update on the available capabilities on either end once the session is established
- In any of the scenarios described in section 2.6.3.1 which are relevant to the service.

2.6.3.4 Group Chat

In addition to the general user driven entry points and taking into account:

- The optimizations provided in section 2.6.1.5, and,
- The potential impact of having a SPI relationship with between sender and receiver as described in section 2.6.2.4.

The capability exchange shall take place (when the service capability query is supported by SIP OPTIONS or the contact is not a VIP Contact for SPI):

- Before the initial SIP INVITE is sent to initiate the service to verify if the receiver is ready for the service (unless an exchange of capabilities has just been made based on one of the criteria listed in section 2.6.3.1, as described in section 2.6.4)
- If an error takes place:
  - After the Chat session is abruptly terminated or irregular signalling behaviour during the establishment of the service is detected
  - When selecting the participants of a Group Chat to verify whether they are available

2.6.3.5 File Transfer

In addition to the general user driven entry points and taking into account:

- The optimizations provided in section 2.6.1.5, and,
- The potential impact of having a SPI relationship with between sender and receiver as described in section 2.6.2.4.

The capability exchange shall take place (when the service capability query is supported by SIP OPTIONS or the contact is not a VIP Contact for SPI):

- Before the initial SIP INVITE is sent to initiate the service to verify if the receiver is ready for the service (unless an exchange of capabilities has just been made based on one of the criteria listed in section 2.6.3.1, as described in section 2.6.4)
- If an error takes place:
  - After the service is cancelled either by the sender or receiver
  - After the file transfer is abnormally interrupted as a result of a failure or irregular signalling behaviour during the establishment of the service is detected

2.6.3.6 Content sharing

In addition to the general user driven entry points and taking into account:

- The optimizations provided in section 2.6.1.5, and,
- The potential impact of having a SPI relationship with between sender and receiver as described in section 2.6.2.4.

The capability exchange shall take place:

- Before the initial SIP INVITE is sent to initiate the service to verify if the receiver is ready for the service (unless an exchange of capabilities has just been made based on one of the criteria listed in section 2.6.3.1, as described in section 2.6.4)
- If an error takes place:
  - After the service is cancelled either by the sender or receiver
  - After the sharing is abnormally interrupted as a result of a failure or irregular signalling behaviour during the establishment of the service is detected
  - After the call is no longer active
- In any of the scenarios described in section 2.6.3.1 which are relevant to the service.
- For those content sharing services applicable within a call and for devices, when there is a proximity sensor trigger indicating that the user is holding the device rather than keeping it close to his/her ear.

2.6.3.7 Social presence

Information indicating support for social information via presence is expected prior to a user's attempt to establish a social presence relationship. This supports the "Who Can I Invite" concept; providing the user with a view of the contacts with whom they can attempt to establish a social presence relationship. This information is provided in the following contexts:

- Discovery via SIP OPTIONS.
- Discovery via Presence

Independently of the chosen mechanism,

- If capability discovery indicates that both clients support the "social information via presence" functionality, the user is then presented with the possibility of inviting the contact to share the social presence information. This includes invitation of a previously discovered SPI-enabled contact who is temporarily Not Available. If not, the terminal should not present this possibility to the user for that contact.
- For those contacts who have an active social presence relationship established with the sender, it shall not perform a capability exchange if their capabilities are updated automatically using the standard SPI mechanisms described in section 3.7.4.

2.6.3.7.1 *Discovery via SIP OPTIONS*

To ensure interoperability[12] and enable those Service Providers implementing an SIP OPTIONS based capability/user discovery mechanism as default for their RCS deployments but deploying a Presence Server to additionally provide the social profile information (as described in section 3.7.4.2.2) functionality, the UE shall provide the following procedure:

> Prior to being able to send an invitation to a contact (e.g. from the address book), the terminal will use the OPTIONS mechanism to determine if the other end also supports this feature (that is both ends include the "Social Presence Information" SIP OPTIONS tag in the relevant headers).

2.6.3.7.2 *Discovery via presence*

Prior to being able to send an invitation to share Social Presence with a contact (e.g. from the address book), the terminal may use the Anonymous Fetch mechanism to determine if the other end also supports this feature (that is both ends include an "open" "Social Presence Information" Presence Service Tuple in the Presence Information Data Format

[12] Please note that the present specification allows the deployment of RCS communication services without the need for a Presence Server and the associated XDM servers, therefore, the present specification provide the necessary guidance to secure interoperability.

[PIDF]). This includes inviting a contact who has previously been discovered to be Social presence-enabled even when they are currently offline.

2.6.3.8 IP voice call

The capability exchange is not required for this service. This capability may be used for network internal use and shall not have an impact on the user experience.

2.6.3.9 IP video call

In addition to the general user driven entry points and taking into account:

- The optimizations provided in section 2.6.1.5, and,
- The potential impact of having a SPI relationship with between sender and receiver as described in section 2.6.2.4.

The capability exchange shall take place:

- Before the IP video call service is initiated by the sender to verify if the receiver is ready for the service (unless an exchange of capabilities has just been made based on one of the criteria listed in section 2.5.3.1, as described in section 2.5.4)
- If an error takes place, after the call when the service was abnormally interrupted or irregular signalling behaviour during the establishment of the service is detected.
- In any of the scenarios described in section 2.6.3.1 which are relevant to the service.

2.6.3.10 Geolocation PUSH

In addition to the general user driven entry points and taking into account:

- The optimizations provided in section 2.6.1.5, and,
- The potential impact of having a SPI relationship with between sender and receiver as described in section 2.6.2.4.

The capability exchange shall take place:

- Before the initial SIP INVITE is sent to initiate the service to verify if the receiver is ready for the service (unless an exchange of capabilities has just been made based on one of the criteria listed in section 2.6.3.1, as described in section 2.6.4)
- If an error takes place:
  - After the service is cancelled either by the sender or receiver
  - If an error takes place and as a result the Geolocation PUSH is abnormally interrupted or irregular signalling behaviour during the establishment of the service is detected

2.6.3.11 Geolocation PULL

In addition to the general user driven entry points and taking into account:

- The optimizations provided in section 2.6.1.5, and,
- The potential impact of having a SPI relationship between sender and receiver as described in section 2.6.2.4.

The capability exchange shall take place:

- If an error takes place:
  - After the service is cancelled either by the sender or receiver
  - If an error takes place and as a result the Geolocation PULL is abnormally interrupted or irregular signalling behaviour during the establishment of the service is detected

2.6.4 Capability exchange optimisations

Depending on the circumstances and use cases, there could be occasions where the capability exchange may happen relatively often (in case of very frequent bearer changes for instance).

To avoid the overhead and increase the efficiency, the client may implement a mechanism to reduce the number of requests in situations where the capability exchange is likely to be performed too often. Examples of how this mechanism can be achieved are listed below:

- Introduce a degree of hysteresis (that is a capabilities update is sent/requested only when the circumstances which led to the change remain stable for a certain period of time).
- Implement a validity timer (that is if the latest capabilities we have were fetched less than X seconds ago, they are still considered as valid).

Please note that this specification does not describe detailed implementations to leave room for OEMs and third parties to drive innovative and differentiated solutions. This helps to distinguish their products from competitors.

2.6.4.1 Service Provider Controlled Service Capabilities Handling

The following items can be configured subject to the Service Provider’s policies (see section A.1.10):

1. The maximum amount of capability query operations during a certain time period done by a client (that is, for all contacts)
2. An expiry of the capabilities for a specific contact

This will allow to control the maximum time before a client will discover that one of the contacts is now RCS capable

Note: there might be a conflict between the different provisioning settings controlling the frequency of capability query operations (for example, a too low maximum amount of fetch operation combined with a very low expiry time). In that case an RCS client will prioritize the maximum amount of fetch operations settings over the expiry. A Service Provider deploying RCS is likely to carefully consider the values of these settings and this is therefore not expected to be an issue in actual deployments.

2.7 Capability values and status

The RCS capabilities represent the list of services that an RCS user/client can access at a certain point in time. The capabilities depend on four factors:

1. User Service Provider provisioning status: A Service Provider may choose to limit service to customers depending on subscription status (e.g. chat and file share, but not video)
2. The terminal hardware (HW): A terminal with limited HW (i.e. no capability to process video) may not be able to access all the RCS Services
3. The terminal status: Even if a terminal HW supports all the services, it could be that the device status introduces a limitation (e.g. receiving files is not possible when the file storage is full)
4. Connectivity status: Some services may require a certain level of network Quality of Service (QoS). For example, streaming video over a 2G GPRS does not provide an adequate UX.

In addition to the factors presented above and as presented in Annex A section A.1, it is possible for a Service Provider to select which services are available for a particular user. Therefore, the previous considerations shall only be taken into account assuming that the relevant RCS services are enabled via configuration and consequently, Table 26, assumes that all the user’s devices have been configured with all the RCS services enabled.

As a summary, please find the table below (note that it is assumed the client/terminal and the network supports each of the services as a precondition and that the client/terminal is provisioned to support all the services[13]):

Service	TERMINAL and STATUS REQUIREMENTS	Data Bearer					
		2G	EDGE	3G	HSPA	LTE	Wi-Fi
Standalone messaging	None	Y	Y	Y	Y	Y	Y
Chat (1-to-1 or group)	None	Y	Y	Y	Y	Y	Y
File Transfer (FT)	Minimum threshold of free space to store files	Y	Y	Y	Y	Y	Y
Content share: Image Share	Minimum threshold of free space to store files. The terminal should be on an active call[14] with the user the image is willing to be shared with. Not available in multiparty calls.	Y[15]	Y[14]	Y	Y	Y	Y
Content share: Video Share during a call (IR.74)	Support video profile (encoding /decoding). The terminal should be on an active call[14] with the user the video is willing to be shared with. It is not available in multiparty calls.	N	N	Y One Way Only	Y[16]	Y[16] Higher video profile	Y[16]
Content share: Video Share without a call (IR.84)	Support video profile (encoding /decoding).	N	N	Y One Way Only	Y[16]	Y[16] Higher video profile	Y[16]
SPI	N/A	Y	Y	Y	Y	Y	Y
IP Voice Call	N/A	N	N	N	Y (IR.58)	Y (IR.92)	Y RCS-AA only
IP Video Call	Support video profile (encoding /decoding).	N	N	N	Y RCS-AA only	Y (IR.94)	Y RCS-AA only

[13] As presented in Annex A section A.1, it is possible for a Service Provider to select which services are available for a particular user.

[14] In this context, the term active call is used to indicate that a voice call is taking place with the user the image is shared with and that this call is not on-hold, waiting or forwarded/diverted. This limitation is not applicable for broadband access devices for the handling of a received capability request or an incoming invitation. The restrictions fully apply for outgoing requests.

[15] Note that it is only possible if device and the cellular network support Dual-Transfer Mode (DTM)

[16] In this case both ends may share video simultaneously meaning that there is a possibility to have a bi-directional flow of video (see the other party's video while I am also sharing video with him/her). The meaning is that if a user is already sharing video with the other end, the other user may decide to also share video simultaneously, not that the two-ways Video Share can start simultaneously.

Service	TERMINAL and STATUS REQUIREMENTS	Data Bearer					
		2G	EDGE	3G	HSPA	LTE	Wi-Fi
Geolocation PUSH	Minimum threshold of free space to store files From the capability exchange point of view there are no additional terminal requirements however on the sender the service shall be only available if the terminal (UE) provides a mean to access the location information required for the service.	Y	Y	Y	Y	Y	Y
Geolocation PULL	Primary device with capability for locating	Y	Y	Y	Y	Y	Y

Table 26: RCS services: Terminal, status and data bearer requirements

2.7.1 Additional considerations for specific RCS services

2.7.1.1 Chat store and forward: Impact in the capability exchange

As presented in section A.1.3.3 (IM CAP ALWAYS ON), there is the possibility to configure the client to assume that the Service Provider will be providing the Chat store and forward functionality, which consists of storing messages which are sent to users who are offline (i.e. no data connectivity or device off) at the time the chat message is sent.

If this parameter is enabled, there is an impact from the Chat capability which is presented to the user.

As a consequence, we have 4 different types of contacts for Chat capability:

ID	Targeted contact is RCS Chat capable?	Originating Service Provider supports Store& Forward?	Targeted contact is connected to the network?	Impact on starting Chat
1	NO	N/A	N/A	Chat never possible with that contact
2	YES	NO	NO	Not possible to start a Chat at that time
3	YES	YES	NO	Possible to send a Chat message that will be delivered later by the Store and Forward server as soon as the Contact is connected
4	YES	Not Relevant	YES	Chat is possible and messages are immediately delivered

Table 27: Store and forward possible scenarios

The Chat behaviour on the client is controlled by these configuration parameters (see Annex A for further information):

- IM CAP ALWAYS ON:
  When a Service Provider implements store and forward, they may choose to provision all the RCS users with the IM CAP ALWAYS ON configuration parameter set to enabled. This means that all RCS contacts (currently registered or not) are presented with the Chat service as available (3 and 4 according to Table 27).
  When store and forward is not implemented by the SP, all its RCS customers will have the IM CAP ALWAYS ON configuration parameter is set to disabled (2 and 4 according to Table 27).
  As a summary: IM CAP ALWAYS ON is enabled when store and forward functionality is provided in the network, otherwise it is disabled
- When IM CAP ALWAYS ON is enabled, IM WARN SF can be used to control the UI behaviour:
  If IM WARN SF parameter is enabled: In scenarios 3 and 4, the user shall be made aware that messages delivered to unregistered users will be only delivered once the other party is back online (for example after switching on the device or regaining network coverage).
  If IM WARN SF parameter is disabled, there shall not be any visible difference between scenarios 3 and 4 from the UI point of view. Therefore, the user shall not be made aware of whether the messages are being stored or are delivered directly to the other party.
  When IM WARN SF is enabled, the device/client uses the response from the capability exchange to determine whether a warning is displayed to the user.

When interworking of chat to SMS/MMS is available for users, two more parameters can be used in a similar way: IM CAP NON RCS and IM WARN IW. More information can be found in section A.1.3.3.

2.7.1.2 Video and Image Share additional considerations

2.7.1.2.1 *Bidirectional Video Share*

Bidirectional Video Share means that once User A is sharing a video with User B and providing the right coverage conditions are in place, User B could also start to share a video with User A simultaneously. In this case each Video Share session is independent and is handled separately.

For clarification purposes, the following assumptions are made for the Image and Video Share cases:

- Both the sharing and receiving end are in a call (that may for instance be CS) between them
- The call is not a multiparty call
- The call is not on hold
- The call is not waiting
- A call forward or divert is not in place

Meaning the relevant Image and Video Share tags described in section 2.6.1.1.2 shall be included only if:

1. The OPTIONS exchange happens when the user is on an active call, and,
2. The destination (sending OPTIONS) or the requester (receiving an OPTIONS message which has to be replied with a response) is on the other end of the active call.

Also for clarification, provided other RCS services (e.g., Standalone Messaging, Chat, File Transfer) are available (e.g. the conditions of coverage and space are met and the device UI supports these services simultaneously with the call), the relevant service capability tags should be included with the Image and Video Share tags.

Note that while capability exchange is reciprocal, User A and User B's capabilities may be different and services shall be made available accordingly (e.g. User A may support video encode and User B may support decode, but both need to be under 3G or better data coverage for the service to operate).

In addition to the information presented above, it should also be taken into account that some terminals do not support 2G DTM (Dual-Transfer Mode). When such devices are within a 2G data coverage (meaning that no services are available during the call), the PS connection will automatically drop once they engage in a CS call.

Note: Information on codec support for Video Share is covered in section 3.6.

2.8 RCS protocols

The following table summarises the list of protocols employed by RCS clients. It must be noted that the choice among the options presented will not impact Service Provider interoperability:

Protocol name	Description	Transport layer	Secure transport layer/protocol
Session initiation protocol (SIP)	Client-IMS core signalling protocol	User Datagram Protocol (UDP) over IP or Transmission Control Protocol (TCP) over IP	SIP over Transport Layer Security (TLS) or IP Security (IPsec)
Message Session Relay Protocol (MSRP)	chat messages, media (pictures) and file exchange protocol	TCP/IP	MSRP over TLS
Real-time protocol (RTP)	Real Time Media (voice and video) exchange	UDP/IP	Secure RTP (SRTP) (see [RFC3711])
Internet Mail Access Protocol (IMAP)	Access to Network-based common Message Store	TCP/IP	IMAP over TLS
Hyper Text Transfer Protocol (HTTP)	XML configuration access protocol (XCAP) transactions HTTP configuration mechanism	TCP/IP	HTTPS
Secure User Plane Location (SUPL)	Geolocation positioning	N/A	N/A

Table 28: RCS protocols

According to [RFC3261] RCS clients shall support both SIP/UDP (User Datagram Protocol) and SIP/TCP (Transmission Control Protocol). The choice of whether both are used or only TCP is used to transport the signalling data belongs to each Service Provider and is controlled by the configuration parameter "*psSignalling*" and "*wifiSignalling*" in Annex A section A.2.10.

Regarding the impact of Network Address Translation (NAT) traversal in the different protocols involved in RCS, the following considerations shall be taken into account:

- Regarding the SIP protocol:
  - Carriage Return Line Feed (CRLF) keep-alive [RFC6223] support is MANDATORY when only SIP/TCP or SIP/TLS is used by the RCS client and SIP/UDP is not used. Section C.1 describes how both client and server could initiate the sending of the keep alives.

  - Simple Traversal of UDP through NATs (STUN) keep-alive [RFC6223] support is RECOMMENDED when SIP/UDP is used by the RCS client as it allows network capacity optimization.
  - An RCS client using SIP/UDP:
    - shall support symmetric signalling (That is the IP and port combination used to send SIP messages is the same as the one used to receive SIP messages).
    - shall perform TCP switchover for large SIP messages.
- For handling Message Session Relay Protocol (MSRP) sessions, the RCS MSRP endpoints shall support:
  - [RFC6135]: “The Alternative Connection Model for the Message Session Relay Protocol (MSRP)”
  - The mechanisms described in section 2.8.2 regarding session matching for MSRP.
- Regarding NAT traversal of Real-Time Transport Protocol (RTP) sessions, the RCS client should implement the mechanism described in section 2.8.1.
- For Internet Mail Access Protocol (IMAP), HTTP and Secure User Plane Location (SUPL) no specific mechanisms are mandated in the current specification to support NAT traversal

The support of Transport Layer Security (TLS) based or IP Security (IPsec) based protocols to secure the signalling and TLS based for MSRP and IMAP protocols or Secure Real-Time Transport Protocol (SRTP) for RTP protocols to secure media exchanges is RECOMMENDED particularly for those scenarios where the data is carried over a network outside the Service Provider domain (i.e. Wi-Fi access). For more information on access security, see section 2.13.

Finally, please note that to ensure interoperability of devices across different Service Provider networks (that is when porting devices across networks or using open market devices/clients), the list of preferred options for the transport and security for the signalling (SIP) and media (RTP and MSRP) protocols is included in the configuration parameters (see Annex A, section A.2.10). Consequently, a Service Provider will provide this information as part of the configuration (first-time or re-configuration scenarios as described in section 2.3).

2.8.1 RTP and NAT traversal

As mentioned previously, an RCS client must implement several mechanisms to avoid the negative impact of NAT traversal, which can both occur when connecting over:

- PS: Mainly due to the scarcity of IPv4 public addresses and proxying performed at APN level, or,
- Wi-Fi: In this case due to the fact the network topology between the access point and the Internet may vary between deployments.

To combat the negative effects of NAT traversal on the RTP protocol, the RCS client should implement the following mechanisms:

- shall support a keep-alive mechanism to open and maintain the NAT binding alive regardless of whether the media stream is currently inactive, send-only, receive-only or send-receive. The recommended standard keep-alive mechanism is an empty (no payload) RTP packet with a payload type of 20 (as per [3GPP TS 24.229]).
- shall use symmetric media (that is use the same port number for sending and receiving packets) as defined in [RFC4961] mechanism which is summarized below:

- When an invitation for Video Share is received and accepted, the 200 OK response contains a SDP body containing all the necessary fields (including the destination port) for the sender to send the RTP packets.
- Immediately after sending the 200 OK response, the receiver will send a keep-alive packet back to the sender to secure the media path:
- The source port shall be identical to the one included in the m field of the SDP payload inside the 200 OK response.
- The destination port shall be identical to the one included in the m field of the SDP payload inside the SIP INVITE message.
    - The sender should allow enough time for the media path to be secured.

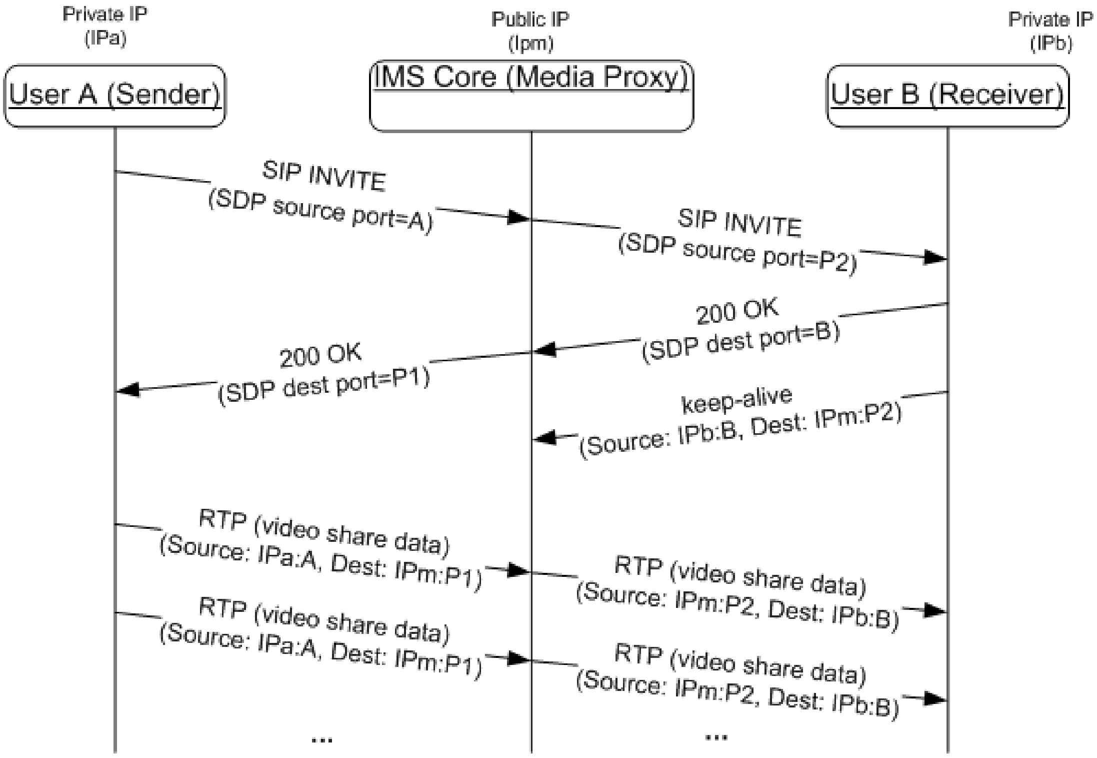


Figure 23: RTP symmetric media path establishment

Note: as a general recommendation, User A should also send a keep-alive once it receives the SDP from the other side.

- shall use the Real-Time Transport Control Protocol (RTCP)

The symmetric media procedure described for the RTP protocol is, in general, applicable to any UDP stream. As the usage of RTCP is also mandatory, an analogous mechanism shall be implemented to prevent any RTCP streams from being blocked. Therefore, the symmetric media procedure described in this section for RTP is also applicable to RTCP and shall be employed (that is a dummy packet is sent by the receiver to secure the RTP flow and a second one is used to secure the RTCP flow). Also the sender device/client shall send a dummy packet when the session is established to secure the RTCP flow on their side and ensure the reception of any RTCP RR (Receiver Report) sent by the receiving side. The dummy packet format recommended for establishing the RTCP flow is an empty RTCP RR or empty RTCP SR (Sender Report).
Note: For a VoLTE/VoHSPA enabled device, RTCP usage for a voice session shall be as defined in section 3.2.4 of [PRD-IR.92]

Please note that for readability purposes, the procedures described in this section have not been included in the diagrams in section 3.6 covering the Video Share functionality.

2.8.2 MSRP session matching

Note: The text in this section is based on the text contained in the now expired IETF internet draft draft-ietf-simple-msrp-sessmatch-10:

This section defines how an MSRP entity (e.g. an RCS Client, Messaging Server or other node handling MSRP within the network) matches an incoming MSRP message to an MSRP session. The difference between the session matching mechanism in [RFC4975] and the one defined here is that while the mechanism in [RFC4975] uses the MSRP URI comparison rules for session matching, for RCS, only the session-id part of the MSRP URI is used.

When an MSRP entity receives the first MSRP request for an MSRP session, the To-Path header field of the request should contain a URI with a session-id part that was provided in the SDP associated with the MSRP session. The entity that accepted the connection looks up the session-id part of the MSRP URI in the received requests, in order to determine which session it matches. The session-id part is compared as case sensitive. If a match exists, the entity shall assume that the host that formed the connection is the host to which this URI was given. If no match exists, the entity shall reject the request with a 481 error response. The entity shall also check to make sure the session is not already in use on another connection. If the session is already in use, it shall reject the request with a 506 error response.

2.9 RCS and Access Technologies

2.9.1 RCS and Cellular Access

A device enabled for VoLTE/VoHSPA (see section 2.2) shall implement the domain selection function as described in [PRD-IR.92] and [PRD-IR.58]. The domain selection function selects whether the CS or IMS domain is used for the voice service.

The home Service Provider can use the configuration mechanisms defined in section 2.3.3 to configure the IMS Management Object defined in [3GPP TS 24.167] (see section A.1.6) to set the parameter “Voice_Domain_Preference_E_UTRAN” to value 1 “CS Voice only”, to configure the device as RCS-CS device. Device configured as "CS voice only" shall behave as RCS only capable device with regard to registration in the IMS, Only a Service Provider who supports both VoLTE and RCS needs to provide this setting. The device will determine the domain used for voice as specified in [3GPP TS 23.221].

Note that when "CS Voice only" is used, then LTE radio capability of the device will be disabled for a voice centric UE if CS Fallback (SGs interface) is not supported in the LTE network.

If the device only supports CS voice, [PRD-IR.92] or [PRD-IR.58] do not apply.

The aim of the present section is to give an overview of the possibilities to complement and integrate LTE, High Speed Packet Access (HSPA) and RCS.

2.9.1.1 Access used by RCS in relation to VoLTE/VoHSPA

For devices enabled for VoLTE/VoHSPA (see section 2.2), LTE/HSPA is used for RCS features. VoLTE is assumed to be natively implemented and integrated within the device. The IMS registration shall be shared between VoLTE/VoHSPA and RCS if the device is under VoLTE enabled LTE coverage or VoHSPA enabled HSPA coverage.

For devices where VoLTE is not enabled, LTE access is used for RCS features provided that the device is camping in those networks and capable of using those PS radio access technologies..

LTE devices not enabled for VoLTE will fall back to CS for voice calls. Once CS fallback occurs, LTE access is dropped, and RCS functionality is provided via 3G/2G access.

HSPA devices not enabled for VoHSPA will use CS for voice calls (unless it is a PS only deployment), and RCS will continue to use HSPA.

For devices enabled for VoLTE/VoHSPA but not on a network supporting VoLTE/VoHSPA, LTE or HSPA access is used for RCS features provided that the device is camping in those networks.. These devices always use the IMS APN for accessing the RCS services.

Devices enabled for VoLTE/VoHSPA but not on a network supporting VoLTE/VoHSPA, will fall back to CS for voice calls. Once CS fallback occurs, LTE access is dropped and RCS functionality is provided via 3G/2G access. HSPA can continue to be used.

2.9.1.2 LTE and HSPA Radio Capabilities

Radio bearers, UE Discontinuous Reception (DRX) and Discontinuous Transmission (DTX) modes of operation, Radio Link Control (RLC) configurations, and Guaranteed Bitrate (GBR) and Non-Guaranteed Bitrate (NBGR) services, GBR Monitoring Function and Conversational Traffic Class Handling are all as specified in [PRD-IR.92] and [PRD-IR.58] for the RCS-LTE and RCS-HSPA devices respectively. None of this is applicable to the RCS-AA device.

2.9.1.3 Bearer aspects

For all IMS traffic the following applies for an RCS device enabled for VoLTE/VoHSPA:

- APN usage shall be according to [PRD-IR.92] or [PRD-IR.58] section 4.3.1 including the one used for XCAP (Note: according to [PRD-IR.92] the APN used for XCAP could be a different APN to the IMS APN)
- For LTE and HSPA bearer management see section 4.3 of [PRD-IR.92] and [PRD-IR.58] respectively.

For all RCS IMS traffic the following applies:

- For an RCS device enabled for VoLTE: LTE QCI (QoS class identifier) 8 and 9 shall be supported so that either may be used for MSRP traffic.
- For an RCS device enabled for VoHSPA following bearers shall be supported so that either may be used for MSRP traffic:
  - Universal Mobile Telecommunications System (UMTS) bearer with interactive traffic class, Traffic Handling Priority (THP) 3 and no Signalling, and
  - UMTS bearer with background traffic class

For an RCS-AA device the following applies for all RCS IMS traffic:

- When connecting through cellular access the RCS-AA shall use an APN obtained through client configuration
  Note: the Service Provider should ensure that the configured APN can handle XCAP traffic;
- For other ways of connecting by RCS-AA (e.g. Wi-Fi, fixed broadband and so on): no requirements.

2.9.1.4 APN and roaming considerations

General technical guidelines on how roaming is handled for the RCS services shall follow [PRD-IR.65].

Guidance given for RCS and access technologies as documented in Chapter 2.9 are applicable also in the roaming scenarios. Specific roaming considerations for the different RCS device types (as specified in section 2.2):

- RCS-LTE device shall follow the general rules as per [PRD-IR.88], APN usage as per [PRD-IR.92]
- RCS-HSPA device shall follow the general rules as per [PRD-IR.33], APN usage as per [PRD-IR.58]
- RCS-AA device: no specific requirements

The APN to be used to access the RCS services[17] depends on the capacity of the device to support an IMS APN as per [PRD-IR.88]:

- When the device and the network support the use of the IMS APN (e.g. RCS-LTE devices in a VoLTE enabled network), the IMS APN shall also be used to access the RCS services;
- For other cases, either the Internet APN or an APN to be used only for RCS shall be used when accessing via PS (i.e. not accessing via WiFi)
  - For these devices and within the scope of the RCS services, a new APN is defined: the RCS only APN;
  - Analogously to the IMS APN defined in [PRD-IR.88] the RCS only APN only provides access to the IMS services, and in this particular case, only to RCS services;
  - The RCS only APN is configured via the RCS-E ONLY APN parameter presented in section A.1.11 in Table 59;
  - If the RCS-E ONLY APN parameter has no value, then only the Internet APN[18] shall be allowed in the home network and a roaming network.

An RCS Switch at UI level may be shown upon a Service Provider decision. The purpose of this local client switch is to protect users from unexpected charges, especially when roaming. Depending on the ENABLE RCS-E SWITCH parameter, the RCS Switch can be enabled/disabled by the user at any time, only when roaming, or never:

- If the configuration parameter ENABLE RCS-E SWITCH is set to 1, (see Table 59), the RCS Switch can be enabled/disabled at any time;
- If set to 0, it is up to Service Provider decision to show it only while roaming[19].

The behaviour of the RCS Switch is different depending on whether the device and network support the IMS APN:

- If the IMS APN is supported, the behaviour is shown in the following table:

RCS Switch	APN to use for RCS services	Result
Disabled	IMS APN	Among the RCS services, the client shall only register in IMS for IP Voice Call, IP Video Call and Standalone Messaging.
Enabled or not available	IMS APN	Standard configuration, the client shall register in IMS for any supported RCS services

Table 29: APN configuration proposal for RCS for a device supporting the IMS APN

[17] This section only covers the APN behaviour for RCS services. These settings shall not be taken into account for the usage of other APNs by non-RCS services.

[18] By Internet APN, we understand the default APN configured by the Service Provider to provide Internet connectivity on the device.

[19] Open market/non-customized devices shall show the RCS Switch when roaming.

- If the IMS APN is not supported, the RCS Switch will determine whether the client shall register or not for RCS services as shown in the following table:

In addition to this and in devices that do not support simultaneous use of the Internet and RCS only APN, two different APNs are considered:

1. The Internet APN, and,
2. The RCS only APN that, similar to the IMS APN defined in [PRD-IR.88], only provides access to the IMS services, and in this particular case, to RCS services.

In such devices the user shall be able to configure to allow or disallow RCS and/or internet traffic in the device settings when roaming according to the following alternatives:

Data traffic switch **(combination of main data switch and roaming data switch)**	**RCS switch**	**APN to use for RCS services**	**Result**
Enabled	Disabled	N/A	RCS client shall not register on the IMS network.
Enabled	Enabled or not available	Internet APN	Standard configuration
Disabled	Enabled	RCS only APN	RCS only configuration This configuration is only available if the RCS-E ONLY APN is configured to a non-empty value
Disabled	Disabled	None	No data configuration

Table 30: APN configuration proposal for data traffic and roaming

2.9.1.4.1 *Data connection notifications*

For a device enabled for VoLTE, the device will take be responsible for initiating a PS connection using the required APN and it should not be necessary to notify the user.

In other cases, taking into account the regulatory frameworks applying to some markets, it could be necessary to notify the user when a PS connection is going to be initiated. From the data connection notification point of view, there are three possible configurations:

Setting	**Terminal behaviour**
never connect	• connection disabled • no pop-up
always ask	• pop-up*: requesting confirmation to go online and informing about possible data charges • user has the following options: reject, confirm to connect once or to switch to ‘always connect’ and connect • when user confirms the connection is enabled *Alternatively, a shortcut to the device data settings, together with a warning that data charges might apply, is presented where the user may enable the connection.
always connect	• connection enabled • no pop-up

Table 31: Data connection notification options

Consistently with the configuration switches presented in the previous section (RCS on/off, data on/off), an RCS device shall be able to apply the data connection notification options (described in Table 31) individually to each of the following connections:

- Internet home: Standard data connection occurring within the Service Provider’s home network.

- Internet roaming: Standard data connection when roaming.
- RCS home: Data connection required for RCS occurring within the Service Provider's home network.
- RCS roaming: Data connection required for RCS when roaming

Regarding the data connection switches presented in section 2.9.1.4, it is to the decision of each Service Provider to define during customization on whether to:

- Define the default settings ("always connect" for the "home" connections and "always ask" for the "roaming" connections)
- Define if the data connection notification settings are shown as part of the device configuration settings (that is the user is able to change the notification behaviour) instead.

2.9.2 Other access networks

2.9.2.1 Overview

In addition to the cellular PS access networks described in sections 2.9.1.4 and 2.9.1, the RCS framework and services can be used over any IP access over which the Service Provider's IMS core and application servers can be reached, provided that it offers sufficient bandwidth and an acceptable latency. Section 2.7 provides a guideline for which services can be used when connected through different types of access networks including broadband access.

These other networks can be both trusted and untrusted networks. In this context "Trusted" means that the access network itself provides the necessary authentication and encryption for end-user traffic. The access network is integrated into the Service Provider core infrastructure in such a way that the whole path from a mobile to services is secure and under the control of respective Service Providers. Fixed access networks including ADSL (Asymmetric Digital Subscriber Line), cable modem access, and FTTH (Fibre To The Home) can therefore be considered as "Trusted" network if they are entirely Service Provider controlled. The same holds for clients using a cellular PS connection as broadband access.

Untrusted broadband networks however are at least partly controlled by some 3rd party and may therefore require more elaborate security measures to guarantee privacy and authenticity of the signalling and media traffic. As in this case the network does not provide the support for functionality such as encryption natively, it needs to be added to it before that particular network can be used to access the IMS core system. Direct access from an untrusted broadband network such as public Wi-Fi hotspots to the IMS core system should not be allowed due to security risks such as Denial of Service attacks towards Service Provider core components. There is a requirement for additional secure access mechanisms to be deployed.

Many such secure access mechanisms are possible and can either be xSIM based or use other types of credentials. For commercial deployments the choice will be dependent on the type of client and on the environment. For example the same type of client could only use PS Mobile Broadband Access, access over the internet or only over a fixed ADSL line / FTTH access which may require using different mechanisms for each case. Therefore given that this choice will end up being specific to each deployment, it is not considered in scope of RCS to specify an exhaustive list of supported access mechanisms.

As described in section 2.8 both trusted and untrusted networks need to be able to provide access and authentication over NAT. This must be taken into account for example when xSIM based access, IPSec or other fixed access authentication mechanisms are used.

This support for access over non-cellular networks can be used in two ways:

1. As an offloading capability for the cellular network
   This will be controlled by the device itself:
   - When a device is enabled for VoLTE/VoHSPA (see section 2.2), it is expected that the device remain on LTE/HSPA access as long as it is available.
   - When the voice service is provided via CS access, it is up to the device when and whether to move to non-cellular (e.g., Wi-Fi) access. If a device moves to a non-cellular network, it is expected that the device first de-registers in IMS from the cellular network, and then registers in IMS in the non-cellular network, or vice versa when moving in the other direction.
2. As a means of access for dedicated broadband clients using the identity of the mobile device
   These can be either as a standalone client when there is no mobile device using that same identity or as secondary client to a mobile device sharing the same identity (see chapter 2.5). In the latter case the user will have multiple devices sharing the same identity. Chapter 2.11 provides further details on how this can be realized. These differences are further detailed in section 2.9.2.2.

2.9.2.2 Dedicated Broadband Access clients

Next to clients using mobile access, RCS also supports dedicated clients using broadband access. Such a client can operate in two significantly different modes:

1. As a secondary client, adding performance (such as larger keyboard, a screen with higher resolution and so on) to the primary mobile client with RCS functionality. Such a secondary client is designed with user experience aspects, storage accessibility and so on, but is not designed to act as a primary telephony device. In this case the primary client retains aspects a user would associate with their device, for example regulatory functions, quality of service and full access to the telephony functions.

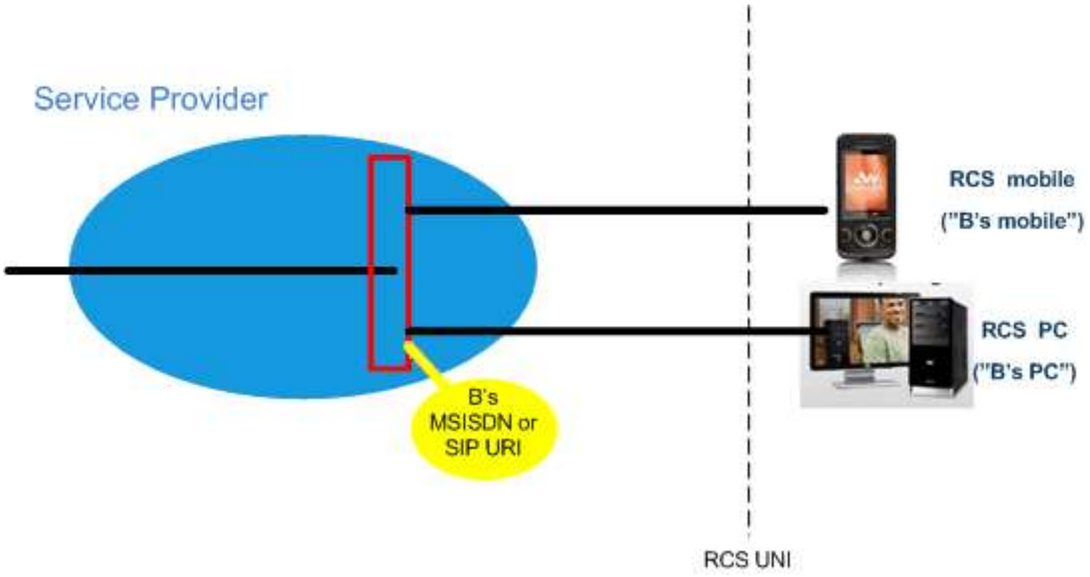


Figure 24: RCS Broadband Access client used as a secondary client

Note: Other combinations of multiple devices, such as support of multiple mobile clients, are out of scope for RCS. However, this does not restrict a Service Provider to deploy proprietary solutions to achieve this.

2. As a primary client, replacing the user's mobile client. A primary client has to meet all regulatory requirements (emergency calling, lawful intercept, etc.), and perform to meet the traditionally expected telephony functionality and demonstrate the reliability, performance and quality of service of a primary device. The precondition for its use is

that basic telephony services are already available in the Broadband Access network. For these services, the local regulations are already fulfilled.

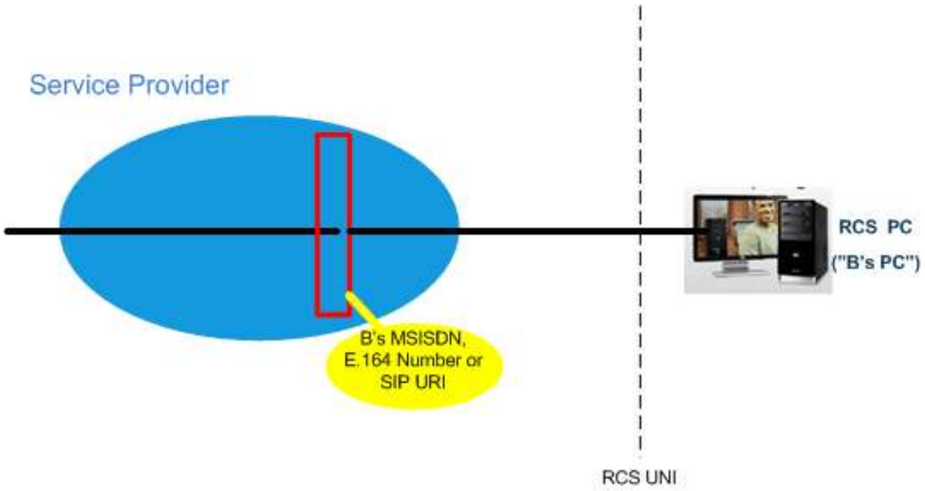


Figure 25: RCS Broadband Access client used as a primary client

2.10 End User Confirmation Requests

The following section provides a framework that will allow the Service Provider to inform the end user about a certain situation by opening a dialog in the device presenting all the available information and asking the user to confirm or decline the proposed request.

The End User Confirmation Request is implemented using a SIP MESSAGE[20] method containing a XML payload type "*application/end-user-confirmation-request+xml*" that will be sent by the Service Provider serving the end user to his RCS device/client. A specific device can be addressed using a GRUU or a sip.instance feature tag (see section 2.11.3). If the user is required to answer from every device, the devices should be addressed individually using a GRUU or a sip.instance feature tag.

Upon the reception of the SIP MESSAGE, the end user terminal will check the *P-Asserted-Identity* of the incoming message and match it against the configured URI for the service (END USER CONF REQ ID) as defined in Table 60 and extract the request information from the XML payload body. A dialog or notification will be displayed to the End User (UX dependent) showing the confirmation request and related information.

The End User Confirmation Response will be encapsulated in an XML body with a payload type "*application/end-user-confirmation-response+xml*" and returned back to the Service Provider in a new SIP MESSAGE

The information contained in the end user confirmation request is the following

- **Id**: Unique identifier of the request.
- **Type**: Determines the behaviour of the receiving device. It can take one of the following two values:

[20] Please take into account that according to [RFC3428], the size of MESSAGE requests outside of a media session MUST NOT exceed 1300 bytes, unless the UAC has positive knowledge that the message will not traverse a congestion-unsafe link at any hop, or that the message size is at least 200 bytes less than the lowest MTU (Maximum Transmission Unit) value found en route to the UAS. Larger payloads may be sent by the Service Provider in the initial confirmation request and/or ack (Acknowledgement) using content-indirection as specified in [RFC4483]. Therefore, this shall be supported by the devices/clients.

   a) *Volatile*, the answer shall be returned inside of a new SIP MESSAGE request. The request may time out without end user input, in which case it will be discarded.
   b) *Persistent*, the answer shall be returned inside of a new SIP MESSAGE request. The confirmation request does not time out.

- **Pin**: Determines whether a pin is requested to the end user. It can take one of the following two values: *true* or *false*. If the attribute is not present it shall be considered as *false*. This pin request can be used to add a higher degree of confirmation and can be used to allow certain operations like parental control for example.
- **Subject**: text to be displayed as notification or dialog title.
- **Text**: text to be displayed as body of the dialog.
- **Timeout**: Time period in seconds during which a volatile request is valid. After the timeout expires, the device shall discard any UX notifications silently.

For volatile type requests an optional timeout attribute may be present in the XML representing the validity period in seconds. If this attribute is not present a default value of 64*T1 seconds (with T1 as defined in [RFC3261]) shall be used.

The End User Confirmation Request initiates a dialogue to the user on the device. For specific use cases it may be necessary that the user accepts external End User Confirmation Requests which cannot be authenticated appropriately. This acceptance can either be done by configuration or by entering a specific mode on the device UI and avoids unwanted UI dialogues on the devices caused by malicious usage by other person. One use case described in sections 2.3.3.2.6.2 and 2.3.3.2.6.3 is the configuration of additional RCS clients via Internet. To identify such messages following attribute is provided:

- externalEUCR: Determines that this is an End User Confirmation Request initiated by an external unsecure source, e.g. via the Internet. If the optional attribute externalEUCR is set to true in the End User Confirmation Request and the device does not allow such external End User Confirmation Request, the End User Confirmation Request shall be ignored. An End User Confirmation Request response shall not be sent back in that case. The device shall show all End User Confirmation Request requests where the attribute externalEUCR is set to false or does not exist.
  If the device or client has not implemented the processing of the attribute externalEUCR, it shall be ignored and therefore all End User Confirmation Requests are allowed and shown in the UI.

In addition, to allow Service Providers more flexibility the two following optional button labels will be defined. For backward compatibility: if the optional button labels are not used, default values will be used instead.

- **ButtonAccept**: text to display on the button.
- **ButtonReject**: text to display on the button.

To ensure compatibility with future versions, the RCS client/device shall silently discard any unknown node or attribute in the XML structure.

Several Subject or Text nodes can be present in the XML body to be able to support multiple languages. If more than one element is presented a language (*lang*) attribute must be present with the two letter language codes according to the ISO 639-1. RCS clients shall verify the language attribute and display the text data of the element that matches the current language used by the user. If there is no language matching the users, the first node of Subject and Text shall be used.

If the type of confirmation request is persistent the Service Provider can send an optional acknowledgement message of the transaction back to the user with a welcome message, an error message or further instructions. This acknowledgement message will be encapsulated in an XML body with a payload type "*application/end-user-confirmation-*

ack+xml" and returned in a separate SIP MESSAGE. If the acknowledgement refers to the message which is currently displayed, it shall be discarded even if no answer was sent. This allows sending a message to all active devices of a user also in case a response from a single device is sufficient. For that reason it is also possible to send acknowledgements without Subject or textual content.

The following table specifies the XML Schema Definition (XSD) of the XML payload for the End User Confirmation Request:

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
           xmlns:xml=”http://www.w3.org/XML/1998/namespace”
           elementFormDefault="qualified">
      <xs:import namespace=”http://www.w3.org/XML/1998/namespace”
                schemaLocation="http://www.w3.org/2009/01/xml.xsd"/>
      <xs:element name="EndUserConfirmationRequest">
            <xs:complexType>
                 <xs:sequence>
                      <xs:element ref="Subject" maxOccurs="unbounded"/>
                      <xs:element ref="Text" maxOccurs="unbounded"/>
                      <xs:element ref="ButtonAccept" minOccurs="0" maxOccurs="unbounded"/>
                      <xs:element ref="ButtonReject" minOccurs="0" maxOccurs="unbounded"/>
                 </xs:sequence>
                 <xs:attribute name="id" type="xs:string" use="required"/>
                 <xs:attribute name="type" type="xs:string" use="required"/>
                 <xs:attribute name="pin" type="xs:boolean" use="optional"/>
                 <xs:attribute name="timeout" type="xs:integer" use="optional"/>
                 <xs:attribute name="externalEUCR" type="xs: boolean" use="optional"/>
            </xs:complexType>
      </xs:element>
      <xs:element name="Subject">
            <xs:complexType>
                 <xs:simpleContent>
                        <xs:extension base=”xs:string”>
                                <xs:attribute ref="xml:lang"/>
                        </xs:extension>
                 </xs:simpleContent>
            </xs:complexType>
      </xs:element>
      <xs:element name="Text">
            <xs:complexType>
                 <xs:simpleContent>
                        <xs:extension base=”xs:string”>
                                <xs:attribute ref="xml:lang"/>
                        </xs:extension>
                 </xs:simpleContent>
            </xs:complexType>
      </xs:element>
      <xs:element name="ButtonAccept">
            <xs:complexType>
                 <xs:simpleContent>
                        <xs:extension base=”xs:string”>
                                <xs:attribute ref="xml:lang"/>
                        </xs:extension>
                 </xs:simpleContent>
            </xs:complexType>
      </xs:element>
      <xs:element name="ButtonReject">
            <xs:complexType>
                 <xs:simpleContent>
                        <xs:extension base=”xs:string”>
                                <xs:attribute ref="xml:lang"/>
                        </xs:extension>
                 </xs:simpleContent>
            </xs:complexType>
      </xs:element>
</xs:schema>
```

Table 32 : End User Confirmation Request XSD

The information contained in the End User Confirmation Response is the following:

- **Id**: Unique identifier of the request.
- **Value**: with the end user confirmation. It can take one of the following two values accept or decline.

- **Pin**: if the request has the “*pin*” attribute set to true, the response will contain the pin value introduced by the user.

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
                xmlns:xml=”http://www.w3.org/XML/1998/namespace”
                elementFormDefault="qualified">
        <xs:import namespace=”http://www.w3.org/XML/1998/namespace”
                        schemaLocation="http://www.w3.org/2009/01/xml.xsd"/>
        <xs:element name="EndUserConfirmationResponse">
                <xs:complexType>
                        <xs:attribute name="id" type="xs:string" use="required"/>
                        <xs:attribute name="value" type="xs:string" use="required"/>
                        <xs:attribute name="pin" type="xs:string" use="optional"/>
                </xs:complexType>
        </xs:element>
</xs:schema>
```

Table 33: End User Confirmation Response XSD

The information contained in the End User Acknowledge Response is the following

- **Id**: Unique identifier of the original request. If the ID matches the ID of the currently shown message, this message shall be discarded even if no answer was sent from the receiving device.
- **Status**: of the End User Confirmation. It can take one of the following two values: *ok* or *error*.
- **Subject**: text to be displayed as notification or dialog title
- **Text**: text to be displayed as body of the dialog.

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
           xmlns:xml="http://www.w3.org/XML/1998/namespace"
           elementFormDefault="qualified">
      <xs:import namespace="http://www.w3.org/XML/1998/namespace"
                 schemaLocation="http://www.w3.org/2009/01/xml.xsd"/>
      <xs:element name="EndUserConfirmationAck">
            <xs:complexType>
                  <xs:sequence>
                        <xs:element ref="Subject" maxOccurs="unbounded"/>
                        <xs:element ref="Text" maxOccurs="unbounded"/>
                  </xs:sequence>
                  <xs:attribute name="id" type="xs:string" use="required"/>
                  <xs:attribute name="status" type="xs:string" use="required"/>
            </xs:complexType>
      </xs:element>
      <xs:element name="Subject">
            <xs:complexType>
                  <xs:simpleContent>
                        <xs:extension base="xs:string">
                              <xs:attribute ref="xml:lang"/>
                        </xs:extension>
                  </xs:simpleContent>
            </xs:complexType>
      </xs:element>
      <xs:element name="Text">
            <xs:complexType>
                  <xs:simpleContent>
                        <xs:extension base="xs:string">
                              <xs:attribute ref="xml:lang"/>
                        </xs:extension>
                  </xs:simpleContent>
            </xs:complexType>
      </xs:element>
</xs:schema>
```

Table 34: End User Confirmation Acknowledgement XSD

To provide more flexibility a Service Provider shall be able to send only notification messages to the end user. This notification message shall be implemented similar to confirmation dialog using a SIP MESSAGE method containing an XML payload type "*application/end-user-notification-request+xml*". A notification will be displayed to the end user (UX dependent) showing the related information.

The information contained in the end user notification is the following:

- **Id**: Unique identifier of the request.
- **Subject**: text to be displayed as notification or dialog title
- **Text**: text to be displayed as body of the dialog.
- **ButtonOK**: text to display on the button.

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
            xmlns:xml=”http://www.w3.org/XML/1998/namespace”
            elementFormDefault="qualified">
      <xs:import namespace=”http://www.w3.org/XML/1998/namespace”
                 schemaLocation="http://www.w3.org/2009/01/xml.xsd"/>
      <xs:element name="EndUserNotification">
            <xs:complexType>
                 <xs:sequence>
                         <xs:element ref="Subject" maxOccurs="unbounded"/>
                         <xs:element ref="Text" maxOccurs="unbounded"/>
                         <xs:element ref="ButtonOK" minOccurs="0" maxOccurs="unbounded"/>
                 </xs:sequence>
                 <xs:attribute name="id" type="xs:string" use="required"/>
            </xs:complexType>
      </xs:element>
      <xs:element name="Subject">
            <xs:complexType>
                 <xs:simpleContent>
                         <xs:extension base=”xs:string”>
                                 <xs:attribute ref="xml:lang"/>
                         </xs:extension>
                 </xs:simpleContent>
            </xs:complexType>
      </xs:element>
      <xs:element name="Text">
            <xs:complexType>
                 <xs:simpleContent>
                         <xs:extension base=”xs:string”>
                                 <xs:attribute ref="xml:lang"/>
                         </xs:extension>
                 </xs:simpleContent>
            </xs:complexType>
      </xs:element>
      <xs:element name="ButtonOK">
            <xs:complexType>
                 <xs:simpleContent>
                         <xs:extension base=”xs:string”>
                                 <xs:attribute ref="xml:lang"/>
                         </xs:extension>
                 </xs:simpleContent>
            </xs:complexType>
      </xs:element>
</xs:schema>
```

Table 35: End User Notification XSD

2.10.1 Example Use Case 1: Accepting terms and conditions

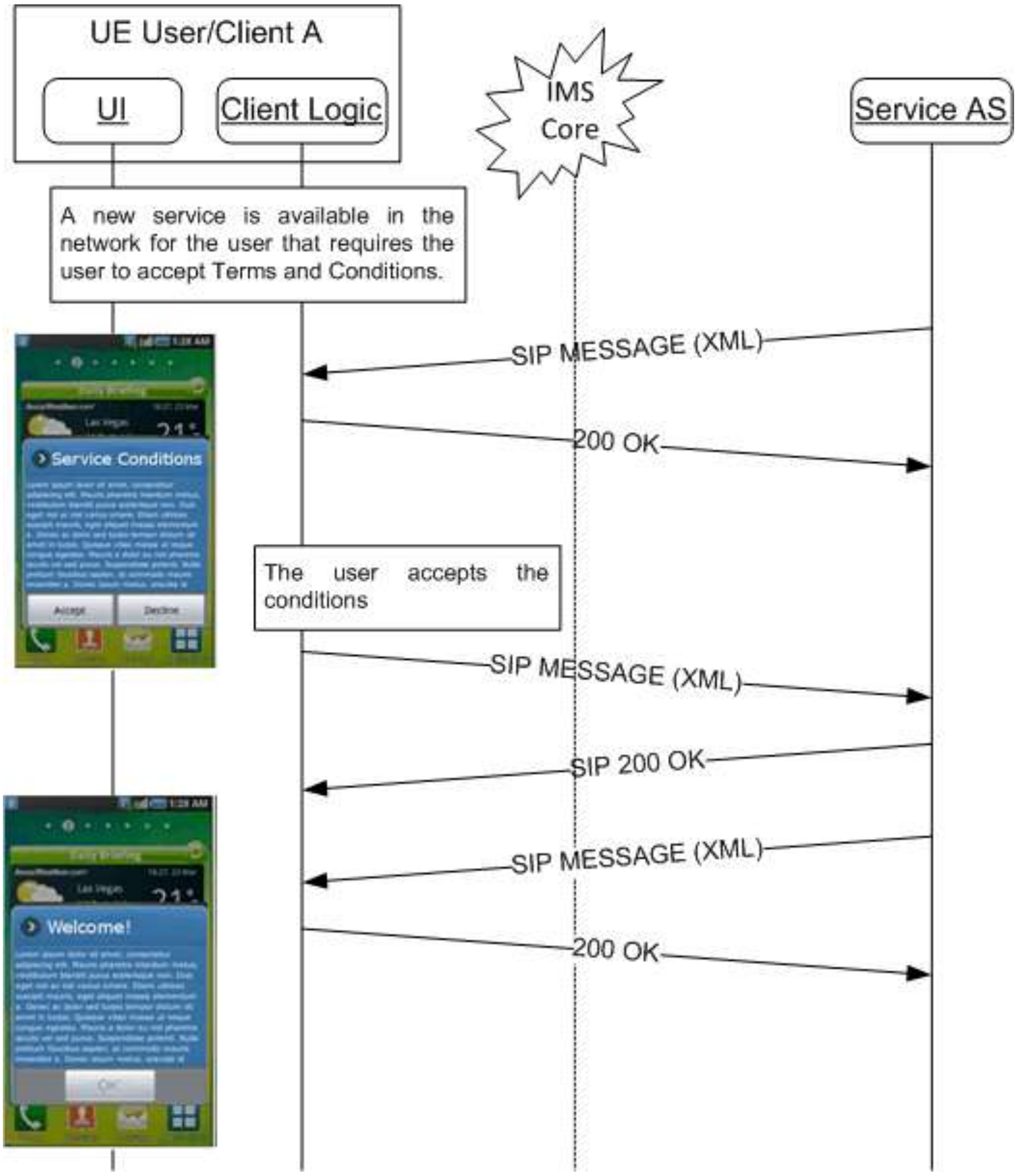


Figure 26 : Terms and Condition Use Case example

2.10.2 Example Use Case 2: Notification

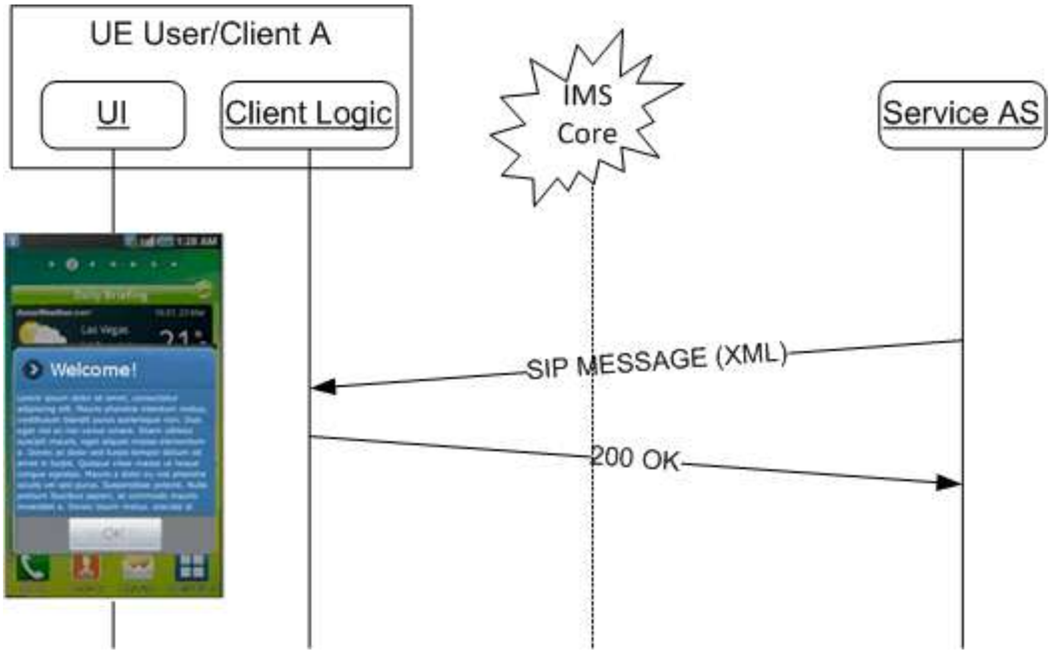


Figure 27: User Notification example

2.11 Multidevice support

2.11.1 Overview

As shown in section 2.9.1.4, the use of a broadband access client leads to the possibility of the user having multiple devices that share the same (public) identity, a MSISDN for instance. Depending on the services that are deployed, this multidevice environment allows a user to:

- Answer a call or respond to a message from a device/client that suits their purpose
- Have a single buddy list shared between the devices/clients
- Authorize invitations to share Social Presence Information from every device/client
- Have a single Social Presence Information that can be seen and maintained from every device/client that is used

The general communication behaviour in this environment is that when the recipient has multiple devices/clients in use and a call or a message is received every recipient’s device will alert. The recipient may then respond to the call or to the message from any of their devices; whichever device is the best for the current situation. In addition when the recipient accepts or rejects a call from any of the devices, all the other devices will stop alerting.

To achieve this, an RCS client shall send a SIP 603 DECLINE response to the invite request when an RCS User explicitly declines a session invitation for a SIP session based service like for example an IP Voice Call, File Transfer, Video and Image Share.

As a fallback for legacy services where this general communication behaviour cannot be realised a call or message might be directed to a certain device.

2.11.2 Control of Service delivery

This feature is applicable to secondary clients only and does not affect the primary device that will always receive all supported communications that it’s capable of given the circumstances.

This feature gives the user an option to control the flow of communication. In some cases a user may not be willing to answer calls from a secondary device (for example a PC). The difference between muting and control of service delivery is that the control of service delivery:

- Disables the service: the user no longer receives calls, messages or requests for the service
- When the service is disabled the user cannot use the service to make calls, send messages or requests

To provide a good user experience, the device/client must clearly show that the service/services are disabled in the device/client user interface.

As a default setting the secondary device will receive all the communication that it can support. Whether the settings are maintained after a restart of the client when the user had changed them, is out of scope of this document is the choice of the device/client vendor.

When an end-user decides that they do not want to use a certain service on a secondary client, that client shall reject any incoming requests related to that service, with SIP 486 BUSY HERE without alerting the end-user. Furthermore, the client would not offer the possibility to use that particular service.

The control of service delivery can be offered for following services:

- Voice Calls
- Video Calls
- Chat
- Text Messaging
- Multimedia Messaging
- File Transfer
- Video Sharing
- Image Sharing
- Geolocation PUSH

The actual set of services on which this control of service delivery will be offered to the end user may be a subset of the above list. Which service is/is not part of that subset shall be determined by the client capabilities and a Service Provider controllable parameter (See Annex A).

2.11.3 Addressing of individual clients

If a client obtains GRUUs from the registrar as described in section 2.4, the public GRUU shall be used as device identifier. The client shall use the public GRUU as a URI parameter for the client in non-REGISTER requests and responses that it sends, for example, an INVITE request and 200 OK response where the GRUU will be included in the Contact Header.

If a client does not obtain a GRUU from the registrar, the sip.instance feature tag and value shall be used as the device identifier. The client shall include the sip.instance feature tag in the Contact header with the same instance-id value in any non-REGISTER request and responses that it sends.

Note: a scenario when the network does not support GRUU and the device has been configured with a DEVICE-ID value set to zero or the value is omitted (to comply with IR.92), causes a privacy issue since the device will send a plain IMEI in all SIP requests/responses thus revealing the IMEI to remote end.

For delivery and display notifications for chat messages which are expected to be directed to the original sender of a message, the client builds the SIP request to send the notification using the received device identifier.

If an *IMDN-Record-Route* header was received in the corresponding chat message, the recipient client shall include in the Request-URI the topmost entry from the *IMDN-Route* header.

Otherwise if no *IMDN-Record-Route* header (see [RFC5438]) was received in the CPIM wrapper (see [RFC3862]) of the message, then if the original SIP request associated with the message included the GRUU parameter in its Contact header, the recipient client adds the GRUU as the Request-URI when it builds the SIP request to send the notification. In both cases if a GRUU was received, the recipient client shall set the CPIM *To* header in the notification to the public GRUU of the received SIP INVITE request.

If the original SIP request associated with the message had no GRUU parameter, but did have a *sip.instance* feature tag in the *Contact* header, the recipient client sends the notification with a separate *Accept-Contact* header to carry the *sip.instance* feature tag and its value. The client shall include the *explicit* and *require* tags on that header.

If the original SIP INVITE request delivering the chat messages contained a *Conversation-ID* header (as described in [RCS5-CPM-CONVFUNC-ENDORS]), the recipient client should include the *Conversation-ID* with the same value and should include a *Contribution-ID* header (as described in [RCS5-CPM-CONVFUNC-ENDORS]) with a newly generated value.

For standalone messages, similar procedures are followed as explained in sections 7.2.4.1 and 7.2.4.2 of [RCS5-CPM-CONVFUNC-ENDORS].

For file-transfer service, in case of file resume, the file recipient needs to address the device that sends the file initially. If the file transfer is resumed from the file sending side, the file sending client needs to address the device of the file recipient that has accepted the original file transfer. If present in the initial SIP INVITE, the device identifier (sip.instance) or GRUU shall be used accordingly (for details, see section 3.5.4).

For simplicity and given that the long-term approach using GRUU as defined in [RFC5627] is preferred, the diagrams contained in Annex B show the network supporting *pub-gruu*. The diagrams for a network supporting the *sip.instance* tag only, would be equivalent except for changing the mechanism to carry the device identifier (*sip.instance* instead *pub-gruu*).

2.12 Interconnect principles and guidelines

The Service Provider’s IMS NNI shall follow the provisions in [PRD-IR.65] sections 3, 4, 5 and 6.

The Service Provider’s RCS NNI shall follow the provisions in [PRD-IR.90]. The implementation could be any of the three connectivity options for RCS NNI defined in [PRD-IR.90].

The Service Provider’s RCS interconnection shall follow the provisions in [PRD-AA.60] including the service specific annexes.

2.13 Security and privacy

2.13.1 Access Security for the User-to-Network Interface (UNI)

2.13.1.1 Access Signalling Security Methods

Several SIP signalling access security and authentication methods are specified in [3GPP TS 33.203] and [3GPP TS 24.229] for access to the IMS core and IMS based services such as RCS. The applicability and choice of method is highly dependent on the RCS client and access type (e.g. trusted or untrusted) including what is supported or required by the IMS core.

2.13.1.1.1 *GPRS IMS Bundled Authentication (GIBA)*

GIBA is an “early” IMS access authentication method for access over a GSM/GPRS or UMTS network whereby the underlying PS domain is providing the access security and authentication on behalf of the IMS core. In this scenario, the Gateway GPRS Support Node (GGSN) allocates a PDP (Packet Data Protocol) context for the mobile device and in doing so the assigned IP address, along with the IMSI and MSISDN is sent to a RADIUS server/Home Subscriber Server (HSS) for the PS domain. Authentication to the IMS core is done by ensuring that the IP address (policed by both the GGSN and P-CSCF) and the IMS identities received in SIP signalling correspond to those allocated for the mobile’s PDP context in the PS domain.

GIBA is generally applicable for GPRS or UMTS access from mobile devices which do not support AKA based xSIM credentials or for devices or IMS core networks which do not support “*ipsec-3gpp*” established using the SIP Security Agreement (*sec-agree*) and IMS AKA as specified in [3GPP TS 33.203].

2.13.1.1.2 *IMS AKA with IPsec*

IMS AKA with IPsec is the preferred long term approach in IMS for access signalling security from a cellular PS network. Such access requires the IMS client device to possess an AKA based credential (e.g. Universal SIM (USIM)/IP Multimedia Services SIM (ISIM)) and support the “*ipsec-3gpp*” procedures specified in [3GPP TS 33.203] and [3GPP TS 24.229].

IMS AKA with IPsec is the access signalling approach specified for Voice over LTE (VoLTE) ([PRD-IR.92]).

2.13.1.1.3 *SIP Digest Authentication and TLS*

SIP Digest is a username and password challenge based authentication (based on HTTP Digest) which is suited for broadband access to IMS or for RCS clients which do not possess AKA based credentials (e.g. xSIM) or do not support IMS AKA based IPsec. SIP Digest is widely implemented in Internet Engineering Task Force (IETF) based SIP clients and is often deployed with TLS. Support for SIP Digest with and without TLS is specified in [3GPP TS 33.203] and [3GPP TS 24.229] for access to IMS from “non-3gpp” defined access networks (e.g. broadband/fixed access networks).

When an RCS client is enabled for SIP Digest authentication, the client will use the pre-configured SIP username and password as specified in Table 55 to authenticate to the IMS core. For the initial SIP REGISTER message (before a digest challenge) the RCS client shall include an authorization header (as per [3GPP TS 24.229]) which includes the SIP digest username and an empty digest authentication response parameter. This allows the IMS core to treat the SIP digest username as an IMS private user identity (IMPI) which is distinct from the IMS public user identity (IMPU), allowing the same SIP public user identity (or IMPU) to be registered from multiple RCS clients/devices.

The IMS registration flow for SIP digest authentication is shown in Figure 28. In this example flow, the RCS client is connected to the IMS core over a Wi-Fi internet broadband connection.

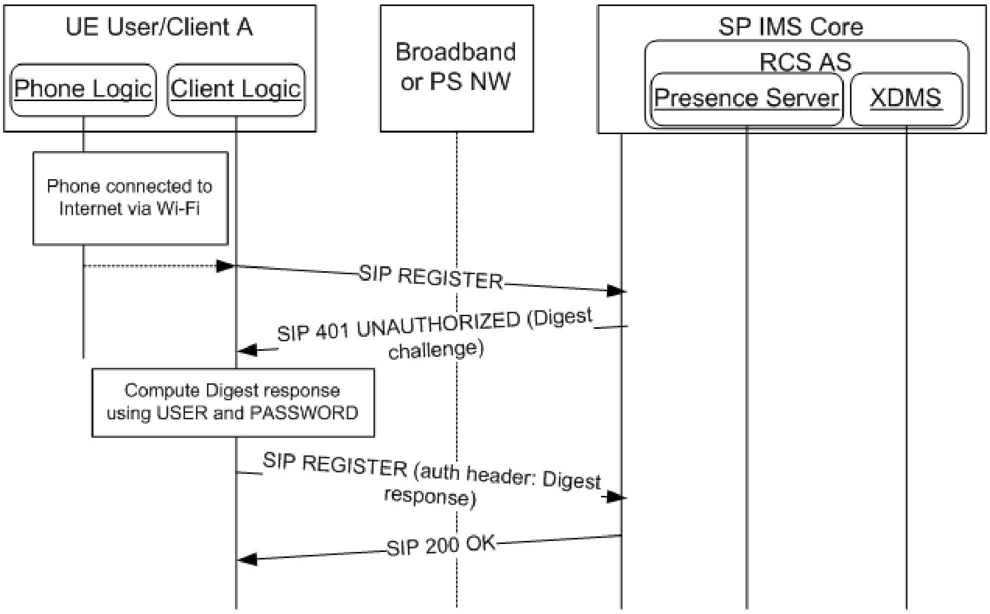

UE User/Client A
Phone Logic
Client Logic
Broadband or PS NW
SP IMS Core
RCS AS
Presence Server
XDMS
Phone connected to Internet via Wi-Fi
SIP REGISTER
SIP 401 UNAUTHORIZED (Digest challenge)
Compute Digest response using USER and PASSWORD
SIP REGISTER (auth header: Digest response)
SIP 200 OK

Figure 28: Registration with SIP Digest Authentication

The use of SIP Digest with TLS is recommended for access from untrusted access networks (including WLAN with no encryption). TLS provides per message authentication, integrity protection and encryption for SIP signalling. TLS with server side certificates also provides authentication of the IMS core to the RCS client. Note that this requires the client to possess a root or intermediate certificate of a Certificate Authority (CA) that is in the certificate signing chain for the IMS core's (e.g. P-CSCF) TLS certificate.

When an RCS client is enabled to use SIP/TLS it should use the SIP TLS port obtained through P-CSCF discovery procedures (e.g. through DNS SRV records [Service records]) or configuration. However, if RCS client is not able to determine a SIP TLS port through these means, it shall use the default SIP port for TLS as specified in [RFC3261].

The RCS client enabled to use SIP/TLS should first use the SIP security agreement (sec-agree) [RFC3329] as specified in [3GPP TS 24.229] to first negotiate the use of TLS with its SIP Proxy (P-CSCF). Alternatively an RCS client may first try to establish a TLS session with the SIP proxy (P-CSCF) before sending an initial SIP Register message which does not include sec-agree for TLS. However, with this approach the S-CSCF may challenge subsequent non-Register messages with a 407 Proxy Authentication Required unless configured to trust SIP Digest without signalling security indicated or if the P-CSCF is able to provide this indication despite not using sec-agree.

Note in both cases SIP proxy (P-CSCF) authenticates to the RCS client using a TLS server certificate.

When SIP Digest is not used with TLS, the IMS core may require non-REGISTER SIP requests to be authenticated using the same SIP Digest challenge mechanisms used during registration. However, in this case the SIP digest challenge is sent in a 407 (Proxy Authentication Required) response. An RCS client that receives a 407 (Proxy Authentication Required) response shall respond by sending an authenticated SIP request which includes a Proxy Authorization header with the digest response. The RCS client shall cache the digest challenge data (e.g. server nonce) for use in authenticating subsequent SIP requests using a nonce-count value (for replay protection) as per [RFC2617] and including a Proxy Authorization header with an updated digest response. This avoids the need for the IMS core to challenge each SIP request before the authentication data expires. Once the digest authentication data expires a new challenge will be issued.

Note: the IMS core may also support binding the RCS client’s IMS identities authenticated during registration with a source IP address (and port if [RFC5626] “SIP Outbound” is used). In such cases, the IMS core may not require subsequent non-registration based SIP messaging to be authenticated using SIP Digest if the identities and source addresses in the messaging matches the binding obtained during the Digest authenticated registration process.

2.13.1.2 Access Signalling Security Profiles for RCS

As there are several considerations which access signalling security method should be used for access to RCS services, the following table defines authentication and access signalling security mechanisms as per RCS device and access type.

Device	Access	Applicable Security Methods	Applicability and Suitability
Non VoLTE/VoHSPA enabled mobile client (RCS-CS)	Cellular PS Access	GIBA or SIP Digest (with or without TLS) or IMS AKA with IPsec	GIBA (e.g. SSO) applies only to GPRS and UMTS access for mobile devices IMS AKA with IPSec may be used when supported by both device and the network. SIP Digest with or without TLS is used in cases when pre-configured or where GIBA is pre-configured, but not supported by the network
	Non-cellular broadband (WiFi) access	SIP Digest, SIP Digest with TLS or IMS AKA with IPsec	SIP Digest with TLS is recommended over SIP Digest without TLS SIP Digest with or without TLS is used in cases when pre-configured or where GIBA is pre-configured or when the mobile device does not support IMS AKA for WLAN access
VoLTE/VoHSPA enabled mobile client	Cellular PS Access	IMS AKA with IPsec[21] Note that the configuration to any other method is not possible.	AKA credentials stored securely in a UICC such as an xSIM.
	Non-cellular broadband (WiFi) access	SIP Digest, SIP Digest with TLS or IMS AKA with IPsec[21].	SIP Digest with TLS is recommended over SIP Digest without TLS SIP Digest with or without TLS is used in cases when pre-configured or where GIBA is pre-configured or when the mobile device does not support IMS AKA for WLAN access.
Broadband Access Enabled (RCS-AA)		SIP Digest or SIP Digest with TLS	SIP Digest with TLS is recommended over SIP Digest without TLS SIP Digest is used for mobile devices which do not support IMS AKA for WLAN access.

Table 36: Access Signalling Security Profiles for RCS

For RCS devices which can access the IMS core from both mobile and broadband/fixed networks (e.g. Wi-Fi) a separate access signalling security method and corresponding authentication credential may be required. If the security mechanism is not pre-configured as per section A.1.6.3 and A.2.10, the RCS device negotiates the set of security mechanisms using the SIP security agreement [RFC3329] as specified for IMS in [3GPP TS 33.203] and [3GPP TS 24.229]. If the client is pre-configured with a specific access signalling security mechanism, the client uses the signalling corresponding to this security method in the initial registration procedure, and the IMS core determines (based on signalling) which mechanism is being used/requested and then determines (based on security policy) if the access signalling security method is allowed.

[21] Requires UDP encapsulation of IPsec for NAT traversal

Note: the RCS device shall support a configuration option for each of these profiles (where applicable).

For those cases where the GIBA is pre-configured, but the client supports also SIP Digest, behaviour shall be as follows:

- SSO/GIBA authentication takes place first
- If it fails (e.g. Service Provider network equipment does not support it) digest authentication is then tried

2.13.1.3 Access Media Security

2.13.1.3.1 *Secure RTP (SRTP)*

SRTP [RFC3711] may be used to provide per message authentication, integrity protection and encryption for both RTP and RTCP streams involved in real-time video and voice sessions. The use of SRTP is recommended for communications over any untrusted network in which confidentiality (or lack of) is a concern. As an example, a voice or video call over a Wi-Fi network (e.g. “Hot Spot”) without any WLAN (Wireless Local Area Network) encryption is highly susceptible to eavesdropping.

The establishment and key exchange for SRTP in RCS shall be based on SDES (Session Description Protocol Security Descriptions for Media Streams, cf. [RFC4568]) which is transported within SDP, following the SIP SDP offer/answer model. SDES and SRTP profiles for media security in IMS are specified in [3GPP TS 33.328].

Note that [3GPP TS 33.328] defines two modes of operation for SDES/SRTP: e2ae (end-to-access edge) mode and e2e (end-to-end) mode. For the e2ae mode, SDES is run between an IMS client and a SIP edge proxy, i.e. a P-CSCF (IMS-ALG). An IMS access Gateway controlled by a P-CSCF (IMS-ALG [Application Layer Gateway]) provides the SRTP termination for the “Access Edge”. In the e2e mode, SDES and SRTP is transported end-end between two end user clients.

An RCS client that supports SRTP and SDES and support e2ae mode shall indicate this during the IMS registration according to [3GPP TS 24.229]. The P-CSCF (IMS ALG), if supporting e2ae mode, indicates this to the UE as part of the IMS registration procedures according to [3GPP TS 24.229]. The use of SRTP is enabled through the client configuration parameters (see section A.2.10).

However not all end user clients may support SRTP. Therefore the Service Provider’s network equipment should support e2ae mode. An RCS client that supports SRTP and SDES shall also support e2ae mode.

When using SRTP/SDES, the RCS client can include preference of security mode to use in accordance to [3GPP TS 33.328]. It is recommended that e2ae mode is used by the UE, if also indicated to be supported by the P-CSCF. Otherwise, the RCS client may try e2e by not indicating any preference during the session setup. Note that this does not exclude that the Service Provider network still may decide to terminate the media security in the network (P-CSCF).

For terminating session, the P-CSCF (IMS ALG), if supporting SRTP / SDES e2ae mode, decides based on local policy, whether to apply SRTP / SDES towards the UE.

2.13.1.3.2 *MSRP*

MSRP is used in many RCS services which involve the exchange of images, files and instant messages (e.g. session based). Similar to RTP, MSRP is established through SDP exchanges in SIP signalling and it relies heavily on the security provided in signalling. The use of cryptographically strong random values appended to MSRP URIs exchanged within SDP provides binding between the SIP and MSRP sessions and any identities exchanged within SIP.

For RCS, the use of TLS mode as specified in [RFC4975] is recommended when MSRP is transported over an unsecure network (e.g. Wi-Fi). Consequently, a client configuration parameter to enable Message Session Relay Protocol over Transport Layer Security (MSRPoTLS) is specified in section A.2.10.

The use of self-signed TLS certificates are recommended to produce fingerprints (e.g. secure hash) of the certificate which are exchanged during the SDP negotiation associated with the invitation and MSRP establishment procedure. The certificate fingerprint used for MSRP follows the same fingerprint mechanism specified in [RFC4572]. This binding of the certificate fingerprint to SIP signalling relies on the underlying security and trust provided by SIP signalling (e.g. IPsec, SIPoTLS (SIP over TLS), etc.). As a consequence, it is assumed that MSRPoTLS connections shall only happen when combined with the use of encrypted SIP signalling.

When using MSRPoTLS, and with the following two objectives:

- Avoid a complex end-to-end negotiation, and
- Allow compliance to the legal interception procedures.

The MSRP encrypted connection shall be terminated in an element of the Service Provider network providing service to that UE.

When the alternative connection model for MSRP is used as specified in [RFC6135] (see section 2.8) the TLS session for MSRP may be initiated by either MSRP endpoint in the MSRP communication.

2.13.1.4 XCAP Authentication and Security

XML Configuration Access Protocol (XCAP) exchanges between the RCS client and the XDMS requires authentication and in most cases transport layer security.

Authentication may be provided through the use of HTTP Digest authentication and may use the same credential (e.g. username and password) as SIP based Digest authentication when applicable. For RCS clients that use IMS AKA based credentials for SIP access (e.g. VoLTE), a separate credential may be required unless the IMS Generic Authentication Architecture (GAA) is supported, along with the procedures in [3GPP TS 33.222] for obtaining a suitable credential (e.g. HTTP digest secret) for HTTPS based access such as for XCAP. In GAA, the IMS AKA credential is used in a “bootstrapping” process to obtain other types of credentials from the “bootstrapping” server.

For RCS clients enabled for VoLTE/VoHSPA (see section 2.2), the same authentication specified for VoLTE use of XCAP as defined in [PRD-IR.92] or [PRD-IR.58] shall be supported as follows:

- For RCS clients (and IMS core) that support GAA, the RCS client shall use their AKA credential to fetch an HTTP digest credential using the 3GPP Generic Bootstrapping Architecture (GBA). The RCS client authenticates to an Authentication Proxy (AP) over an HTTP/TLS (HTTPS) secured session using HTTP Digest as per [RFC2617].
- For RCS clients (and IMS core) that do not support GAA, the RCS client shall use its pre-configured credential (e.g. username and password) to authenticate to the AP over an HTTP/TLS (HTTPS) secured session using HTTP Digest as per [RFC2617].

For non-VoLTE/VoHSPA enabled RCS clients, the use of HTTP authentication ([RFC2617]) over an HTTP/TLS (HTTPS) secured session shall be supported for XCAP authentication to the XDMS (or AP).

The HTTP digest credentials (e.g. username and password) for XCAP are specified in section A.1.2.

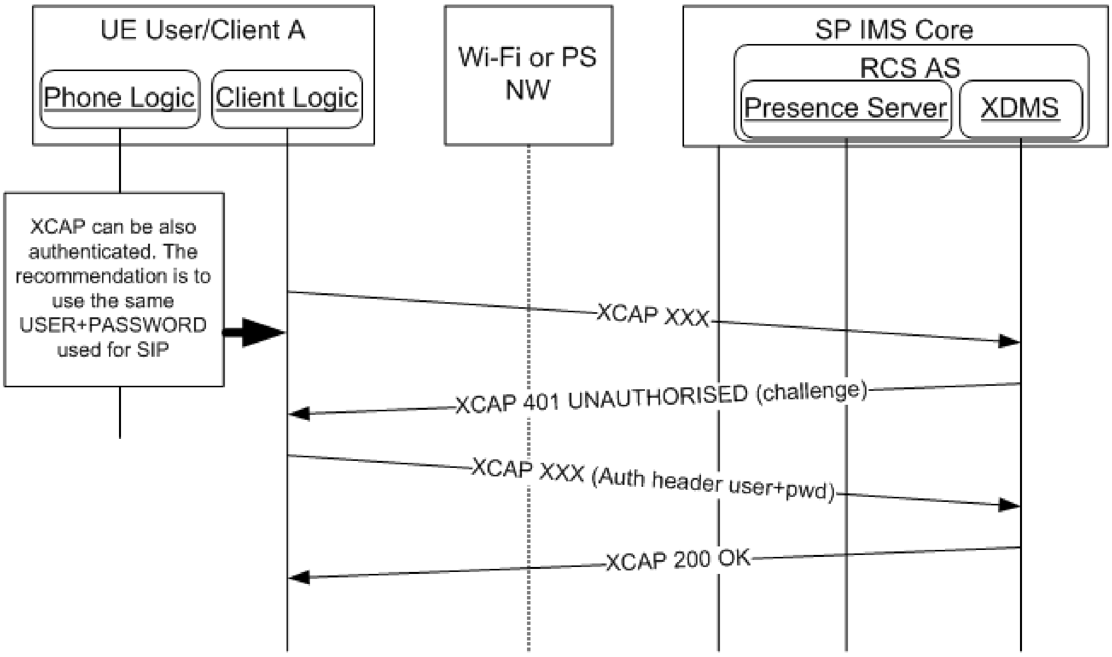

UE User/Client A
Phone Logic
Client Logic
Wi-Fi or PS NW
SP IMS Core
RCS AS
Presence Server
XDMS
XCAP can be also authenticated. The recommendation is to use the same USER+PASSWORD used for SIP
XCAP XXX
XCAP 401 UNAUTHORISED (challenge)
XCAP XXX (Auth header user+pwd)
XCAP 200 OK

Figure 29: XCAP authentication using HTTP Digest

In the case of “Early IMS Security” in which GIBA is used for SIP authentication to the IMS core, the use of a credential such as a username and password (or IMS AKA) may not be required to authenticate to the XDMS (or an AP). A similar IP address based authentication approach as GIBA is specified in [3GPP TR 33.978] for access to HTTP based services using Early IMS Security. Support for this mechanism requires the XDMS or an AP to support the procedures in [3GPP TR 33.978] to fetch the IP address binding of the RCS client from the HSS, using the “*X-3GPP-Intended-Identity*” header provided by the client.

2.13.1.5 Message Content Store Authentication and Security

The RCS client shall support the authentication and security mechanisms described in [RCS5-CPM-MSGSTOR-ENDORS] for access to the Message Content Store using IMAP.

Authentication shall be based on username and password stored on the RCS client and one of the following IMAP authentication methods:

- Plaintext username and password sent using the LOGIN command as specified in [RFC3501]
- Simple Authentication and Security Layer (SASL) based mechanism using the AUTHENTICATE command as specified in [RFC3501].

For the SASL based authentication, the “PLAIN” SASL authentication method shall be used as specified in [RFC3501] and [RFC2595].

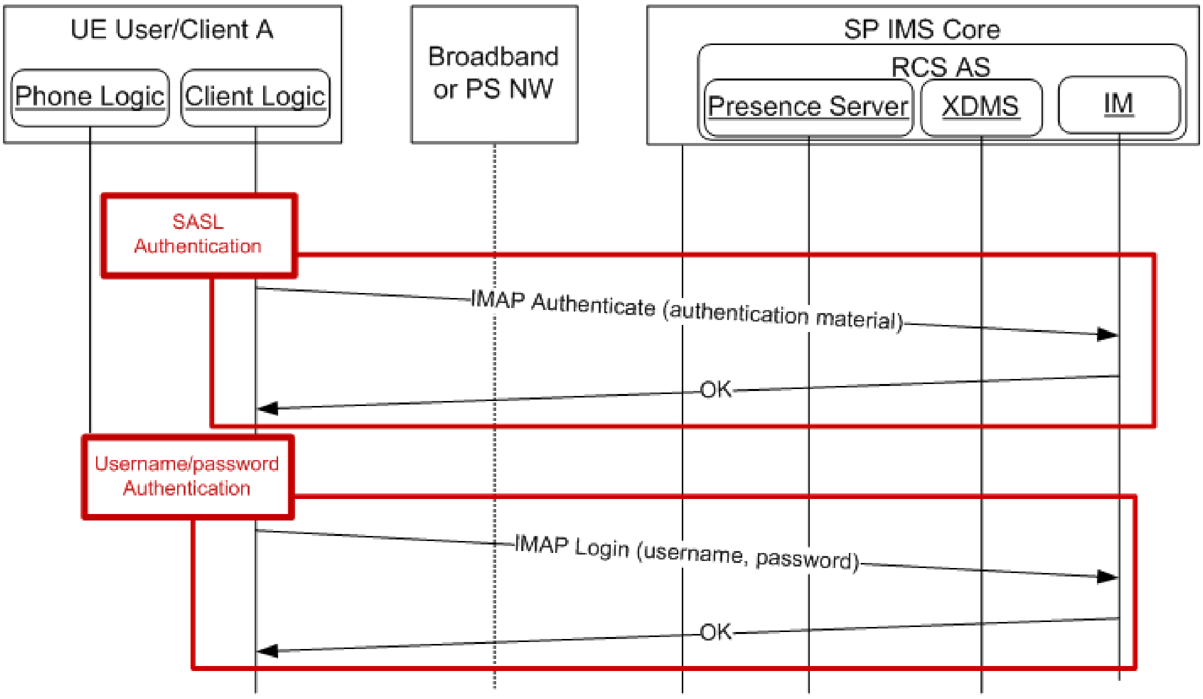


Figure 30: IMAP authentication with SASL or plain text login

TLS shall be used to provide message authentication, integrity protection and confidentiality for the IMAP protocol as specified in [RCS5-CPM-MSGSTOR-ENDORS]. TLS must first be established using the STARTTLS command before any IMAP based authentication occurs using either the LOGIN or AUTHENTICATE command.

The Message Content Store server shall authenticate itself towards the RCS client using certificate based TLS authentication. The client shall support certificates based on a Public Key Infrastructure (PKI) for which the RCS client is pre-configured with a root or intermediate CA (which is recommended to be a public CA root authority) certificate in the signing chain of the certificate.

2.13.2 Privacy

2.13.2.1 Overview

A key element of promoting user adoption of RCS is gaining the user’s trust with regards to privacy. Service Providers need to provide security mechanisms to ensure unwanted parties cannot gain access to RCS user communications and provide adequate mechanisms to enable users to control the information they share. The key security measures to meet these requirements are outlined in section 2.13.1 and privacy controls are summarised in section 2.13.2.2.

2.13.2.2 Privacy controls

Mechanisms provided in RCS 5.0 to enable users to control their privacy are identified in this section.

2.13.2.2.1 *Capabilities Privacy*

The RCS user shall have the option to control the sharing of RCS capabilities information.

2.13.2.2.2 *Multidevice Privacy*

Where an RCS user has RCS active across multiple devices this fact shall be obscured from other users.

Note: Where an RCS user has RCS active across multiple devices this fact cannot be obscured from other devices, since the GRUU and/or sip.instance feature tags reveal the fact to these other devices.

2.13.2.2.3 *Presence information Privacy*

The RCS user shall have the option of controlling who they share their presence information with through a process of accepting, blocking or ignoring an invitation to establish a presence relationship (see section 3.7.4.5).

2.13.2.2.4 *Video Privacy*

The RCS client shall provide the RCS user with control over when any camera on the device is active.

2.13.2.2.5 *Social Presence Information Privacy*

The RCS user shall have the option to disable sharing of social presence information.

2.13.2.2.6 *Network Address Book Privacy*

The Service Provider shall ensure access control to the Network Address Book via a process of authentication.

2.13.2.2.7 *Location Privacy*

The RCS user shall have the option to control sharing of location information (see section 3.10.1.2).

2.13.2.2.8 *Messaging and Chat*

An RCS user shall have the option to control information communicated about their actions during messaging communications and chat sessions, including the suppression of “display” notifications and “IsComposing” notifications.

3 RCS 5 Services

3.1 General Service Overview

RCS 5.0 provides several services that fit into the framework defined in section 2. As mentioned in section 1.2 all of these services are optional for a Service Provider to deploy.

The first set of services is intended to enhance the user's messaging experience. Section 3.2 describes the standalone messaging service based on OMA CPM that is considered as an evolution of the SMS/MMS messaging services providing fewer restrictions and provides the interworking capability with those services. Section 3.3 introduces the 1-to-1 chat service that provides a more real-time experience through "IsComposing" indications next to the store and forward functionality, including delivery and display notifications, that allows reaching users while they are offline. In section 3.4 it is described how the 1-to-1 chat service is extended to multiparty scenarios. For both the 1-to-1 chat and for this Group Chat, the technical realization can be based on either OMA SIMPLE IM or OMA CPM. Interworking between these realisations has been described to manage these as a single service providing transparency and an enhancement to the UX.

As a service that is closely related to the messaging in that it is used for the exchange of discrete content and is based on the same underlying technology, chapter 3.5 describes the File Transfer service allowing a user to exchange any type of file with another user.

Chapter 3.6 introduces the content sharing services allowing the user to exchange a video or image in real-time with another user. For video sharing this can be done both within a call and outside of a call, while the sharing of images is only available during a call. In other circumstances the File Transfer service could be used.

The social presence service in chapter 3.7 allows the user to announce a status including a picture, a link and possibly even information related to his location to a subset of his contacts while at the same time receiving status updates from those same contacts. Depending on the user's preference regarding a contact, they could be informed about such status changes in real-time or after a potentially long delay.

Section 3.8 and 3.9 describe respectively an IP based voice and video call functionality for broadband access clients and mobile devices on HSPA and LTE. These services include support for a set of supplementary services and ensure the quality of service delivery when used on HSPA and LTE access. For the voice call, a mobile device on HSPA and LTE provides continuity to a CS call if network coverage circumstances require this. These services are based on [PRD-IR.58] and [PRD-IR.92] for the voice call and [PRD-IR.94] for the video call.

A geolocation service is introduced in section 3.10 which allows a user to share their location (or any other desired location) with a contact including requesting the location of a contact.

All these services can be invoked either from within the address book provided that the contact has the corresponding capability (see section 2.6) and the current network connectivity allows using the service (see section 2.6.4.1) or directly from the device's menu. Additional entry points may be the chat and call history, the media gallery and camera application depending on what is suitable for the service.

Most of the NNI handling is done as described in section 2.12.

3.2 Standalone messaging

RCS 5.0 provides a Standalone Messaging service as described in [RCS5-CPM-CONVFUNC-ENDORS]. It includes both text and multi-media messaging services using IMS-based OMA CPM Standalone Messaging instead of the SMS and the MMS.

The use of OMA CPM Standalone Messaging removes some of the limitations associated with a messaging service deployment based on the SMS and MMS services, e.g., the 160-character message size, content type, lack of display notifications for text messages and support for the service users with multiple devices.

In addition, the RCS 5.0 Standalone Messaging service supports interworking to SMS and MMS as described in [RCS5-CPM-IW-ENDORS].

A conversational view of the CPM standalone messaging is used in RCS 5.0, and it can be synchronized between a user's multiple devices, by making use of the CPM Network-based Common Message Store as described in [RCS5-CPM-MSGSTOR-ENDORS].

3.2.1 Feature description

The feature list of the RCS 5.0 standalone messaging service includes the following main features:

- Standalone messaging (text and multimedia)
- Delivery and Display Notifications
- Support for multiple devices per user
- Deferred Messaging
- Central Message Storage
- Interworking with legacy messaging services

These features are further described in sections below.

3.2.1.1 Standalone messaging

The RCS 5.0 standalone messaging capability employs the OMA CPM's SIP-based standalone messaging as described in [RCS5-CPM-CONVFUNC-ENDORS]. It evolves the two separate text and multimedia messaging mechanisms into one single and unified messaging framework. This converged messaging mechanism uses the combination of the Pager Mode messaging mechanism and the Large Message Mode messaging mechanism. The mode is selected based on the message size. Smaller messages are sent via Pager Mode and larger messages via Large Message Mode. This built-in capability of the RCS 5.0 Standalone Messaging enhances the user experience by making the selection transparent to the user: the user does not have to choose between messaging technologies based on either the media type or artificially imposed size limits. In addition the RCS 5.0 Standalone Messaging further facilitates the transition from the currently distinct SMS and MMS messaging services towards a single all-IP Messaging services.

The RCS 5.0 standalone messaging includes support for the following specific features:

1. In supporting both text and multi-media messaging, it does not make a distinction between text and multimedia messages.
2. Its message delivery includes both 1-to-1 and group messaging including support for "reply-to-all" functionality.
3. Imposes no limitations on the message size and media types. However, the maximum message size can be controlled by Service Providers.
4. Capabilities for both broadband access and mobile access terminals.
5. It can store a message exchange both in the local and central message storages and to present a conversational view of the exchanged messages.
6. Provides message delivery and display notifications.

3.2.1.2 Delivery and display notifications

Upon sending an RCS 5.0 Standalone Message including a request for message disposition state, the sender shall receive a delivery notification and may receive a display notification.

If an RCS 5.0 Standalone Message contains a disposition notification request targeted at a group of recipients or when multiple disposition notifications are expected to arrive for the same standalone message, the originating user may receive aggregated disposition notifications based on Service Provider policies. Aggregating disposition notifications may be performed by the originating Participating Function or the Controlling Function.

In the case of delivering an RCS Standalone Message to multiple devices of the same contact/user, the terminating Participating Function shall, for each disposition notification type (i.e. delivery and display notifications), forward the first disposition notification received to the originator of the message and shall suppress the forwarding of subsequent disposition notifications received from the other devices that the message was delivered to.

3.2.1.3 Support for multiple user devices

The RCS 5.0 standalone messaging supports users with multiple devices. The RCS 5.0 standalone messaging service shall be available on all of the RCS 5.0 capable devices/clients of a user. More specifically, an incoming message shall be delivered to all clients of a user, which are online and capable of handling the RCS 5.0 standalone messaging service. If all clients of a user were offline when a message has to be delivered, the message will be delivered to the first client that comes online if the message has not expired in the meantime. The procedures for handling the multiple devices are described in [RCS5-CPM-CONVFUNC-ENDORS].

3.2.1.4 Deferred Messaging

As opposed to immediate message delivery, the RCS 5.0 “deferred messaging” is to temporarily hold the message in the terminating Participating Function and deliver it at a later time. Furthermore, the deferred messaging is to defer the delivery of standalone messages when none of the terminating RCS user’s devices is registered and available to receive the messages. In this case, the undelivered messages stay in the RCS Participating Function until they are either delivered to the user devices, are deleted or expire. The procedures for handling the deferred standalone messages are described in [RCS5-CPM-CONVFUNC-ENDORS].

3.2.1.5 Network-based common message storage

In RCS 5.0, a Network-based Common Message Store is used to store messages (standalone text or multimedia and chat messages). An RCS user will have control over the messages to be stored in their message storage. The network-based common message storage allows a user to improve their organization of their stored messages. In addition to this, the Network-Based Common Message Store is used to provide storage for all messages sent and received by a client supporting the RCS 5.0 text and multimedia messaging service which also includes any other messages that they receive.

The RCS 5.0 network-based common message storage supports synchronization of stored objects with the local storage in all registered RCS devices

The storage is always subject to operator-controlled message size and storage quota limitations.

Relevant storage usage information can be collected to allow a service provider to apply usage based charges.

3.2.1.6 Interworking with legacy messaging services

The purpose of this feature on interworking between the RCS 5.0 standalone messaging and the legacy messaging services, e.g., SMS, MMS, is to communicate, in a seamless manner, with devices or networks that support legacy SMS and/or MMS messaging services.

3.2.2 Interaction with other RCS features

There are no interactions between the RCS 5.0 Standalone Messaging service and other RCS services.

3.2.3 High Level Requirements

This section contains Standalone Messaging service's high level requirements. These requirements are listed in two separate support aspects for client and server as follows:

3.2.3.1 Client/device support

3-2-1 Network-based Common Message Store capability: The ability for RCS users to store and manage their messages if the network-based common message storage is deployed and the user has a subscription to the Network-based Common Message Store.

3-2-2 Delivery and Display Notifications: Supporting RCS user to request and receive notifications on the disposition state of a standalone message they have sent. Furthermore, the client device should allow both the sending and receiving users to optionally enable/disable the display notifications request and response, respectively.

3.2.3.2 Server support

3-2-3 Number of recipients: For the Standalone Messaging to support both 1-to-1 and 1-to-many (group) messaging features including “reply-to-all” for the group messaging.

3-2-4 Multiple clients/devices: The ability to support RCS users employing multiple RCS capable devices/clients.

3-2-5 Interworking with legacy SMS and/or MMS: The ability to interwork and communicate with other messaging servers supporting legacy SMS and/or MMS messaging services.

3-2-6 Deferred messaging: To defer the delivery of an RCS Standalone Message when none of the terminating RCS devices is registered and available to receive the RCS Standalone Message.

3-2-7 Network-based common message storage capability: For storing a user's messages and synchronizing them across RCS user's multiple devices.

3-2-8 Delivery and Display Notifications: The server shall ensure that requests for disposition notifications and the notifications themselves are delivered correctly

3.2.4 Technical Realization

3.2.4.1 Standalone messaging

The technical realization of the RCS 5.0 standalone messaging is based on the OMA CPM Pager Mode and Large Message Mode mechanisms as described in [RCS5-CPM-CONVFUNC-ENDORS]. These messaging modes in conjunction with the 3GPP IMS functional entities as the infra-structure for the messaging functional entities are used as the platform for providing an end-to-end standalone messaging service.

Both CPM Pager Mode and Large Message Mode Standalone Messaging mechanisms are based on the use of the IETF SIP protocol. The Pager Mode messaging uses the SIP MESSAGE method, which imposes a limitation for the maximum message size, while the Large Message Mode messaging uses dedicated SIP/MSRP sessions set up for the delivery of large messages without limiting the message size.

The maximum size of an RCS Standalone Message to be sent using the Pager Mode messaging cannot exceed 1300 bytes. Messages with size exceeding this threshold will be handled by the Large Message Mode messaging. Therefore, an RCS 5.0 Standalone Message will be sent and delivered using either the Pager Mode or the Large Message

Mode depending on the size of the message. This procedure is transparent to the user, i.e., the user does not make the decision to use either Pager Mode or Large Message Mode messaging nor do they see a difference in the service behaviour.

From the user access perspective, the same technology is used for simultaneous delivery to mobile and broadband access clients.

3.2.4.1.1 *Pager Mode Messaging*

Figure 31 presents an architectural view of the RCS 5.0 standalone messaging employing Pager Mode messaging.

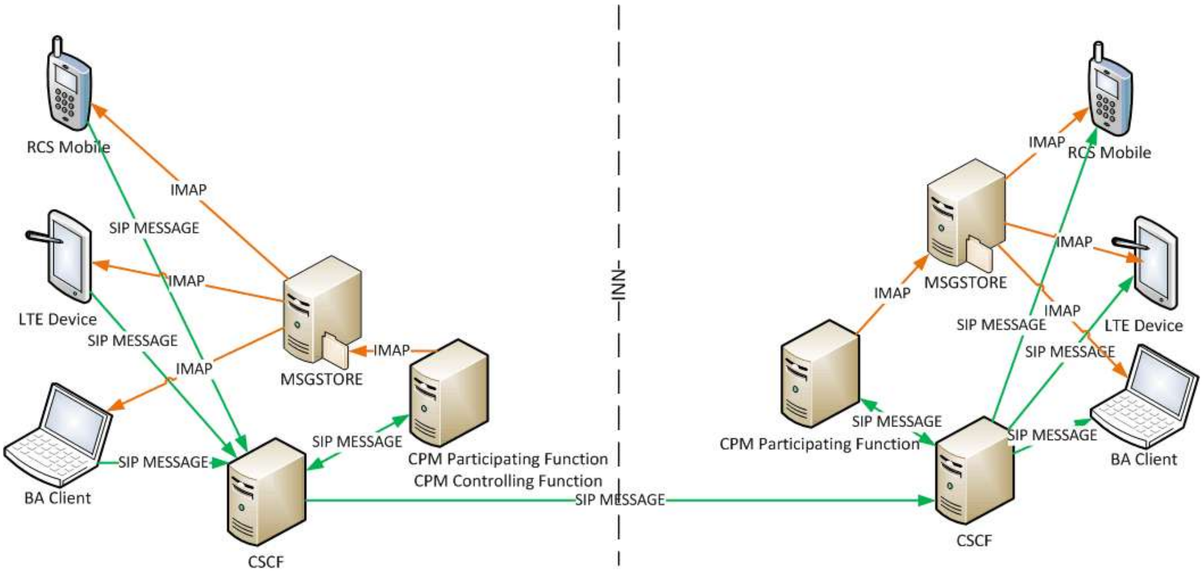


Figure 31: Standalone Messaging using Pager Mode

The detailed procedures for the sending and delivering of a message to the recipient are described in [RCS5-CPM-CONVFUNC-ENDORS]. From the sending user client/device, the message will pass through the Participating Functions at the originating and terminating sides to be delivered to the intended receiving client(s).

If the message is targeted for a group of recipient users, it will be sent from the Participating Function in the originating side to a Controlling Function, also in the originating side, that will then perform the procedures for distributing the message to the Participating Functions attending the intended recipient clients.

The RCS Standalone Message delivery and display notifications will follow the reverse path that was used for sending the message.

As described in [RCS5-CPM-CONVFUNC-ENDORS], if the Network-based Common Message Store is provided any standalone message that is sent or received will be stored in the corresponding RCS user’s Message Store as described in Section 3.2.4.6.

3.2.4.1.2 *Large Message Mode Messaging*

Figure 32 presents an architectural view of the RCS 5.0 Standalone Messaging employing the Large Message Mode messaging.

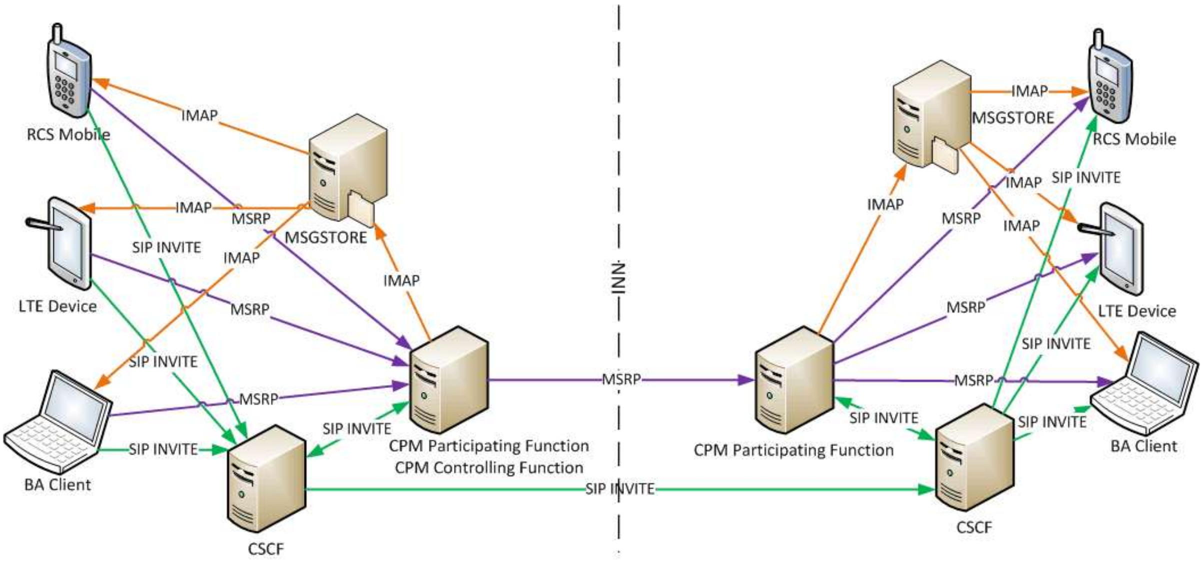


Figure 32: Standalone messaging using Large Message Mode

A large text or multimedia message is sent from an RCS client and delivered to the target client using the Large Message Mode messaging mechanism as described in [RCS5-CPM-CONVFUNC-ENDORS]. Through an MSRP session established following a successful SIP INVITE, the message will be passed through the Participating Functions in the originating and terminating sides to reach the intended recipient. The SIP INVITE includes the size of the standalone message and the content type(s) used in the message.

The terminating Participating Function, amongst other procedures, performs the procedures for deferring messages if none of the intended recipient's RCS capable devices is online.

If the message is targeted for a group of recipient users, it will pass through the Participating Function in the originating side to the Controlling Function also at the originating side before reaching the Participating Function(s) at the terminating side(s). The Controlling Function handles the distribution of the message to various target recipients. As in this case, a list of recipients will be provided along with the delivered message, each recipient has the possibility to send a reply to the sender as well as to all the other users that were addressed in the original message.

The delivery and display notifications of a sent standalone message will follow the reverse path of the sent message.

As described in [RCS5-CPM-CONVFUNC-ENDORS], if the Network-based Common Message Store is provided any standalone message that is sent or received will be stored in the corresponding RCS user's Network-based Common Message Store as described in Section 3.2.4.6.

3.2.4.2 Delivery and Display Notifications

The disposition status notifications for a sent standalone message will follow the reverse path of the sent message. The disposition notifications for the standalone messaging could be used for the 1-to-1 or 1-to-many messaging and for two types of notifications, delivery and display, as specified in [RCS5-CPM-CONVFUNC-ENDORS].

For network optimization purposes, the aggregation of IMDNs as specified in [RFC5438] may be supported for network initiated IMDNs:

- Within the Service Provider's own network, the aggregation of IMDN may be supported (per local policy).
- For inter-Service Provider interoperability, the individual IMDN will always be sent to the target network, where the aggregation of IMDN is up to the target network (per local

policy). That is, if the aggregated IMDNs received by the Messaging Server contain IMDNs that need to be sent to another network, the Messaging Server will repackage the aggregated IMDNs accordingly before sending them to the Chat message sender on the other network.

- If the aggregated IMDNs received by the Messaging Server contain both in-network and inter-Service Provider Chat message senders, the Messaging Server will repackage the aggregated IMDNs according to in-network Chat message senders and inter-Service Provider Chat Message senders.

3.2.4.3 Deferred Messaging

The terminating Participating Function, amongst other procedures, performs the procedure for deferring messages if none of the RCS capable devices of the recipient is online.

When no RCS 5.0 target recipient client is registered, the terminating Participating Function holding the message for delivery may decide to defer the standalone message for delivery at a later time. For the delivery of a deferred standalone message, the Participating Function has the following options as specified in [RCS5-CPM-CONVFUNC-ENDORS]:

1. To send a notification to the RCS clients of the target recipient and wait for these client(s) to take action,
2. To push the deferred standalone messages once one of the clients of the target recipient RCS user becomes available.

Note: Service provider’s policies may guide which option to adopt.

If a deferred standalone message expires before it is delivered, the terminating Participating Function shall handle the deferred message by discarding it.

3.2.4.4 Multidevice handling

The RCS 5.0 supports delivering of standalone messages to multiple devices. As described in [RCS5-CPM-CONVFUNC-ENDORS], the delivery of RCS 5.0 Standalone messages will be delivered to all the user’s RCS 5.0 devices that are online. Also, when applicable, the message is delivered to a single non-RCS 5.0 device of the user through interworking with either SMS or MMS as explained in Section 3.2.4.5.

The support of the RCS 5.0 multidevice environment includes the following major features:

1. When a user sends a message from one of their devices capable of handling the RCS 5.0 standalone messaging and a Network-based Common Message Store is available, all other online devices capable of handling the RCS 5.0 standalone messaging services shall display the message along with related information such as message state and its disposition.
2. If a Network-based Common Message Store is available, all offline clients supporting the RCS 5.0 standalone messaging service will be capable of showing the messages that the user has sent and received (except for already deleted messages) when the clients are back online.
3. Handling of delivery and display notifications when multiple clients receive a message, the terminating RCS 5.0 Participating Function shall support forwarding both delivery and display notifications to the originating client, by forwarding the first disposition notification received from one of the devices that the standalone message was delivered to. It suppresses forwarding subsequent disposition notifications received from the other devices to which the message was delivered.

All procedures for sending and receiving standalone messages and their disposition notifications in an RCS 5.0 multidevice environment, where the RCS 5.0 user employs multiple devices, are performed as described in [CPM-SYS_DESC] and specified in [RCS5-CPM-CONVFUNC-ENDORS]

3.2.4.5 *Interworking with Legacy Messaging services*

The [RCS5-CPM-IW-ENDORS] document describes general interworking procedures applicable to both SMS and MMS and the realization details for the SMS and MMS interworking. The interworking procedures for the SMS include references to 3GPP's IP-SM-GW (IP Short Message Gateway) as described in [RCS5-3GPP-SMSIW-ENDORS].

3.2.4.5.1 *Interworking procedure*

The procedures for the RCS 5.0 standalone messaging service feature interworking to SMS and MMS legacy messaging services are performed by two interworking functional entities, the Interworking Selection Function (ISF) and the Interworking Function (IWF). After the Participating Function has decided that the message has to be interworked the selection of whether to interwork to SMS or MMS is done in the ISF as described in [RCS5-CPM-IW-ENDORS]. The actual interworking procedure is performed by the SMS and MMS gateways described in [RCS5-3GPP-SMSIW-ENDORS] and [RCS5-CPM-IW-ENDORS]. These functions also interwork the delivery notifications received from the SMS and the delivery and display notifications received from the MMS message recipient(s) and forward them to the sending Participating Function to be passed on to the sending RCS client.

The interworking functions also interwork any incoming SMS or MMS messages to RCS messaging.

3.2.4.5.2 *Interworking with SMS*

When the target recipient device for an RCS Standalone Message is a non-RCS 5.0 capable, an SMS capable device, the process of interworking with legacy SMS is invoked according to [RCS5-CPM-CONVFUNC-ENDORS]. In Figure 33, an architectural view of the RCS 5.0 standalone messaging service interworking with the legacy SMS is shown. The legacy mobile device is shown as a non-RCS 5.0 device.

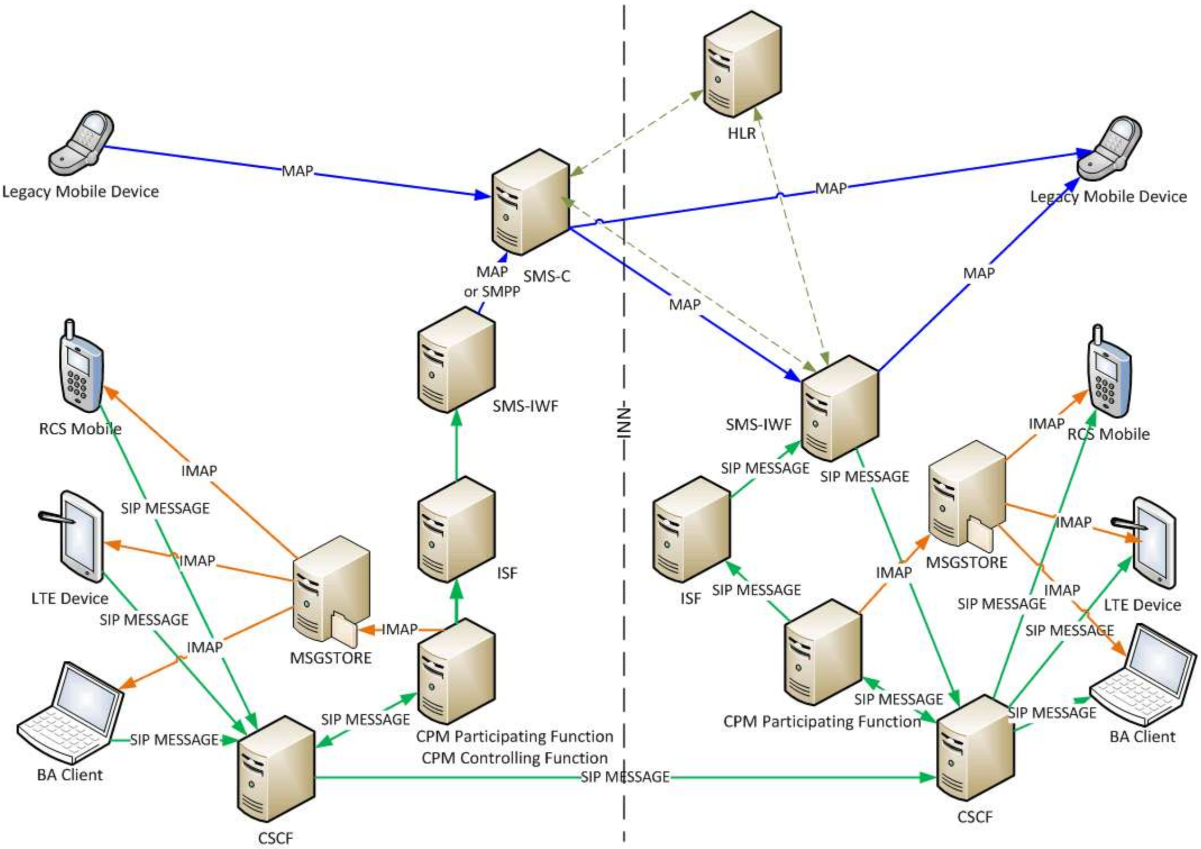


Figure 33: Standalone Messaging interworking with SMS

When the SMS interworking function (IP-SM-GW or SMS-IWF) receives a SIP MESSAGE request with the OMA CPM IMS Communication Service Identifier (ICSI) "*3gpp-service.ims.icsi.oma.cpm.msg*", it checks the size of the received payload of the SIP MESSAGE request. If the size of the payload is too large to be sent as one SMS message, the payload will be divided into concatenated SMS messages. The SMS-IWF will send the request(s) generated based on the received SIP MESSAGE request towards the SMS-C (Short Message Service Centre) using either the SMPP (Short Message Peer-to-Peer) or MAP (Mobile Application Part) protocols, depending on the type of SMS network in which it is deployed, as specified in [RCS5-CPM-IW-ENDORS] or [RCS5-3GPP-SMSIW-ENDORS] respectively.
Note: For clarity, Figure 33 mainly shows the latter deployment option since the differences between both options are in the existing SMS deployments and therefore have no impact on the Standalone Messaging service.

Breakout to SMS can be done at the originating side if the addressed user is not an IMS user. This is determined based on the standalone messaging capability information, on local information the Messaging Server may have about the recipient, or when the Messaging Server receives an error response. Otherwise, the breakout at the terminating side is done, if either the addressed user is an RCS user using SMS instead of RCS 5.0 standalone messaging service or the user is using a mixture of legacy and RCS devices.

The following error responses to the SIP MESSAGE (or, for the IP-SM-GW realisation, optionally for a Large Message Mode message the SIP INVITE) request indicate that the recipient is not an RCS contact and these responses can be used to trigger interworking:

- 404 Not Found;
- 405 Method Not Allowed;
- 410 Gone;
- 414 Request URI Too Long;
- 415 Unsupported Media Type;
- 416 Unsupported URI Scheme;
- 488 Not Acceptable Here;
- 606 Not Acceptable.

The case for delivering text messages to a (primary) broadband client of a non-Standalone Messaging user is beyond the SMS interworking gateway of the standalone messaging and its platform. It is not shown in Figure 33 to avoid overloading it. In that scenario the MAP (Mobile Application Part) or SMPP request from the SMS-IWF to the legacy Mobile Device for the incoming SMS message would be replaced by a SMSoIP (SMS over IP) request, which is relayed to the legacy BA Client via the Serving Call Session Control Function (S-CSCF).

3.2.4.5.3 *Interworking with MMS*

When the target recipient device for standalone messaging is not an RCS 5.0 device and the message to be sent is a multimedia message, the process of interworking with legacy MMS is invoked according to [RCS5-CPM-CONVFUNC-ENDORS].

Figure 34 presents an architecture view of the interworking for multimedia messaging. As shown, the legacy mobile device at the terminating side may either be an RCS user's primary device that uses MMS instead of RCS 5.0 Standalone Messaging or a non-RCS device capable of receiving MMS.

Depending on the size of the standalone message, it could be either a text message with a large payload or a multi-media standalone message. In the former case the interworking with SMS would apply as described in section 3.2.4.5.2 if the message were small enough for a concatenated SMS. Otherwise, the interworking would be to the MMS service, hence sending a SIP INVITE request to the RCS 5.0 MMS-IWF.

When the RCS 5.0 MMS-IWF receives a SIP INVITE request containing the OMA CPM ICSI "*3gpp-service.ims.icsi.oma.cpm.largemsg*" for a Large Message Mode standalone message, it will send a 200 "OK" response if no errors are found in the SIP INVITE request or an appropriate error response. This is followed by the MMS-IWF's subsequent receiving of an MSRP SEND request for the establishment of the MSRP session, and the process then continues as described in [RCS5-CPM-IW-ENDORS].

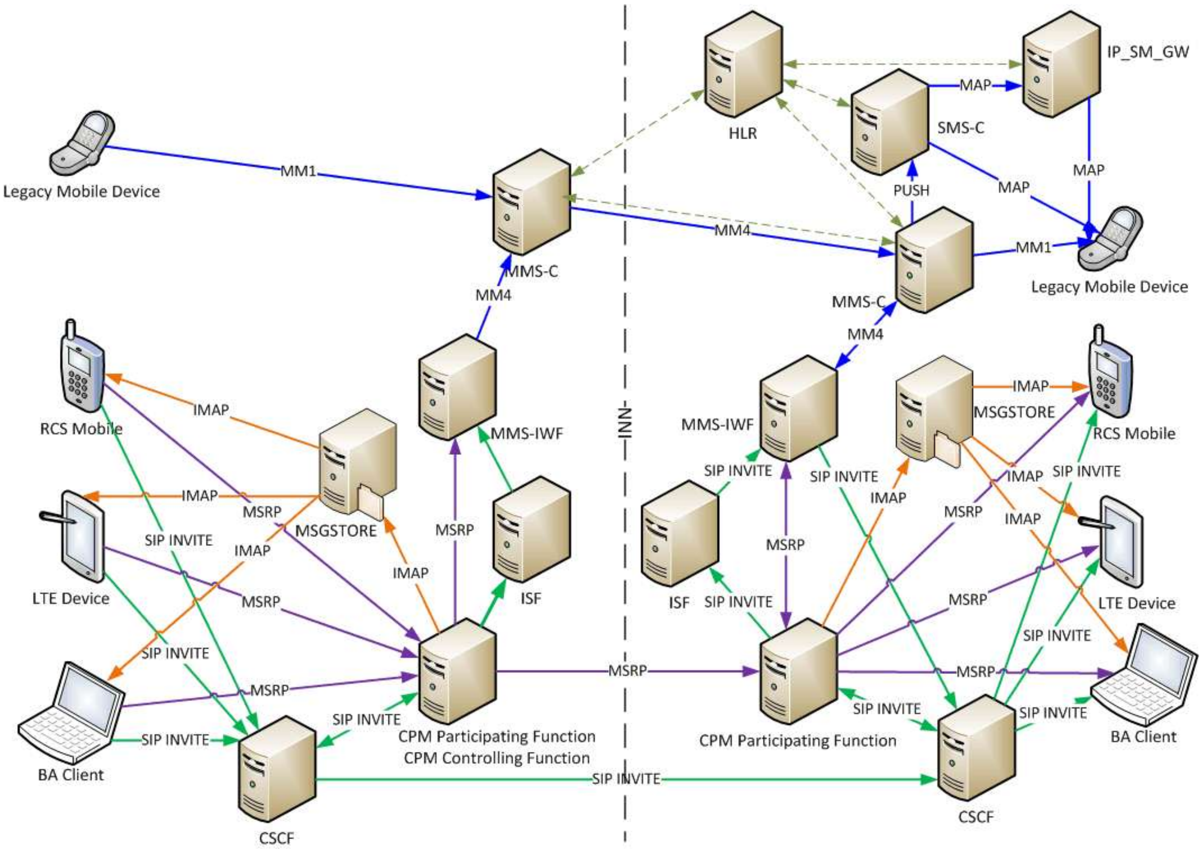


Figure 34: Standalone messaging interworking with MMS

Breakout to MMS can be done at the originating side if the addressee is not an IMS user either based on local information the Messaging Server may have about the recipient, or when it receives an error response. Otherwise, the breakout at the terminating side is done if either the addressee is an RCS user using MMS instead of RCS 5.0 standalone messaging service or the user is using a mixture of legacy and RCS devices.

The following error responses to the INVITE request indicate the recipient is not an RCS contact and can be used to trigger interworking:

- 404 Not Found;
- 405 Method Not Allowed;
- 410 Gone;
- 414 Request URI Too Long;
- 415 Unsupported Media Type;
- 416 Unsupported URI Scheme;
- 488 Not Acceptable Here;
- 606 Not Acceptable.

Similar to SMS interworking, in the MMS interworking of Figure 34, the case for delivery of the multimedia message to a Broadband Access client of a non-RCS 5.0 user is not shown to not overload the figure.

3.2.4.6 Network-based common message storage

RCS 5.0 supports a "network-based common message storage" as described in Section 5.5 of [CPM-SYS_DESC] and specified in [RCS5-CPM-MSGSTOR-ENDORS]. Using IMAP connection, an RCS 5.0 user can access and manage their stored objects, as described in [RCS5-CPM-MSGSTOR-ENDORS] regardless of their RCS 5.0 service registration.

3.2.5 NNI and IOT considerations

For the Standalone Messaging service three NNI interfaces are possible:

- The NNI described in section 2.12 carrying the standalone messaging service across RCS 5.0 compliant networks
- SMS NNI
- MMS NNI

Which of these interfaces is used is decided based on the Service Provider's policies and the applicable interworking agreements.

3.2.6 Implementation guidelines and examples

From the RCS 5.0 user experience, the following three possible entry points to the standalone messaging may be supported:

1. Standalone Messaging screen/window
   There may be a dedicated "Standalone Messaging" application point of entry in the device menu. From this Standalone Messaging screen/window, a standalone message can be initiated or received using the relevant menu items and the device's supported keypad/keyboard. This application may also provide access to the user's message store for viewing and managing stored messages, e.g. message history.
2. Integrated messaging screen/window
   There may be a dedicated integrated messaging application point of entry in the device menu. From this integrated screen/window, a message can be initiated or received using the relevant menu items and the device's supported keypad/keyboard. This application may also provide access to the user's message store for viewing and managing stored messages, e.g. message history.
3. Address book window
   Using this entry point, a message may be initiated with any contact. The experience when interacting through this entry point is identical to that of the messaging screen/window.

3.3 1-to-1 Chat

3.3.1 Feature description

3.3.1.1 General

The Chat service enables users to exchange messages between two users instantly.

The following RCS 5.0 1-to-1 Chat features are described:

- Store and forward
  This feature requires a Messaging Server to store messages and notifications (delivery and display) when the destination user is not online and deliver them to the user when he comes online again (i.e. store and forward).
- Interworking of Chat to SMS/MMS
  This feature requires a Messaging Server to interwork the messages to and from SMS or MMS.

- "Delivered" message notification
  This allows the sender of a message to be notified when their message has been delivered to the recipient.
- "Displayed" message notification
  This allows the sender of a message to be notified when their message has been displayed on one of the recipient’s devices. Note that this notification cannot certify that the recipient has actually read the message. It can only indicate that the message has been displayed on the recipient's terminal User Interface (UI).
- Delivery of notifications (delivered and displayed) outside a session
  It should be possible to deliver notifications independently of whether a 1-to-1 chat is established or not.
- IsComposing indications
  This allows a user in a chat conversation to see when another user is typing a new message/reaction.
- Local Black List
  The terminal/client may support a locally stored Black List to handle incoming chat requests. Users are allowed to qualify undesired incoming chat as spam. This prevents subsequent messages from those originators to be shown or even notified to the user. Also, this undesired traffic will not be acknowledged to have been read. The Black List behaviour applies not only to Chat but also to File Transfer.
- Local Conversation History
  The terminal/client supports a locally stored conversation.
- A Network-based Common Message Store
  A Network-based Common Message Store for the chat sessions may be used to synchronize the messages between devices. It also allows the user to keep a back-up of important conversations in the network.
  In the device, alignment is expected between the local Conversation History and the synchronization with the Network-based Common Message Store. How this alignment is done is left up to the device implementation.
- User Alias (Display Name)
  A user defined display name may be sent when initiating a communication with another user.
- Flexibility to allow multimedia messages within a chat conversation
  Multimedia message exchange is supported in a chat session. However, whether or not multimedia messages are allowed during a Chat session is up to a Service Provider and controlled by a configuration parameter (see MULTIMEDIA IN CHAT in Table 52 of Annex A).

3.3.2 Interaction with other RCS features

3.3.2.1 Switching to Group Chat

A Group Chat can only be initiated from a user on a Service Provider which has deployed a Messaging Server. It is optional for a Service Provider to provide the Group Chat functionality. Therefore from the terminal perspective, if there is no OMA SIMPLE IM parameter CONF-FCTY-URI (see Table 52 in Annex A) configured, the terminal should not allow the user to add additional parties to the chat or start a Group Chat.

A 1-to-1 Chat can be converted into a Group Chat by either of the two Users A and B by adding new users to it. User A and User B are given the option in their UI to add one or more chat partners to the conversation. A user may be limited to the contacts known by their devices to be RCS users. Otherwise the originating user's Messaging Server needs to be prepared to potentially interwork messages to non-RCS Users via SMS or MMS.

A real time check of contacts capabilities may be performed when initiating a Group Chat (section 3.3.6.3). A new Group Chat composing window is created in the initiating device, for example, User A’s device, and the result of this check is visible here.

When User A sends the first message a new Group Chat is opened between all the selected users, and User A and User B as described in section 3.3.6.3.

For User B a new Group Chat composing window is created in the user’s device.

3.3.2.2 File Transfer within 1-to-1 chat and interaction with the spam/blacklist feature

During a 1-to-1 chat, either user is able to initiate a File Transfer from the chat composing window towards the other user. The File Transfer is established using a new SIP session and is carried in a new MSRP session which is different from the one used for the chat session.

On the device involved in the chat, the receiving user receives the File Transfer invitation inside the chat window with the sending user and is able to accept or decline it from that window. In a multidevice environment, the File Transfer invitation is also shown on the other devices of the user allowing them to accept or decline the invitation also from those devices.

If the user accepts the File Transfer, the terminal will either ask the user the location to store the file or use a default directory. Once received, the user can open the file from the chat composing window.

Please note that the spam/blacklist behaviour applies to File Transfer, and not only to Chat messages. If an invitation to receive a file is received from a blacklisted user, the client/device implementation should, from the UI point of view, not notify the user on receipt of a File Transfer invitation from a blacklisted sender. Instead it should log the event in the spam folder (e.g. “User A tried to send a file on TIME/DATE”).

See section 3.5 for more details on File Transfer.

3.3.3 High Level Requirements

The following list of high level requirements applies to 1-to-1 chat:

- Clients/devices:

3-3-1 "Delivered" message notification request and response

3-3-2 "Displayed" message notification request and response
Note that the client device should allow the user to enable or disable the displayed notifications request and response

3-3-3 Delivery of notifications (delivered and displayed) outside a session

3-3-4 IsComposing indications

3-3-5 Procedures associated with the store and forward of both messages and notifications performed by the Messaging Server

3-3-6 Messaging Server: In addition to the requirements presented above

3-3-7 Store and forward of both messages and notifications
Please note this is a function which is provided on the terminating Service Provider’s network however a Messaging Server may additionally provide originating store and forward to avoid dependencies with another Service Provider network’s implementations.

3-3-8 Interworking of Chat to SMS/MMS

3.3.4 Technical Realization

Two different technical realizations of 1-to-1 chat are available. The first section describes the features common to both, and the following two sections describe what is unique to each of technical realizations. Whether a device uses one technical realization or the other depends on the setting for CHAT MESSAGING TECHNOLOGY defined in Table 52 in Annex A).

3.3.4.1 Technical Realization of 1-to-1 Chat features common to both OMA SIMPLE IM and OMA CPM

At a technical level the Chat service implemented using OMA SIMPLE IM or OMA CPM relies on the following concepts:

- OMA SIMPLE IM as described in [RCS5-SIMPLEIM-ENDORS], or OMA CPM as described in [RCS5-CPM-CONVFUNC-ENDORS], thereby relying on SIP procedures for the setup of sessions using MSRP for the message exchange;
- In the SDP of the SIP INVITE request and response, the *a=accept-types* attribute shall include only *message/cpim* and *application/im-iscomposing+xml*, i.e., "*a=accept-types:message/cpim application/im-iscomposing+xml*".
- If initiating or accepting this chat would have increased the number of concurrent chat sessions above the Service Provider configured maximum limit (see MAX CONCURRENT SESSIONS in Annex A), the device would close one of the other active chat sessions (for example, a chat that has not been used for the longest period of time) before initiating a new one.
- When a session is set up, messages are transported in the MSRP session. Each MSRP SEND request contains a request to receive an Instant Messaging Disposition Notification (IMDN) 'delivery' notification, and possibly a request to receive an IMDN 'display' notification. The receiving devices must generate an MSRP SEND request containing the IMDN status when the user message is delivered and if requested, another MSRP SEND request when the message is displayed.
  Note: If there is not an already established MSRP session between sender and receiver, the Pager Mode (i.e. SIP MESSAGE) is used to transport IMDNs (delivery notification, display notifications)
- IMDN [RFC5438]: RCS relies on the support of IMDN as defined in [RFC5438] and [RFC5438Errata] to request and forward disposition notifications of all the exchanged messages (See also section C.2 for the errata mentioned in [RFC5438Errata]);
- The CPIM/IMDN wrapper shall be UTF-8 encoded to avoid any potential internationalization issues.
- The device identification uses the mechanisms described in section 2.11.3;
- IMDN message identification for all messages (including those conveyed in the SIP INVITE and notifications delivered via SIP MESSAGE) as defined in [RFC5438];
- For network optimization purposes, the aggregation of IMDNs as specified in [RFC5438] may be supported for network initiated IMDNs:
  - Within the Service Provider's own network, the aggregation of IMDN may be supported (per local policy).
  - For inter-Service Provider interoperability, the individual IMDN will always be sent to the target network, where the aggregation of IMDN is up to the target network (per local policy). That is, if the aggregated IMDNs received by the Messaging Server contain IMDNs that need to be sent to another network, the Messaging Server will repackage the aggregated IMDNs accordingly before sending them to the Chat message sender on the other network.
  - If the aggregated IMDNs received by the Messaging Server contain both in-network and inter-Service Provider Chat message senders, the Messaging Server will repackage the aggregated IMDNs according to in-network Chat message senders and inter-Service Provider Chat Message senders.

- Auto-acceptance of store and forward Messaging Server PUSH of stored notifications. Only the device which has sent the relevant message shall accept the notification;
- Store and forward Messaging Server PUSH of stored messages;
- An IMAP based Network-based Common Message Store expected to store OMA SIMPLE IM and CPM chat messages, described in [RCS5-CPM-MSGSTOR-ENDORS];
- Chat inactivity timeout: When a device or the network detects that there was no activity in a chat for IM SESSION TIMER, a configurable period of time (see Table 52 in Annex A), it will close the established Chat session;
- When reopening an older chat on the device, that contains messages for which a “display” notification should be sent, these notifications shall be sent as follows:
  - If there is no session established with the sender, the device will send the notifications outside a session (since there is no current session to send them to);
  - If there is an active session but that session is with a device of the sender other than the one that was used to send the message to which this notification relates, the Messaging Server will ensure that these notifications are delivered outside of that session;
- The "IsComposing" notification is generated and processed according to the rules and procedure of [RCS5-SIMPLEIM-ENDORS], and for OMA CPM, is generated and processed according to the rules and procedures of [RFC3994]. Consequently, the ‘IsComposing’ indication is not sent with CPIM headers, and a delivery and/or displayed notification shall not be requested.
- The transfer of files while a Chat session is taking place shall be performed in a separate session. Note that this is only at protocol level. From the user experience perspective, they should be able to transfer files whilst in chat. Messages over a maximum size (MAX SIZE 1-to-1 IM in section A.1.3.3) should be transferred using File Transfer or a Large Message mode standalone message. When a network does not allow multimedia within a chat (see MULTIMEDIA_IN_CHAT in section A.1.3.3), all multimedia messages shall be transferred using File Transfer or a Large Message mode standalone message.

3.3.4.1.1 *Spam/Black List Handling*

When receiving a message from a sender included in the Black List (i.e. a spam sender) the receiving client’s/device’s implementation shall:

- Terminate the transaction with a 486 BUSY HERE sent back to the sender.
- The receiver will still issue a delivery notification with status “delivered” which will be sent back to the sender.
- From the UI point of view, the receiver should not be notified on the reception of a message from a blacklisted sender and the message should be copied to the spam filter.

3.3.4.1.2 *Chat abnormal interruption*

If a device in a chat suffers an abnormal termination of the Chat session, for example loss of coverage, the “Send” button may be disabled. If the device determines that a message could not be sent (e.g. failed response or received no response), it shall inform the user that the chat message was not sent. If the TCP connection is lost, the client should re-send it in a new chat session once re-registered.

Note that if the Messaging Servers involved in the chat have implemented store and forward functionality, then the Messaging Servers shall be responsible for storing any messages received while a chat has been abnormally interrupted.

In temporary interruption cases, for example a device was out of network coverage but is now again within network coverage, the chat can be continued from the same conversation window. In this case a new session has to be established with a SIP INVITE request.

3.3.4.1.3 *Store and Forward Mode*

The store and forward functionality in the network is optional and it is up to each Service Provider to decide whether to deploy it (that is to deploy a Messaging Server supporting store and forward).

A Messaging Server is required to provide the store and forward functionality. There are three possible scenarios to fulfil the store and forward requirement:

1. Sender and receiver are on networks with a Messaging Server supporting store and forward: In this case the receiver's side Messaging Server has the responsibility to store and forward IMs which are not delivered. The sender's side Messaging Server has the responsibility of storing the delivered/displayed notifications if the sender is offline.
2. Only the sender is on a network with a Messaging Server supporting store and forward: The sender's side Messaging Server has the responsibility to store and forward chat messages and/or delivered/displayed notifications if immediate delivery was not possible. As it is in the sender's network, the Messaging Server will not have information on when the receiver is online, therefore a retry mechanism is used. Note that it is the Service Provider's decision whether they provide store and forward for chat messages on behalf of the receiver who is in a different network that does not support store and forward.
3. Only the receiver is on a network with a Messaging Server supporting store and forward: The receiver's side Messaging Server has the responsibility to store and forward Chat messages and/or delivered/displayed notifications if they cannot be delivered. As it is at the receiver's side, that Messaging Server will not have information on when the sender is online. Therefore a retry mechanism is used to store and forward notifications that could not be delivered right away. Note whether a Service Provider provides store and forward for delivered/displayed notifications on behalf of the sender who is in a different network that does not support store and forward is optional.

The Messaging Server stores undelivered messages for a period that is determined by local server policy. If at the end of this period the messages have not been delivered, the Messaging Server discards them. This applies to notifications as well as messages.

3.3.4.1.4 *Delivering stored notifications*

To be able to deliver delivered/displayed notifications that were stored to a sender's device that has come online again, without disrupting the user experience, the Messaging Server supporting the store and forward functionality shall initiate a special session for the purpose of delivering these notifications. This special session shall be automatically accepted by the device. It is recognized by the device by means of the well-known URI (*rcse-standfw@<domain>*) uniquely identifying the store and forward service identity that is provided in the *P-Asserted-Identity* header field. Optionally an operator can disable the delivering of the stored notifications when the RCS user is roaming in a foreign network.

NOTE: The Messaging Server may also use Pager Mode messaging to deliver stored delivery and displayed notifications.

The Messaging Server supporting the store and forward functionality is required to send the delivered/displayed notifications to the exact device that has previously sent the associated messages. Therefore the Messaging Server implementing multidevice handling shall support device identification as specified in section 2.11.3 (i.e. both GRUU and sip.instance support).

Finally, please note that store and forward functionality on the network side is optional, therefore there is a dedicated configuration setting (IM CAP ALWAYS ON, see Table 52 in

Annex A for further reference) which is used to configure the client to use or not use this functionality which may have implications on the user experience.

3.3.4.1.5 *Interworking to SMS/MMS*

The functionality for interworking of the chat service to SMS/MMS is optional and it is the decision of each Service Provider whether to deploy it. This deployment involves

- the Messaging Server described in [RCS5-SIMPLEIM-ENDORS] or [RCS5-CPM-CONVFUNC-ENDORS]
- The ISF described in [RCS5-CPM-IW-ENDORS] which is responsible for selecting the appropriate interworking function for a new session
- The IWF for SMS and MMS described in respectively [RCS5-3GPP-SMSIW-ENDORS] and [RCS5-CPM-IW-ENDORS] which are responsible for doing the actual interworking (that is the protocol conversions) between RCS based chat and SMS or MMS

Based on service-level agreements (SLAs), interworking of chat may occur on the originating side or the terminating side, the same circumstances as for interworking of messages with SMS/MMS described in section 3.2.3. In brief, the interworking is initiated by the Messaging Server either based on local information it may have about the recipient, or when it receives one of the following error responses on the INVITE request that indicate that the recipient is not an RCS contact:

- 404 Not Found;
- 405 Method Not Allowed;
- 410 Gone;
- 414 Request URI Too Long;
- 415 Unsupported Media Type;
- 416 Unsupported URI Scheme;
- 488 Not Acceptable Here;
- 606 Not Acceptable.

3.3.4.1.5.1 Interworking at Originating Side

When a Chat session invitation needs to be interworked on the originating side, the CPM Participating Function will route the invitation to the ISF, which will select either SMS or MMS interworking based on applicable service provider policy. The ISF will then route the message to the selected IWF, which will either accept the chat invitation automatically on behalf of the SMS/MMS user, or will convert the chat invitation to an SMS/MMS invitation message and deliver it to the terminating network using the appropriate SMS/MMS NNI. The response to the chat invitation from the SMS/MMS user must be received through the same SMS/MMS interface to associate correctly the response with the earlier invitation. The SMS/MMS response (either accept or decline) to the invitation is converted to the appropriate SIP response and conveyed back to the RCS user.

3.3.4.1.5.2 Interworking at Terminating Side

When a Chat session invitation needs to be interworked on the terminating side, the invitation will be first routed to the terminating network as described in previous sub-sections, and then the same procedures as for interworking of chat invitations on the originating side will apply.

3.3.4.1.6 *Multidevice handling*

Multidevice handling occurs when a user has more than one device (e.g., PC and mobile) connected simultaneously.

When a new 1-to-1 chat is initiated and a message is sent from User A to a User B with User B having multiple devices registered at the same time, the network or Messaging Server forks the Chat session invitation to the different devices. Note that it is assumed that the originating user uses one device per session.

Each of User B’s devices that receive the session invitation generates a SIP MESSAGE request to carry the delivered IMDN. In a multidevice scenario, if a sender receives more than one IMDN for a sent message, it shall discard all copies except the first one it receives.

User B is able to respond to the chat from any of their devices. When they answer and send a message from one of the devices, that device (B1) becomes the only active device for User B and all the Chat sessions towards the other devices are terminated. All the subsequent messages sent to User B are received only by the active device B1 using the already established Chat session.

Device switching:

1. If User B closes the Chat session from the active device (either by closing the chat conversation from the chat window or due to an abnormal termination), any new messages sent by User A through the chat will make the Messaging Server establish the chat again using one Chat session per connected device of User B and send the message to them all.
2. If User B changes from one device B1 to another B2 by sending a new message to the chat from the new device B2, B2 will send a new INVITE request that will go to User A’s device. When User A’s device detects a new INVITE request from User B which already has an established session with User A’s device it shall end that session and accept the new one. All subsequent messages are received only by device B2. Device B2 must then store the received messages and display them appropriately. If User A still has delivery and display reports for device B1, they should be sent before User A’s device closes the old session.

3.3.4.1.7 *Emoticons*

Selected emoticons are displayed graphically but sent and received as text. The list of supported emoticons is defined in [RCS5-SIMPLEIM-ENDORS] Appendix N.

3.3.4.1.8 *Chat message size limitations*

The maximum size is controlled through the MaxSize1To1 configuration parameter defined in Table 52 in section A.1.3. If the message is larger than the maximum size, the message can be delivered either by file transfer or by a Large Message Mode standalone message.

3.3.4.2 Technical Realization of 1-to-1 Chat features when using OMA SIMPLE IM

At a technical level the Chat service implemented using OMA SIMPLE IM extends the concepts from section 3.3.4.1 with the following concepts:

- For OMA SIMPLE IM, first message is always in a CPIM/IMDN wrapper of the SIP INVITE request, so the configuration parameter FIRST_MSG_IN_INVITE in Annex A is always set to enabled.
- If auto-accept is not used, then the devices each send a SIP 180 response toward A.
- The received Chat session invitation contains an IMDN requesting 'delivery' notification. So each receiving device sends back a SIP MESSAGE request containing the IMDN indicating successful delivery of the original message sent by A.
- The receiving clients each send a 486 BUSY HERE response to the outstanding INVITE when a new INVITE arrives from the same user so that there is not more than one outstanding INVITE from one user. The IMDN for 'delivery' notification is requested and sent similarly to the first session invitation.

- No support for exchanging multimedia content within a chat so the configuration parameter MULTIMEDIA_IN_CHAT in Annex A is set to disabled to reduce the complexity associated with the store and forward feature. Therefore in the SDP of the SIP INVITE request and response, the *a=accept-wrapped-types* attribute shall only include text/plain, i.e., *a=accept-wrapped-types:text/plain*. To transfer multimedia content during a chat, File Transfer is used.
- When one of User B's devices detects user activity relevant to the consumption of the message contained in the invitation (e.g. click on a pop-up to go to the Chat window) a 1-to-1 chat session is established according to the following possible criteria:
  a) The respective client returns a 200 OK response, signalling the initiation of the remaining procedures to establish the chat when User B reacts to the notification by opening the chat window. This is the default criteria for RCS 5.0 and, consequently, all the diagrams shown in this document reflect this behaviour.
  b) The 200 OK response is sent when User B starts to type a message, or
  c) The 200 OK response is sent when User B sends a message. Please note that in this case User B’s message will not generate an invite but is buffered in the client until the MSRP session is successfully established.
  d) The 200 OK response is sent immediately since the devices receiving the invitation are configured to auto-accept the session invitations (IM SESSION AUTO ACCEPT configuration parameter defined in Table 52 in section A.1.3.3).

  Please note that:

  - The behaviour for criteria a), b) and c) is configured via the IM SESSION START parameter as defined in Annex A section A.1.3.3. The behaviour for criteria d) is configured via the IM SESSION AUTO ACCEPT configuration parameter defined in Table 52 in section A.1.3.3.
  - For a), b) and c), the 200 OK is sent if the chat invitation has not expired. Otherwise, User B's message shall be sent in a new invitation (from User B to User A).

  If the Chat session invitation from User A contained an IMDN *Disposition-Notification* header requesting a 'display' notification and if the privacy settings allow it, the device User B is using shall generate an MSRP SEND request toward User A that contains the IMDN 'display' status for the message received from User A.

  It may be the case that multiple Chat sessions from User A are pending on User B's side, that is the last received Chat session is established and the other pending sessions are answered with a 486 BUSY HERE response. In such cases, if the Chat session invitations from User A contained a IMDN Disposition-Notification header requesting a 'display' notification, the device of User B that accepted the SIP INVITE generates an MSRP SEND request toward User A that contains the IMDN 'display' status for each message received from User A.
- Note: The statement in section 3.3.4.1 that the CPIM/IMDN wrapper shall be *UTF-8* encoded to avoid any potential internationalization issues also applies to the IMDN requested in the SIP INVITE request.
- A Messaging Server supporting store and forward behaves as a back-to-back user agent handling the SIP INVITE requests that are used to establish the chat session. While doing this it may have to return a different response to the INVITE request on the originating leg than the one it received on the INVITE request on the terminating leg. The mappings shown in Table 37 will be applied:

Response received on terminating leg	Response sent on originating leg	Store the message
480 Temporarily unavailable	200 OK	Y
408 Request Timeout	486 Busy Here	Y
487 Request Terminated	486 Busy Here	Y
500 Server Internal Error	486 Busy Here	Y
503 Service Unavailable	486 Busy Here	Y
504 Server Timeout	486 Busy Here	Y
600 Busy Everywhere	486 Busy Here	Y
603 Decline	486 Busy Here	Y
Any other response (including 404 Not Found and 200 OK)	Received response (that is no mapping is done)	N

Table 37: Mapping of received Error Responses by the Messaging Server

- To reduce the complexity at protocol level and avoid potential TCP switchover, it is recommended to limit the maximum size of a chat message to avoid the SIP INVITE request to be longer than the path MTU (e.g., 1300 bytes) and, consequently, trigger the TCP switchover. This maximum size is controlled through the MaxSize1To1 configuration parameter defined in Table 52 in section A.1.3.3 and applies to both the first message in the INVITE and to messages sent via MSRP. If the user attempts to send a first or subsequent chat message larger than this limit (all headers and wrappers of the corresponding SIP INVITE request and the included CPIM body are included in the count), then the user shall be notified that the message is too large.

3.3.4.2.1 *Clarifications on Chat race conditions*

- Two simultaneous invites. Though unlikely, it may be possible that two users decide to invite each other simultaneously for a chat. In this situation the behaviour of the clients should be the following:
  - User A sends an invite to User B for Chat
  - Before a final response for that invite is received, User A receives an invite from User B for Chat
  - User A will send a 486 BUSY HERE response to User B. In addition to this, User A will send the correspondent delivery and read notification using SIP MESSAGE.
  - From the UX point of view, the message sent by B will be displayed as received.
  - User B will behave as user A, potentially resulting in both session invitations being turned down with a SIP 486 BUSY HERE response. Users will have to retry session setup until successful.
- New invite sent after a previous invite has been accepted. Though unlikely, the following scenario can take place:
  - User A sends an invite for chat to User B
  - User B accepts the chat a 200 OK response is sent back to User A
  - In parallel and before receiving the 200 OK response, User A sends a new invite with a new message
- To resolve the race condition:
  - When User B receives the new invitation, it should terminate the current MSRP session (if established) by sending a SIP BYE
  - Once the initial session is terminated, a new 200 OK response should be issued which will trigger the establishment of a new MSRP session.

For additional clarification, explanatory diagrams have been included in Annex B, sections B.1.9 and B.1.10.

3.3.4.3 Technical Realization of 1-to-1 Chat features when using OMA CPM

At a technical level the Chat service implemented using OMA CPM extends the concepts from section 3.3.4.1 with the following concepts:

- It is an UNI implementation to include the first chat message in the CPIM/IMDN wrapper of the SIP INVITE request through the setting of the FIRST_MSG_IN_INVITE configuration parameter in Annex A. The RCS 5.0 NNI shall follow the OMA CPM v1.0 standards, which does not carry user message in the SIP INVITE.
- If a Service Provider expects that the first chat message be sent after the session is established, the configuration parameter FIRST MSG IN INVITE in Annex A is set to disabled.
  Please note that this is the recommended approach when using OMA CPM as this secures compatibility to the existing standards.
- If a Service Provider expects that the first message be in a CPIM/IMDN wrapper of the SIP INVITE request, the configuration parameter FIRST_MSG_IN_INVITE in Annex A is set to enabled.
- If auto-accept is not used, then the devices send a SIP 180 response toward A.
- When users are allowed to have multiple devices and those devices are configured to auto-accept (IM SESSION AUTO ACCEPT set to 1, as defined in section A.1.3.3), the Messaging Server is required to be able to fork the incoming 1-to-1 Chat session request to each of the receiving user's devices to set up an MSRP session with each of them.
- The receiving clients (or their Participating Function on their behalf) each send a 486 BUSY HERE response to the outstanding INVITE request when a new INVITE request arrives from the same user so there is not more than one outstanding INVITE request from one user.
- If multimedia content within a Chat session is a requirement the configuration parameter MULTIMEDIA IN CHAT in Annex A section A.1.3.3 is set to enabled. Therefore in the SDP of the SIP INVITE request and response, the *a=accept-wrapped-types* attribute shall only include either *, or a complete list of all content types supported during the Chat session, e.g., *a=accept-wrapped-types:**.
  Note that if the SIP INVITE is allowed to carry the first chat message, that message should not be multimedia content, and if it is, File Transfer should be used.
- If multimedia content within a Chat session is not a requirement, the configuration parameter MULTIMEDIA IN CHAT in Annex A is set to disabled. Therefore in the SDP of the SIP INVITE request and response, the *a=accept-wrapped-types* attribute shall only include text/plain, i.e., *a=accept-wrapped-types:text/plain*. To transfer multimedia content during a chat, File Transfer is used.
- When one of User B's devices detects user activity relevant to the consumption of Chat session invitation (e.g. click on a pop-up to go to the Chat window) a 1-to-1 chat session is established according to the following possible criteria:
  a) The respective client returns a 200 OK response, signalling the initiation of the remaining procedures to establish the chat when User B reacts to the notification by opening the chat window. This is the default criteria for RCS 5.0 and, consequently, all the diagrams shown in this document reflect this behaviour.
  b) The 200 OK response is sent when User B starts to type a message, or
  c) The 200 OK response is sent when User B sends a message. User B’s message is buffered in the client until the MSRP session is successfully established.

d) The 200 OK response is sent immediately if the devices receiving the invitation are configured to auto-accept[22] the session invitations (IM SESSION AUTO ACCEPT configuration parameter defined in Table 52 in section A.1.3.3).

Please note that the behaviour for criteria a), b) and c) is configured via the IM SESSION START parameter as defined in Annex A section A.1.3.3. The behaviour for criteria d) is configured via the IM SESSION AUTO ACCEPT configuration parameter defined in Table 52 in section A.1.3.3.

3.3.5 NNI and IOT considerations

3.3.5.1 Chat session interworking when one side carries a message in the INVITE request

Interworking from a Chat session with a chat message in the INVITE request to a Chat session where the INVITE request does not carry any chat message requires that the Messaging Server (or a separate network entity) performing the interworking store the message in the INVITE until the Chat session without first message in INVITE is set up. If multiple Chat session INVITEs with chat messages arrive before the Chat session on the other side is set up, multiple chat messages are stored, however it is recommended that the Messaging Server automatically accept the session on behalf of a user in a network not supporting first message in the INVITE request. If no Chat session is set up on the other side, the chat messages are kept and delivery is attempted at a later time in the same way as already specified when chat messages are stored on the originating side.

Interworking from a Chat session without first message in INVITE to a Chat session with a message in the INVITE requires that the Messaging Server accept the Chat session without any message on behalf of the recipient user and once the first chat message is received via MSRP, initiate an INVITE towards the recipient, including the first chat message as a CPIM body in the INVITE. Providing the recipient, or the recipient's Messaging Server on behalf of the recipient, does not set up a session, the Messaging Server performing the interworking continues to generate INVITEs towards the recipient for each new chat message received.

See the flows in Annex B for more information.

3.3.5.2 Interworking between a Chat session not allowing multimedia content and a Chat session allowing multimedia content

To allow interworking between a Chat session not allowing multimedia content as in section 3.3.4.1, and a Chat session allowing multimedia content as in section 3.3.4.2, SDP negotiation of the types of media and wrapped media allowed in the Chat session shall be used as specified in [RFC4975], and shall be respected by the devices and other endpoints involved in the session.

This occurs in NNI situations when one user is served by a network supporting multimedia content in Chat sessions and another user is served by a network supporting text only in Chat sessions. A Messaging Server where only text is allowed in Chat sessions shall ensure that the *a=accept-wrapped-types* attribute in the SDP used to negotiate use of MSRP only contains the *text/plain* content-type.

See the flows in Annex B for more information.

3.3.5.3 SIMPLE IM session and CPM session interworking of feature tags

The mapping of the appropriate SIMPLE IM session feature tags is done as per Appendix G in [RCS5-CPM-CONVFUNC-ENDORS] when it is determined that the remote network requires such interworking. Also once a session is set up with the recipient, the Messaging

[22] Note that the Service Provider multidevice policy has to be consistent with Chat auto-acceptance policy.

Server or a separate network entity performing the interworking ensures that messages exchanged via MSRP are sent end to end.

See the flows in Annex B for more information.

3.3.6 Implementation guidelines and examples

Please note that where the specification describes the user interface, it should be taken as guidance.

3.3.6.1 General

End to end flows for store and forward 1-to-1 chat with notifications can be found in Annex B.

The following sections show the relevant chat message flows and reference user experience. Please note that the following assumptions have been made:

- For simplicity, the internal mobile network interactions are omitted in the diagrams shown in the following sections.
- Each Service Provider may deploy a Messaging Server (that is the use of a Messaging Server is optional in RCS deployments), to manage all messages from its customers.
- Prior to the chat, the user will have accessed their address book or Chat application to start the communication. As described previously, while these actions are performed an OPTIONS or Presence request is sent to verify the available capabilities. In the following diagrams it is assumed that this exchange (OPTIONS/Presence request and response) has already taken place, and therefore, both ends are aware of the capabilities and the available RCS services of the other side. If that is not the case, the OPTIONS (or Presence) request should be sent at the same time the chat is being set up.

Service Provider support of the store and forward functionality is optional in RCS. To allow a Service Provider to provide store and forward functionality to its customers even in cases where the Chat session is established towards a user of a Service Provider that does not support store and forward, the messages can optionally be stored and forwarded from the sender’s Messaging Server, based on operator's policy.

If the Network-based Common Message Store is available, the device should synchronize with the Network-based Common Message Store when a user is about to initiate a chat with another user. Note, however, that this may not be desirable in roaming scenarios.

3.3.6.2 Entry points to the chat service

From the UX perspective there are three possible entry points to this service:

1. <u>Address book/Call-log</u>: chat can be initiated to any RCS contact with Chat capability as described in section 2.6.

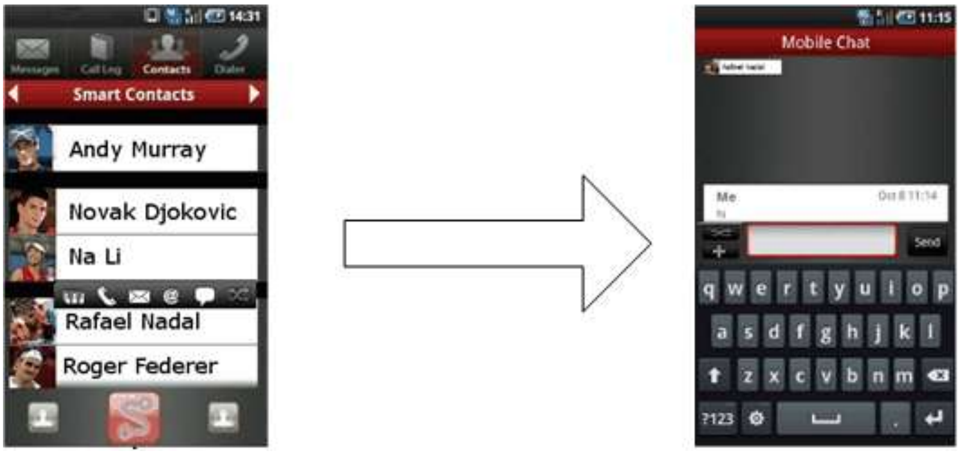


Figure 35: Reference UX for accessing chat from address book/call-log

2. Chat application: There should be a dedicated Chat application entry point in the device menu – task oriented initiation. This application will provide access to the chat history and gives the possibility to start a new chat.

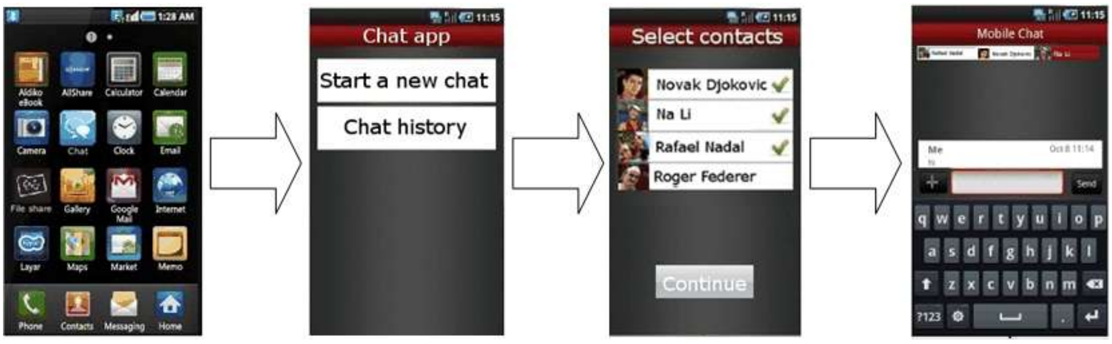


Figure 36: Reference UX for starting a chat from the Chat application

Once the Chat application is opened, the user is presented with the complete list of RCS contacts with Chat capability. Whether or not contacts which are currently not registered are shown depends on the Chat store and forward policy chosen by the Service Provider.

In addition to the “start a new chat” functionality, the Chat application allows the user to browse the Chat History, both 1-to-1 and Group Chat sessions:

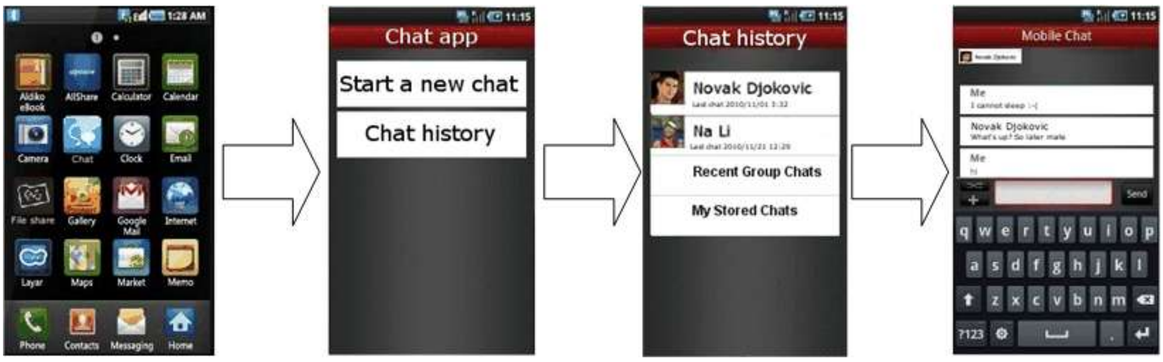


Figure 37: Reference UX for starting chat from the Chat application history

In this case, when the chat is started the last messages exchanged with that contact (or group of contacts) are shown even though the conversation might have been from another device. In the chat history the user can also browse through chat sessions that he has selected for permanent storage (if the message storage feature is available for the user) and start a conversation from those. The context of the past chat is not relayed to the other party/parties.

3. File Transfer (receiver): When transferring a file and with the aim of establishing a communication context for the transfer (the receiver may want to know for instance why the sender is sharing that file), after the transfer has been accepted the file transfer is presented to the receiver as a chat UX with a file being transferred. Please note that at the time the File Transfer request is presented, the chat session is not started; the chat session will only start when/if the receiver sends a chat message back to the sender.

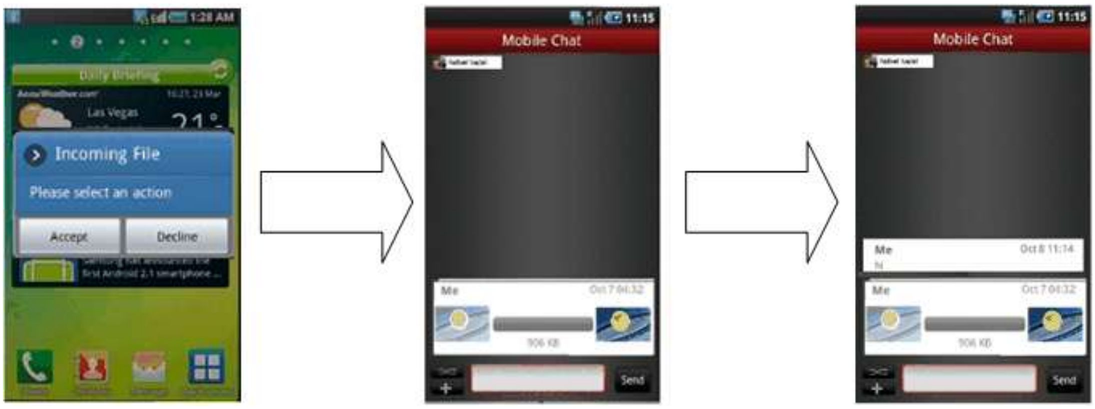


Figure 38: Reference UX for File Transfer on the receiver side

Please note section 3.5 covers the RCS File Transfer service in detail.

3.3.6.3 Initiating a chat

RCS User A initiates a chat by selecting one of his contacts User B from the Address Book, Contact List or Chat application in one of his devices.

The device of User A determines whether User B is available to use the Chat service at that time, using one of the methods in section 2.6.

If User B is not available and there is no Chat store and forward Server on User A's side nor on User B's side, or no chat interworking to SMS/MMS, or if an answer to the query is not received in less than a time lapse (left to OEM User Experience criteria), then the contact is shown as 'Not available for a Chat session', and the SMS/MMS service or CPM Standalone Messaging service could be offered as a messaging option. Once the availability of the chat service is ensured end-to-end and User A performs the appropriate UI actions on the device, a message composer and an empty chat window are opened.

When User A types the first message and presses the "Send" button, device A will initiate a Chat session invitation toward B (for the multidevice scenario see multidevice handling in section 3.3.4.1.6).

The one or more devices of User B receiving a Chat session invitation, may either all be configured to auto-accept the invitation, or the devices may wait for user action before accepting the invitation. If a spam filter or a black list is implemented on any one of User B's receiving devices and User A is in the black list, the invitation is terminated following the procedure described in section 3.3.4.1.1.

On the User B side, a notification (UI dependent) is displayed on each receiving device to inform the user about the incoming message. The user is able to read the message and go to the chat window to answer the message on the device of his choice.

User A can type additional messages before the chat is answered, that is before the Chat session is established. On User B's side, a notification may be displayed for each received message (UI dependent). The sender's device may buffer the messages if the device is configured to wait for a Chat session to be set up before sending messages.

3.3.6.4 Answering a chat

There may or may not be an explicit acceptance of the user to answer a chat.

3.3.6.5 Messages exchanged in an established chat

Providing a Chat session is established, messages are exchanged between User A and User B. A delivery notification is requested for each message and a display notification is optionally requested.

The recommendation is to show the information received in the delivery and display notifications only within the Chat window without the need for a pop-up or information message when the user is outside of the Chat application.

3.3.6.6 Message display and message storage

All messages are stored in the participating devices, together with a time indication and an appropriate indication of the sender and the receiver of each message.

When a Network-based Common Message Store is available for the user, the messages are synchronized with the Message Store as specified in [RCS5-CPM-MSGSTOR-ENDORS].

When the storage limit is reached, deletion might occur on a first in/first out (FIFO) queue policy. It is open to OEM criteria how to implement other opt-in deletion mechanisms (e.g., ask always, delete always, delete any conversation/message from specific contacts, etc.).

3.3.6.7 Leaving the chat composing window

Once a 1-to-1 chat is established any of the two users can leave the composing window without closing the chat. For example, a user could move to his mobile home screen to check an incoming email, or make a phone call.

While the chat composing window is not shown (that is, it is not the foreground window) any incoming message belonging to that chat will trigger a status notification (UI dependent) so the user is aware of the new message and, may return to the chat composing window to answer it.

Also, the user could decide to return to the chat composing window and send a new message without receiving one. The user would be able to achieve this via the Chat application, which will display the ongoing chats, or via the Address Book by clicking on the contact with whom he is involved in the chat session.

In both cases, when the user returns to the chat composing window, all the messages are displayed.

3.3.6.8 'IsComposing' notification

When a user starts typing in the chat composition window and privacy settings allow it, an 'IsComposing' notification is sent to the other user. That user's UI will then display an indication in the chat composing window to indicate it (UI dependent).

The recommendation is to show the information received in the 'IsComposing' notification only within the Chat window without the need for a pop-up or information message when the user is outside of the Chat application.

The 'IsComposing' indication is removed from the UI when a new message is received, when a timeout occurs without receiving a new message, or when a new 'IsComposing' notification arrives.

3.3.6.9 Closing a chat / Re-opening a chat

Any of the two users can close the Chat session. This can be achieved from the chat composing window or from the Chat application.

The user should be able to re-open the chat. However the resulting action at protocol level would depend on whether the Chat session is still open or not.

Closing the Chat session may not be notified to the remote user in the chat. At protocol level, the session is terminated. Therefore if the remote user sends a message, a process similar to the initiation of a Chat session is performed as described in 3.3.6.3.

3.3.6.10 Re-Opening an older chat

An old chat conversation can be re-opened. From the user perspective, it is the same procedure as for initiating a chat (see section 3.3.6.3), except that when a message is sent, a new Chat session is established.

The device will then display the previously stored conversations with that contact preceding the current active one. If any displayed notifications still need to be generated, they are sent towards the original message sender.

3.3.6.11 User experience regarding notifications when several store and forward messages arrive in a short period of time

If a user has several chat messages waiting in storage in the Messaging Server to be delivered, the UX may be impacted if many Chat message notifications appear at the sender's device when the messages are delivered to the receiver after the receiving user gets registered again.

To avoid this situation and, specifically, when receiving stored and forwarded messages, the suggested experience follows:

- Only the delivery and/or display of the first message is shown in a notification to the sending user. The remaining store and forward messages are delivered but they do not cause a notification to be shown to the message sender.
- If messages from several sending users are received, only one message notification per user containing the first delivered message per sender is shown to the recipient user.

As mentioned previously this is a suggested guide and not mandated behaviour.

Note: the described behaviour refers to notifications shown on screen to the message recipient and does not affect the behaviour with regard to the sending of delivery notifications. Those are still sent for all received messages for which such a notification was requested.

3.4 Group Chat

3.4.1 Feature description

The Group Chat service enables users to exchange messages between many users instantly.

The following RCS features are described:

- Interworking of participants in a Group Chat to SMS/MMS
  This feature requires a Messaging Server to interwork the messages for participants without an RCS device to and from SMS or MMS.
- "Delivered" message disposition
  This allows the sender of a message to be notified when a message has been delivered to the recipient.
- "Displayed" message disposition
  This allows the sender of a message to be notified when a message has been displayed on one of the recipient's devices. Note that this notification cannot certify that the recipient has actually read the message. It can only indicate that the message has been displayed on the recipient's terminal User Interface (UI).
- Delivery of notifications (delivered and displayed) inside a Group Chat
  Notifications are delivered only within the Group Chat.

- IsComposing indications
  This allows a user in a Group Chat conversation to see when another user is typing a new message/reaction.
- Local Black List
  The terminal/client may support a locally stored Black List to handle incoming Group Chat requests. Users are allowed to qualify undesired incoming Group Chat requests as spam. This prevents subsequent messages from those originators to be shown or even notified to the user. Also, this undesired traffic will not be acknowledged to have been read. The Black List behaviour applies not only to Group Chat but also to Chat and to File Transfer.
- Local Conversation History
  The terminal/client supports a locally stored conversation.
- User Alias (Display Name)
  A user defined display name can be sent when initiating a communication with another user.

A Group Chat can only be started by a user belonging to a Service Provider which has deployed a Messaging Server.

When a Service Provider has deployed a Messaging Server the OMA SIMPLE IM configuration parameter CONF-FCTY-URI (see Table 52 in Annex A) should be correctly set. The CONF-FCTY-URI is used by the device for initiating a normal ad-hoc Group Chat.

It is optional for a Service Provider to provide the Group Chat functionality, so from the terminal perspective, if there is no CONF-FCTY-URI configured, the terminal should not allow the user to add additional parties to the a 1-to-1 chat or to start a Group Chat. Please note that even if the feature of starting a Group Chat is not available in this scenario, it does not restrict the possibility to join a Group Chat session. Therefore, the device should support both the 1-to-1 and Group Chat experiences including those users without a configured CONF-FCTY-URI.

If starting this Group Chat would have increased the number of concurrent chat sessions above the Service Provider configured maximum limit (see MAX CONCURRENT SESSIONS in Annex A), the device would close one of the other active chat sessions (for example, the chat that has not been used for the longest period of time) before initiating this new one.

3.4.2 Interaction with other RCS features

Interaction of Group Chat with other RCS features is described in section 3.3.2.

If the user wishes to transfer a file to Group Chat participants, the user’s device must do this by sending the file one by one to each Group Chat participant, and it may or may not appear in the Group Chat window.

3.4.3 High Level Requirements

The following list of high level requirements applies to Group Chat:

- Client devices:

3-4-1 "Delivered" notification request and response

3-4-2 "Displayed" notification request and response
Note that the client device should allow the user to enable or disable the displayed notifications request and response

3-4-3 Delivery of notifications (delivered and displayed) outside a session

3-4-4 IsComposing indications

- Messaging Server: In addition to the above requirements:

3-4-5 Interworking of Group Chat to SMS/MMS

3.4.4 Technical Realization

Group Chat technical realization is based on the “Ad-Hoc Session Mode messaging” as described in [RCS5-SIMPLEIM-ENDORS] and in [RCS5-CPM-CONVFUNC-ENDORS], (depending on the setting for CHAT MESSAGING TECHNOLOGY defined in Table 52 in Annex A).

Support for delivery and display notifications within a Group Chat is added to the functionality endorsed in [RCS5-SIMPLEIM-ENDORS] and [RCS5-CPM-CONVFUNC-ENDORS]. For OMA CPM, also the functionality to support sending “IsComposing” messages within a Group Chat is added.

3.4.4.1 Technical Realization of Group Chat with Delivery and Display Notifications

3.4.4.1.1 *Initiating a Group Chat*

User A initiates a chat by selecting some of his contacts (Users B, C and so on, up to a limit set by the OMA SIMPLE IM parameter MAX_AD-HOC_GROUP_SIZE – see Annex A) from the Address Book or from the Chat application in his device, or from the Contact List from the Broadband Access PC client. This choice may be offered only among the contacts known by his devices to be RCS users with Chat capability. It may be offered for all contacts if a Chat interworking service to SMS/MMS is available from the Service Provider (See configuration parameter IM CAP NON RCS, in Table 52 in Annex A).

If the IM CAP NON RCS is disabled, then the device recognizes whether the Chat/Group Chat service is available for a particular contact by using the service capability exchange via Presence or OPTIONS as described in of section 2.6.

After User A types the first message or types a subject of the group chat and presses the “Send” button, device A initiates a Chat session with the Messaging Server. The Messaging Server initiates Chat sessions with the other participant users. The list of invited participants is sent in the Group Chat invitation, and is also sent out to all invited participants.

When a user’s client receives a Group Chat invitation from the Messaging Server, the user may accept or reject the invitation. Alternatively the user’s client may auto-accept[23] a Group Chat invitation, depending on a configuration parameter IM SESSION AUTO ACCEPT GROUP CHAT as defined in Annex A.

When at least one invited participant accepts the invitation, the 200 OK response is sent back to User A and the Group Chat is set up.

After acceptance the client shall subscribe to the conference event package to retrieve the list and status of the users in the Group Chat.

User A’s device shall also subscribe to the conference event package. The identity of each user shall be matched against the Contact List in the device to present a user friendly name. If a user is not found in the Contact List, the display name from the invitation received from that user should be used.

The Messaging Server will open sessions to Users A, B, C and so on, up to a configured limit which should be set to the same OMA SIMPLE IM parameter value configured in the clients, i.e. MAX_AD-HOC_GROUP_SIZE.

In the user interfaces of the receivers’ client, a notification (UI dependent) shall be displayed to inform the user about the incoming invitation. This notification should clearly state that it is an invitation to a Group Chat making the users aware of this fact.

[23] Note that the Service Provider multidevice policy has to be consistent with the Group Chat auto-acceptance policy.

3.4.4.1.2 *Adding participants to a Group Chat*

Once a Group Chat is established, the local Service Provider policy decides whether only the initiator is allowed to add participants to the Group Chat or whether any participant is allowed to add more participants. A Service Provider may choose to have a local policy that allows participants that are their own subscribers to add participants, but participants from other Service Providers would not be allowed.

In any event, participants may be added providing the general limit MAX_AD-HOC_GROUP_SIZE has not been reached or local Service Provider policy allows it.

If adding participants fails because of one of the reasons above, it is expected that the Messaging Server's error response include a Warning header and appropriate explanatory text as per the [RCS5-SIMPLEIM-ENDORS] or [RCS5-CPM-CONVFUNC-ENDORS] (depending on the setting for CHAT MESSAGING TECHNOLOGY see Table 52 in Annex A).

3.4.4.1.3 *Closing Group Chat*

Any of the participants can close their Chat session associated with an established Group Chat. This can be done from the chat composing window or in the Chat application. When a participant leaves the Chat session, his device unsubscribes from the participant information.

When User C closes their Group Chat session the other users will be notified in the chat through a predefined indication “User C has left the conversation”, and their devices will remove him from the displayed recipients. A conversation history will exist in User C's device history with the messages associated with the chat from the point they left.

A Group Chat session is closed when less than the minimum number of participants as defined in the Messaging Server, for a Group Chat remain in the Group Chat, all participants close their Chat session, or when a chat inactivity timeout expires, or based on local policy in the Messaging Server, if the originator leaves the Group Chat.

3.4.4.1.4 *Chat message size limitations*

This maximum size is controlled through the MaxSize1ToM configuration parameter defined in Annex A. Endpoints and the Messaging Server are expected to make use of the SDP attribute a=max-size to indicate the maximum message size to participants.

If the user attempts to send a message larger than this limit, the message is not sent, and the user should be informed that messages of that size cannot be sent in the conversation.

3.4.4.1.5 *Delivery and Display notifications within Group Chat*

Each message sent within a Group Chat may request a delivery notification and may request a display notification, similar to the previously described 1-to-1 chat (see section 3.3.4.1).

When a message has been delivered, the recipient client generates a delivery or display notification as described for 1-to-1 chat (see section 3.3.4.1), with the difference that the CPIM TO header shall be set to the sender of the message instead of to the unique URI assigned to the Group Chat.

This requires that the Messaging Server support Private Messages within Group Chat.

If there is no ongoing Group Chat in which to send these notifications, they shall be sent using SIP MESSAGE with Request-URI set to the sender of the original message. Note that the SIP MESSAGE may not arrive at the sending device in a multidevice scenario.

3.4.4.1.6 *Interworking to SMS/MMS*

For a Group Chat the behaviour for interworking to SMS/MMS is similar to interworking of a 1-to-1 Chat described in section 3.3.4.1.5 with the same entities being involved. The only difference being that the decision to interwork may be taken by the Controlling Function of the Messaging Server based on the same criteria used by the Participating Function for the case of a 1-to-1 session (e.g., based upon error), or by the terminating Participating Function (e.g. based upon error or Service Provider policy). Furthermore as described in [RCS5-CPM-IW-ENDORS] and [RCS5-3GPP-SMSIW-ENDORS] the IWF will subscribe to the participant information and use that information to inform the SMS or MMS user of who also is taking part in the Group Chat.

Note that messages sent during any interval that a participant becomes unavailable or loses connectivity during the Group Chat will not be available for that participant.

3.4.5 NNI and IOT considerations

3.4.5.1 SIMPLE IM Group Chat – CPM Group Chat interworking

Interworking a participant with SIMPLE IM Group Chat towards a CPM Group Chat server, and a participant with CPM Group Chat towards a SIMPLE IM Group Chat server is done as per the [RCS5-CPM-CONVFUNC-ENDORS], via mapping of the appropriate Chat session feature tags when it is determined that the remote network requires such interworking.

3.4.5.2 Messaging Server handling of delivery notifications when not supported by device

For devices (e.g. RCS-e 1.2.1) that a Messaging Server recognizes do not support generation of delivery notifications within a Group Chat, it is permitted for the Messaging Server to generate them on behalf of the devices if such notifications are requested. By what method the Messaging Server determines whether a device generates delivery notifications is outside the scope of this specification.

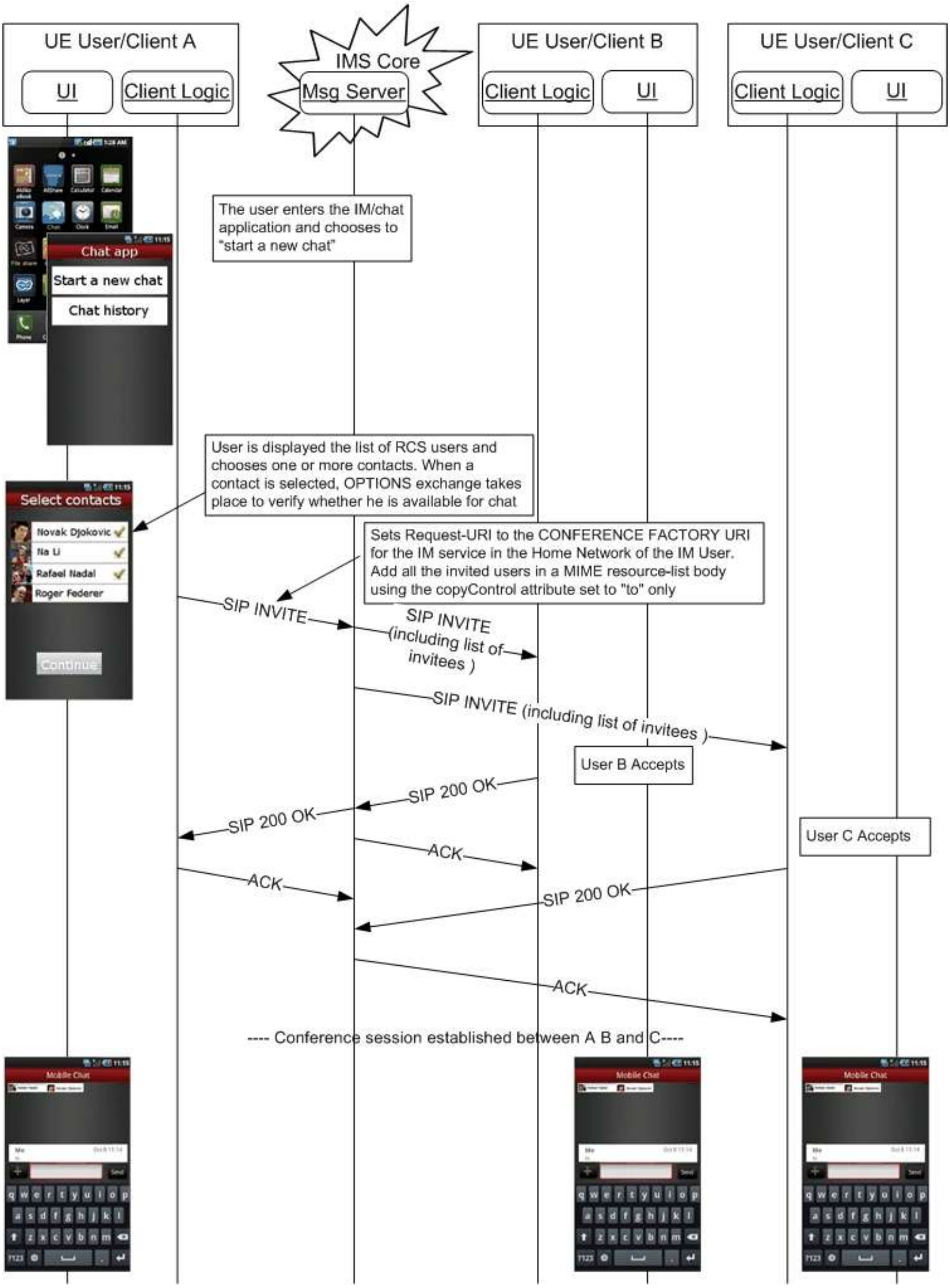
A device that does not generate delivery or display notifications is still expected to receive the CPIM IMDN header in an MSRP SEND that is used to request notifications, and to just ignore this header.

3.4.6 Implementation guidelines and examples

Please note that the following sections propose an experience which is aimed to be employed as a reference for OEM implementations.

3.4.6.1 Protocol flow diagrams

3.4.6.1.1 *Start a Group Chat from the Chat application*



The user enters the IM/chat application and chooses to "start a new chat"

User is displayed the list of RCS users and chooses one or more contacts. When a contact is selected, OPTIONS exchange takes place to verify whether he is available for chat

Sets Request-URI to the CONFERENCE FACTORY URI for the IM service in the Home Network of the IM User. Add all the invited users in a MIME resource-list body using the copyControl attribute set to "to" only

Figure 39: Start a Group Chat from the Chat application

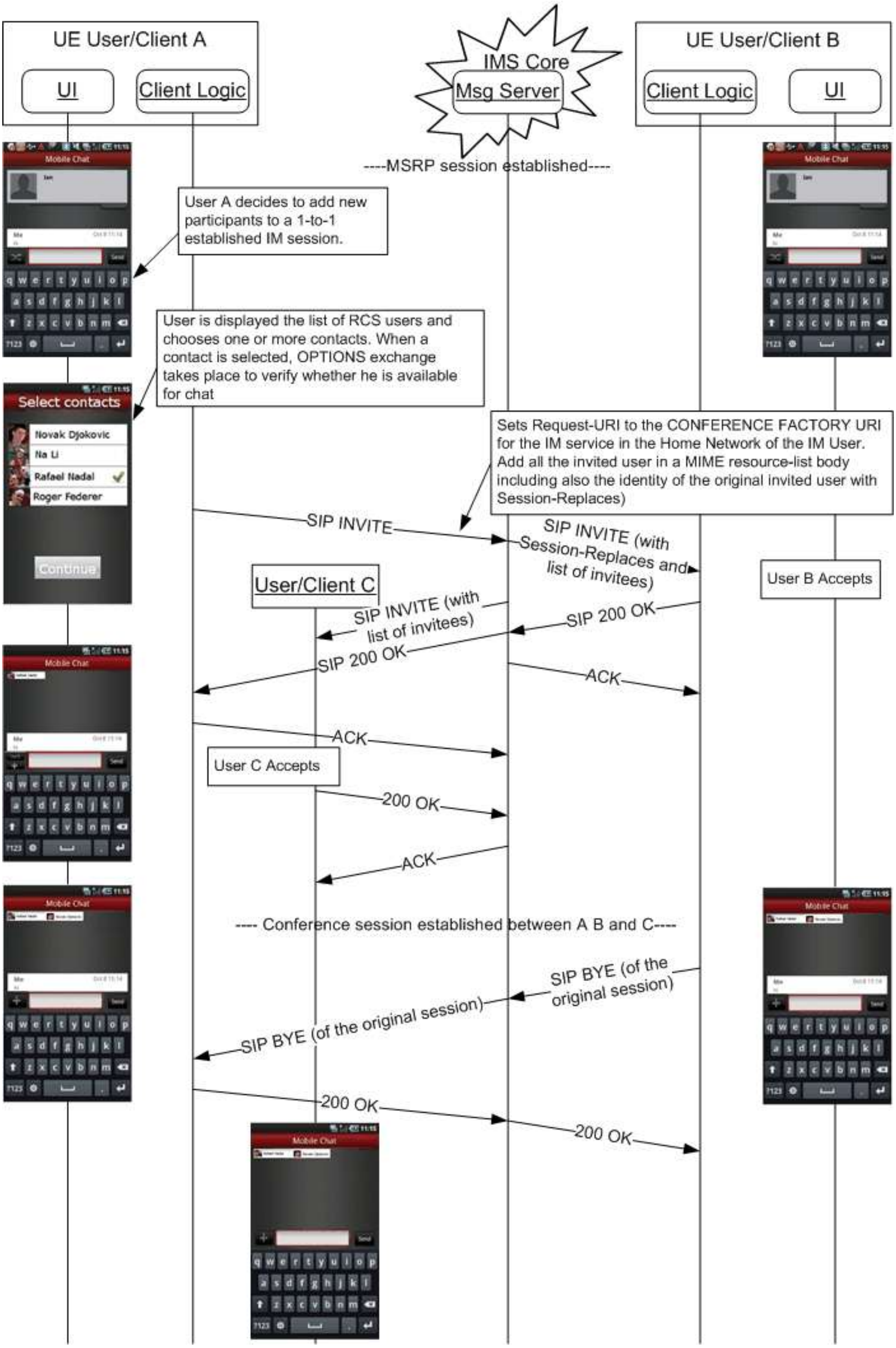
Note: The above flow mentions that OPTIONS is used for service capability exchange, which is the case when the DEFAULT_DISCOVERY_MECHANISM is set to ‘OPTIONS’. When it is set to ‘Presence’, then Presence is used.

The UX associated with an RCS Group Chat should provide the following functionality:

- Displaying the list of participants of the current Group Chat and providing of notifications when a new participant is joining and when a participant is leaving the current Group Chat
- When starting a Group Chat session, the invitation shown to the invited users should list the participants invited to the Group Chat before accepting the invitation (e.g. "You're invited to a group chat with A, B & C" instead of "A is inviting you to a group chat")

3.4.6.1.2 *Start a Group Chat from the Chat composition window*

In this case, Users A and B are in a chat, and User A decides to add a third user (User C) to the chat session. The relevant UX and flow sequence is presented below:



User A decides to add new participants to a 1-to-1 established IM session.

User is displayed the list of RCS users and chooses one or more contacts. When a contact is selected, OPTIONS exchange takes place to verify whether he is available for chat

Sets Request-URI to the CONFERENCE FACTORY URI for the IM service in the Home Network of the IM User. Add all the invited user in a MIME resource-list body including also the identity of the original invited user with Session-Replaces)

Figure 40: Group Chat session initiation

Note: The above flow mentions that OPTIONS is used for service capability exchange, which is the case when the DEFAULT_DISCOVERY_MECHANISM is set to ‘OPTIONS’. When it is set to ‘Presence’, then Presence is used. `

3.4.6.1.3 *Get participants of Group Chat*

The following flow is complementary to the previous use case as it presents in detail how to get information on the chat participants. Please note that these exchanges were omitted in the previous diagram:

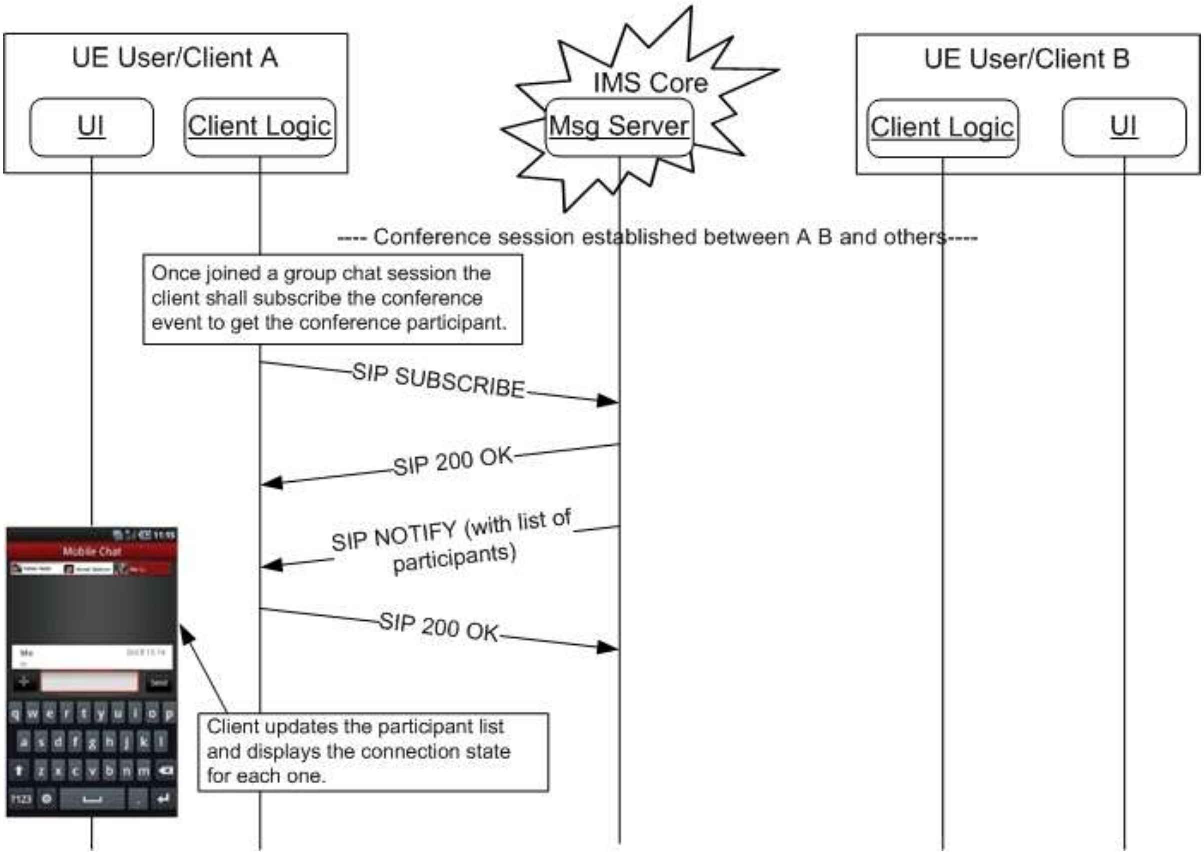

UE User/Client A
UI
Client Logic
IMS Core
Msg Server
UE User/Client B
Client Logic
UI
---- Conference session established between A B and others----
Once joined a group chat session the client shall subscribe the conference event to get the conference participant.
SIP SUBSCRIBE
SIP 200 OK
SIP NOTIFY (with list of participants)
SIP 200 OK
Client updates the participant list and displays the connection state for each one.
Mobile Chat

Figure 41: Group Chat session initiation (II): Get participants

3.4.6.1.4 *Add a participant to an already established Group Chat*

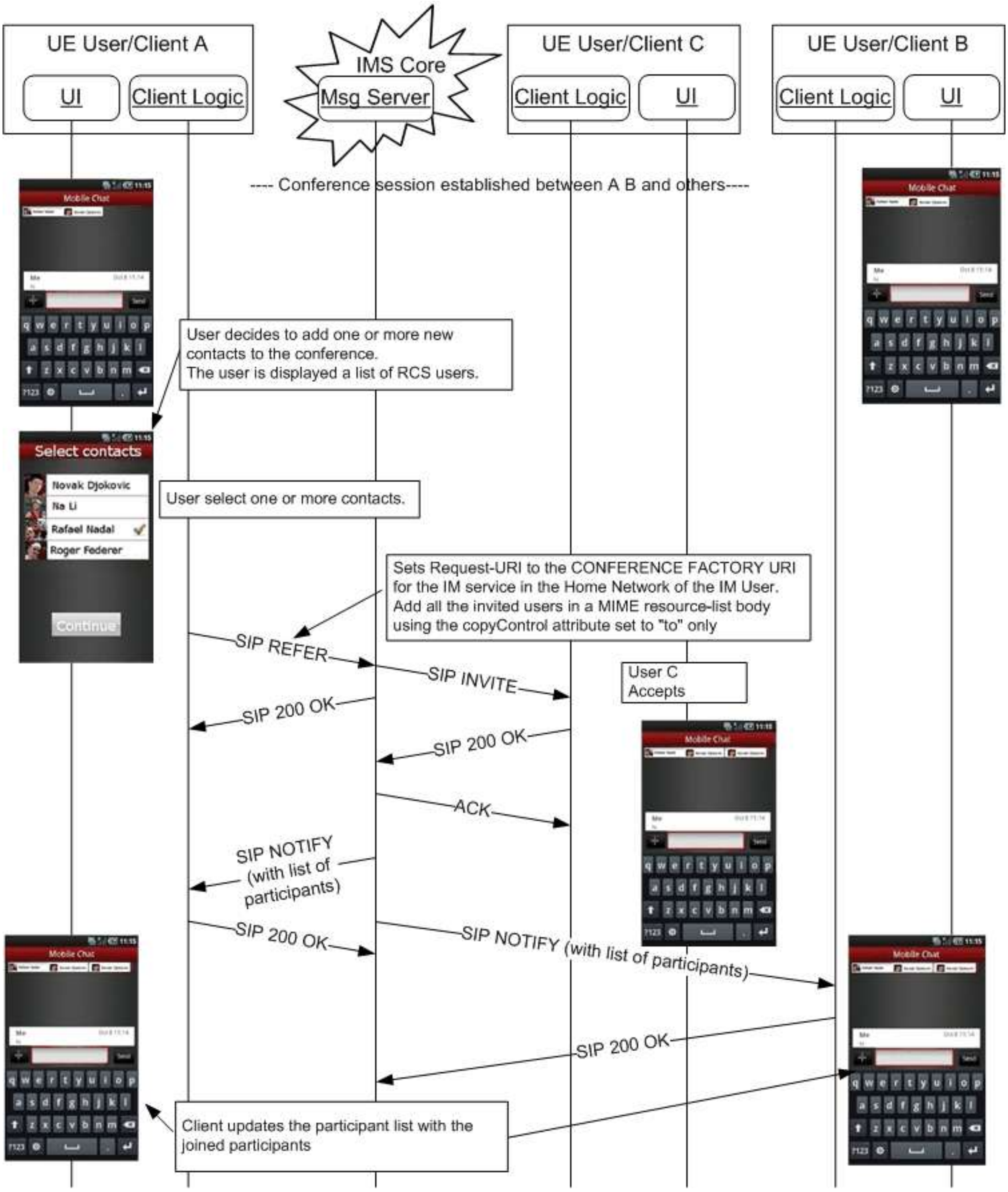

UE User/Client A
UI
Client Logic
IMS Core
Msg Server
UE User/Client C
Client Logic
UI
UE User/Client B
Client Logic
UI
---- Conference session established between A B and others----
User decides to add one or more new contacts to the conference.
The user is displayed a list of RCS users.
Select contacts
Novak Djokovic
Na Li
Rafael Nadal
Roger Federer
Continue
User select one or more contacts.
Sets Request-URI to the CONFERENCE FACTORY URI for the IM service in the Home Network of the IM User.
Add all the invited users in a MIME resource-list body using the copyControl attribute set to "to" only
SIP REFER
SIP INVITE
User C Accepts
SIP 200 OK
SIP 200 OK
ACK
SIP NOTIFY (with list of participants)
SIP 200 OK
SIP NOTIFY (with list of participants)
SIP 200 OK
Client updates the participant list with the joined participants
Mobile Chat

Figure 42: Adding new users to a Group Chat

3.4.6.1.5 *Sending a Chat message from the Group Chat window*

Note: the flow does not show Client C generating a delivery notification for the received chat message, however it is expected that Client C generate one if it was requested.

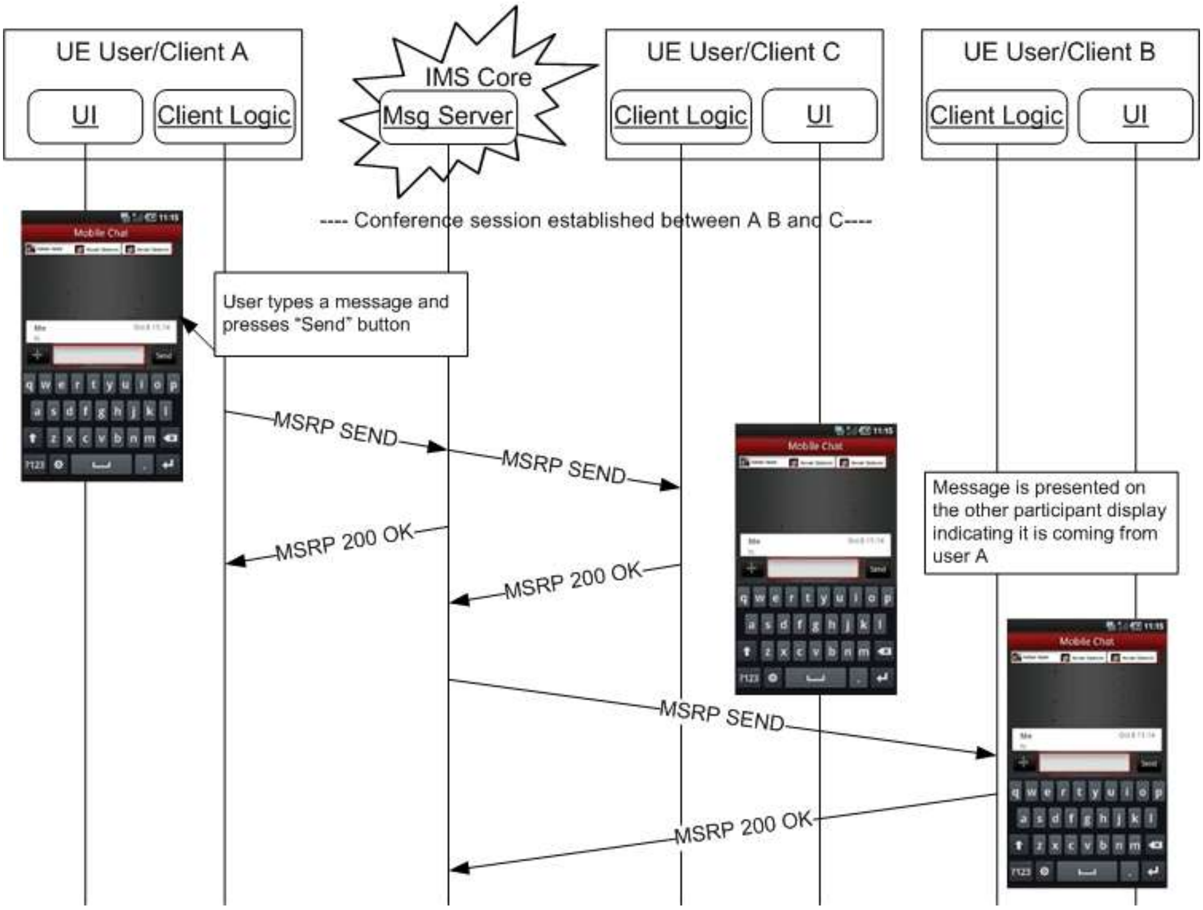

UE User/Client A
UI
Client Logic
IMS Core
Msg Server
UE User/Client C
Client Logic
UI
UE User/Client B
Client Logic
UI
---- Conference session established between A B and C----
User types a message and presses "Send" button
MSRP SEND
MSRP SEND
MSRP 200 OK
MSRP 200 OK
Message is presented on the other participant display indicating it is coming from user A
MSRP SEND
MSRP 200 OK
Mobile Chat

Figure 43: Chat message sequence for a Group Chat

3.4.6.1.6 *User in a Group Chat goes offline*

In the following flow, Users A and B are in a chat among others (Group Chat); suddenly User B goes offline (due to the loss of the connection to the network for example):

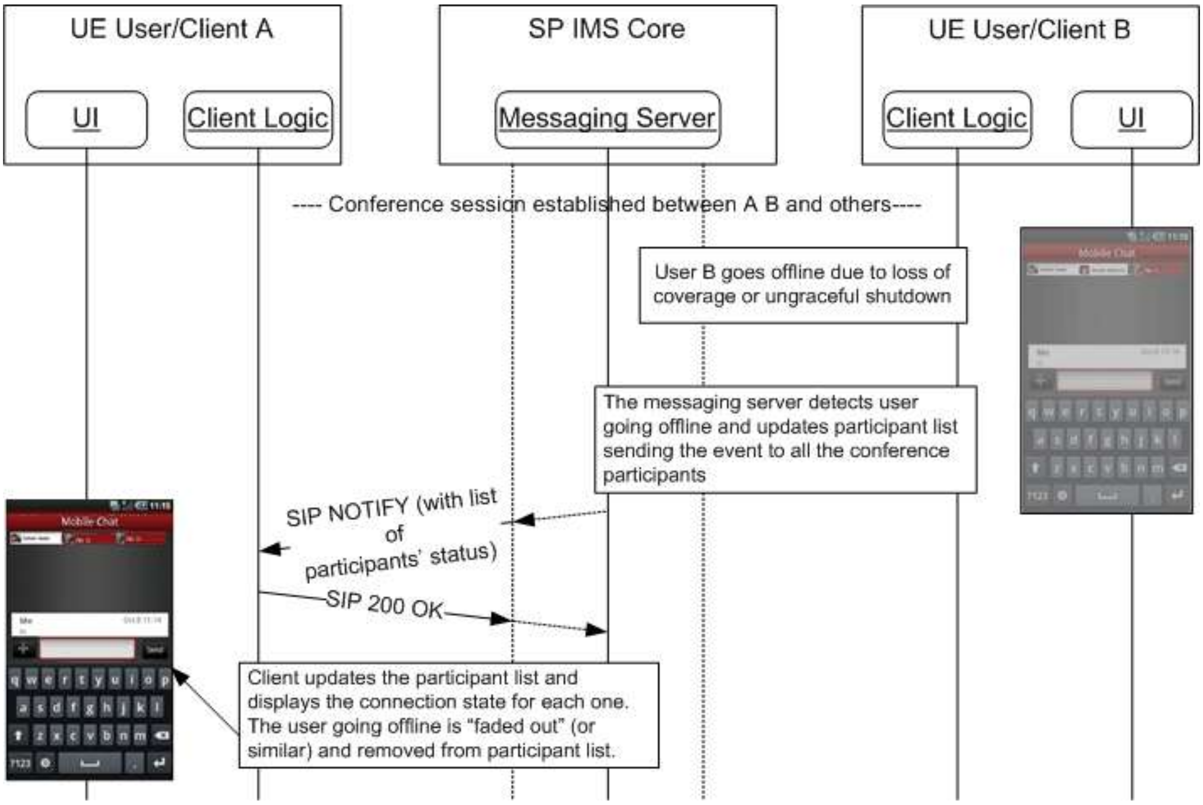

UE User/Client A
UI
Client Logic
SP IMS Core
Messaging Server
UE User/Client B
Client Logic
UI
---- Conference session established between A B and others----
User B goes offline due to loss of coverage or ungraceful shutdown
The messaging server detects user going offline and updates participant list sending the event to all the conference participants
SIP NOTIFY (with list of participants' status)
SIP 200 OK
Client updates the participant list and displays the connection state for each one. The user going offline is "faded out" (or similar) and removed from participant list.

Figure 44: Forced chat termination in a Group Chat

3.4.6.1.7 *Leaving a Group Chat*

This case is equivalent to the previous one. In this case however, User B leaves the chat intentionally:

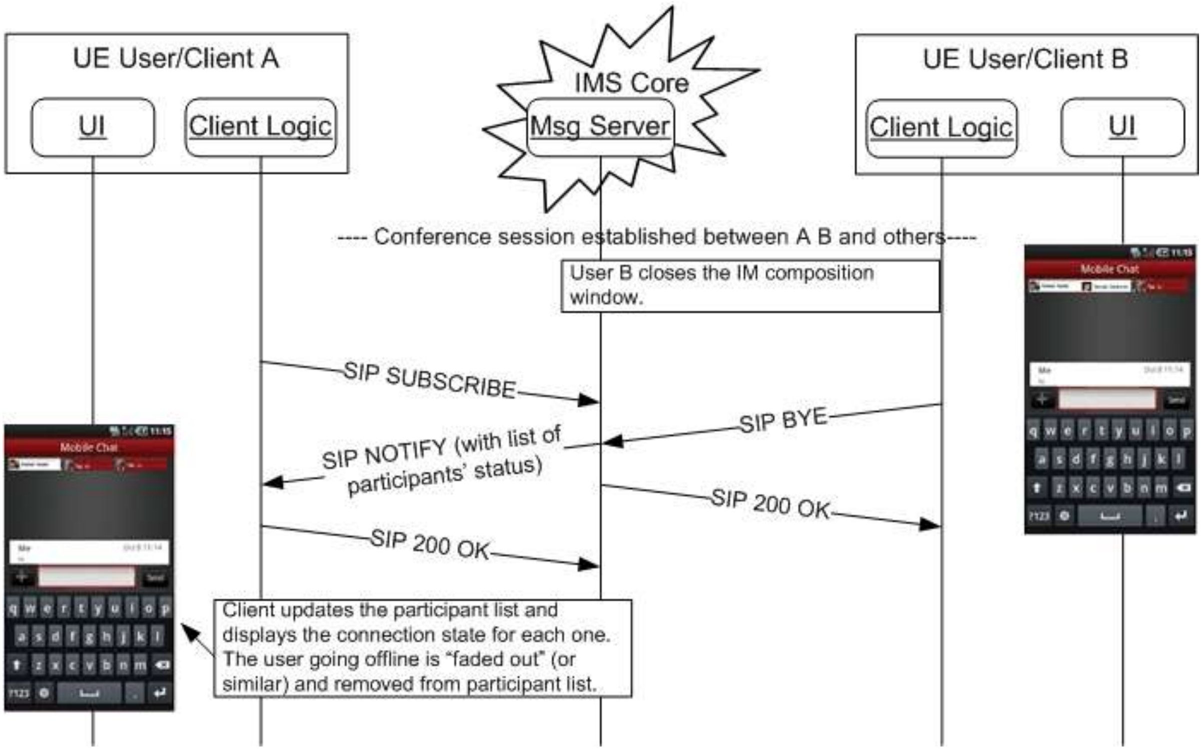

UE User/Client A
UI
Client Logic
IMS Core
Msg Server
UE User/Client B
Client Logic
UI
---- Conference session established between A B and others----
User B closes the IM composition window.
SIP SUBSCRIBE
SIP BYE
SIP NOTIFY (with list of participants' status)
SIP 200 OK
SIP 200 OK
Client updates the participant list and displays the connection state for each one. The user going offline is "faded out" (or similar) and removed from participant list.

Figure 45: Leaving a Group Chat

3.5 File Transfer

3.5.1 Feature description

File Transfer is the ability for users to exchange different types of content (files), during an ongoing session or without having an ongoing session.

This service comes with some requirements (such as bandwidth and free space on the receiver's device); therefore, even if an RCS contact is registered, it may not be possible to share files.

On the sender's side, before sending the request to the intended recipient, the file to be transferred and the recipient have to be selected (refer to use cases in section 3.5.6).

For pictures or video clips it is a significant added value if the recipient receives a preview of the proposed file before accepting or declining the transfer. Therefore, whenever possible, the sender of the file should include a thumbnail of the file in the File Transfer invitation. A client receiving a File Transfer request with a thumbnail should display the thumbnail in the pop-up presenting the File Transfer invitation.

The request for File Transfer is sent to all of the recipients' devices, and will trigger a pop-up indicating to the user that a contact wishes to send them the depicted file. The recipient is able to select the device to which the file is transferred by accepting or refusing the File Transfer invitation on that device.

Prior to the actual transfer of a file, the intended recipient is given the opportunity to learn about the proposed File Transfer (size, name, preview and type of file in addition to the identity of the sender) and then to accept or decline the File Transfer based on this information.

If a File Transfer is interrupted for any reason, the receiver can request resumption of the File Transfer without having to re-start from the beginning.

Users are allowed to qualify undesired incoming File Transfer requests as spam. To this end, clients may support a locally stored black list to handle incoming File Transfer requests. This is the same black list as it is used for incoming chat requests. If an invitation to receive a file is received from a blacklisted user, the client should reject the File Transfer request, and from the UX, not notify the user. Instead it may log the event in the spam folder (e.g. "User A tried to send a file on TIME/DATE").

The File Transfer feature has the following limitations:

- In the RCS 5.0 UNI specification, sharing files with a group of users is not considered and it is only possible between two users. Nevertheless, a device UI could allow serialization of FT to multiple users**.**
- Files cannot be stored in the network and then forwarded later, i.e., File Transfer works only between connected participants.
- Only one file can be sent per file transfer.

3.5.1.1 Handling of specific content

For some of the content exchanged during a file transfer specific handling is provided. This is described in the following subsections

3.5.1.1.1 *Card Push*

Sharing contact information brings different opportunities to RCS, all of them increasing end user contact possibilities e.g. allowing RCS Users to connect with other RCS or non-RCS Users.

Currently manufacturers are saving the contact info in their address books without following a fully open standard and, as a consequence, sharing this information effectively with other device manufacturers becomes a challenge.

Also, the concept of ‘personal’ and ‘business’ card, representing the user’s own contact information, which may be stored in the address book, is not used simply because this is not an explicit option of the address book menus of existing devices.

This specification aims to:

- Move towards a standard format compliant with all kinds of devices for keeping contact information.
- Create and manage personal and business cards and share them with selected contacts and giving this option visibility in the address book menus.
- Exchange contact information in a secure way.

RCS brings File Transfer as a new service, which becomes a very good bearer for exchanging of contact cards among users. Those contact cards can be sent to another user, like any other file format, using File Transfer.

3.5.2 Interaction with other RCS features

File Transfer is not linked to other services (for example CS-voice call or ongoing chat session) and can be used either during or outside of other communication sessions. The procedure for any file transfer within an ongoing 1-to-1 chat session is implemented as a separate session in parallel with the ongoing 1-to-1 chat and therefore is the same as the procedure for initiating a separate session for File Transfer.

Different types of content (files) can be exchanged during an ongoing session or without having an ongoing session, i.e., during or outside a call or 1-to-1 chat session.

When transferring a file while not in an existing session (that is when not in a call or chat session with the contact with whom the file is to be shared) and after the transfer has started (that is the receiving user accepted the incoming file) the file transfer is presented to the recipient in a chat context. This establishes a communication context for the transfer since the recipient may want to know why the sender is sharing the file. At the time the file is presented, the chat session is not started. The chat session will only start if and when the receiver sends a chat message back to the sender of the file transfer.

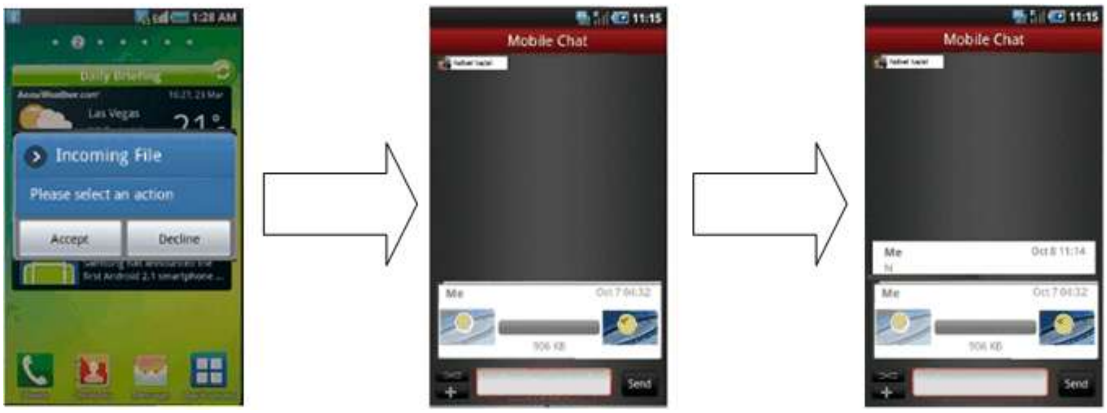


Figure 46: Reference UX for file transfer on the receiver side

When a file transfer is started during a call with the receiver of the file transfer, the file transfer continues until it is completed or cancelled, i.e., the file transfer will not be terminated when the call ends.

3.5.3 High Level Requirements

3-5-1 Files can be exchanged during a session (e.g. CS voice call or message conversation)

3-5-2 A File Transfer can be initiated by either end point while having an ongoing session (e.g. the caller or the callee)

3-5-3 End of file transfer shall not lead to termination of a simultaneous ongoing session

3-5-4 End of a voice call shall not lead to termination of ongoing file transfer

3-5-5 Files can be exchanged without having an earlier established session (e.g. directly from a multimedia gallery).

3-5-6 The receiver must be able to accept or reject offered files. The invitation procedure shall include an indication to the receiving party concerning file size and type.

3-5-7 The receiver shall have the possibility to save the transferred files.

3-5-8 It shall be possible to assign a service provider configurable maximum file size allowed for File Transfer.

3-5-9 The sending and receiving client shall be able to resume an interrupted file transfer. It is up to Service Provider policy whether only the receiving client or either client can initiate the resume request.

3-5-10 The sending client shall have the possibility to include a thumbnail preview of an offered file.

3.5.4 Technical Realization

File Transfer is based on [RCS5-SIMPLEIM-ENDORS] and [RCS5-CPM-CONVFUNC-ENDORS], as well as on the extensions described in [RFC5547]. The technology choice is controlled by the configuration parameter CHAT MESSAGING TECHNOLOGY as described in section A.1.3.3.

SIP INVITE requests for file transfers will be forked to all the recipient’s devices. If the recipient accepts the invitation on one device, the corresponding client shall respond with a 200 OK response. If they reject the session, the client shall respond with a 603 response. In both cases, the IMS network of his Service Provider will cancel the invitations to his other devices.

The extensions described in [RFC5547] are used as follows:

- The SDP payload for File Transfer requests is populated according to [RFC5547], i.e. both sending and receiving clients need to support all elements of [RFC5547]. For populating the file-selector attribute, it is preferable to use the hash-selector, in addition to the other selectors possible. The reason being that the hash-selector uniquely identifies a file, and can also be used to verify the correct transfer of the entire file. The SDP payload shall contain the file size.
- An interrupted file transfer can be resumed by the recipient sending a new SIP INVITE to the originator asking for the missing part of the file. For this it uses the file-range attribute (to denote the missing part) including the file-selector (to denote the file). Note that absence of the file-range attribute denotes transfer of the entire file.
  For such a pull-style operation, the SDP attributes, including file-range and file-selector are populated as described in [RFC5547]. Especially note that from the viewpoint of [RFC5547] this is a new file transfer and hence it will carry a new file-transfer-id attribute.
  To support multiple devices on the originating side, the file recipient should address the originating RCS UA via device identifier (sip.instance or GRUU, see section 2.11.3) to be able to resume the file transfer at a later stage. If the device identifier of the file sender is included in the initial SIP INVITE received by the file recipient, it has to be included by the file recipient in the new SIP INVITE sent to the originator. If the device-id is not included in the SIP INVITE received by the file recipient it cannot be included in

the new SIP INVITE, and the SIP INVITE will be forked to all the registered devices of the originator. In that case, any device which has stored the requested file will answer the SIP INVITE with 200 OK if accepted by the user or the RCS client.
For security reasons, an auto-acceptance of resumption requests shall only be offered in case a clear correlation between the initial file transfer and the related resumption request can be ensured by the client implementation. In case of manual acceptance, the RCS client application may notify the user that this is a file pull for sake of a resumption request (rather than an ordinary file transfer).

- Generic file pull scenarios (as described in [RFC5547]), i.e., scenarios that do not pursue on a preceding file transfer as described above, are not supported in this specification.
- In scenarios where the file sender notices that an initiated file transfer could not complete successfully, such an interrupted file transfer can also be resumed by the file sending client.
  - The procedure for resumption by the file sending client corresponds to the resumption by the file receiving client described above except for the following differences:
    - The file sending client will send a new SIP INVITE request with a file selector and a proposed file range in the SDP based on information the file sending client has upon detection of the failure condition.
    - The file receiving client will use the file selector and the file range attribute to determine it is a resume request (for this the receiving client may keep information of interrupted file transfers). The file receiving client should include the exact file range required in the SDP returned in the 200 OK on the SIP INVITE request initiating the resumption.
    - Upon reception of the SDP in the 200 OK, the file sending client shall always use the file range specified by the file receiving client for the resume operation.
  - If the file receiving client does not support resumption, the SIP INVITE for the resume will be rejected. The file sending client that initiates the resumption should not continue the resumption. Alternatively, it might then re-send the entire file.
  - For the case where the file recipient user has multiple devices, the file recipient client needs to address the correct file sending client by using the device identifier (sip.instance or GRUU) it received in the original file transfer invitation response if any as described in section 2.11.3.
  - If both clients initiate resume, the file recipient's request should be given preference since the file recipient has accurate information about the missing parts of the file. This means that in that case the file recipient client will decline the SIP INVITE request issued by the file sending client.
- A preview of an offered file can be added to the SDP description of the SIP INVITE request by using the file-icon attribute of [RFC5547]. Other SDP attributes will be populated as described in [RFC5547].
  - The procedure describing how to create the thumbnail itself, in its raw binary form, is out of scope of this specification. For a picture, the raw binary result shall be a thumbnail of the picture itself. For a video clip, the raw binary result shall be a thumbnail of the first I-Frame at 20% of the total length of the video clip.
  - The size of a thumbnail should be restricted to the minimum number of octets that provide significance.

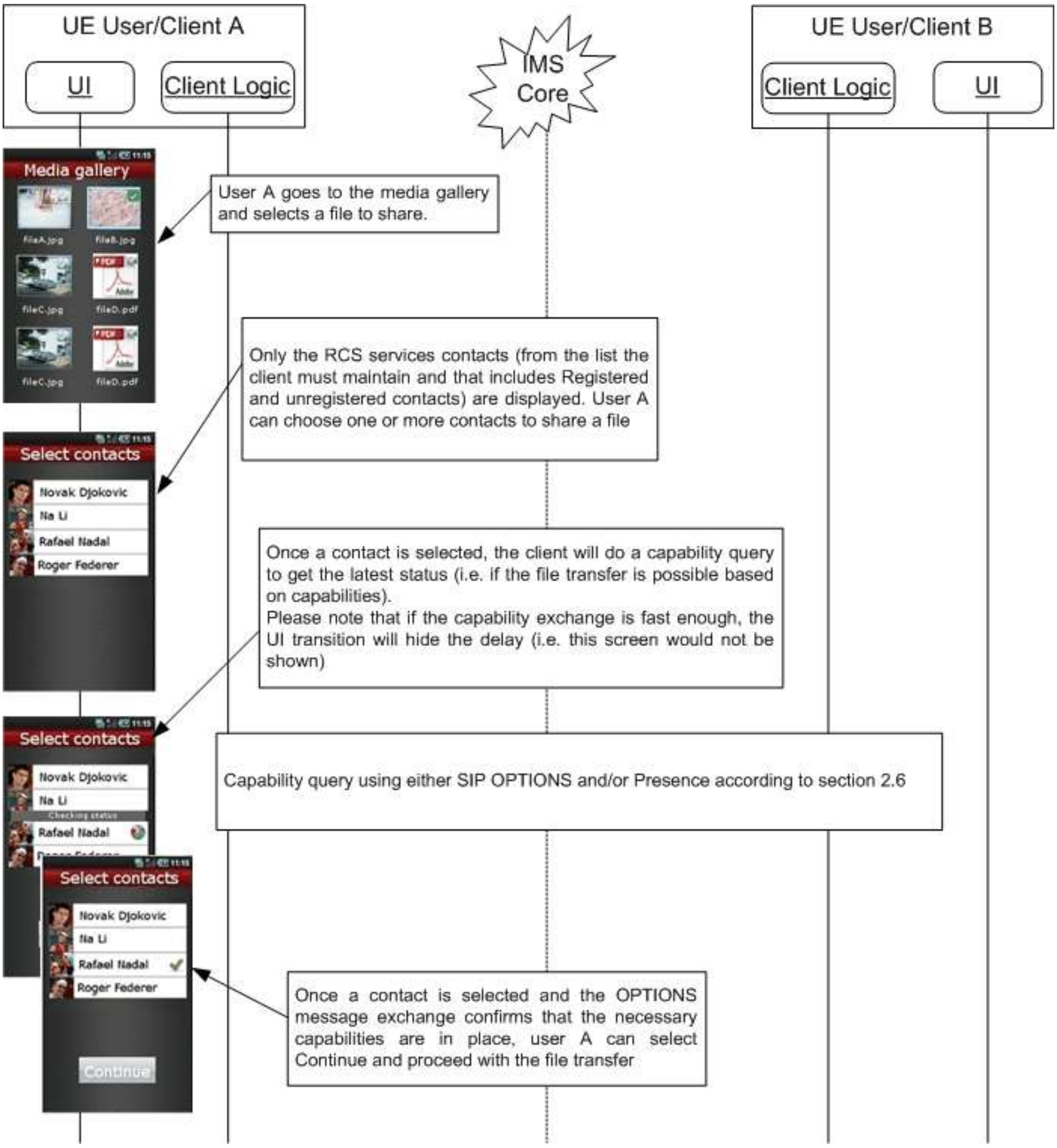
In the following sections, the relevant message flows and reference UX are shown. These are based upon the following assumptions:

- For simplicity, the internal mobile network interactions are omitted in the diagrams that are shown.
- It is assumed that by the time the file transfer begins, both the sender and the recipient have exchanged their capabilities using an OPTIONS or Presence exchange. Note that if there is a UX flow that does not show this, the assumption is that the OPTIONS or Presence requests were exchanged between the sender and the receiver (bidirectional) prior to starting the flow.

3.5.4.1 Selecting the file transfer recipient(s)

The user willing to share a file from the media gallery or file browser will to select the file and choose the user with whom the file will be shared. The list that is presented initially to the user may contain RCS contacts not currently registered. In addition, the capabilities the client has for a contact may not have been updated.

Therefore, the first step is to determine whether the file can be shared with the selected user (that is that user should be registered and the right capabilities should be in place).



User A goes to the media gallery and selects a file to share.

Only the RCS services contacts (from the list the client must maintain and that includes Registered and unregistered contacts) are displayed. User A can choose one or more contacts to share a file

Once a contact is selected, the client will do a capability query to get the latest status (i.e. if the file transfer is possible based on capabilities).
Please note that if the capability exchange is fast enough, the UI transition will hide the delay (i.e. this screen would not be shown)

Capability query using either SIP OPTIONS and/or Presence according to section 2.6

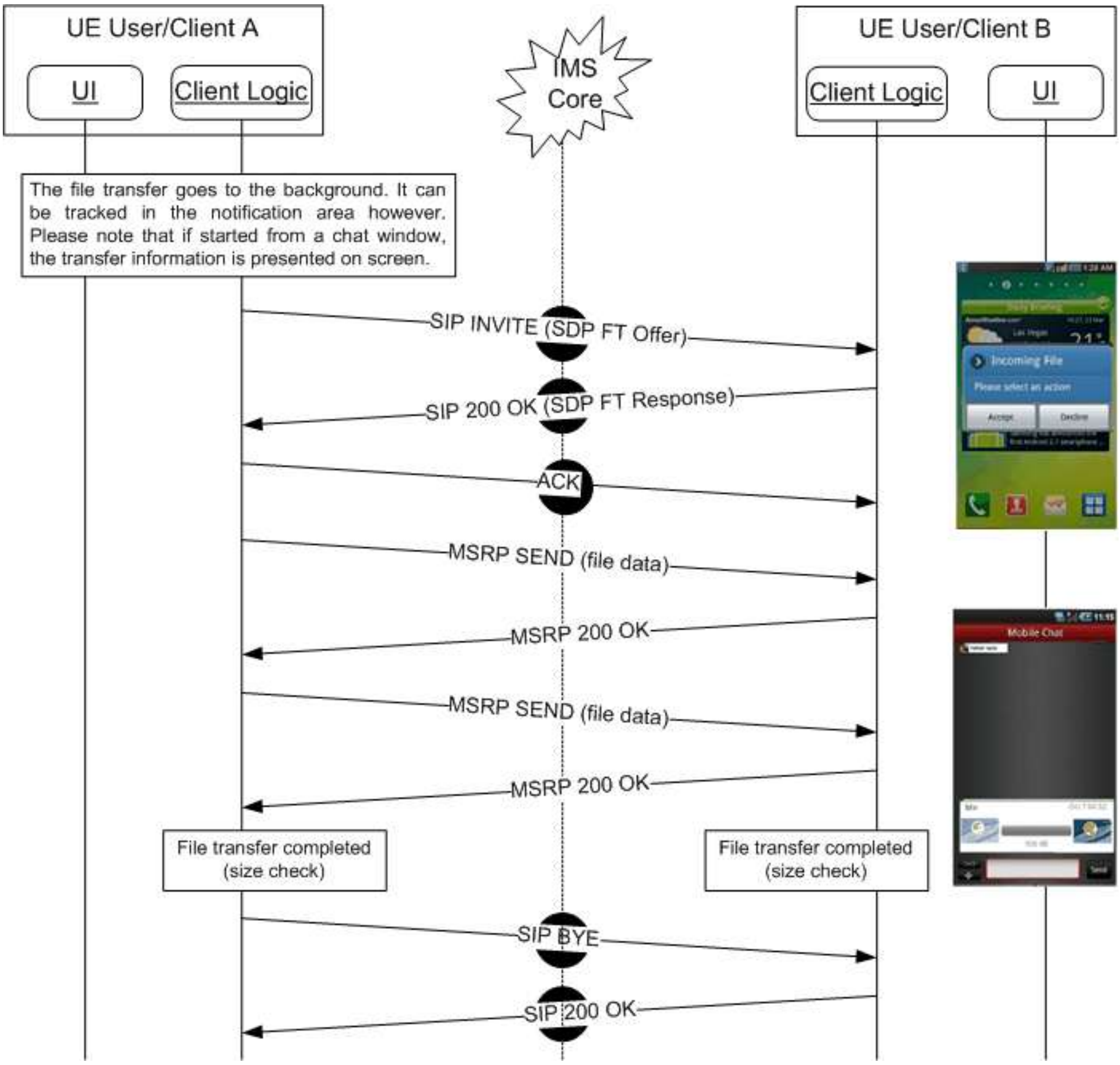
Once a contact is selected and the OPTIONS message exchange confirms that the necessary capabilities are in place, user A can select Continue and proceed with the file transfer

Figure 47: Selecting users when sharing a file from the media gallery/file browser

3.5.4.2 Standard file share procedure

Independently of the file share UX entry point, once the file and recipient are selected, the transfer can begin. If a user chooses to share several files, the individual file transfers (in each transfer only a single file is shared) are serialised by waiting for a SIP BYE before issuing the SIP INVITE request for the next file to transfer.

In the following diagram, it is assumed the receiver accepts the transfer.



The file transfer goes to the background. It can be tracked in the notification area however. Please note that if started from a chat window, the transfer information is presented on screen.

File transfer completed (size check)

File transfer completed (size check)

Figure 48: Standard file transfer sequence diagram – Successful transfer

In the following diagram, User B rejects the transfer.

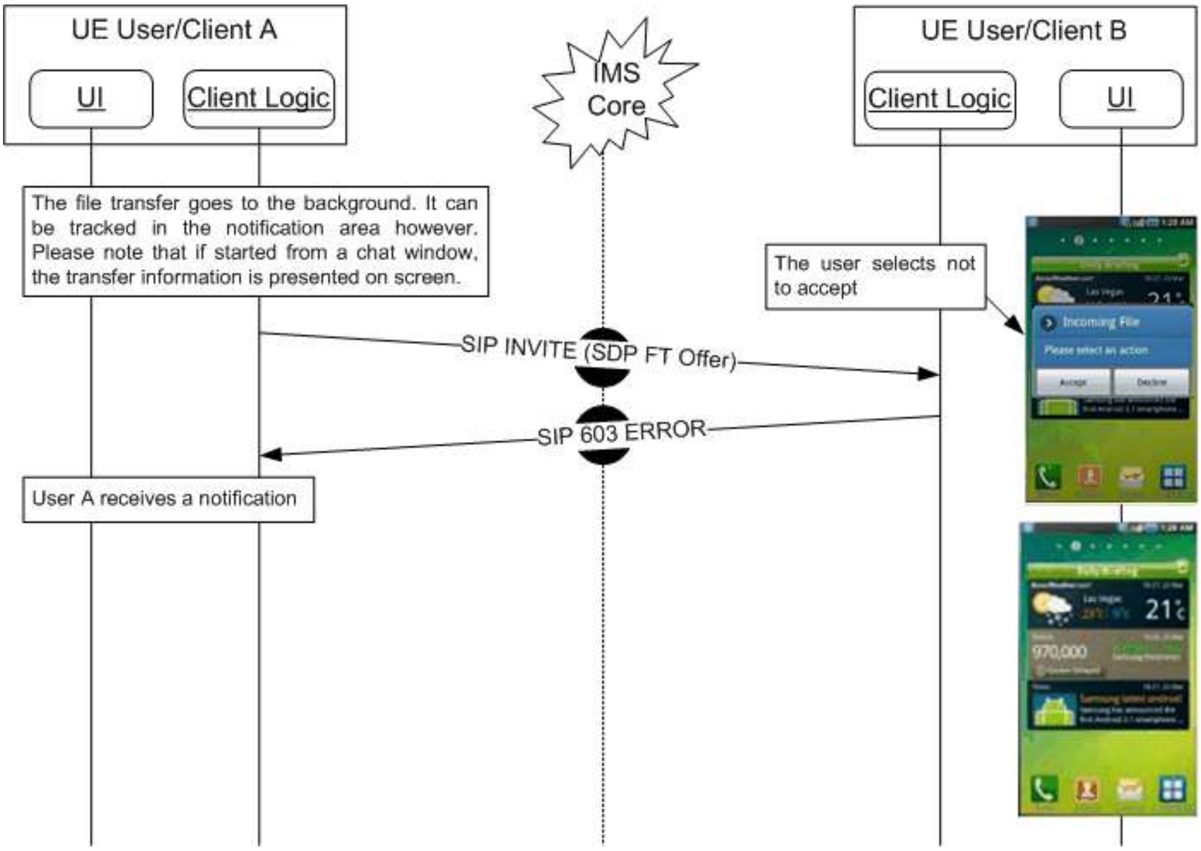

UE User/Client A
UI
Client Logic
IMS Core
UE User/Client B
Client Logic
UI
The file transfer goes to the background. It can be tracked in the notification area however. Please note that if started from a chat window, the transfer information is presented on screen.
The user selects not to accept
Incoming File
Please select an action
Accept
Decline
SIP INVITE (SDP FT Offer)
SIP 603 ERROR
User A receives a notification

Figure 49: Standard file transfer sequence diagram – Receiver rejects the transfer

3.5.4.3 File share error cases

There are several scenarios in which a file transfer can result in an error:

Either the sender or the receiver decides to cancel the operation before the transfer is completed. The relevant sequences are equivalent to the diagrams presented for image sharing during a voice call in sections 3.6.4.3.8 and 3.6.4.3.9.

Either the sender or the receiver loses the connection to the network before the transfer is completed. The relevant sequences are equivalent to those presented for image sharing during a voice call in sections 3.6.4.3.12 and 3.6.4.3.13.

When transferring larger files, the probability is higher that such a transfer would be interrupted. If such an interrupt leads to termination of the underlying MSRP session, the receiving client, knowing the overall size of the file in transfer, will become a requester of a file (as described in [RFC5547]) and sends a SIP INVITE request, specifying in the SDP payload this file (by using the file-selector as described in [RFC5547]) and the missing part of the file, using the file-range attribute.

Finally, note that if during a file transfer the capabilities of one of the ends change, the file transfer may be affected:

- If the receiver runs out of storage space, the sequence should be equivalent to that presented in section 3.6.4.3.10.
- If on one of the ends a handover into 2G (2G GPRS data coverage) occurs without losing the IP configuration, the file transfer should continue until finished.

3.5.4.4 File share and file types

In principle the RCS file transfer service comes without a limitation on the file sizes or types. This means that any kind of file can be transferred using this service. Taking this into account and with the aim of providing all the necessary facts to the receiver allowing making an informed decision on whether to accept or to reject the file, a user receiving a file transfer invitation should be informed at a minimum of:

- The size of the file: This is mainly to protect the user from unexpected charges and/or long transfers. Note: this also applies to the sender.
- The file type: In this case and to make it more intuitive, the device should present to the user whether the file which is being transferred can be handled/displayed by the device.

For example, if a user receives an invitation to receive a PDF (Portable Document Format) document and their device cannot process that document, an informative message with the size and the fact that the file type is not supported should be presented to the user prior to the user making the decision on accepting or rejecting the file transfer.

Finally note that each individual Service Provider may introduce restrictions taking into account different considerations such as security, intellectual property and so on.

3.5.4.5 File size considerations

To prevent both the abuse of the file transfer functionality and protect customers from unexpected charges, a configurable size limitation (refer to FT WARN SIZE and FT MAX SIZE in Table 53 for reference) may be enabled.

From the user experience perspective and assuming that the size limitation is in place (i.e. the values are non-zero):

- If a file transfer (send or receive) involves a file bigger than FT WARN SIZE, the terminal should warn the user of the potential associated charges and get confirmation from the user to proceed.
- If the file is bigger than FT MAX SIZE, a warning message is displayed when trying to send or receive a file larger than the mentioned limit and the transfer will be cancelled (that is at protocol level, the SIP INVITE request will never be sent or an automatic rejection response will be sent to the other end depending on the scenario).

3.5.4.6 Handling of specific content

3.5.4.6.1 *Personal Card format*

Current implementations of the vCard standard by different device manufacturers leads today to data loss of certain contact information, when this information is exchanged among devices or synced with network address books. An RCS compliant device shall support receiving at a minimum, vCard 2.1 [vCard21] and vCard 3.0 formats [RFC2425], [RFC2426] and may support also the Personal Contact Card (PCC) format [CAB_TS].

The following fields are considered key fields. No data of these fields should be lost when contact information is exchanged by any means (peer to peer contact sent, uploaded, synchronized, etc.):

- Name
- Telephone numbers
- Email addresses

The Minimum subtypes that should be supported are defined in the PCC definition in [CAB_TS]:

- Name: Composed names (such as “Jean-Baptiste”) shall be supported properly
- Telephone number: At least the following subtypes of telephone number shall be supported:
  - Land home
  - Land work

  - Land other
  - Mobile home
  - Mobile work
  - Mobile other
  - Fax work
  - Fax other
  - Beeper
  - Other
- Email addresses: The following subtypes shall be supported:
  - Email work 1
  - Email work 2
  - Email home 1
  - Email home 2
  - Other

Sending and receiving a contact card via File Transfer is technically the same as sending any other file.

If the format for pushing a contact card file is vCard 2.1 or 3.0 formats, the MIME (Multipurpose Internet Mail Extensions) type that shall be used for the file transfer is "*text/vcard*".

If the format for pushing the contact card is CAB (Converged Address Book) 1.0 PCC XML format, then the CAB PCC MIME type "*application/vnd.oma.cab-pcc+xml*" shall be used.

On the receiving side, after the receiving RCS user accepts the contact card file delivered through File Transfer, the receiving RCS client shall apply the mapping of the RCS supported fields between the received format (CAB PCC XML for example) and the used format of the local address book database[24].

vCard 3.0 format is recommended in RCS 5.0.

If the receiving side does not support the offered format identified in *the a=file-selector* attribute of the SIP INVITE SDP, it should reject the File Transfer invitation with an error response indicating it does not support the content-type, which then causes the sending side to initiate a second File Transfer, this time sending the contact card in a different format.

3.5.5 NNI and IOT considerations

In addition to what is defined in Section 2.12, the mapping of the appropriate File Transfer feature tags is done by the Messaging Server, as per Appendix G in [RCS5-CPM-CONVFUNC-ENDORS] when it is determined that the remote network requires such interworking.

3.5.6 Implementation guidelines and examples

From the UX perspective there are five possible entry points to this service:

1. Address book/Call-log: A file transfer can be initiated with any registered contact providing the correct capabilities are in place. This is contact oriented initiation.

[24] In case the conversion between PCC and vCard is required, please see [CAB_TS] section 5.4.3 "Format Adaptation".

Following the address book interaction, the list of available files is displayed allowing the user to select one or more files to share. Once the file transfer commences, the progress can be checked in the standard notification area.

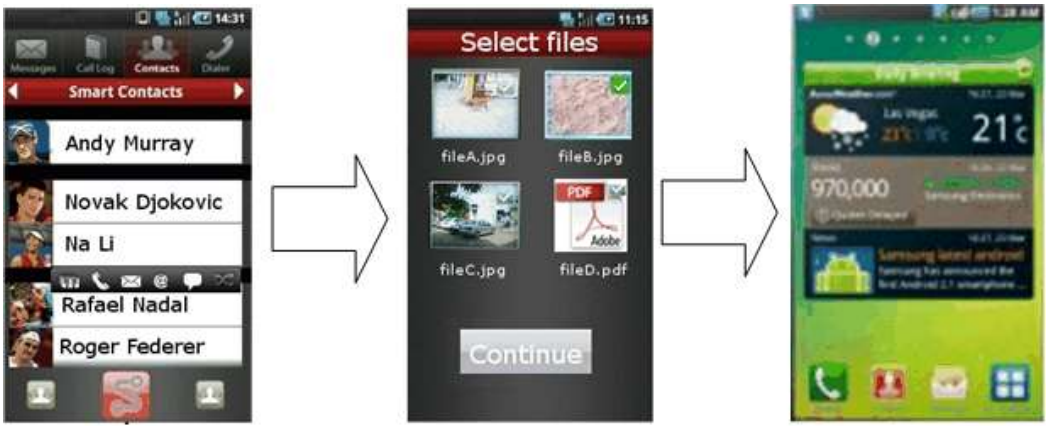


Figure 50: Reference UX for accessing file share from address book/call-log

2. Media gallery/File browser: The user can browse, select a file (or multiple files) and then share these with one or more RCS users. This is task contact oriented initiation. Only RCS capable users shall be displayed as candidate recipients of the file.

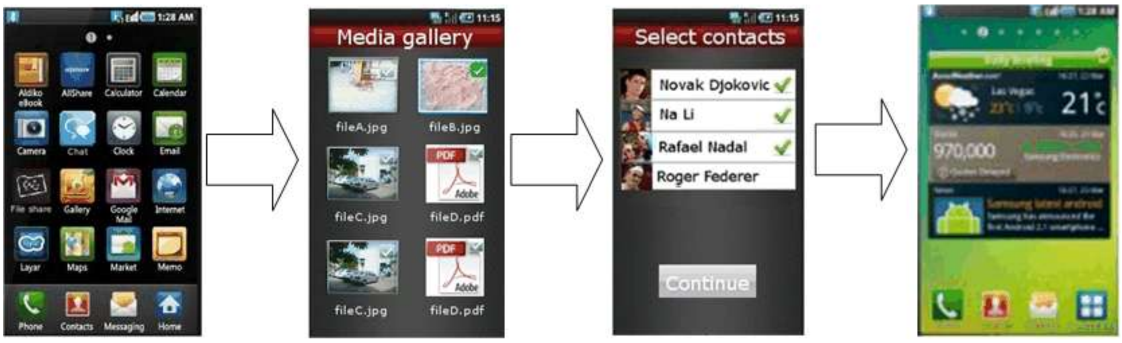


Figure 51: Reference UX for accessing file share from media gallery or file browser

In the previous figure, once File Transfer is selected, the user will be presented with the complete list of RCS contacts (including contacts which are currently not registered).

In this case, a SIP OPTIONS or Presence exchange is triggered once a contact is selected from the list.

3. Camera application: The experience is similar to the media gallery/file browser experience with the difference being that the user is able to select only the last picture or video (and, in some cases, a picture or video from the camera gallery) to be shared.
4. Chat window: From the Chat (only in one-to-one chat) window a file can be shared using the relevant button/icon. The experience is identical to the address book/call-log. The user is redirected to the media gallery or file explorer where the user can choose a file which, is then shared with the conversation partner.

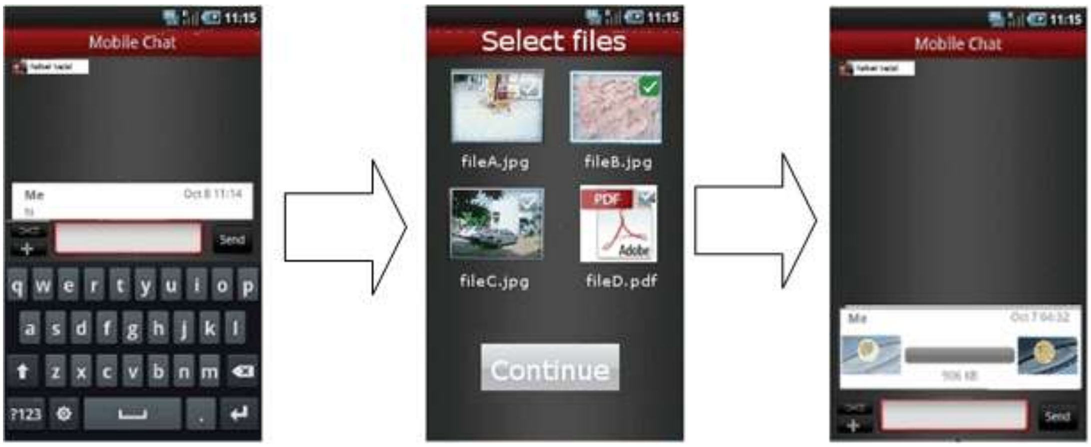


Figure 52: Reference UX for accessing file share from a Chat window

5. Call screen (Image Share): a picture can be shared either from the camera (front or back) or by choosing a file from the media gallery. Please note this case has been covered in detail in section 3.6.6.1.2.

3.5.6.1 *Handling of specific content*

3.5.6.1.1 *Personal Card handling*

The personal and business cards of the RCS user may be stored in a way that is compliant to the CAB 1.0 PCC data in the RCS client which enables the RCS user to create and populate any number views on the personal and/or business contact information as needed. A client may tag these with their dedicated purposes (professional, friends, etc.).

A Personal Card is, from a technical perspective, the same as any other contact card. This functionality only requires certain user experience changes. In particular:

- Visibility as an option in the address book menu.
- A special name/mark in the address book to easily distinguish it from the rest of the contacts.

It is recommended to support at least three Personal Cards. In particular:

- Business Card: For professional use.
- Two more Personal Cards to allow social uses (e.g., a contact card to be exchanged with closest friends for having fun, including frequently updated fields such as a personal picture) and an additional one to allow having a stable personal profile for non-professional uses.

3.5.6.1.2 *Personal Contact Card entry points*

Sending a contact card

The user selects any of the contacts in the Address Book. Entry points for sending a contact could be:

1. Chat
2. Address Book
3. Call log

Before sending a contact card the user should have the option to preview the information. The possibility of editing the information should be available so that filtering the contact information to be sent is also allowed. Once the contact information is confirmed the contact card is sent over File Transfer.

Receiving a contact card

When a new contact card is received, the user is prompted to accept the file. Once accepted, two options are given:

1. Save contact card
2. View contact card

If ‘Save Contact information’ is chosen proper options will be given depending on whether the contact received already exists or not in the receiver’s address book. If it exists the existing contact information will be implemented with the additional information received.

3.6 Content sharing

3.6.1 Feature description

3.6.1.1 Overview

Content sharing provides the capability to share videos and pictures in near real-time. This functionality can be used both in connection to a voice call and in a standalone manner when there is not an ongoing call. When the receiving user has multiple devices the content sharing requests are sent to all those devices. Therefore when used in combination with a voice call, the user can decide to accept the shared content on a different device than the one they are using for the voice call if that device has better display capabilities for instance.

There can be different sources for the shared content:

- The front camera (“me”)
- The rear camera (“what I see”)
- A file (“video streaming” or “sending of a stored image”)

A Service Provider configurable parameter allows the Service Provider to set the maximum duration of a Video Share session (see VS MAX DURATION in section A.1.5) and the max size of a file transferred during Image Share (see IS MAX SIZE in section A.1.5).

3.6.1.2 Content Sharing during a voice call

The content share services during a voice call are linked to the call. Therefore they are also automatically terminated when the call ends.

All services are delivered as one to one only and there is no multiparty sharing provided. For the content sharing during a call, the user should be able to recognize whether one or both content sharing services (i.e. Video and Image Share) are available to use with their conversation partner. Therefore both ends need to be updated on the respective capabilities to avoid showing a service as available when this is no longer the case. This is achieved through the capability exchange described in section 2.6.

Both Video and Image Share are unidirectional and do not need a dedicated audio path. It is possible however to establish simultaneous Image and/or Video Share sessions in each direction. For example when referring to bidirectional Video Share, this means that once User A is sharing video with User B, User B can also start to share video with User A simultaneously, provided the right coverage conditions are in place. In this case each Video Share session is independent and should be handled separately. The same example would also apply to Image Share or to a combination of Video Share in one direction and Image Share in the other.

3.6.1.3 Content Sharing without a voice call

For the sharing without a call the user is aware which services are available through the regular RCS capability query mechanisms defined in section 2.6. For sharing files or images the File Transfer service as described in section 3.5 is used.

Note: It is possible to use the content sharing without a voice call also with the conversation partner during a voice call. In that case, the sharing session will be independent of that voice call. This means that it can continue after the voice call ends and must be explicitly terminated. Furthermore for live video sharing, audio will be sent in the voice call in addition to the audio stream that is part of the sharing session.

Similar to the content sharing during a call, the Video Share session is unidirectional. However it is not possible to establish simultaneous Video Share sessions with the same or different users as that might result in user experience issues such as the audio from one session being retransmitted in another. To establish a Video Share session in the other direction, the already established session must therefore be terminated first.

3.6.1.4 *Use Cases*

3.6.1.4.1 *Share Video during a voice call*

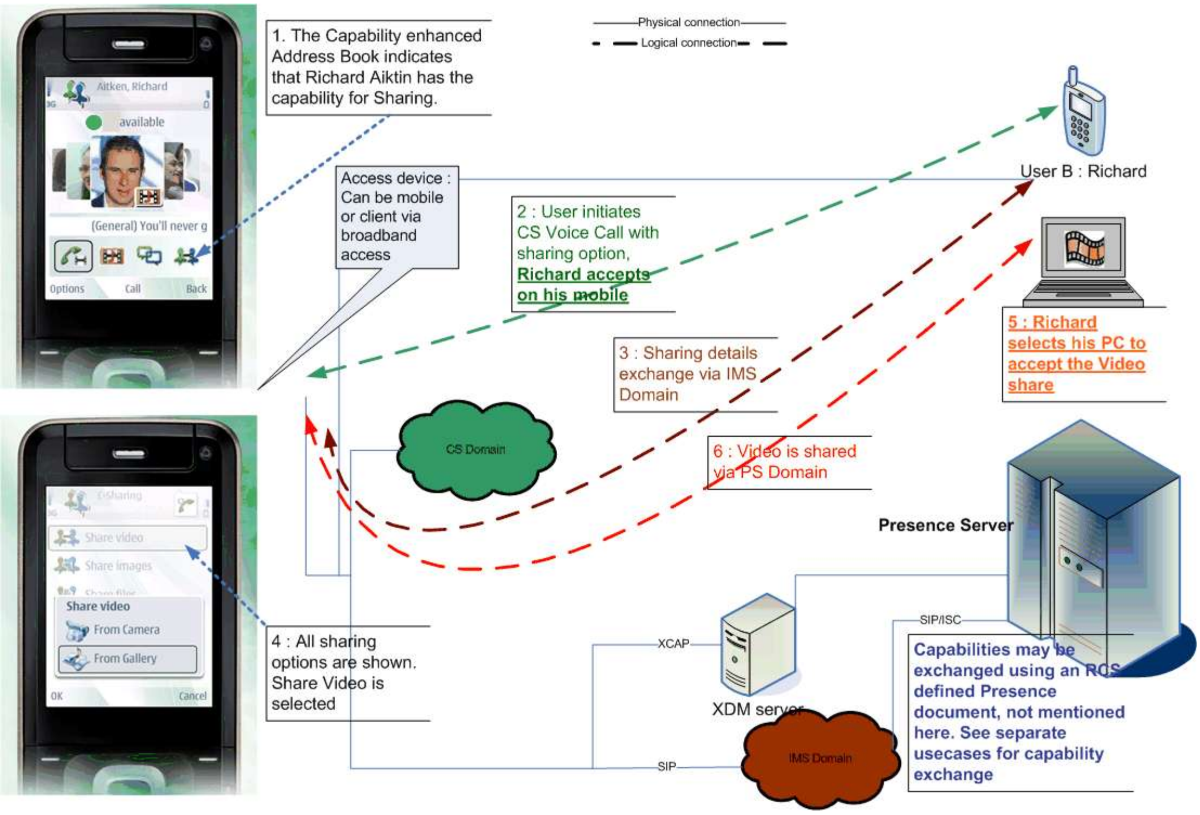

Aitken, Richard
available
(General) You'll never g
Options
Call
Back
1. The Capability enhanced Address Book indicates that Richard Aiktin has the capability for Sharing.
Physical connection
Logical connection
User B : Richard
Access device : Can be mobile or client via broadband access
2 : User initiates CS Voice Call with sharing option, Richard accepts on his mobile
5 : Richard selects his PC to accept the Video share
3 : Sharing details exchange via IMS Domain
CS Domain
6 : Video is shared via PS Domain
Presence Server
C-Sharing
Share video
Share images
Share video
From Camera
From Gallery
OK
Cancel
4 : All sharing options are shown. Share Video is selected
XCAP
SIP/ISC
XDM server
SIP
IMS Domain
Capabilities may be exchanged using an RCS defined Presence document, not mentioned here. See separate usecases for capability exchange

Figure 53: Sharing video during a voice call

Figure 53 illustrates the behaviour when the voice call is set up in the CS domain. Apart from the voice call itself, the behaviour would be identical though in case one or both parties used the PS domain for the voice call as specified in section 3.8 since the sharing service functions independently of the voice call.

Note: When both of the devices involved in the sharing are on a high bandwidth access, for example LTE, the perceived video quality will be higher.

3.6.1.4.2 *Sharing video during a call in the multidevice environment*

User A has a mobile device and a broadband access device (RCS PC client). User B has a mobile device.

- User B has travelled to Hong Kong and is visiting the Victoria's peak. The view from top of the peak is astonishing and they would like to share the experience with their friend User A.
- User B makes a call to User A

- User A answers on the mobile.
- User B tells User A about the view they are viewing. To prove this User B decides to share a video with User A.
- User B sees from the call menu that they can share video with User A. User B sends the request to share video, for example, by clicking the Video Share icon.
- The request is sent to both User A's mobile and PC; both mobile and PC will alert.
- As User A is sitting in front of their PC he/she decides to take the video to the PC for example, by clicking accept button on the PC client.
- User A's mobile will then stop alerting.
- User A will now see the beautiful scenery shared by User B in their PC while still having the voice call on the mobile.

Note: this was illustrated previously in Figure 53. The behaviour would be similar when sharing an image.

3.6.1.4.3 *Share an Image during a call*

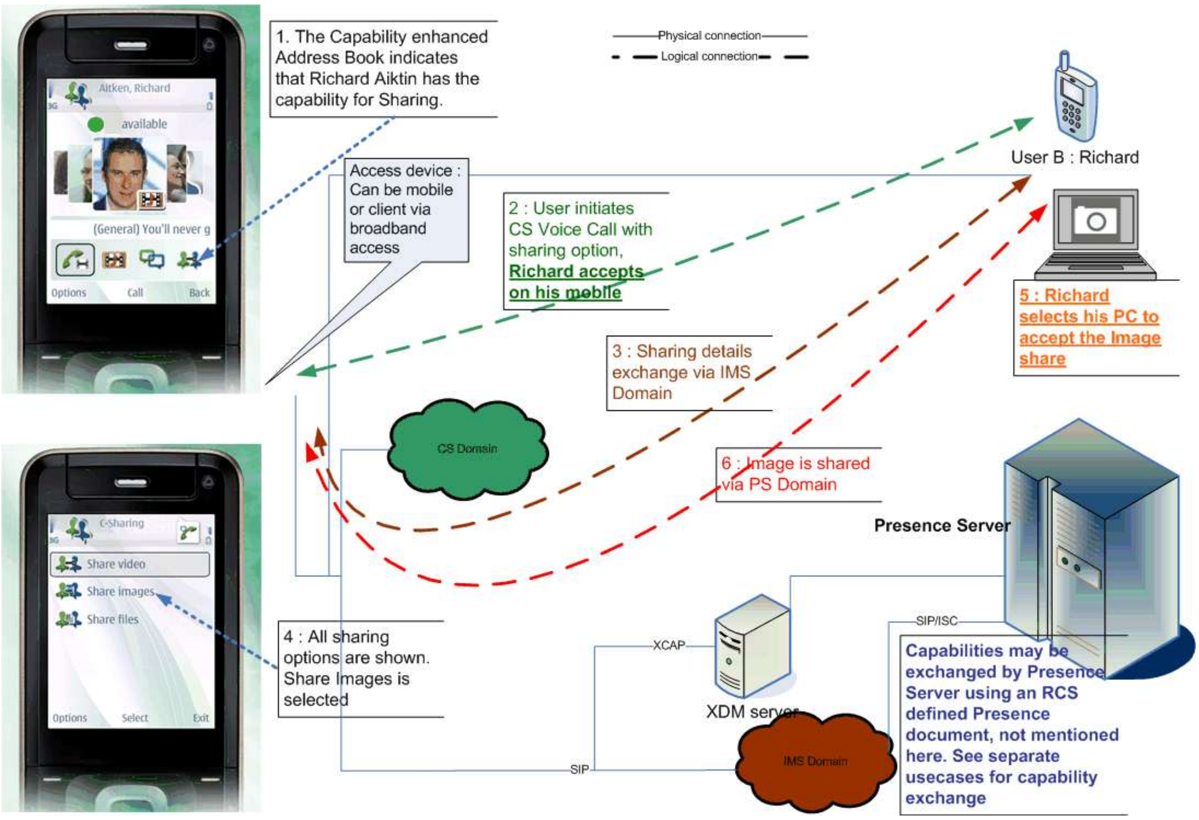
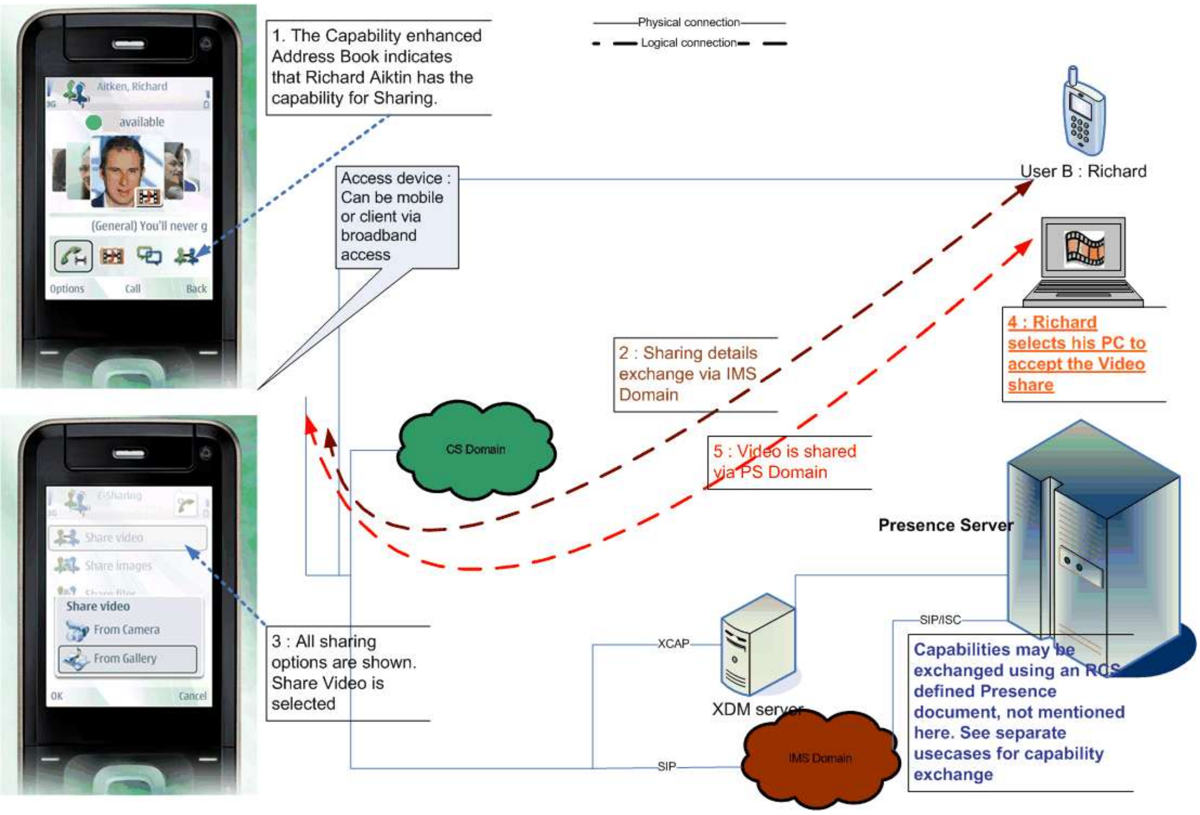

Aitken, Richard
available
(General) You'll never g
Options
Call
Back
1. The Capability enhanced Address Book indicates that Richard Aiktin has the capability for Sharing.
Physical connection
Logical connection
User B : Richard
Access device : Can be mobile or client via broadband access
2 : User initiates CS Voice Call with sharing option, Richard accepts on his mobile
5 : Richard selects his PC to accept the Image share
3 : Sharing details exchange via IMS Domain
CS Domain
6 : Image is shared via PS Domain
Presence Server
C-Sharing
Share video
Share images
Share files
Options
Select
Exit
4 : All sharing options are shown. Share Images is selected
XCAP
SIP/ISC
XDM server
SIP
IMS Domain
Capabilities may be exchanged by Presence Server using an RCS defined Presence document, not mentioned here. See separate usecases for capability exchange

Figure 54: Sharing an image during a call

Figure 54 illustrates the behaviour when the voice call is set up in the CS domain. Apart from the voice call itself, the behaviour would be identical though if one or both parties used the PS domain for the voice call as specified in section 3.8 since the sharing service functions independently of the voice call.

3.6.1.4.4 *Share a video without a voice call*



1. The Capability enhanced Address Book indicates that Richard Aiktin has the capability for Sharing.

Access device : Can be mobile or client via broadband access

2 : Sharing details exchange via IMS Domain

3 : All sharing options are shown. Share Video is selected

4 : Richard selects his PC to accept the Video share

5 : Video is shared via PS Domain

Capabilities may be exchanged using an RCS defined Presence document, not mentioned here. See separate usecases for capability exchange

Figure 55: Sharing video without a call

Note: When both of the devices involved in the sharing are on a high bandwidth access, for example LTE, the perceived video quality will be higher.

3.6.2 Interaction with other RCS features

3.6.2.1 *Voice Call*

The sharing during a voice call (either over CS or as specified in section 3.8) interacts with that voice call since the sharing is automatically terminated when the call is terminated. There is also an interaction with the supplementary services of that voice call.

3.6.2.1.1 *Multiparty call and Image/Video Share*

Once a voice call is established between two users, it is possible for one of them to add another party to the call, and consequently, initiate a multiparty call. From RCS services perspective and as presented in section 2.6.4.1, the Image and Video Share services are not available during a multiparty call. Therefore the terminal should manage the following scenarios:

- The users were in a voice call without using the Image or Video Share services: In this case, when switching to a multiparty call the client starting the process has to send a SIP OPTIONS request with a capability update (as described in section 3.6.4.3.2) indicating that the Content Sharing services during a call are no longer available. The on-screen icons/layout should be updated accordingly.
- The users were in a voice call using Video Share: In this case, switching to a multiparty call means ending the Video Share service. This can either be sender or receiver terminated, depending upon the circumstances, as described in sections 3.6.4.3.4 and 3.6.4.3.5 respectively. In both cases, a capabilities exchange using SIP occurs and, consequently, the client initiating the multiparty call should report that the Content

Sharing services/capabilities during a call are no longer available. The on-screen icons/layout should be updated accordingly.

- The users were in a voice call using Image Share with the transfer not yet completed: In this case, switching to a multiparty call means ending the Image Share service. This either can be sender or receiver terminated, depending upon the circumstances, as described in sections 3.6.4.3.8 and 3.6.4.3.9 respectively. In both cases, a capabilities exchange using SIP OPTIONS occurs and, consequently, the client initiating the multiparty call should report that the Content Sharing services/capabilities during a call are no longer available. The on-screen icons/layout should be updated accordingly.
- The users were in a voice call using Image Share after the transfer has completed: In this case, switching to a multiparty call means that the picture is no longer shown in the call screen and that the client starting the process has to send a SIP OPTIONS message with a capability update (as described in section 3.6.4.3.2) indicating that the Content Sharing services during a call are no longer available. The on-screen icons/layout should be updated accordingly.

It should be also noted that from the moment the users enter in a multiparty call, it is not necessary to perform the capability exchange described in section 3.6.4.3.2.

Finally, if the multiparty call is converted into a standard call (That is it becomes again a 1-to-1 call), this event should be treated as a new call establishment meaning that a capability exchange via OPTIONS needs to take place and, consequently, the relevant on screen icons need to be updated.

3.6.2.1.2 *Call on hold and Image/Video Share*

Once a voice call is established between two users, it is possible for one of them to put the other party on hold. From RCS services perspective and as presented in section 2.6.4.1, the Image and Video Share services are not available during a call which is not active, therefore, the terminal needs to manage the following scenarios:

- The users were on a voice call without using the Image or Video Share services: In this case, when putting the call on hold the client starting the process has to send an SIP OPTIONS request with a capability update (as described in section 3.6.4.3.2) indicating that the Content Sharing services during a call are no longer available. The on-screen icons/layout should be updated accordingly.
- The users were in a voice call using Video Share: In this case, putting the call on hold means ending the Video Share service. This can either be sender or receiver terminated, depending upon the circumstances, as described in sections 3.6.4.3.4 and 3.6.4.3.5 respectively. In both cases, a capabilities exchange using SIP OPTIONS occurs and, consequently, the client putting the call on hold should report that the Content Sharing services/capabilities during a call are no longer available. The on-screen icons/layout should be updated accordingly.
- The users were in a voice call using Image Share with the transfer not having completed: In this case, putting the call on hold means ending the Image Share service. This can either be sender or receiver terminated, depending upon the circumstances, as described in sections 3.6.4.3.8 and 3.6.4.3.9 respectively. In both cases, a capabilities exchange using SIP OPTIONS occurs and, consequently, the client putting the call on hold should report that the Content Sharing services/capabilities during a call are no longer available. The on-screen icons/layout should be updated accordingly.
- The users were on a voice call using Image Share after the transfer has completed: In this case, putting the call on hold means that the picture is no longer shown in the call screen and that the client starting the process has to send a SIP OPTIONS message with a capability update (as described in section 3.6.4.3.2) indicating that the Content Sharing services during a call are no longer available. The on-screen icons/layout should be updated accordingly.

It should be also noted that from the moment the call is put on hold (that is the call is not active):

- It is not necessary to perform the capability exchange described in section 3.6.4.3.2, and,
- If there is another active call, the behaviour regarding the Image and Video Share services (that is both for the capability exchange and the services itself) should not be affected by the fact that another call is on hold.

Finally, if the call is made active, this event should be treated as a new call establishment meaning that a capability exchange via OPTIONS needs to occur and, consequently, the relevant on screen icons need to be updated.

3.6.2.1.3 *Waiting call and Image/Video Share*

A waiting call is a non-active call therefore, consequently with the information presented in section 2.6.4.1, it should not be possible to access the Image and Video Share services between the caller and receiver.

Please note having a waiting call will not affect the behaviour for Image and Video Share (that is both for the capability exchange and the services itself) on the active call.

3.6.2.1.4 *Calls from private numbers*

When a call is received and the caller cannot be identified (because a hidden number is used for instance), it should not be possible to access the Image and Video Share services between the caller and receiver.

3.6.2.1.5 *Call divert/forwarding*

If the receiver has call divert/forwarding active (the calls are for instance forwarded to another number or to voicemail), it is not possible to access the Image and Video Share services from the caller to the receiver.

3.6.2.2 Chat

As for the sharing without a call there is not necessarily a communication context allowing the receiving user to get some background on why the sharing is done, the receiving user should be able to easily establish communication with the user who is sharing the content. The chat service is one of the prime candidates for this. See also the guidelines provided in section 3.6.6.2.

3.6.2.3 Video call

Please refer to section 3.9.2.2.

3.6.2.4 File Transfer

Since from a UX perspective File Transfer and Image Share are very similar services, content sharing without a voice call is limited to the sharing of videos. For sharing files or images when there is no voice call the File Transfer service as described in section 3.5 is used.

3.6.3 High Level Requirements

3-6-1 Content can be shared while on a CS or PS Voice call, thus it must be possible to have a voice and a data stream running simultaneously.

3-6-2 Each time a voice call is established, the user shall be offered the possibility to share content whenever possible

3-6-3 It shall be possible to establish a Content Sharing Session without an accompanying CS and PS Voice call.

3-6-4 It shall be possible to stream audio, along with video, during a Content Sharing session without a CS and PS Voice call.

3-6-5 Content Sharing shall be uni-directional. During a single content sharing session, the originator of the content sharing session can share content with the terminating party, but the terminating party cannot share content with the originator in the same session.

3-6-6 When sharing during a call, the receiving party may be offered the possibility to establish a session in the other direction when circumstances allow.

3-6-7 For content sharing without a voice call only one session may be established at a time. That is simultaneous sessions (regardless of the direction) are not allowed.

3-6-8 The content sharing service can be initiated by either end point involved in the voice call (e.g. the caller or the receiver). When a user initiates content sharing, an invitation is automatically sent to the other contact, which may be accepted or rejected. An acceptance shall stand for all the contents shared during the call.

3-6-9 End of communication (case of content sharing while on a voice call) shall be handled as follows:

- Content sharing session termination shall not lead to voice termination
- Voice call termination shall automatically terminate the content sharing session

3-6-10 The receiver shall have the possibility to save the shared content on his/her device if allowed by the sender

3-6-11 It shall be possible to assign a Service Provider configurable maximum content size allowed to be sent in an Image Share session. This enables the Service Provider of the inviting user’s RCS client to control the maximum size of the content that the inviting user’s RCS client is authorized to send in an Image Share session. The limitation should be transparent to the end-user.

3-6-12 It shall be possible to assign a Service Provider configurable maximum duration time allowed for a Video Share session. This enables the Service Provider of the inviting user’s RCS client to control the maximum duration time of a Video Share session that the inviting user’s RCS client is authorized to handle the limitation should be transparent to the end-user.

3-6-13 Shared content can be video and still images.

3-6-14 When a content sharing session is set up all of the recipient’s devices shall alert the user

3-6-15 The recipient shall decide on which device they accept the call or session

3-6-16 When a call or a session is accepted or rejected from one device the pending invitation(s) shall be cancelled on all other devices that the recipient has.

3-6-17 When a call or a session is cancelled by the calling device, it shall be cancelled in all devices that the recipient has.

3-6-18 It shall be possible for a terminating party or an originating party to terminate the Content Sharing session.

3.6.4 Technical Realization

3.6.4.1 Video Share

3.6.4.1.1 *Video Share during a voice call*

Video Share during a voice call shall follow [PRD-IR.74] and take into account the handling of service capabilities and OPTIONS queries defined in sections 2.6.4.1 and 2.6 respectively. Furthermore to allow the user to accept the sharing on any device a Broadband Access client (see section 2.9.1.4) shall not automatically reject the INVITE request if it is not in a voice call with the sender. It shall therefore alert the user as if it was and handle the user's response as specified in section 2.11.

Interworking with Video Share terminals based on legacy specifications (i.e. the "already deployed terminals" option in [PRD-IR.74]) is not applicable in RCS.

3.6.4.1.2 *Video Share without a voice call*

A detailed description of this feature can be found in [PRD-IR.84] in sections 2.6.1 and 2.6.1.1 of that document. Additional information can be found in Sections 2.3.2 and 2.5.3 of [PRD-IR.84].

This means that for most cases the flows for setting up a session are very similar for the sharing with or without a voice call. The main difference for Video Share is that in the latter case the INVITE request includes instead of the complementary services feature tag ("*+g.3gpp.cs-voice*"), the ICSI feature tag with the MMTel ICSI and the IARI feature tag with the Video Share phase 2 IARI. That is respectively *+g.3gpp.icsi-ref="urn%3Aurn-7: %3A3gpp-service.ims.icsi.mmtel"* and *+g.3gpp.iari-ref="urn%3Aurn-7%3A3gpp-application.ims.iari.gsma-vs"*.

3.6.4.1.3 *Video Share Recording*

A new SDP attribute in the media level is defined to be used by the Video Share sender to indicate, in the SIP INVITE, to the recipient RCS client that the shared media can be recorded/saved.

The new SDP attribute as defined in [IETF-DRAFT-SIPREC-PROTOCOL]:
`a=recordpref-attr = "a=recordpref:" pref where pref is set to "nopreference"`

An SDP example is *a=recordpref:nopreference*

If the shared media in a Video Share session is allowed (determined by the sender) to be recorded/saved, the sender RCS client should include the above SDP attribute in the SIP INVITE toward the recipient when setting up the Video Share session. If the shared media in a Video Share session shall not be saved by the recipient RCS client the sender RCS client shall not include the above SDP attribute in the SIP INVITE.

A Service Provider can provision its RCS clients to not always include this SDP attribute in the SIP INVITE setting up the Video Share session so the shared media will not be recorded/saved by the recipient RCS client.

If the new SDP attribute is included in the SIP INVITE setting up the Video Share session, it is to the decision of the recipient RCS client (under the instruction of the recipient user or user preference) to determine if the shared media will be recorded/saved.

3.6.4.1.4 *Video interoperability and encoding requirements*

As presented in section 2.6.4.1, the Video Share service availability is mainly dependent on the network coverage. This is based on the assumption that both ends (source and destination) share the ability of handling a common video format and specific profile.

To guarantee the interoperability of RCS clients during Video Share scenarios, all RCS devices supporting the Video Share service (during or without a call) shall, at least, support the following video format:

- Video format: H.264/MPEG-4 (Moving Pictures Experts Group) Part 10 // AVC (Advanced Video Codec)
- H.264 Profile: Baseline Profile (BP)
- H.264 Level: 1b[25]

Note: Please note that including this, it is highly recommended to support also the H.263-2000 codec with profile 0 Level 45 which is mandatory in RCS Release 1-4 Video Share that is based on [PRD-IR.74].

Next to these mandatory codecs, it is recommended to support additional video formats providing different levels of quality and to use them in an adaptive fashion depending both on the terminal status and the network conditions/coverage. As specified [RFC3264], formats must be listed in order of preference in the SDP media description. As such, additional codecs providing better quality than these mandatory ones should be listed in the SDP before the mandatory codecs.

Note that as for H.264 only one level and profile can be indicated in the SDP, a client supporting other H.264 encodings should indicate the highest level and profile that it supports.

Should an RCS terminal support several profiles, the final choice should be based on the outcome of the SDP media negotiation where both ends (sender and receiver) will present the supported video formats at that particular point (that is taking into account each device and network/connectivity status).

The receiving clients should preserve the aspect ratio of the incoming video stream, avoiding that video is stretched to fit the UI. The sending client may redefine the aspect ratio when supporting a flexible handling interface that could alternate between landscape and portrait (e.g. from 4:3 to 3:4 after the sending device has been rotated).

3.6.4.1.5 *Video interoperability in LTE/HSPA*

Video Share used over high bandwidth connections such as LTE or HSPA allows high bitrate bearers, thus allowing better user experience e.g. when using a large screen.

As specified in [PRD-IR.74] and [PRD-IR.84], an RCS device shall support the H.264 video codec with baseline profile and level 1.3[26] to provide 768 kilobits per second (kbps) video over an LTE bearer or over a similar high bitrate bearer. Please note that this codec is considered in addition to the mandatory formats specified in section 3.6.4.1.4.

If a second Video Share session is established in parallel, the H.264 video codec with baseline profile and level 1.2[27] shall be used instead. The assumption for the use of a high bitrate bearer is that the connectivity and video parts of both terminals support it and have LTE or another high bitrate broadband access; otherwise the video bitrate will be reduced to the level 1b (as presented in section 3.6.4.1.4) to assure compatibility.

3.6.4.1.6 *Video Share duration*

A configurable parameter allows the Service Provider to set the maximum duration of a Video Share session (see VS MAX DURATION in section A.1.5) in the UE. When the UE

[25] The H.264 baseline profile 1b shall be encoded using the profile-level-id set to 0x42900B

[26] The H.264 baseline profile 13 shall be encoded using the profile-level-id set to 0x42800D

[27] The H.264 baseline profile 12 shall be encoded using the profile-level-id set to 0x42800C

detects that the maximum duration is reached, it shall tear down the Video Share session by sending a SIP BYE request.

3.6.4.2 Image Share

Image Share during a voice call shall follow [PRD-IR.79] where the SIP OPTIONS query shall be handled as specified in section 2.6 of this document. Furthermore to allow the user to accept the sharing on any device a broadband access client (see section 2.9.1.4) shall not automatically reject the SIP INVITE request if it is not in a voice call with the sender. It shall alert the user and handle the user's response as specified in section 2.11.

To ensure that the request is sent to all devices with equal priority, clients using a PS voice service as defined in section 3.8 shall include the *+g.3gpp.cs-voice* feature tag in the Accept-Contact and Contact headers of the SIP INVITE request for content sharing. Unlike what is indicated in section 3.2 of [PRD-IR.79], those clients shall not include the MMTEL ICSI *urn:urn-7:3gpp-service.ims.icsi.mmtel* in these requests. This behaviour is in line with the other sections of [PRD-IR.79]. As described in [PRD-IR.79] the Image Share IARI is also included in the Accept-Contact and Contact headers (see Table 12 in section 2.6.1.1.2).

If the UE detects that the file being transferred exceeds the Service Provider configured maximum size (see IS MAX SIZE in section A.1.5), it shall either not set up the session or tear it down depending on whether it is the initiator or the receiver.

Note that all RCS services using MSRP, including Image Share, shall align with MSRP usage as described in section 2.8.

Details for image format as specified in [3GPP TS 26.141] will be followed.

3.6.4.3 Flows

3.6.4.3.1 *General assumptions*

In the following sections we will show the relevant message flows and reference UX. Please note that the following assumptions have been made:

- For simplicity, the internal mobile network interactions are omitted in the diagrams shown in the following sections.
- The terminal supports 2G DTM and it is therefore always possible to gracefully terminate the content sharing session related to a voice call provided the terminal remains switched on. If 2G DTM is not supported, the case where on one of the ends a handover occurs to 2G would be result in behaviour towards the other end and the network that is equivalent to the one described for the case of a client error.
- The terminal comes with a front and rear camera. If one or both are missing, the user should be notified only with the available options.
- Prior to a voice call, the user accessed the client's address book, call log or dial-pad to make the call. As described in section 2.6, while these actions are performed a capability query is executed to double-check on the available capabilities. As in RCS Release 1 and 2 and RCS-e 1.2 including in some non RCS clients, Video and Image Share services are only available in a call, an OPTIONS exchange is required once the call is established to check on the capabilities during a call. This exchange can be initiated by either the sender or the receiver. In the following diagrams it is assumed that this initial exchange (OPTIONS and response) has already taken place, and therefore, both ends are aware of the capabilities and the available RCS services.
- In the diagrams it is assumed for simplicity that MSRP chunking is enabled. This is for representation purposes and it is up to the OEM to decide whether MSRP chunking is enabled or not.
- The flows in Figure 58, Figure 59, Figure 60, Figure 61, Figure 62, Figure 63, Figure 64, Figure 66, Figure 67 and Figure 68 show an OPTIONS exchange at the end of the flow.

> In case the capability exchange is done using Presence the equivalent Presence mechanism will be used.

As shown in section 3.6.6, the different entry points for sharing without a call lead to different screens. Therefore for consistency the flows highlight the slightly more complex case of sharing during a voice call.

3.6.4.3.2 *Exchange capabilities during a call*

The assumptions in this case are that User A and B are on a call when the capabilities of one of the users change (due to a hand-over to a different data carrier for instance). Therefore the other end has to be informed using the OPTIONS message[28]

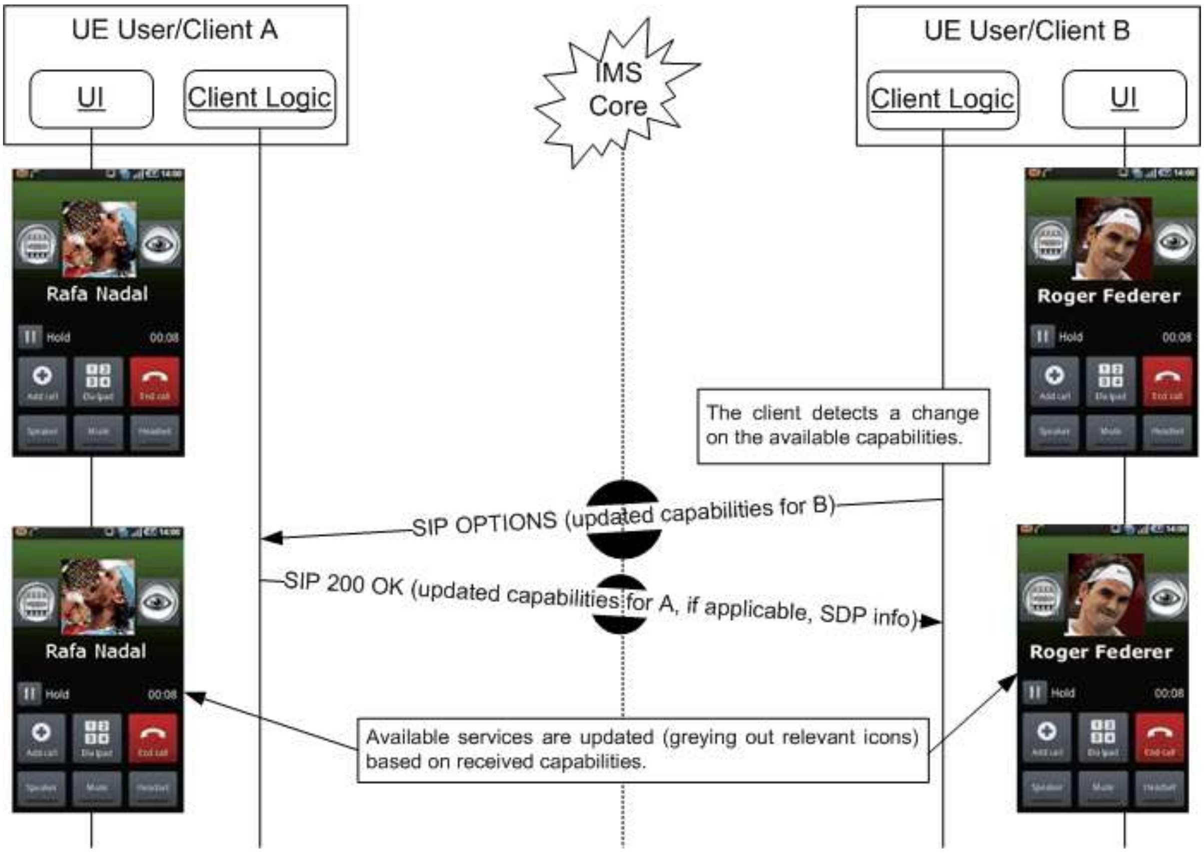

UE User/Client A
UI
Client Logic
IMS Core
UE User/Client B
Client Logic
UI
Rafa Nadal
Hold
00:08
Roger Federer
Hold
00:08
The client detects a change on the available capabilities.
SIP OPTIONS (updated capabilities for B)
SIP 200 OK (updated capabilities for A, if applicable, SDP info)
Rafa Nadal
Hold
00:08
Roger Federer
Hold
00:08
Available services are updated (greying out relevant icons) based on received capabilities.

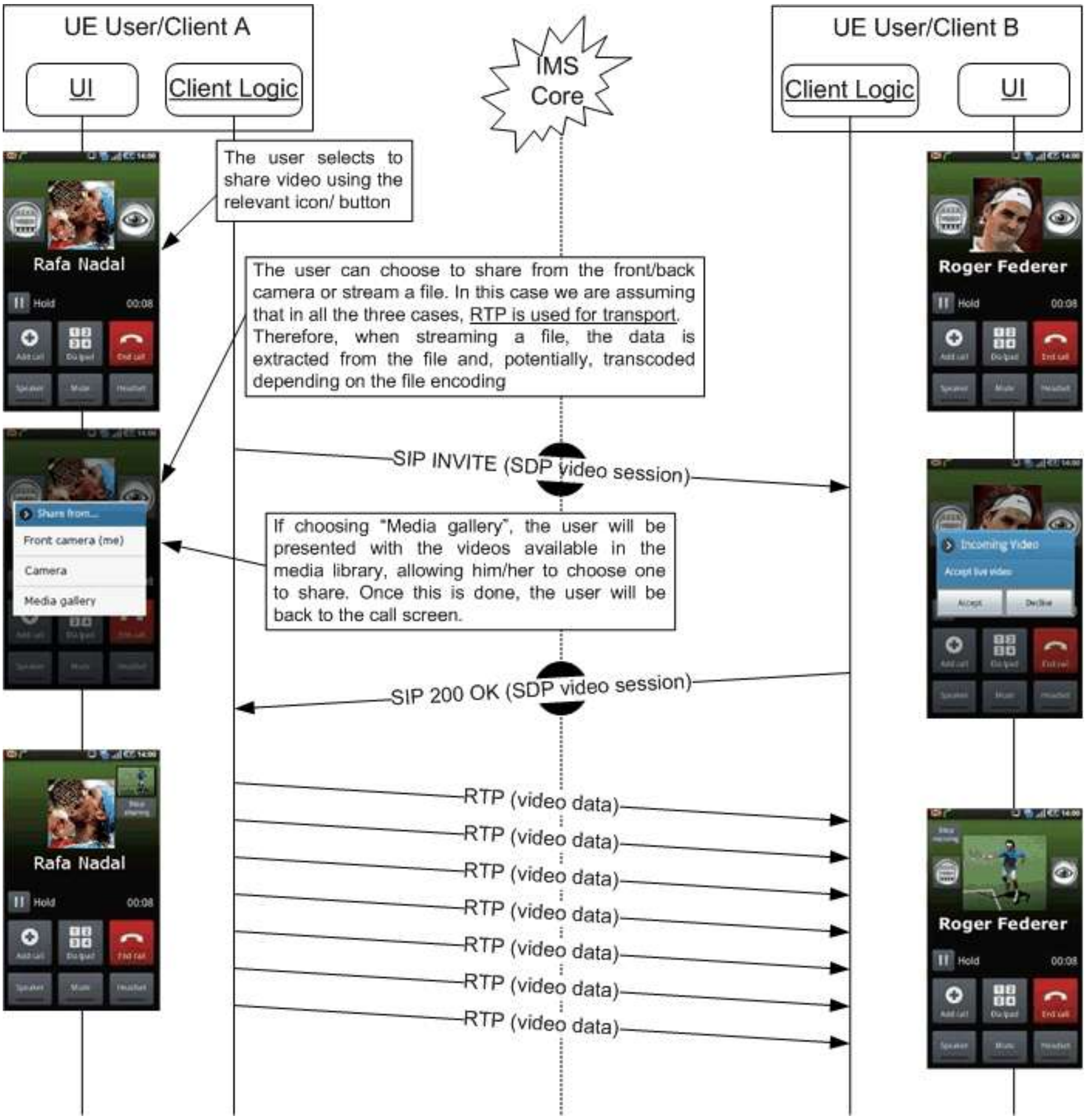
Figure 56: Capabilities exchange during a call

3.6.4.3.3 *Share video*

The assumptions in this case are that both User A (wanting to share video) and User B (recipient wanting to receive it), have successfully performed the capability query, either as shown in section 3.6.4.3.2 or as specified in section 2.6 depending on whether or not the sharing is done in relation to a voice call. Therefore, both clients are aware that video sharing is possible (both UEs on a 3G+ or Wi-Fi).

In this case RTP is the protocol used to stream the video data, so it can be reproduced in real-time on the other end.

[28] The SDP information included in the response to the OPTIONS request is required due to the compliancy to [PRD-IR.74]. This will only be used during OPTIONS exchanges related to a call. The Video Share service shall only be considered to be available if at least one codec in the received SDP is supported by the client.



The user selects to share video using the relevant icon/ button

The user can choose to share from the front/back camera or stream a file. In this case we are assuming that in all the three cases, RTP is used for transport. Therefore, when streaming a file, the data is extracted from the file and, potentially, transcoded depending on the file encoding

If choosing "Media gallery", the user will be presented with the videos available in the media library, allowing him/her to choose one to share. Once this is done, the user will be back to the call screen.

Figure 57: Share Video

3.6.4.3.4 *Stop sharing video (RTP): Sender initiated*

The assumptions in this case are that User A is sharing a video (through RTP) with User B. However User A no longer wants to keep sharing it.

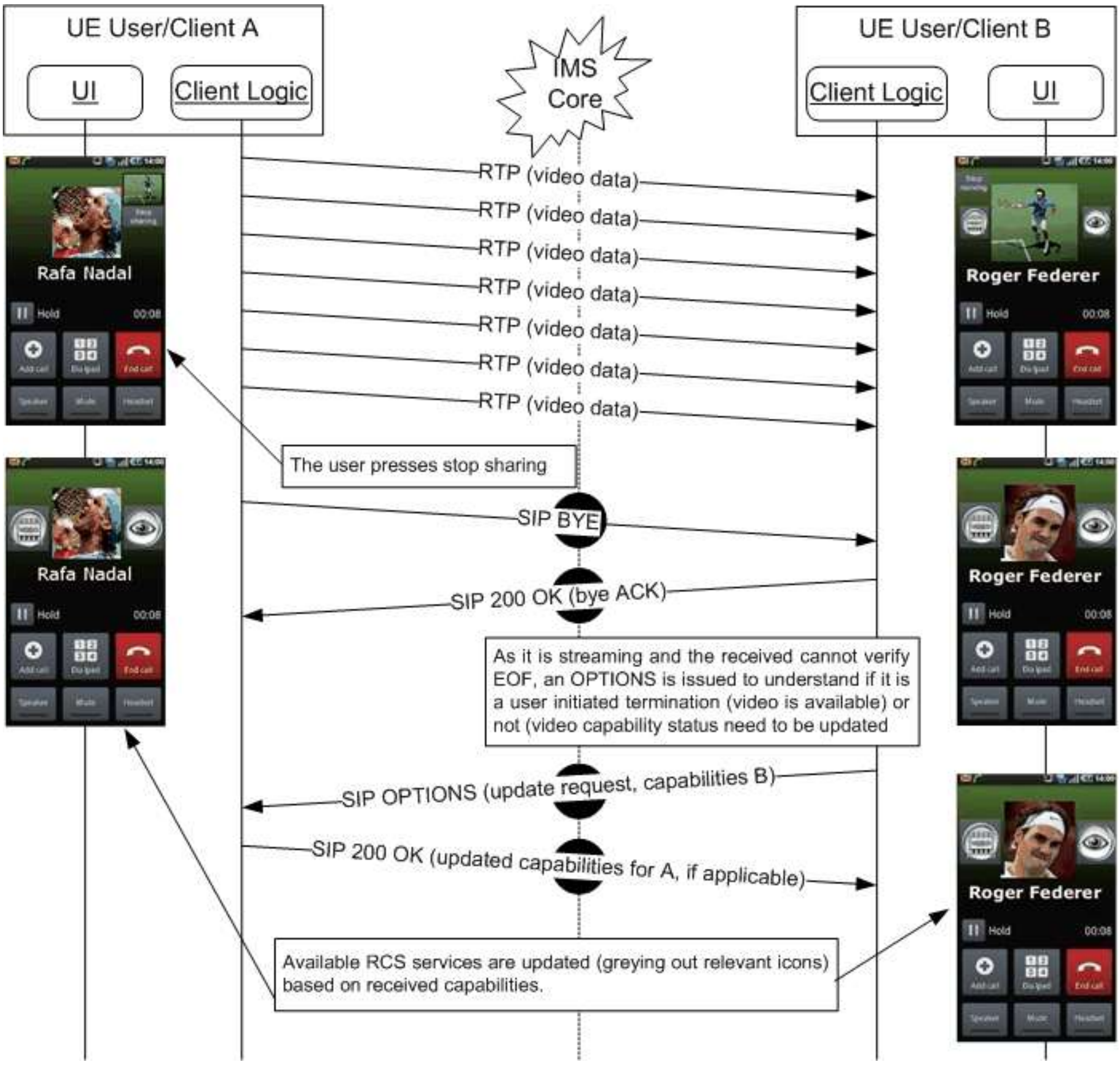
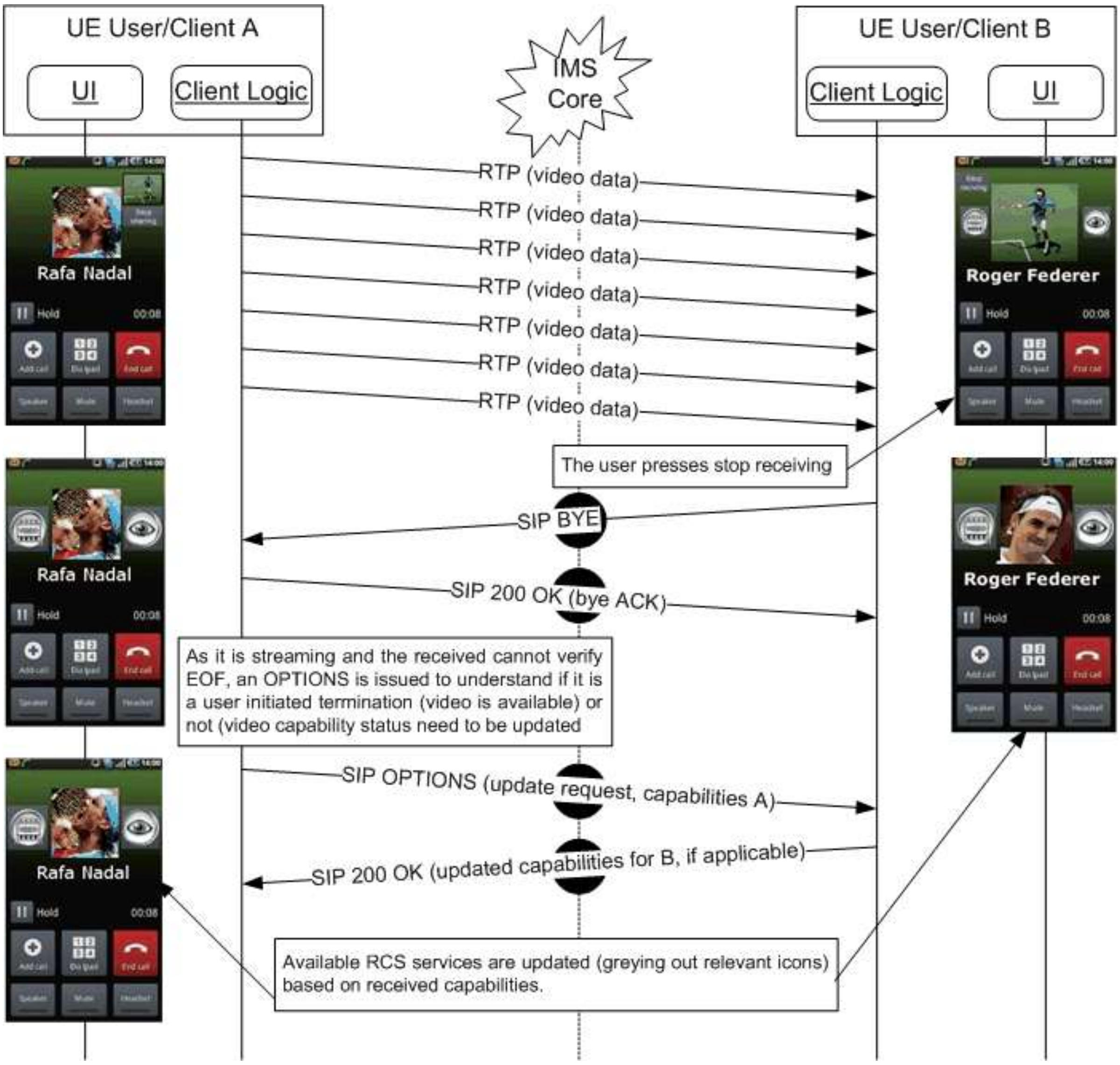

UE User/Client A
UI
Client Logic
IMS Core
UE User/Client B
Client Logic
UI
RTP (video data)
RTP (video data)
RTP (video data)
RTP (video data)
RTP (video data)
RTP (video data)
RTP (video data)
Rafa Nadal
Roger Federer
The user presses stop sharing
SIP BYE
SIP 200 OK (bye ACK)
As it is streaming and the received cannot verify EOF, an OPTIONS is issued to understand if it is a user initiated termination (video is available) or not (video capability status need to be updated
SIP OPTIONS (update request, capabilities B)
SIP 200 OK (updated capabilities for A, if applicable)
Available RCS services are updated (greying out relevant icons) based on received capabilities.

Figure 58: Sender stops sharing video

Note: in case of sharing without a voice call the OPTIONS exchange at the end of the flow is not applicable as for all other services it can be assumed that the other party would be informed if a service is no longer available.

3.6.4.3.5 *Stop sharing video (RTP): Receiver initiated*

This case is equivalent to the previous one. However, it is the receiver (User B) who does not want to keep receiving the video.



The user presses stop receiving

As it is streaming and the received cannot verify EOF, an OPTIONS is issued to understand if it is a user initiated termination (video is available) or not (video capability status need to be updated

Available RCS services are updated (greying out relevant icons) based on received capabilities.

Figure 59: Receiver wants no longer to receive video

Note: in case of sharing without a voice call the OPTIONS exchange at the end of the flow is not applicable as for all other services it can be assumed that the other party would be informed if a service is no longer available.

3.6.4.3.6 *Stop sharing video (RTP) as the required capability is no longer available*

The assumptions in this case are that User A is sharing video (RTP) with User B, and either User A or User B is no longer capable (for instance because the terminal is busy, suddenly has no LTE, 3G+ or Wi-Fi coverage available without triggering an IP reconfiguration or loss of connection) of sending or receiving a video. Please note that in the example, it is assumed that the sender (User A) is the one losing the capability. This sequence will be equivalent in case:

- The receiver (User B) loses the capability to receive video: The BYE and OPTIONS exchange would be initiated by the receiver (User B) in this case.
- Both lose the capability to share video: The BYE and OPTIONS exchange message would be initiated by the client that is the first one to lose the capability in this case.

In losing the capability to send video, the case in which there is an IP reconfiguration is excluded. Please note that this particular case is covered under the “Client Error” section later in this section (see 3.6.4.3.12 and 3.6.4.3.13).

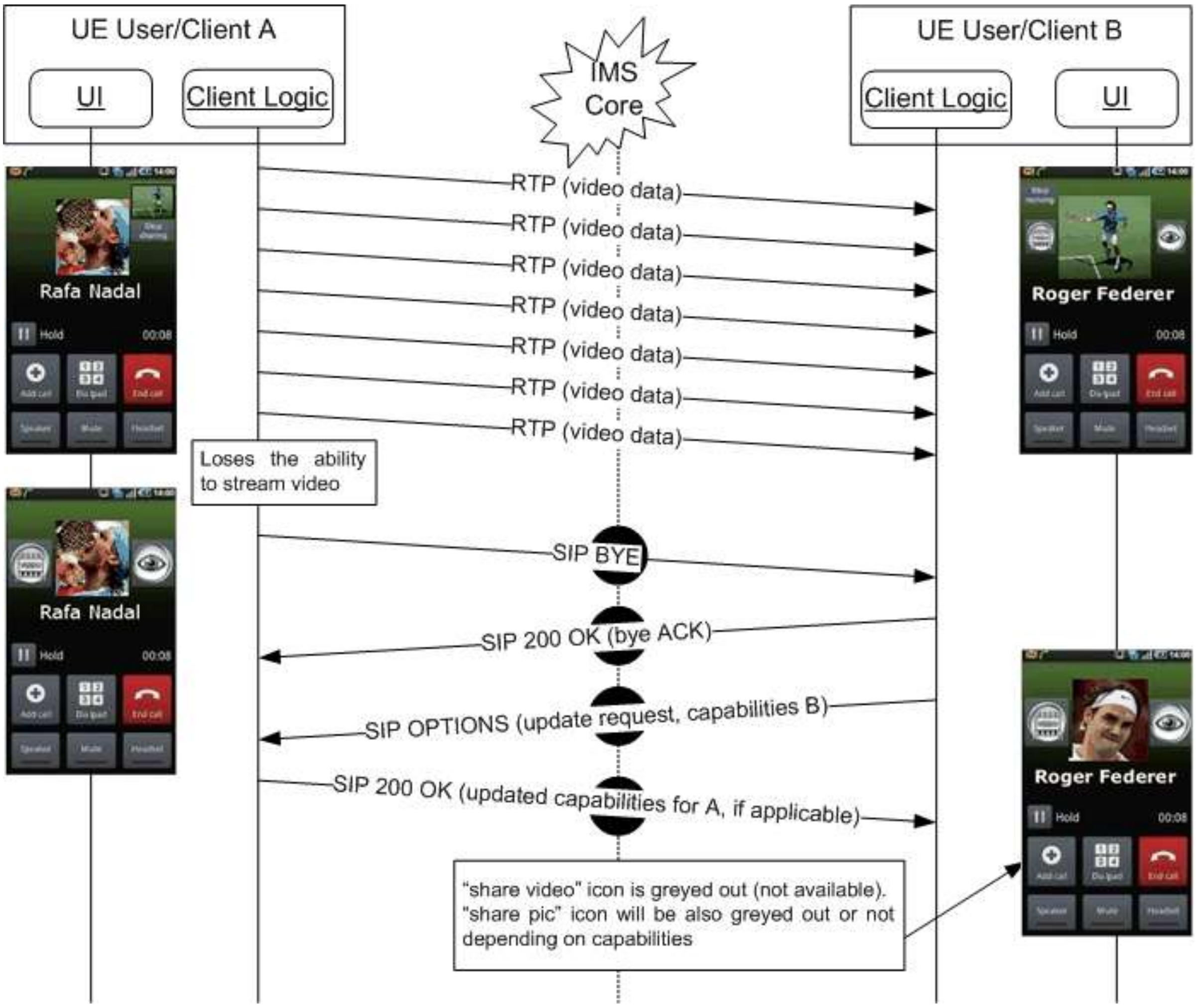
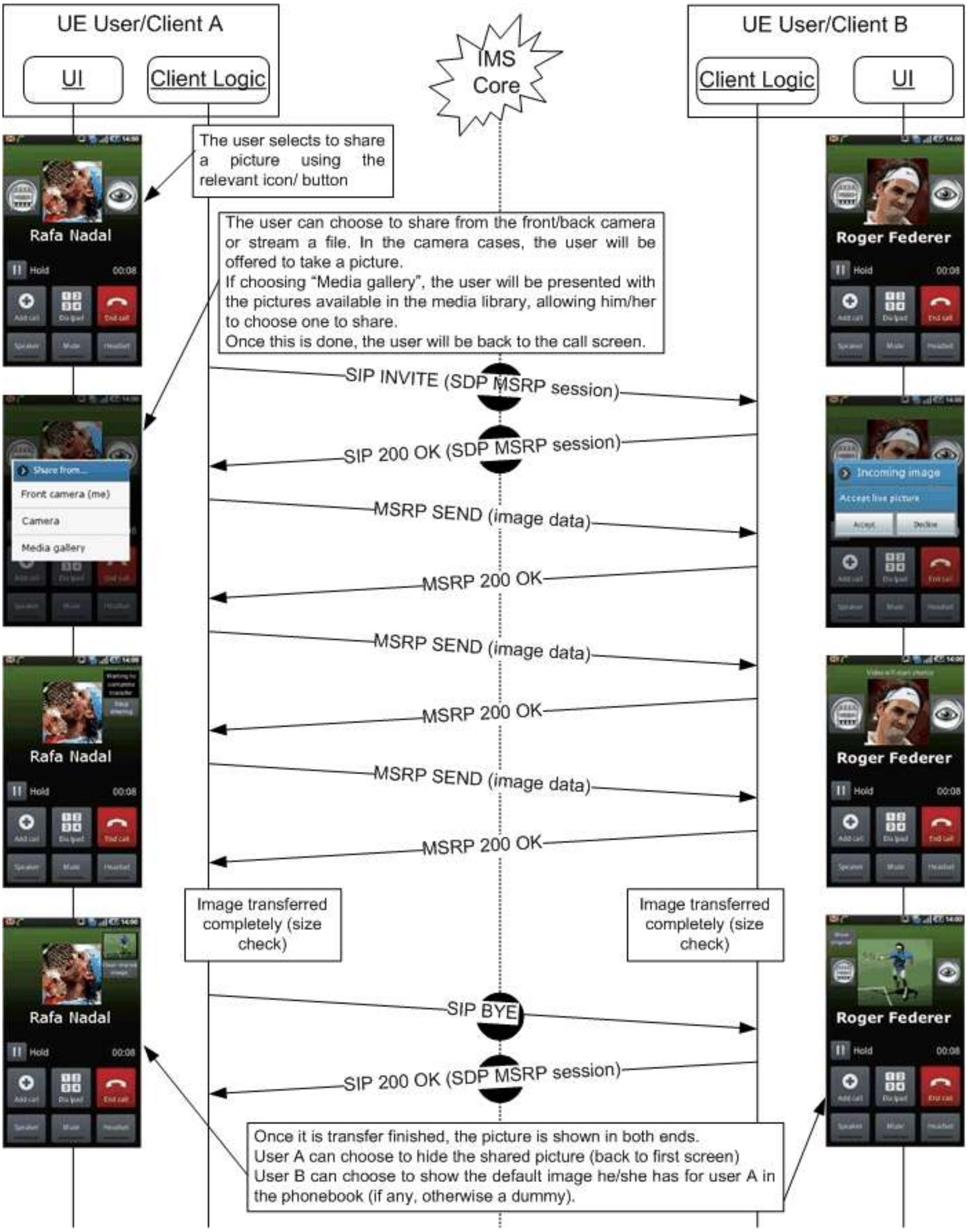

UE User/Client A
UI
Client Logic
IMS Core
UE User/Client B
Client Logic
UI
RTP (video data)
RTP (video data)
RTP (video data)
RTP (video data)
RTP (video data)
RTP (video data)
RTP (video data)
Rafa Nadal
Roger Federer
Loses the ability to stream video
SIP BYE
SIP 200 OK (bye ACK)
SIP OPTIONS (update request, capabilities B)
SIP 200 OK (updated capabilities for A, if applicable)
"share video" icon is greyed out (not available). "share pic" icon will be also greyed out or not depending on capabilities

Figure 60: Video can no longer be shared (capability not available)

3.6.4.3.7 *Share pictures during a call*

The assumptions in this case are that both User A (wanting to share picture) and User B (recipient wanting to receive it), have successfully exchanged the OPTIONS messages. Therefore both clients are aware that Image Share is possible (that is both UEs are on an LTE, 3G+ or Wi-Fi network).



The user selects to share a picture using the relevant icon/ button

The user can choose to share from the front/back camera or stream a file. In the camera cases, the user will be offered to take a picture.
If choosing "Media gallery", the user will be presented with the pictures available in the media library, allowing him/her to choose one to share.
Once this is done, the user will be back to the call screen.

Image transferred completely (size check)

Image transferred completely (size check)

Once it is transfer finished, the picture is shown in both ends.
User A can choose to hide the shared picture (back to first screen)
User B can choose to show the default image he/she has for user A in the phonebook (if any, otherwise a dummy).

Figure 61: Sharing a picture during a call

3.6.4.3.8 *Stop sharing a picture during a call: Sender initiated*

The assumptions in this case are that User A is sharing a picture with User B, the transfer is still ongoing, but User A no longer wants to keep sharing the picture.

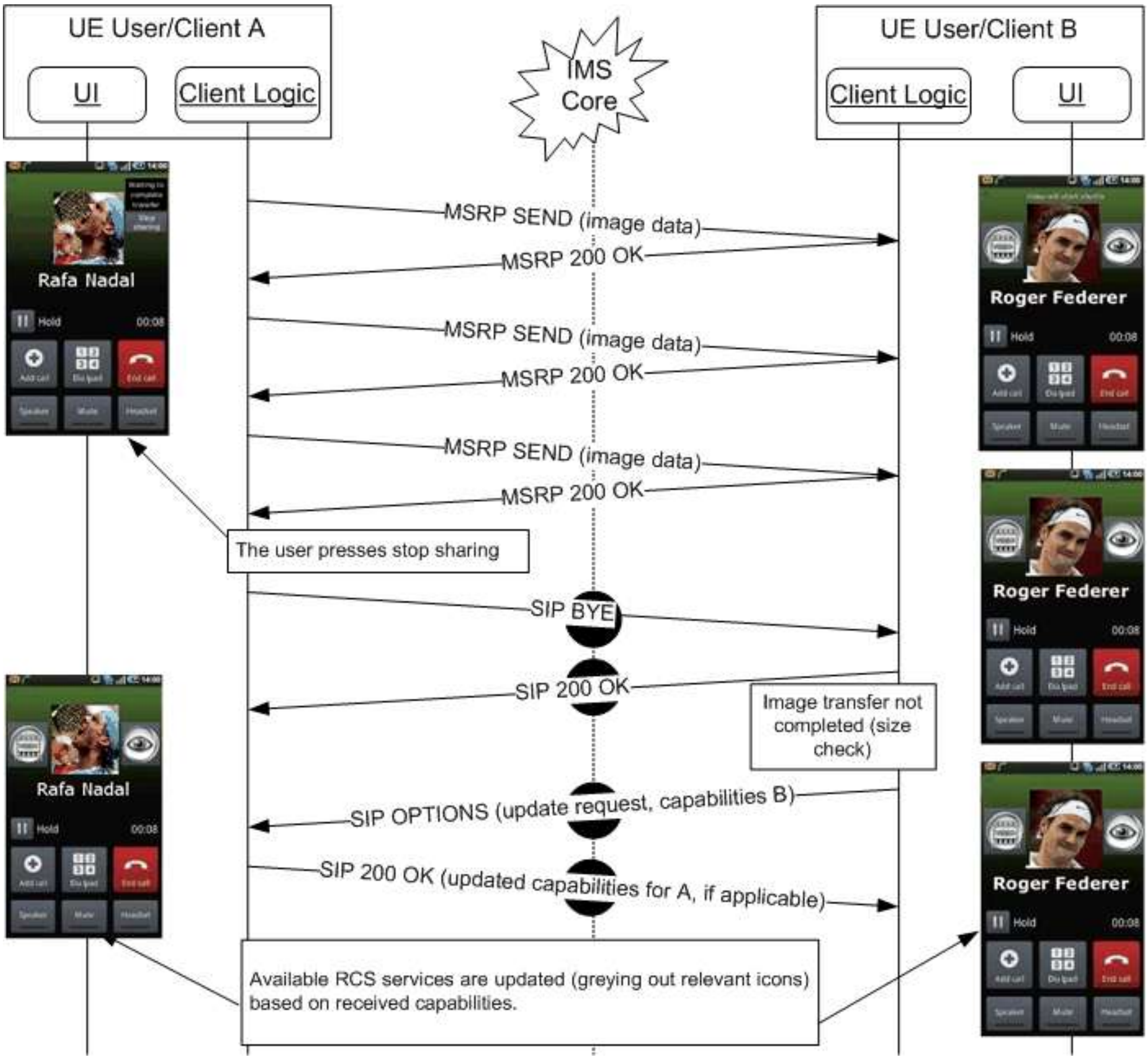

UE User/Client A
UI
Client Logic
IMS Core
UE User/Client B
Client Logic
UI
Rafa Nadal
Roger Federer
MSRP SEND (image data)
MSRP 200 OK
MSRP SEND (image data)
MSRP 200 OK
MSRP SEND (image data)
MSRP 200 OK
The user presses stop sharing
SIP BYE
SIP 200 OK
Image transfer not completed (size check)
SIP OPTIONS (update request, capabilities B)
SIP 200 OK (updated capabilities for A, if applicable)
Available RCS services are updated (greying out relevant icons) based on received capabilities.

Figure 62: Sender stops sharing a picture during a call

3.6.4.3.9 *Stop sharing a picture during a call: Receiver initiated*

This case is equivalent to the previous one. It is however the receiver (User B) who does not want to keep receiving the picture.

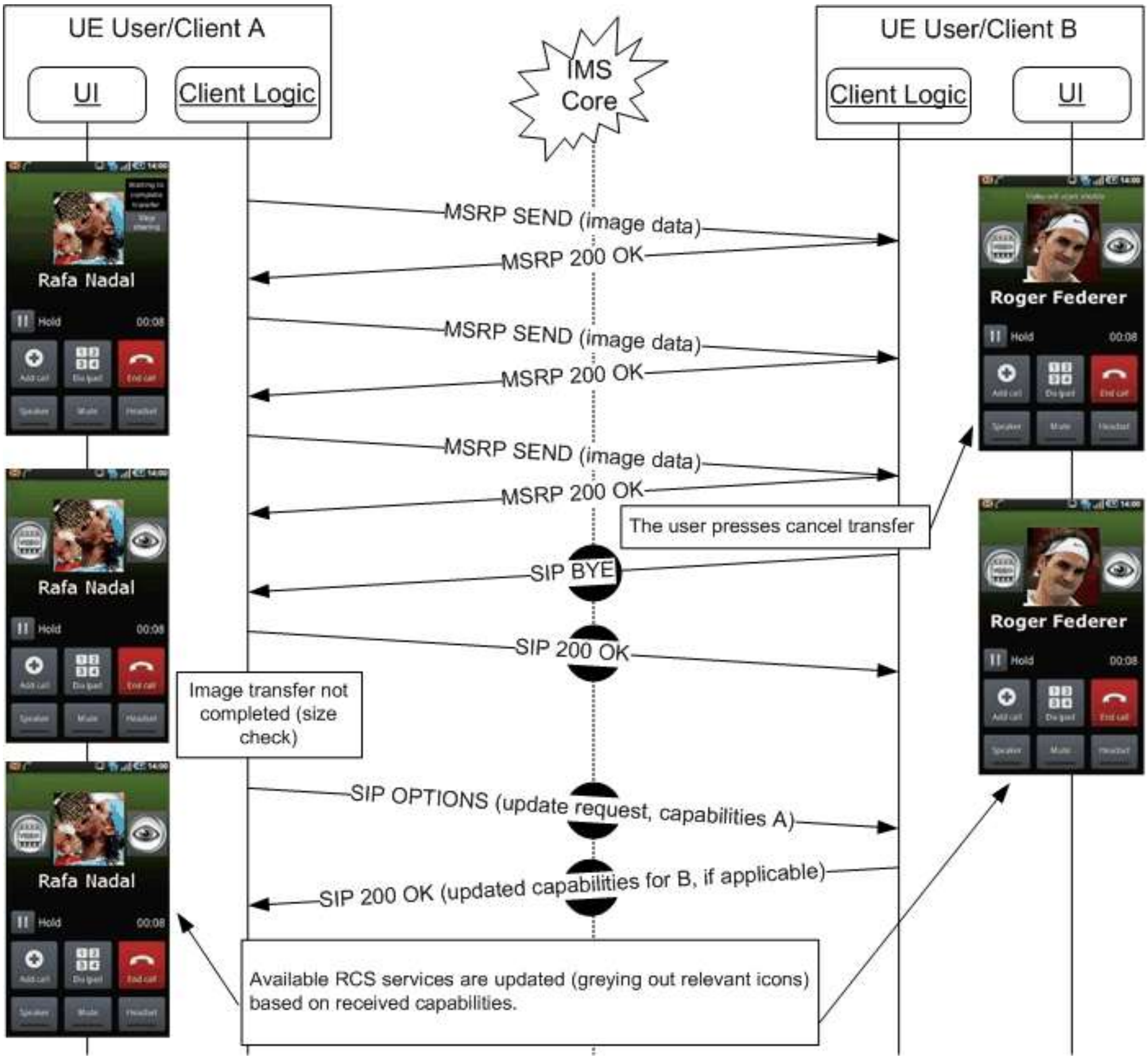

UE User/Client A
UI
Client Logic
IMS Core
UE User/Client B
Client Logic
UI
Rafa Nadal
Roger Federer
MSRP SEND (image data)
MSRP 200 OK
MSRP SEND (image data)
MSRP 200 OK
MSRP SEND (image data)
MSRP 200 OK
The user presses cancel transfer
SIP BYE
SIP 200 OK
Image transfer not completed (size check)
SIP OPTIONS (update request, capabilities A)
SIP 200 OK (updated capabilities for B, if applicable)
Available RCS services are updated (greying out relevant icons) based on received capabilities.

Figure 63: Receiver stops picture sharing

3.6.4.3.10 *Stop sharing a picture during a call as the required capability is no longer available*

The assumptions in this case are that User A is sharing a picture with User B, the transfer has not yet finished, and either User A or User B are no longer capable (for instance because the terminal is busy) to sharing or receiving the image respectively. Please note that in the example it is assumed that the sender (User A) is the client losing the capability. The sequence will be equivalent however for:

- The Receiver (User B) losing the capability to receive pictures: The BYE and OPTIONS exchange would be initiated by the receiving client (User B) in this case.
- Both lose the capability to share pictures: The BYE and OPTIONS exchange would be initiated by the first client to lose the capability in this case.

Please note that there is an exception to stop a file transfer due to capabilities. If one of the users is left with 2G coverage (on a DTM terminal) once a transfer has started, the transfer may continue until completed, provided the handover did not trigger an IP bearer reconfiguration. Once the transfer is completed however, picture sharing will no longer be available as a service during the call.

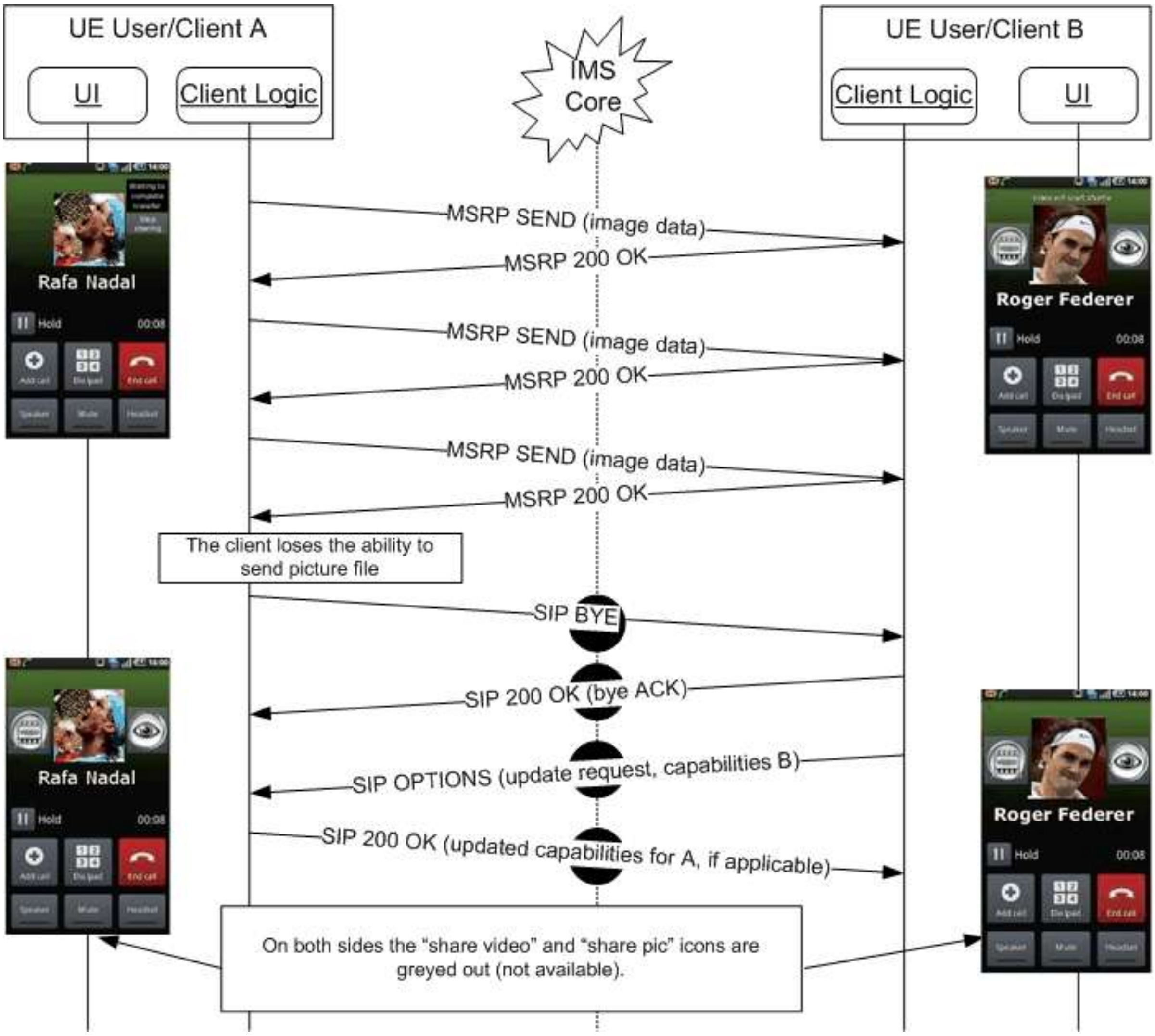

UE User/Client A
UI
Client Logic
IMS Core
UE User/Client B
Client Logic
UI
Rafa Nadal
Roger Federer
MSRP SEND (image data)
MSRP 200 OK
MSRP SEND (image data)
MSRP 200 OK
MSRP SEND (image data)
MSRP 200 OK
The client loses the ability to send picture file
SIP BYE
SIP 200 OK (bye ACK)
SIP OPTIONS (update request, capabilities B)
SIP 200 OK (updated capabilities for A, if applicable)
On both sides the "share video" and "share pic" icons are greyed out (not available).

Figure 64: A picture can no longer be shared during a call (capability not available)

3.6.4.3.11 *Decline share video or picture*

User A wants to share a video or picture with User B. User B however does not want to receive it. Please note that it is assumed that both Video and Image Share is possible (that is the proper capabilities are available).

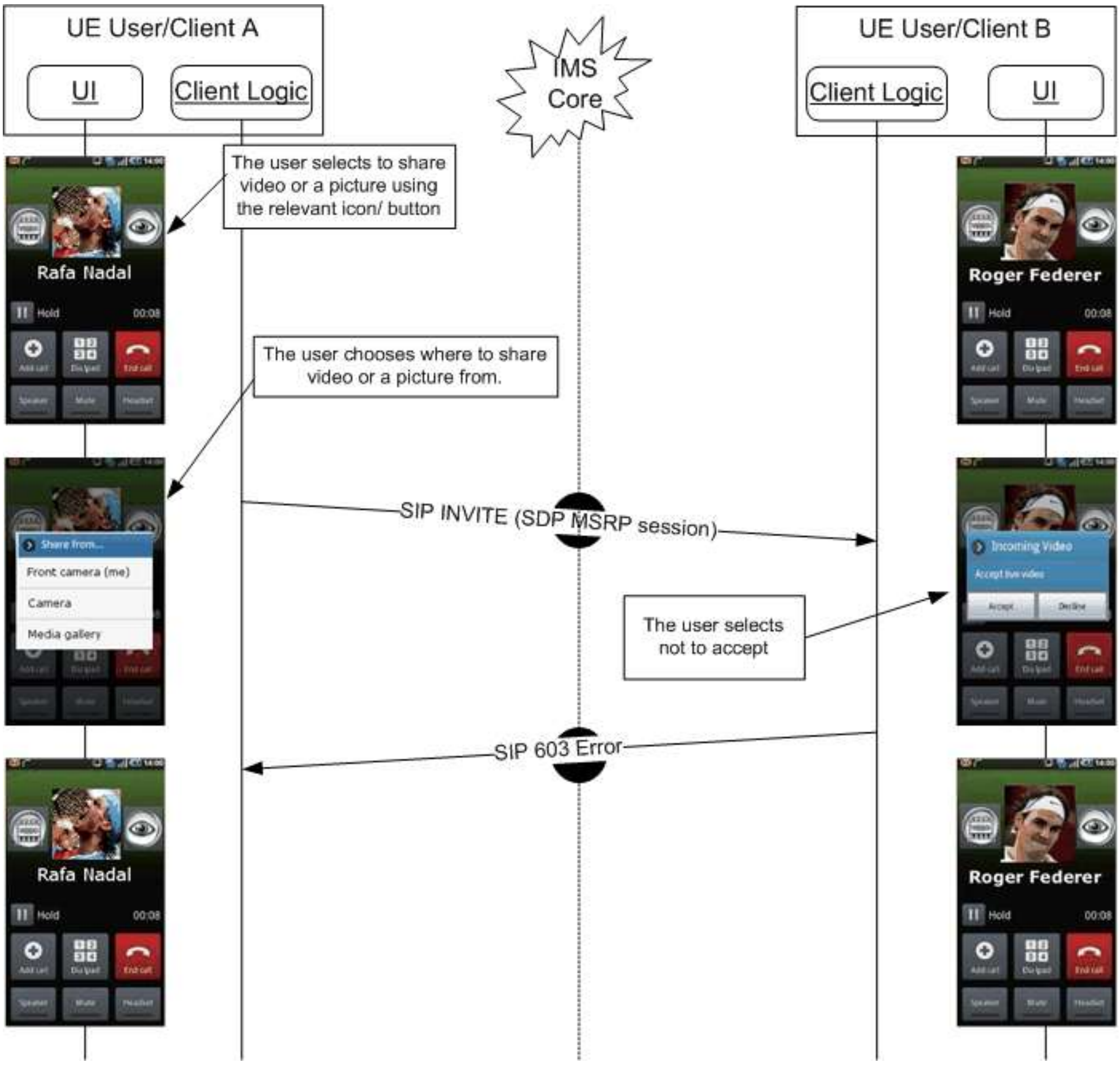


Figure 65: User declines sharing a picture during a call

3.6.4.3.12 *Non-graceful termination (sender): Video or picture sharing*

In this case, User A is sharing video or a picture with User B. Suddenly, User A’s connection to the network fails (This may for instance be due to a client error, a reboot of the device, the loss of the data bearer, a switch in data carrier [for instance 3G+ to 3G] causes an IP layer reconfiguration and so on).

In the following flow, it is assumed a video transfer (RTP) was taking place. It will be equivalent however to the case an MSRP transfer (Image Share or video sharing via File Transfer) was taking place and was not finished:

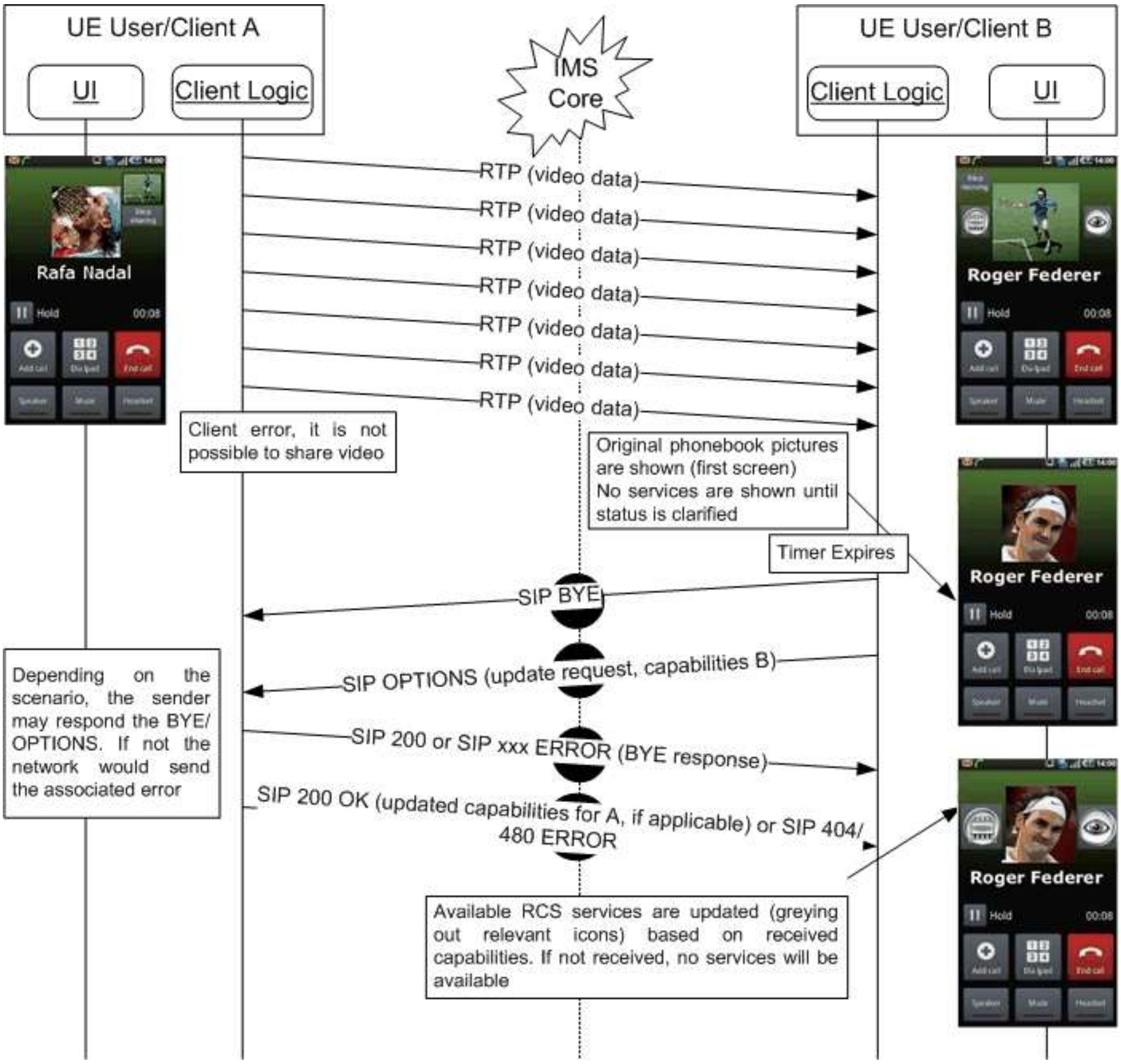

UE User/Client A
UI
Client Logic
IMS Core
UE User/Client B
Client Logic
UI
Rafa Nadal
Roger Federer
RTP (video data)
RTP (video data)
RTP (video data)
RTP (video data)
RTP (video data)
RTP (video data)
RTP (video data)
Client error, it is not possible to share video
Original phonebook pictures are shown (first screen)
No services are shown until status is clarified
Timer Expires
SIP BYE
SIP OPTIONS (update request, capabilities B)
Depending on the scenario, the sender may respond the BYE/ OPTIONS. If not the network would send the associated error
SIP 200 or SIP xxx ERROR (BYE response)
SIP 200 OK (updated capabilities for A, if applicable) or SIP 404/ 480 ERROR
Available RCS services are updated (greying out relevant icons) based on received capabilities. If not received, no services will be available

Figure 66: Non-graceful termination (sender) for video

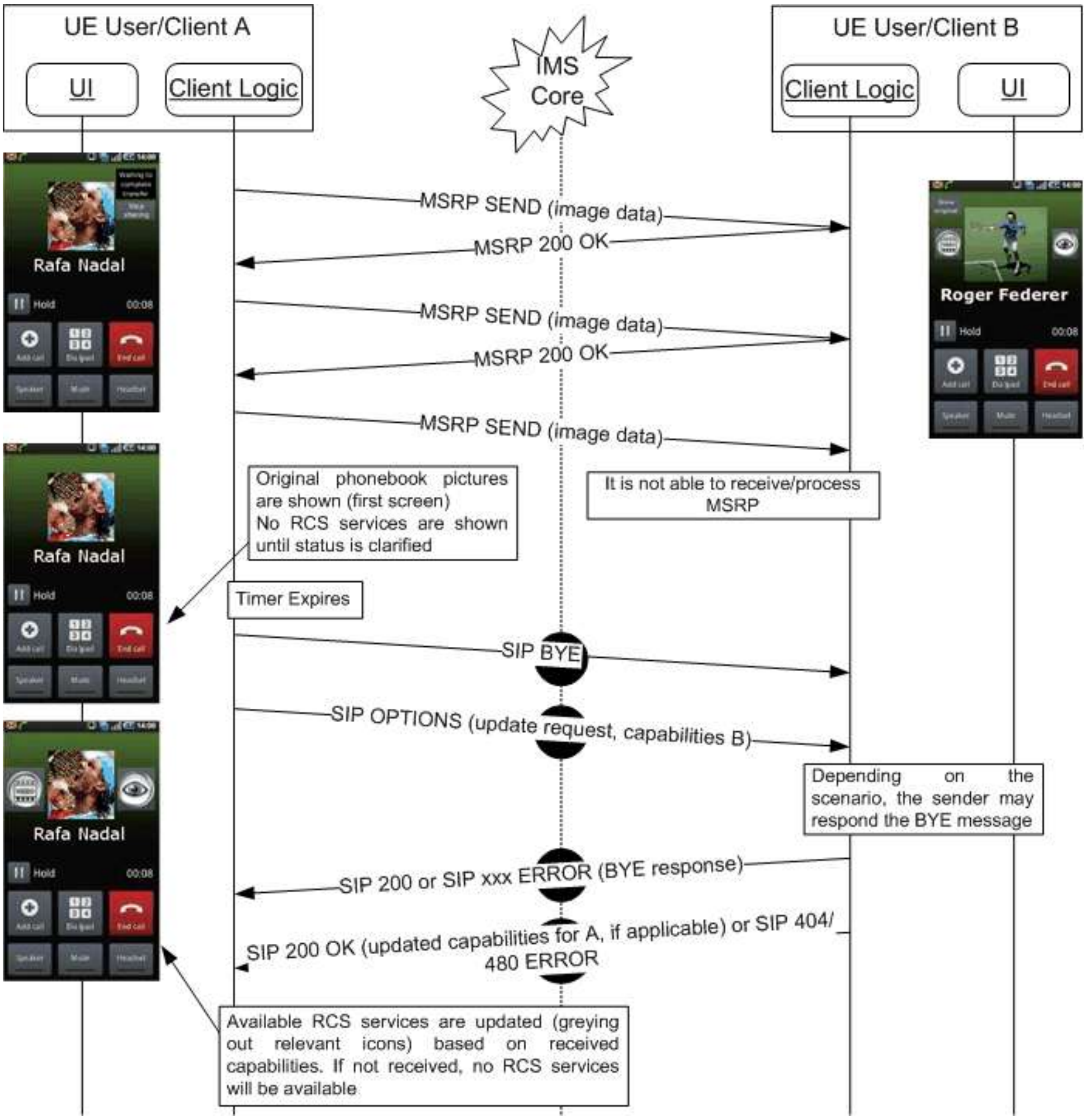
3.6.4.3.13 *Non-graceful termination (receiver): Video or picture sharing*

To protect the IMS Core network from cases where both the sender and the receiver become unresponsive or unreachable before they had time to terminate the SIP session, the RCS Client shall use the procedure described in [RFC4028] in a similar way to the one mandated in [RCS5-SIMPLEIM-ENDORS], that is the RCS client initiating a SIP session must request the role of refresher and the option tag 'timer' must be included in a Supported header.

The Session-Expires and Min-SE values announced by an RCS client must be configurable by the Service Provider.

This use case is identical to the previous use case, except that in this instance User B (receiver) loses the ability to receive/process MSRP messages (this can for example be due to a client error, a reboot of the device, a loss of the data bearer and so on).

In the first flow diagram it is assumed that an Image Share transaction was taking place through MSRP:



Original phonebook pictures are shown (first screen) No RCS services are shown until status is clarified

It is not able to receive/process MSRP

Depending on the scenario, the sender may respond the BYE message

Available RCS services are updated (greying out relevant icons) based on received capabilities. If not received, no RCS services will be available

Figure 67: Non-graceful termination of picture sharing during a call

In the second flow it is assumed that a Video Share transaction was taking place through RTP:

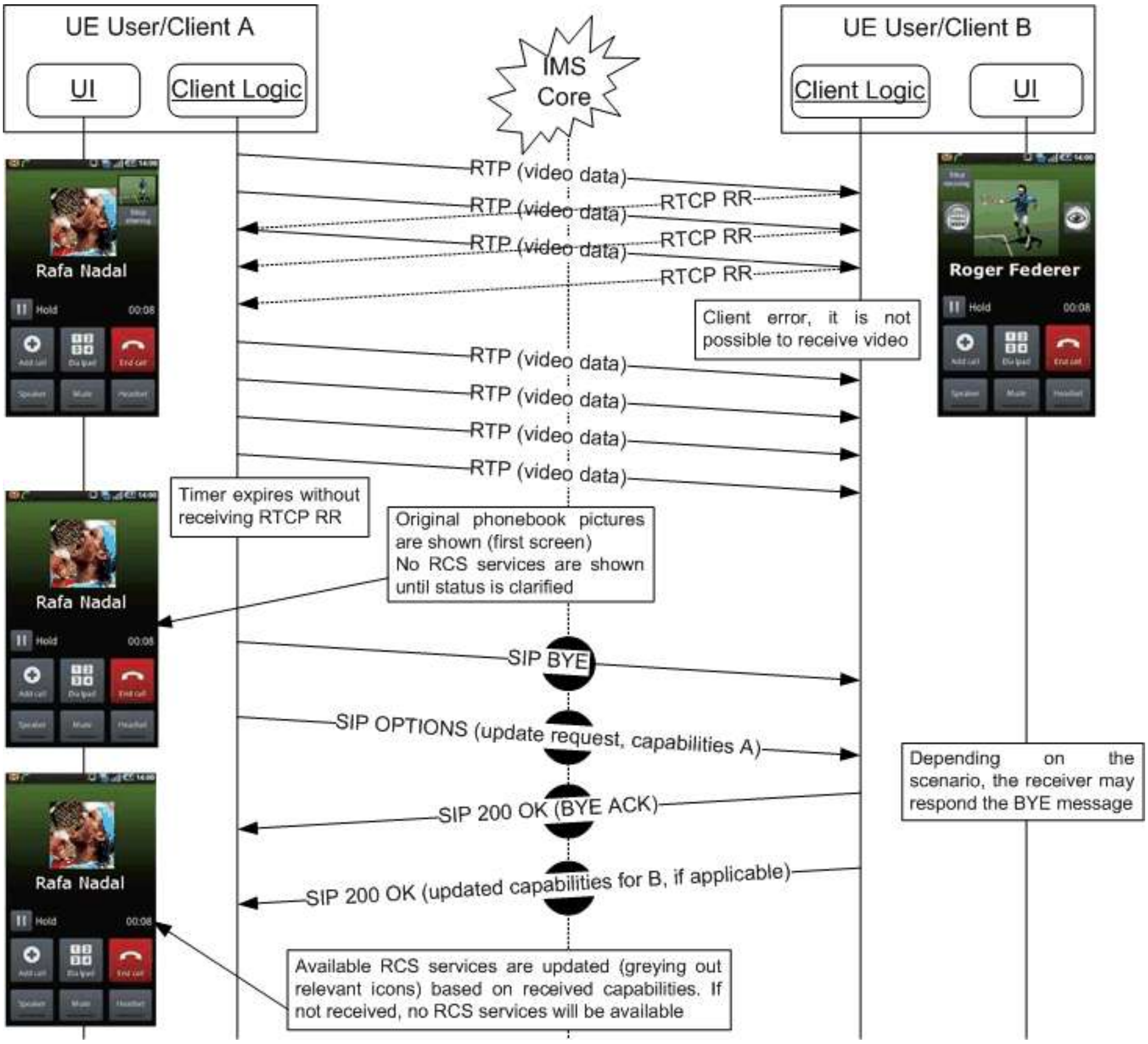

UE User/Client A
UI
Client Logic
IMS Core
UE User/Client B
Client Logic
UI
RTP (video data)
RTP (video data)
RTCP RR
RTP (video data)
RTCP RR
RTCP RR
Rafa Nadal
Roger Federer
Hold
00:08
Client error, it is not possible to receive video
RTP (video data)
RTP (video data)
RTP (video data)
RTP (video data)
Timer expires without receiving RTCP RR
Original phonebook pictures are shown (first screen)
No RCS services are shown until status is clarified
SIP BYE
SIP OPTIONS (update request, capabilities A)
Depending on the scenario, the receiver may respond the BYE message
SIP 200 OK (BYE ACK)
SIP 200 OK (updated capabilities for B, if applicable)
Available RCS services are updated (greying out relevant icons) based on received capabilities. If not received, no RCS services will be available

Figure 68: Non-graceful termination of video sharing during a call

3.6.5 NNI and IOT considerations

The NNI interfaces for content sharing services shall behave according to the procedures described in section 2.12 and referred documents.

3.6.6 Implementation guidelines and examples

3.6.6.1 Content Sharing during a call

As this is about sharing during a call, for both the sender and the receiver the sharing always starts from the call screen where the capabilities for sharing to the conversation partner in the voice call are shown. The user can then select one of the available services after which they will select the source of the sharing. A session will then be set up and the user will see the content that is being shared.

3.6.6.1.1 *Video Share*

The description above leads to following user experience for the initiator of a Video Share:

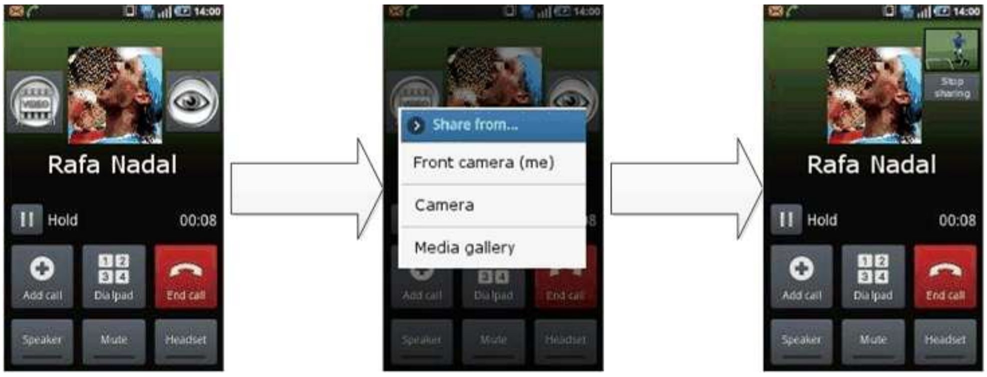


Figure 69: Reference UX for Video Share during a call (initiator)

A user invited for Video Share during a call first receives an additional invitation and if they accept, they are shown the video with the possibility to stop the sharing:

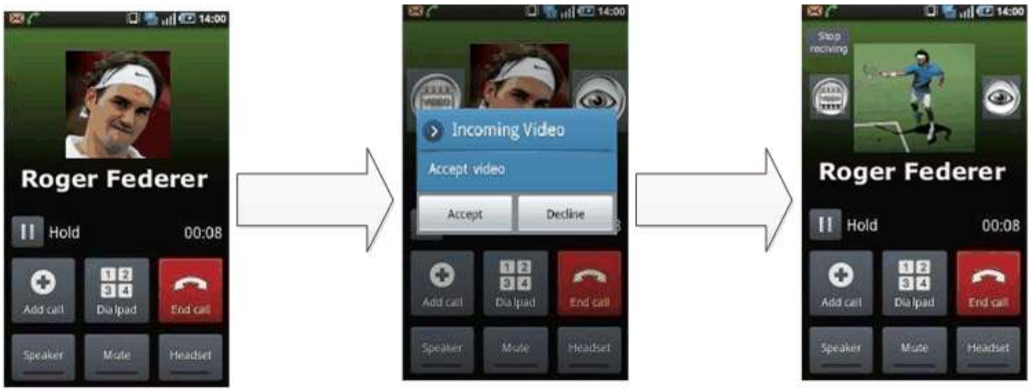


Figure 70: Reference UX for Video Share during a call (recipient)

Note: When the receiver accepts the sharing from the device that is involved in the voice call this acceptance applies automatically to all further sharing requests during that call.

3.6.6.1.2 *Image Share*

For Image Share the experience is similar than the one for Video Share shown in section 3.6.6.1.1. As it requires the transfer of a large file before something can be displayed rather than being able to stream immediately, there is a transfer delay. This leads to the following user experience for the sender:

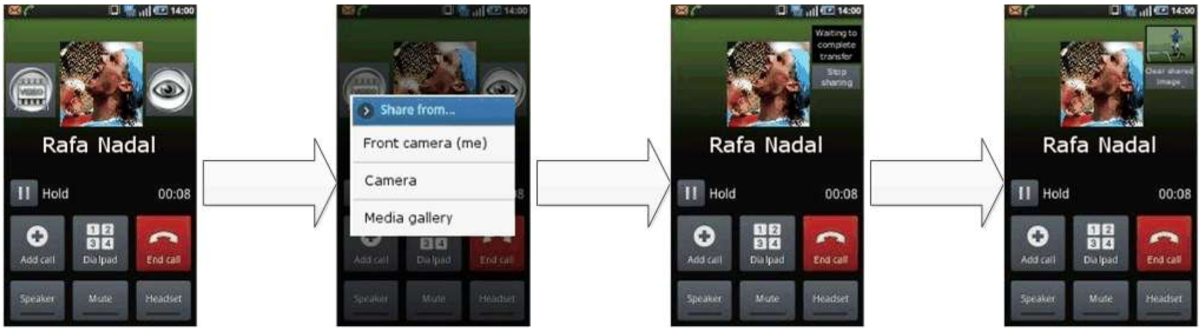


Figure 71: Reference UX for Image Share during a call (sender)

A user invited for Image Share during a call first receives an additional invitation and if they accept, they are shown the image with the possibility to stop the transfer initially and stop displaying the image once transferred:

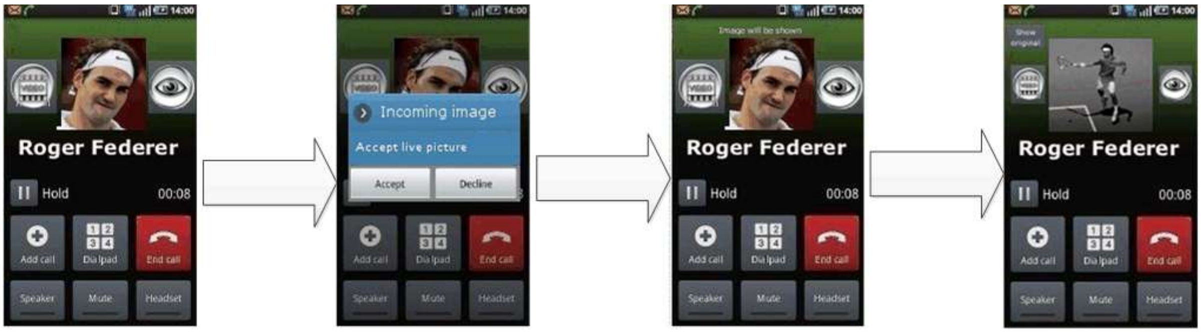


Figure 72: Reference UX for Image Share during a call (receiver)

Note: When the receiver accepts the sharing from the device that is involved in the voice call this acceptance applies automatically to all further sharing requests during that call.

3.6.6.2 Content Sharing without a call

From the UX, there are five possible entry points to these services:

1. Address book/Call-log: Content sharing can be initiated with any registered contact providing the right capabilities are in place – contact oriented initiation.
2. Media gallery/File browser: The user can browse, select a (media) file and then share with an RCS user – task contact oriented initiation. Only RCS capable users shall be displayed as candidate recipient of the sharing. Once video sharing is selected, the user will be presented with the complete list of RCS contacts (including contacts which are currently not registered).
   In this case, a capability exchange as defined in section 2.6.1 is performed once a contact is selected from the list.
3. Camera application: The experience is analogous to the media gallery/file browser experience with the difference that the user is able to only select the last video (and, in some cases, one video from the camera gallery) to be shared.
4. Chat window: From the Chat (one-to-one Chat only) window a video can be shared using the relevant button/icon. The experience is identical to the address book/call-log. The user is redirected to the media gallery or file explorer where he/she can choose a file or media content which then shared.
   The capability exchange as defined in section 2.6.1 is performed when the user opens up the menu in which the available content sharing options are offered
5. Call screen: They can share a video either by using the camera (front or back) or choosing a file from the media gallery. Please note this has been covered in detail in section 3.6.6.1.

When transferring a video whilst not in an existing session (i.e. when not in a call or Chat) and after the transfer has commenced (i.e. the user accepted the incoming file or content sharing session) the shared content is presented to the recipient in a Chat UX. This establishes a communication context for the transfer as the recipient may want to know why the sender is sharing the file. Please note that at the time the sharing is presented, the Chat session is not started; the Chat session will only start if and when the receiver sends a chat message back to the sender.

3.6.6.2.1 *Video Share*

For video transfer the behaviour follows the one described in section 3.6.6.2. Once the sharing commences, depending on the entry point the video is shown in a dedicated screen or within a screen applicable to the context. This leads to following handling for the different entry points

- Address book/Call-log: Following the address book interaction, the user can select the source of the content they would like to share (the media gallery or one of the available cameras). Once the sharing commences, the shared video is shown on the screen until the user terminates the sharing

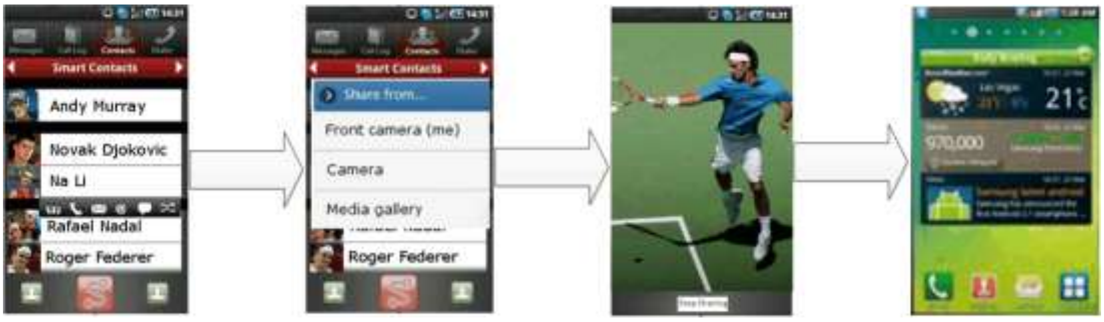


Figure 73: Reference UX for accessing Video Share without a call from address book/call-log

- Media gallery/File browser: The user can browse, select a video to share with another RCS user.

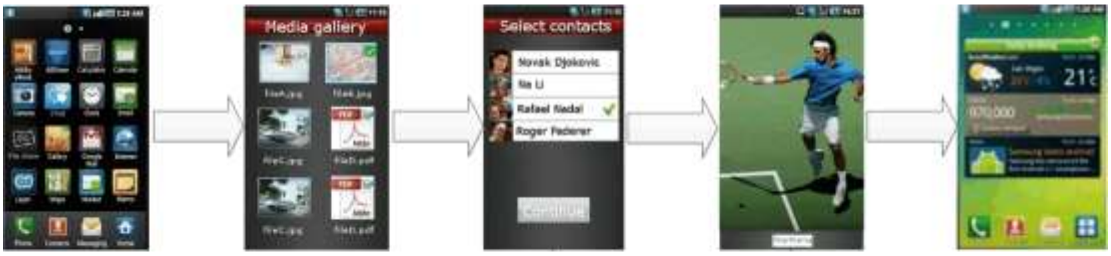


Figure 74: Reference UX for accessing Video Share without a call from media gallery

- Camera application: The experience is analogous to the media gallery/file browser experience with the difference being that the user is able only to select sharing the live image captured by the camera (and, in some cases, the last video or a video from the camera gallery) to be shared.
- Chat window: From the Chat (one-to-one Chat only) window a video can be shared using the relevant button/icon. The experience is identical to the address book/call-log. The user is redirected to the media gallery where they can choose a video which is then shared or use the camera to share a live video.

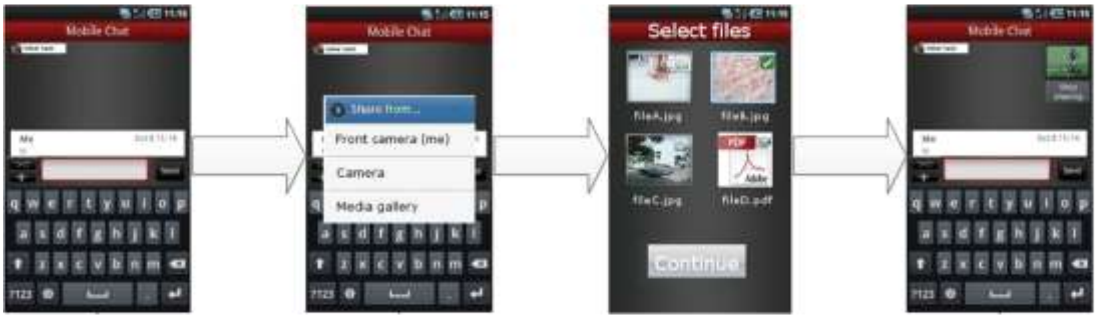


Figure 75: Reference UX for accessing Video Share without a call from chat window

- Call screen: This is video sharing during a call and has been covered in detail in section 3.6.6.1.1

For the recipient the video sharing is handled through a chat user experience meant to provide a communication context to discuss the shared content if needed. The Chat session needed for that will only be established as soon as the recipient wants to send a message to the sender. This leads to following user experience:

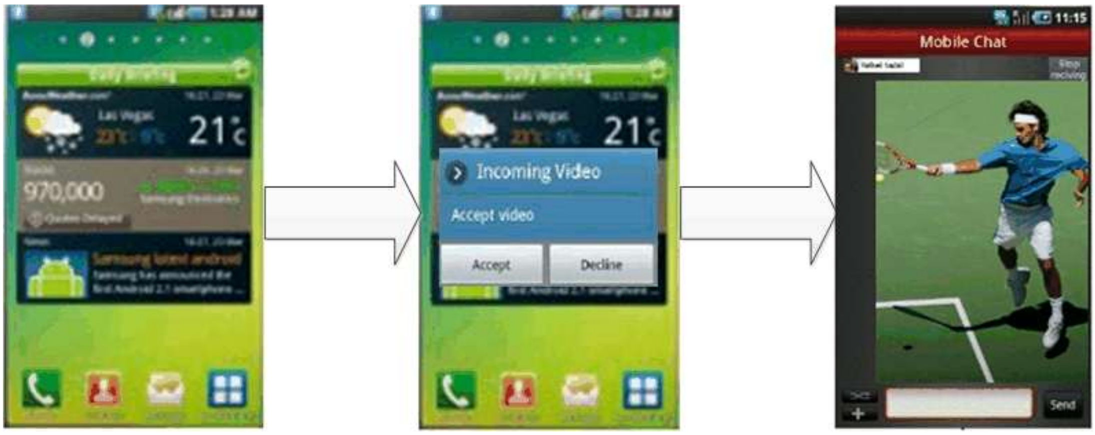


Figure 76: Reference UX for accessing Video Share without a call for the receiving side

If there was already an ongoing chat session when the invitation for Video Share came in, that session is reused for showing the video rather than starting a new one:

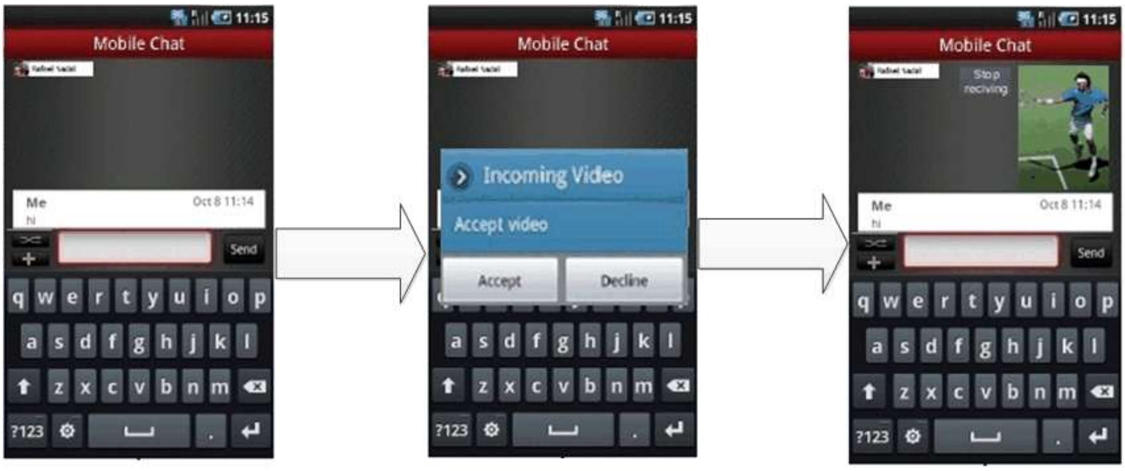


Figure 77: Reference UX for accessing Video Share without a call for the receiving side during a chat

3.7 Social Presence Information

3.7.1 Feature description

3.7.1.1 Social Presence definition

Social presence is seen as a piece of information for buddies to let them know about what you are doing, your mood, status, and so on. The user is given the possibility to publish personal data, which configures the users Social Presence Information, or “personal profile”.

As an illustration, the group of contacts with whom a presence relationship is established can be seen as the closest contacts of a certain user (friends, family, colleagues, and so on.).

Social Presence Information (included in the personal profile) does not replace the legacy contact’s vCard in the address book of the user (for example. the contact name and other contact details shall not be impacted).

The Social Presence Information shall be controlled by the end user and easily configurable.

Having established a Social Presence Relationship with a certain contact, the Social Presence Information shall be visible from the Enhanced Address Book (EAB). It should also be visible from other places on the device, like for example the communications log, or message folders.

3.7.1.2 Service Fundamentals

In the EAB, the contact information is extended with social presence information and foresees the following attributes:

- Availability, indicates the user's (un)willingness to communicate,
- Portrait icon, depicting the user (e.g. a photo or image provided by the contact himself)
- Free text, including textual note and possibility to add emoticons (automatic translation of some specific characters into smileys)
- Favourite link, to publish hypertext link of personal and/or favourite site
- Timestamp, date of the last update of the profile, generated automatically.
- Geolocation, depicts the user location

The attributes Availability, Portrait icon and Favourite link are profiled from the standards bringing a new user experience.

The Availability allows a user to inform a contact that they are currently in a situation when it is possible/not possible to communicate.

The Availability is controlled fully by the user and not automatically switched on or off.

With the portrait icon, it is possible to publish a photo or an icon, which is shown in the EAB of the user's contacts. This is a new user experience while a user has full control of the portrait displayed at his contacts. Within RCS the size and dimension of the photo is specified.

The favourite link attribute allows sharing additional social presence information. Such a link can point to e.g. a blog.

With geolocation, two RCS users are able to see where they are located and share this information with each other.

Authorisation to share social presence is based on the symmetry principle.

If sharing of social presence is accepted after invitation, both parties will see each other's presence attributes. If social presence sharing is terminated by one of both parties, both parties will end seeing each other's social presence attributes.

When a social presence relationship with a contact is set up from one device (e.g. the broadband client on PC) this relationship will also be visible on the other device (e.g. a mobile device).

The RCS invitation experience is improved with a personalized invitation. For easy identification of invitations coming from contacts not yet registered in the user's address book, it is possible to define a nickname to be used in presence invitations.

By choosing whether or not the contact is a VIP contact (see section 3.7.1.4.9), it will be possible to choose for a contact with which social presence is shared whether updates to that contact's social presence information should be reflected in (near) real time or whether those updates should be retrieved through some low frequency polling for them.

3.7.1.3 Social presence attributes

3.7.1.3.1 *Availability status*

A user will be able to set the state of Availability status (as part of Social Presence Information)

There are two possible states that can be selected by the user, from their RCS Client:

1. **State#1.** From the RCS Client, the user can set Availability status information as state#1. This state is informative and means that user is available and willing to communicate The way state#1 is displayed to the user is implementation dependent, and subject to own Service Provider policies.
2. **State#2.** From the RCS Client, the user can set Availability status information as state#2. This state is informative and means that the user is unavailable or not willing to communicate (e.g. busy) and will probably not respond to any incoming calls or messages. The way state#2 is displayed to the user is implementation dependent, and subject to own service provider policies.

These states are informative. When a user sets Availability status information as state#1 or state#2 from the RCS Client, the user still has the possibility to make outbound communications (e.g. calls/messages) and receive inbound communications (e.g. calls/messages).

The Availability status information has a permanent nature. It remains unchanged until the user decides to modify it (as state#1 or state#2) from their RCS client

The Availability status information is not linked with any particular user's network connectivity situation (e.g. temporary loss of network connectivity, device switched off).

The RCS device and the Presence Server shall support the availability status feature.

The Service Provider shall be able to choose to enable or disable use of Availability status feature, according to its own Service Provider policies.

The RCS device of a user whose Service Provider enables the use of the Availability status feature, will not receive any Availability status information associated with a presence-enriched contact, which subscribes to a Service Provider, which has disabled the use of the Availability status feature.

The RCS device of a user whose Service Provider disables the use of the Availability status feature, will not display, subject to Service Provider policies and bilateral agreements between Service Providers, any Availability status information associated with a presence enriched contact which subscribes to a Service Provider which enables use of Availability status feature. Moreover, the RCS device does not offer to the user the ability to set Availability status information.

3.7.1.3.2 *Favourite Link*

One of the attributes in the Social Presence Information allows the user to add or update one hypertext link, which (when selected) may redirect, for instance, to an extension of the user's Social Presence Information (for example a mobile blog).

The user shall be able to edit the hypertext link (expressed as a Uniform Resource Identifier as defined in [RFC2396]) via two modes:

1. Manual mode, where the user types in manually the URI
2. Automatic mode, where the user selects one URI from a predefined list.

The Service Provider shall be able to choose whether to offer its customers only manual mode, only automatic mode, manual and automatic modes, or no mode at all.

A clickable link is displayed in a *detailed view mode* of the Social Presence Information, where shared information about the user (portrait icon, free text and URI) can be seen in larger size than in the EAB itself (*list mode*).

When the user edits a new hypertext link, those contacts, which the user has established a Social Presence Relationship with, are notified, that is a visual change of value of favourite link attribute, for example when the user updates their portrait icon or free text.

When a user clicks on the link of a presence-enriched contact, the appropriate native handler for linked content (for example browser) shall be launched.

When the user closes the handler, they return automatically to the presence enriched contact's *detailed view mode* of the Social Presence Information, from where the handler was launched.

A revoked contact shall not be able to click on the hypertext link. However, please note that there are no restrictions that prevent the watcher from being able to save the URI in their browser and further access to this URI.

It is possible to display a "user friendly" label for the favourite link instead of the actual URI.

Instead of displaying the URI the RCS user can display a personal label. The maximum size of characters recommended is 20 (this can be set by Service Providers as a provisioning parameter). It shall not be larger than 200 characters.

3.7.1.3.3 *Geolocation information*

Geolocation information is a combination of declarative text always manually edited/updated by the user; and/or coordinates information (x, y) that are displayed on a map.

The maximum character size of declarative location text information the end-user can enter can be set by the Service Provider as a provisioning parameter. It shall not exceed 200 characters. The text information on the receiving part cannot exceed 200 characters and is not limited by any provisioning parameter.

Time Zones can be shared as part of geolocation information, allowing users to view what the local time is at their friend's location.

A provisioning parameter can be set in the network by Service Providers to control the maximum time the published location information will be considered to be valid (for example, one month).

The user must be able to delete his location information (empty text field, no position on map).

Location information must be interoperable between RCS clients no matter how users choose to update their information. For example, if User A has updated his location on a map (with x, y coordinates) and User B (authorized contact) is using RCS clients without a map feature (and only supporting declarative text), they must still be able to view User A's location as a intelligible text, using the declarative text information (if available), not as raw x, y information.

To avoid excessive traffic on the network due to very frequent location updates, it is recommended that a provisioning parameter can be set in the network to remotely set a minimum duration between updates sent from the client/device.

The geolocation feature can be provided on non-GPS (Global Positioning System) enabled devices.

3.7.1.4 Social Presence Authorization

RCS users shall feel confident in publishing their Social Presence Information, and be guaranteed that their privacy is respected. Therefore, mechanisms are defined below that allow users to accept/reject an invitation to establish a Social Presence Relationship, since this may imply sharing certain potentially private information, such as portrait icon or free text.

3.7.1.4.1 *Social Presence Information sharing request principles*

Reactive authorization shall be used, that is when User A invites User B to share Social Presence Information, User B receives an authorization request.

When receiving an invitation to share Social Presence Information from User A, User B can:

- **Accept** the invitation.
- **Ignore** the invitation, which requires an explicit action by User B.
- **Block** User A from sending more invitations.
- **Not answer**, that is do nothing with that request

Invitation to share Social Presence Information automatically implies the authorization of the requesting user, that is, when User A invites User B to share Social Presence Information, User A automatically authorizes User B to see their Social Presence Information.

If User A's MSISDN is associated with a contact in User B's address book, the name given to that contact shall be displayed within the invitation to share Social Presence Information.

Symmetric authorization shall be used. The publication of Social Presence Information shall be bidirectional.

User A shall not receive any notification whether User B has not answered, blocked or ignored their invitation to share Social Presence Information.

Once a Social Presence Relationship has been established, the user can stop that relationship via the following action:

Revoke the Social Presence Relationship.

3.7.1.4.2 *Accept*

If User B accepts User A's invitation to share Social Presence Information, User A will see User B's Social Presence Information, and User B will see User A's Social Presence Information.

If User A is not an existing contact in User B's address book, it shall be facilitated that User B stores the contact details of User A in their address book.

3.7.1.4.3 *Ignore*

If User B ignores User A's invitation to share Social Presence Information, neither User A nor User B shall be able to see each other's Social Presence Information.

Ignoring an invitation to share Social Presence Information shall not mean blocking the contact that has sent the invitation, i.e. it shall still be possible to receive more invitations from that contact.

If User B ignores User A's invitation to share Social Presence Information but later, User B decides to share their Social Presence Information with User A, then it is not necessary that a new authorization request is issued to User A. User B, by adding User A to their EAB completes the symmetric authorization process. As a result, User A and User B will be seeing each other's Social Presence Information.

3.7.1.4.4 *Block (refuse to receive any further invitation)*

In order not to receive more invitations from a certain contact, the user shall be given the possibility to add that contact to a list of blocked contacts (blacklist).

The blocking mechanism shall be transparent to the blocked user, that is, if User B blocks User A, User A shall never be notified that he/she has been blocked by User B.

The possibility shall be given to remove a certain contact from the blacklist, i.e. User B shall be able to see in their EAB that User A has been blocked, and to remove them from the blacklist.

3.7.1.4.5 *Not answer (pending invitation)*

If User B does not answer User A’s invitation to share Social Presence Information, the invitation shall be in a pending state, for which an action is expected by User B.

Pending invitations to share Social Presence Information with User A, for which an answer has not yet been provided, shall be accessible for User B, so that User B can choose to answer the invitation that is Accept, Ignore or Block.

Subsequent invitations (from User A to User B) replaces User A's initial invite, and function as a reminder for User B that a corresponding action (on their part) regarding the invitation to share SPI is required. That is, User B needs to choose an option

- Accept,
- Ignore, or
- Block.

3.7.1.4.6 *Revoke*

Once a Social Presence Relationship has been established, the possibility shall be given to stop the sharing of Social Presence Information with a certain contact, while at the same time removing your Social Presence Information from that contact’s EAB.

If User A revokes the Social Presence Relationship with User B, both users shall not receive any further updates of their Social Presence Information, according to the symmetry principle.

When User A revokes the Social Presence Relationship with User B, User B shall no longer be displayed as a presence enriched contact.

User B’s Social Presence Information shall not be shown to User A

Only User B’s contact details (vCard) shall remain visible in User A’s address book (for example name, MSISDN, e-mail, and so on.

If User A revokes the Social Presence Relationship with User B, User B shall no longer have access to User A’s Social Presence Information.

Before actually performing the revoke, User A shall see a notification alert in the client informing him about consequences of this action. These are:

- User A’s Social Presence Information will be removed from User B’s EAB, so User B will notice the revoke after a certain period of time (for example several hours/days)
- It will be possible for User A and User B to invite each other again.

After a Social Presence Relationship has been revoked for a given period of time (for example several hours/days), both users can reinitiate the process of Social Presence Authorization, that is User A shall be able to invite User B to share Social Presence Information, and vice versa.

It must be noted that User A may immediately re-invite User B to share Social Presence Information.

If User A deletes User B’s vCard from their address book, all contact information is deleted from User A’s address book. If a Social Presence Relationship between User A and User B exists at the moment of deleting the contact, this relationship shall be revoked.

3.7.1.4.7 *Personalized Invitation*

To improve RCS invitation experience with a personalized invitation and to ease identification of invitations coming from contacts not yet registered in the user's address book, a nickname feature is provided:

- If the terminal supports configuring a nickname, the user can choose a "nickname" with limited size (recommendation: 20 characters, this size can be set as a provisioning parameter). This nickname is provided in all future invitations to share presence, until it is changed. The maximum number of characters an invitee can view is 200 (this limitation is proposed to ensure interoperability for invitee, regardless of the number of characters implemented by the service provider).
- The invitee, if they do not have the inviter information in their address book, can now see both MSISDN and the nickname of the inviter.
- The nickname is stored permanently to be used for every invitation. Users have the ability to change it every time they send an invitation.
- The nickname does not replace the registered name of a contact already present in the recipient's address book.

Security: it is noted that through the use of the nickname, it is possible to "impersonate" someone. However, that "impersonation" is limited in scope since the inviting user remains identified by his MSISDN and the fact that the feature is only used for MSISDNs that are not already stored in the recipient's address book.

3.7.1.4.8 *Geolocation authorization*

Two users should be able to see where they are located and share this information with each other and they would keep the control over this information:

- No specific invitation process for location.
- When and if a user chooses (by opt-in) to update their location for the first time, by default, users do not share their location information with all their contacts authorized for social presence
- Users have the ability to manually choose contacts with whom they wish to share location information.
- Even if a user is not sharing location information with one of their authorized contacts, that does not prevent them from viewing that contact's location information

Once User A has accepted User B as an RCS authorized contact, User B will be able to see the geolocation information of User A (displayed with a text or a map, or both of them) and all updates of that information.

When a given RCS user (User A) is willing to share Social Presence with another user, User A shall be able to control in the invitation process for sharing Social Presence whether sharing of their location information with this other user is authorized or not.

3.7.1.4.9 *VIP contacts*

As the number of SPI enabled contacts increases in the user's address book, the amount of information that the user receives in the mobile phone will increase making it more difficult to differentiate useful information from noise. In addition, the RCS users will not want to share the same Social Presence Information with all their contacts.

The selection of certain contacts as Very Important Person (VIP) contacts will allow the end user to specify which contacts are the most important ones.

The user should be able to differentiate the contacts, which they share SPI with, between important and unimportant contact. The user shall receive real time notification of status changes from VIP contacts.

The user will be able to choose from the contacts to set them as VIP contacts. The user will then only receive real time notifications of the social presence information from the contacts set as VIP contacts (probably with a phone buzz or light, or via an idle screen widget and so on). The contacts that are not set as VIP contacts will still be updated in the EAB, but not in real time, therefore the user is made aware of the new social presence information when they browse the EAB.

3.7.1.5 Example Use Cases

3.7.1.5.1 *Social Presence Information Use Cases*

3.7.1.5.1.1 Invite Contacts to Share Social Presence

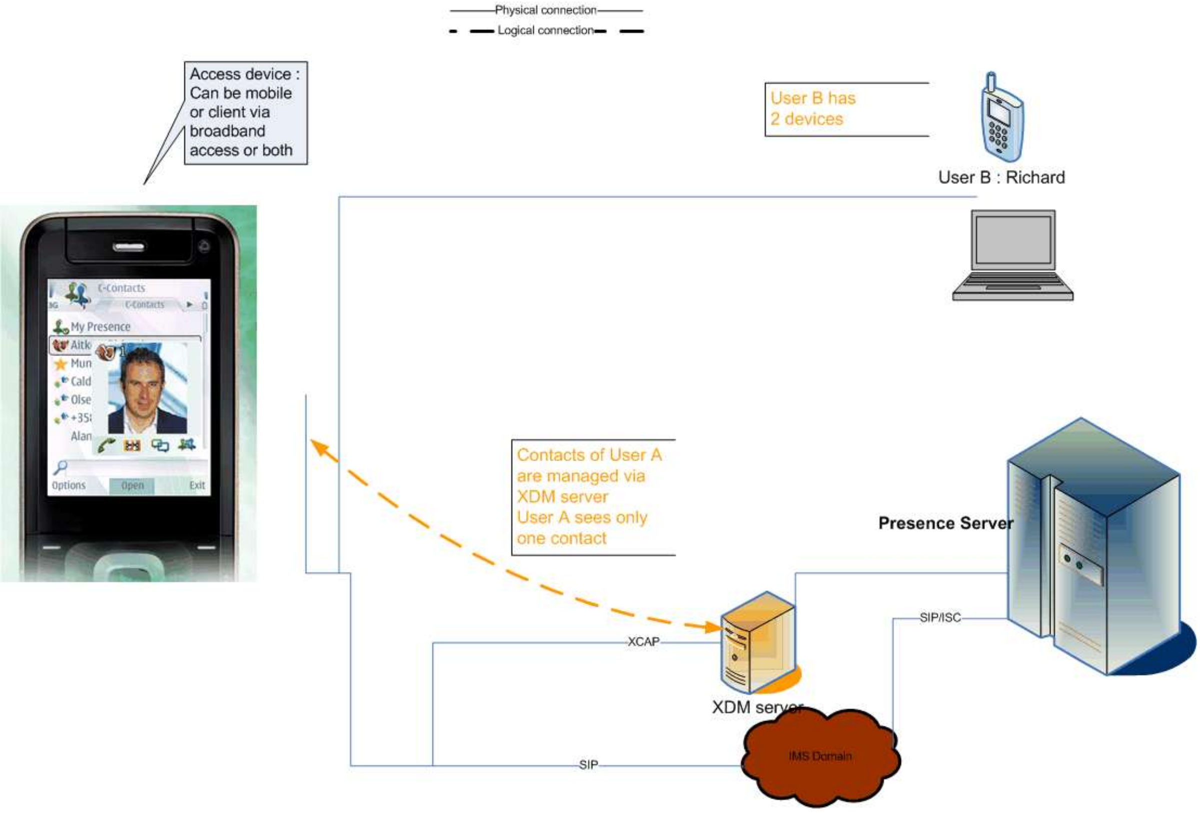


Figure 78: Invite Contacts to Share Social Presence

Authorization to share social presence is based on the symmetry principle.

If sharing of social presence is accepted after invitation, both parties will see each other's presence attributes. If social presence sharing is terminated by one of both parties, both parties will end seeing each other's social presence attributes.

It is possible to share with an invitation for social presence a nickname if the invited party does not have the inviting party's phone number in the device.

3.7.1.5.1.2 Allow Contacts to obtain Location Information

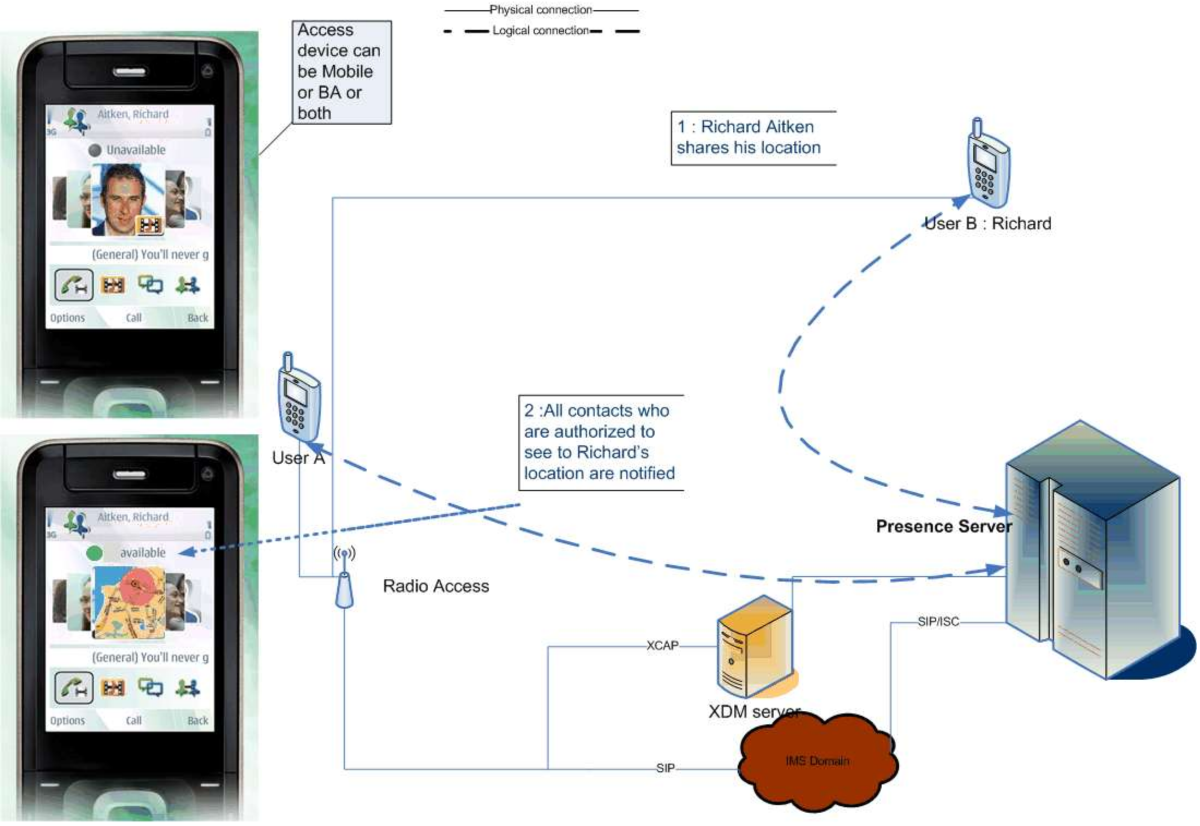


Figure 79: Share Location

This service allows users to show where they are through the RCS EAB and view where their friends are as free text and/or on a map.

Note: If the contact that is updated but not in the VIP group the information (Richard Aitken in the use case) in their VIP group may not be seen immediately. They will only see it when either their client polls for updates of the non-VIP contacts or when they request for an update of the non-VIP contacts themselves. The user may even miss the update altogether if there is another update before the status of the non-VIP contacts is retrieved.

3.7.1.5.1.3 Availability

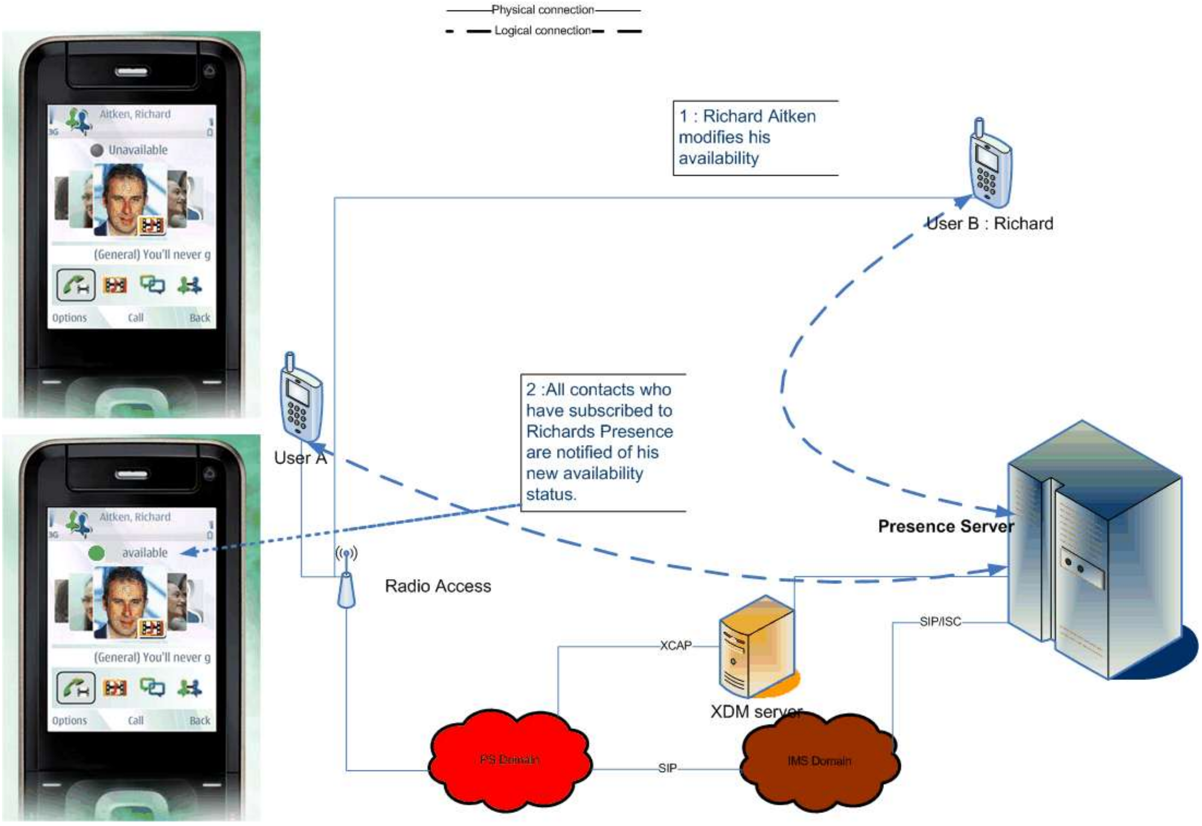
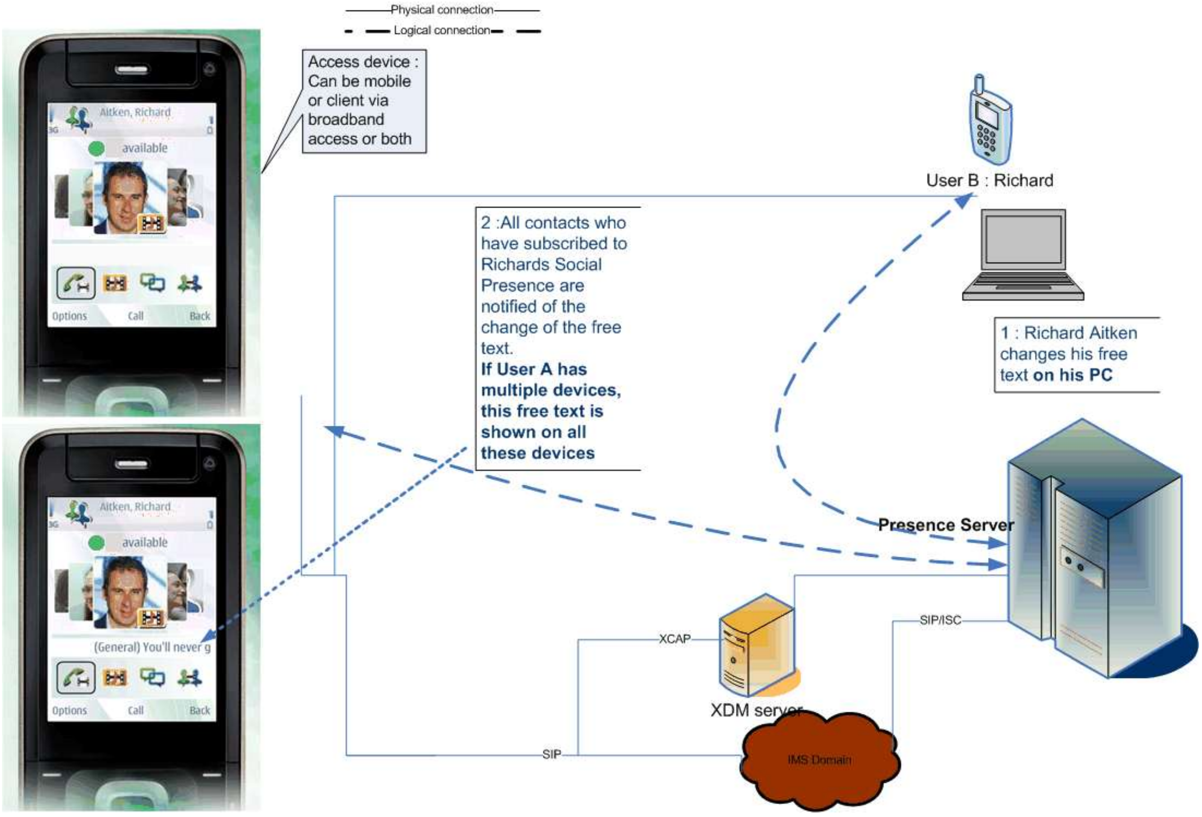


Figure 80: Availability

Note: If the contact that is updated is not part of the VIP group of the user the updated SPI (Richard Aitken’s in the use case) may not be seen immediately. They will only see it when either their client polls for updates of the non-VIP contacts or when they request for an update of the non-VIP contacts themselves. The user may even miss the update altogether if there is another update of the availability status before the status of the non-VIP contacts is retrieved.

3.7.1.5.1.4 Free Text



Access device : Can be mobile or client via broadband access or both

1 : Richard Aitken changes his free text **on his PC**

2 :All contacts who have subscribed to Richards Social Presence are notified of the change of the free text. **If User A has multiple devices, this free text is shown on all these devices**

Figure 81: Free Text

Note: If the contact that is updated is not part of the VIP group of the user, the updated SPI (Richard Aitken’s in the use case) may not be seen immediately. They will only see it when either their client polls for updates of the non-VIP contacts or when they request for an update of the non-VIP contacts themselves. The user may even miss the update altogether if there is another update before the status of the non-VIP contacts is retrieved.

3.7.1.5.1.5 Portrait Icon Exchange

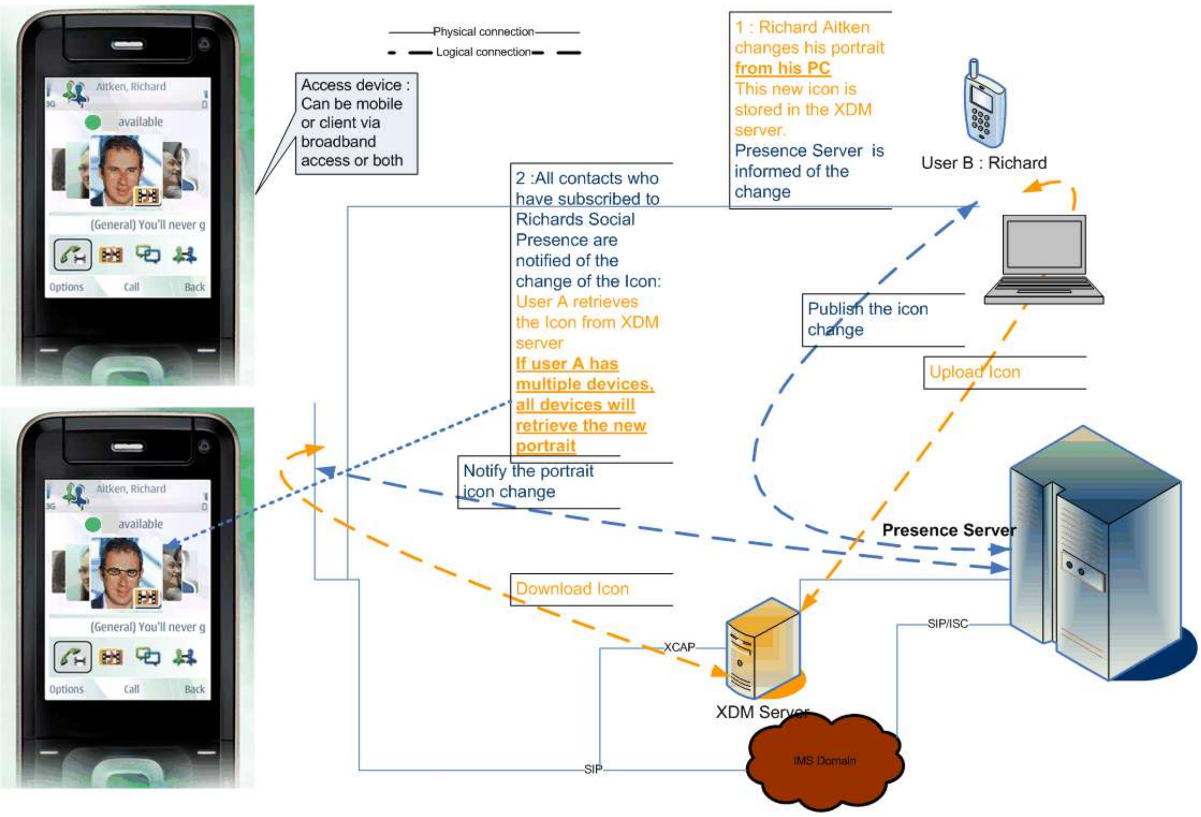

Physical connection
Logical connection
Access device : Can be mobile or client via broadband access or both
1 : Richard Aitken changes his portrait from his PC
This new icon is stored in the XDM server.
Presence Server is informed of the change
User B : Richard
2 :All contacts who have subscribed to Richards Social Presence are notified of the change of the Icon:
User A retrieves the Icon from XDM server
If user A has multiple devices, all devices will retrieve the new portrait
Publish the icon change
Upload Icon
Notify the portrait icon change
Presence Server
Download Icon
XCAP
SIP/ISC
XDM Server
IMS Domain
SIP
Aitken, Richard
available
(General) You'll never g
Options
Call
Back

Figure 82: Portrait Icon Exchange

Note: If the contact that is updated is not part of the VIP group of the user the updated SPI (Richard Aitken’s in the use case) may not be seen immediately. They will only see it when either their client polls for updates of the non-VIP contacts or when they request for an update of the non-VIP contacts themselves. The user may even miss the update altogether if there is another update before the status of the non-VIP contacts is retrieved.

3.7.1.5.1.6 Who Can I Invite?

New user wants to invite their friends to share social presence.

- User A goes to their RCS enhanced address book
- User A traverses through the list of contacts and sees that User B is also an RCS user that supports the SPI service
- User A decides to send an invitation to share Social Presence Information to User B.

3.7.1.5.2 *Personalized Invitation with a Nickname*

3.7.1.5.2.1 User A Invites User B and Fills Out their Nickname. User A Is Present in User B’s Address Book

- When User B receives the invitation, it is the contact name entered in User A’s v-card that is used, not the nickname.
  - For example, User B can read “<User A v-card name> <MSISDN> wants to share presence information with you.”

3.7.1.5.2.2 User A Invites User B and Fills Out His Nickname. User B Has Not Created a Contact Card for User A in their Address Book

- When User B receives the invitation, the nickname is used to present the invitation to User B

  - For example, User B can read "<User A nickname> <MSISDN> wants to share presence information with you."
- If User B accepts the invitation, a contact card is created. User A's nickname can be used to reference the contact card in User B's address book.

3.7.1.5.3 *Geolocation*

3.7.1.5.3.1 Manual Free Text

- User A set his location manually (for example, I am in Paris)
- User B sees that User A is in Paris.

3.7.1.5.3.2 Manual Position on a Map

- User A decides to update his location. They drag and drop a pin on a map and then confirm the position. Even though User A is located in Paris, France, they select New York as a location on the map.
- User B receives a notification.
- User B sees that User A is in New York.

3.7.1.5.3.3 Semi-Automatic Filling

User A decides to edit his location status. They click on the location update button, and their location is automatically filled in the dedicated field decides to edit their location status.

3.7.1.5.3.4 Fully Automatic Opt-In Mode

User A decides that they want their authorized contacts to be informed regarding their position on a regular basis (period to be defined), they click on the "authorize my contacts to view my location" button (opt in). If they decide to end this broadcast they always have the ability to opt out through the same button.

In all cases, User B (authorized contact in User A's address book) is notified as he would be notified of other presence information, such as status text.

3.7.1.5.3.5 Blocking an Authorized Contact from Viewing Location

- User A and B are authorized RCS contacts who have updated their location information
- User A decides to hide their location from User B, while still sharing it with his other authorized contacts
- User A goes to his location settings currently set to "Share my location with all my authorized contacts" to "Prevent some authorized contacts from viewing my location"
- User A adds User B in the list of contacts blocked from viewing their location
- User B does not see User A's location information anymore
- User A still sees User B's location

3.7.1.5.4 *VIP Contacts*

3.7.1.5.4.1 User sets a contact as a VIP

User A is an RCS user.

User B is an RCS user.

User A and User B had established a Social Presence Information sharing relationship.

Call Flow:

- User A sets User B Contact as a VIP contact in his Address Book.
- User B changes their Social Presence Information.

- User A receives an active notification (phone buzz or light, idle screen widget) about the change.

3.7.1.5.4.2 User sets a contact as a non-VIP

User A is an RCS user.

User B is an RCS user.

User A and User B had established a Social Presence Information sharing relationship.

User A had previously set User B as a VIP contact.

Call Flow:

- User A sets User B Contact as a non-VIP contact in his Address Book.
- User B changes their Social Presence Information.
- User A does not receive any active notification about the change but if they access later their EAB and browse to the User B contact, the EAB will display the changed information.

3.7.2 Interaction with other RCS features

Social Presence information in the device is linked with the local address book available in the device:

The social information elements of a contact in an RCS device are, from user interface point of view, associated (as an extension of other address book contact information) with the contact entry of the address book.

This correlation is local:

- Local contact information may be synchronised with a Network address book
- Extended presence information is obtained through the Network Presence enabler

3.7.3 High Level Requirements

3-7-1 An RCS user with broadband access shall be able to access the Enhanced Address Book, supporting all the social presence features.

3-7-2 A broadband access client should support Social Presence Authorization.

3-7-3 The presentity shall be able to edit the Social Presence Information from any of the devices he/she has and shall see the changes from every device he/she has

3-7-4 Social Presence Information shall be handled in such a way that the latest update is presented to the watching user's client

3-7-5 The invitation to share Social Presence Information shall be shown in all of the presentity's devices

3-7-6 The presentity shall be able to authorize watchers from any of the devices they have

3-7-7 If a certain setting may limit the user experience provided to the end user, this information should be clearly shown in the user interface. In addition this allows the user to be aware of this limit while interacting with the service (for example, maximum number of characters to be included in the free text of the Social Presence Information, or maximum size of a file to be transferred).

3-7-8 The User shall be able to share location information as social presence information with his/her authorized contacts

3-7-9 The User shall be able to define a list of contacts blocked from viewing his/her location information, within his list of authorized contacts for presence

3-7-10 The User shall be able to specify their location through manual or automatic modes, as free text or as coordinates on a map

3-7-11 The User shall be able to de-activate automatic updates or delete their location information at any time, to protect their privacy

3-7-12 The User shall be able to share location information even if he/she is using a non-GPS device

3-7-13 The Service Provider shall be able to limit the frequency of automatic updates to avoid network overload

3-7-14 The RCS user shall be able to set an expiration date for location information

3-7-15 The User shall be able to define a nickname transmitted to his contacts when sending invitations, in addition to the MSISDN

3-7-16 The User shall be able to change that nickname at any time, especially before sending invitations

3-7-17 The Service Provide shall be able to specify the maximum length of the nickname

3-7-18 The Nickname shall never automatically replace the existing registered name of a contact in the invitation recipient’s phonebook

3-7-19 The User shall be able to specify a text label displayed in lieu of the personal URL

3-7-20 The User shall be able to change the URL label at any time

3-7-21 The Service Provider shall be able to specify the maximum size of the URL label

3-7-22 An RCS user shall be able to set a contact as a VIP contact.

3-7-23 An RCS user shall be able to unset a contact as VIP.

3-7-24 When a VIP contact updates his Social Presence Information the user shall get a real time notification of the change and it shall be displayed on the RCS client (phone buzz or light indication, idle screen widget).

3-7-25 When a non-VIP contact updates their Social Presence Information, the user shall not be notified in real time about the changed status. The RCS client shall keep that information up to date (but not in real time) so the contact information is updated when the user browses the EAB.

3-7-26 The update mechanism for updating non VIP contacts shall be a periodic polling mechanism from the RCS client resulting in an aggregated notification from the network. The update period shall be configured by the RCS Service Provider by parameter.

3-7-27 In addition, an RCS user shall be able to manually request an update of all the non-VIP contacts.

3.7.4 Technical Realization

3.7.4.1 Network architecture of Presence enabler in RCS 5.0

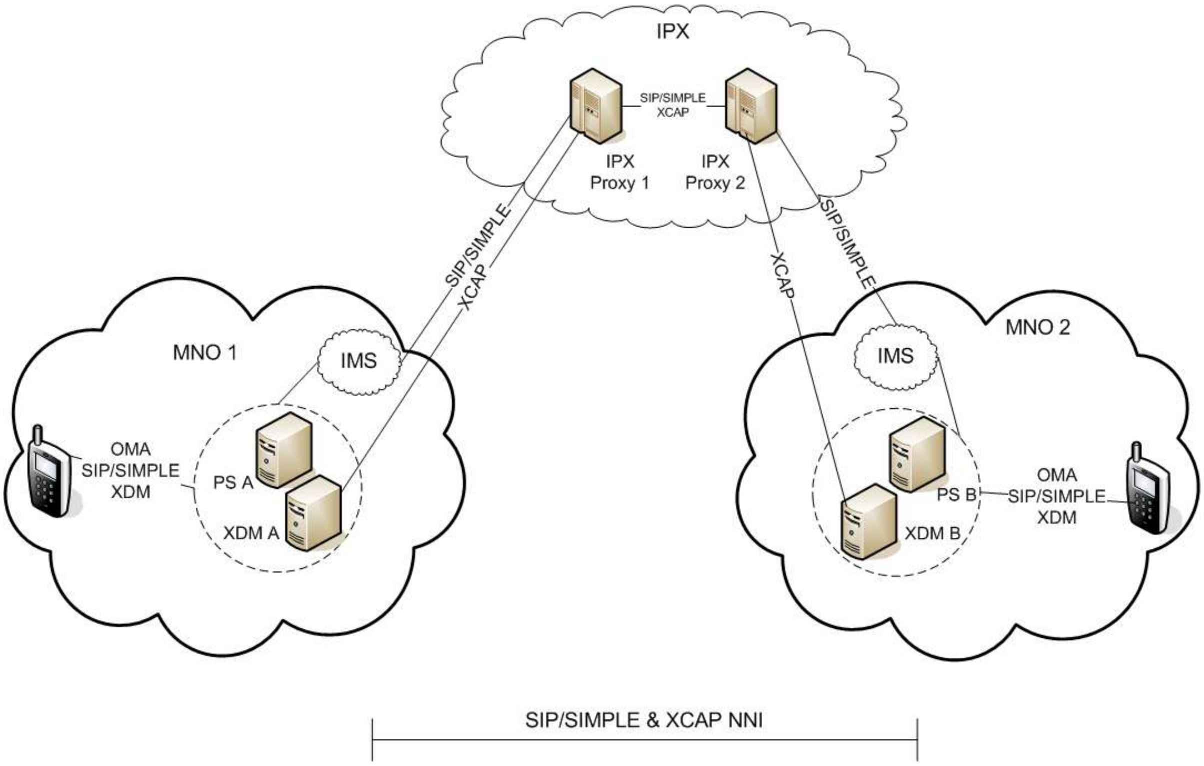


Figure 83: Overall Architecture of Presence as a part of RCS 5.0

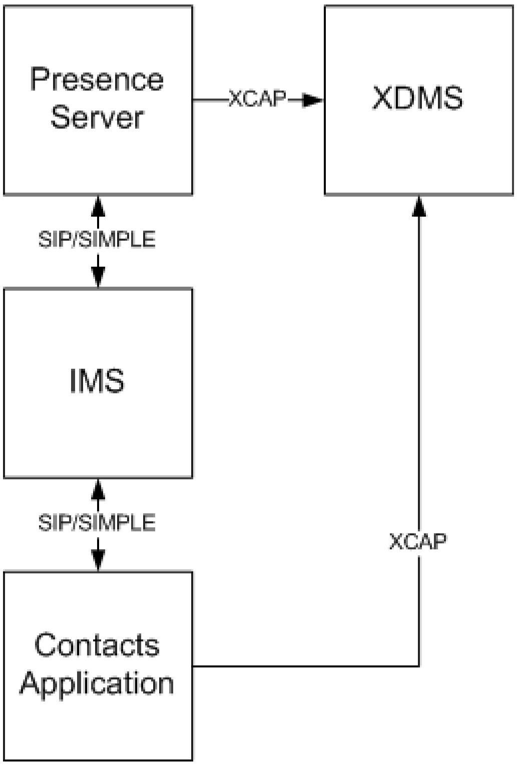


Figure 84: RCS Presence Architecture

Presence and capability architecture in RCS is based on [Presence].

Users share their Social Presence Information (“Presence Enhanced Address Book”)

- Implemented using the Presence SIMPLE protocol

Users share their communication capability information (“Capability Enhanced Address Book”)

- Can be implemented using the Presence SIMPLE protocol (see section 2.6.1.2)

According to [PRD-IR.65], the interworking connection should be carried out via IMS core systems. There is therefore no requirement to interface Presence Servers directly.

Optimization of Presence & XDM enabler according to work in OMA PAG working group has to be taken into account as a very important design principle. It is also important to notice potential issues such as battery drain in the terminal caused by the general always-on functionality and the number of Presence & capability updates.

Generally, the Shared XDMS (XDM server) as defined in [XDM1.1_AD] shall be used for storing all presence-related lists, for example, the list of subscribed contacts (“buddy” list) and the presence authorization lists. In this way, the RCS client only needs to operate on lists in Shared XDMS, and initially set the documents in RLS (Resource List Server) XDMS and Presence XDMS.

3.7.4.2 Presence Data Model

3.7.4.2.1 *Overview*

Implementation guidelines for the size/length of Presence information elements given in [PRESENCEIG] should be followed.

The following sections illustrate the details of the *Person* and *Device* parts of the Presence Data Model. The Service part of the model has been described in section 2.6.1.2.5.

3.7.4.2.2 *Person*

Attribute	Specification	Comment
Person: <presence> -> <person>	[Presence2.0_DDS]	According to the presence schema defined in the [Presence], person related information is modelled with the person element. Each client only publishes one person element.
Willingness: <person> -> <overriding-willingness> -> <basic>	[Presence2.0_DDS]	The presentity terminal publishes this attribute in which it wants to indicate its willingness to communicate: “Open” = Willing “Closed” = Not Willing Attribute not present = Unknown
Icon: <person> -> <status-icon>	[Presence2.0_DDS]	It’s used as dynamic avatar. If the element is not present the client may choose to display icon stored in the address book. The picture shall not be included directly in the presence requests, but a HTTP URL shall be used. Presence Content XDMS procedures as specified in OMA Presence 2.0 and XDM 2.0 is used for uploading, publishing and retrieving the icon For further details see section 3.7.4.2.2.2
Favourite Link : <person> -> <link>	[Presence2.1_DDS]	The <link> element provides a URI pointing to general information about the tuple or person, typically a web home page. This is information is complemented with a “label” attribute set to a value provided by the served RCS presentity and a priority attribute which is intended to cope with situations in which there are multiple <link> elements. In RCS only one such <link> element will be included in the presence document though. The priority attribute will therefore always be set to 0.8.
Descriptive Location Text <person> -> <place-type> -> <other>	[Presence2.0_DDS]	The presentity may provide a descriptive text describing his location See section 3.7.4.2.2.3 for more information on the handling of the expiry of this information Note: Support for the enumerated values defined in [RFC4589] is thus out-of-scope for RCS. It is out of scope of RCS how a client will handle these enumerated values when received nevertheless.
Time Zone <person> -> <time-offset>	[Presence2.0_DDS]	The presentity may use this element to provide information on his current time zone See section 3.7.4.2.2.3 for more information on the handling of the expiry of this information
Geographical Information <person> -> <geopriv> -> <location-info> -> <usage-rules>	[Presence2.0_DDS]	This element can be used to provide geographical location information on the presentity. The accuracy of which can be controlled by the user. See section 3.7.4.2.2.3 for more details on its encoding and on the handling of the expiry of this information
Note: <person> -> <note>	[RFC4479]	The presentity may write a piece of free text and/or to add emoticons to be shown to watchers in their contacts books The list of emoticons in RCS can be found in [RCS5-SIMPLEIM-ENDORS]
Timestamp: <person> -> <timestamp>	[RFC4479]	Timestamp when the presence information was published.

Table 38: Presence data model attributes

Note1: “Willingness” is sometimes indicated in a client as “Availability”. However since it is managed by the user themselves and does not imply that communication is not possible, within OMA specifications this is considered as willingness. Availability indicates that on a technical level communication will be possible. Service Availability and Willingness are study items for later releases.

Note 2: the priority of 0.8 for the link was included to allow including links with higher priority in some future RCS release.

3.7.4.2.2.1 Willingness

A Service Provider provisioning parameter (AVAILABILITY AUTHORIZATION as described in section A.1.1.2) is provided indicating whether or not the use of willingness is enabled by the service provider. If it is disabled, no OMA <*overriding-willingness*> element is included in the presence document. If the willingness is enabled, the RCS client will include in the presence document an OMA <*overriding-willingness*> element as specified in [Presence2.0_DDS] with the <*basic*> sub-element set to “closed” when the user has indicated that he’s not willing to communicate. Otherwise if willingness is enabled, the published presence document will indicate a value of “open” for the <*basic*> sub-element of <*overriding-willingness*>.

3.7.4.2.2.2 Icon

The icon shall have following characteristics:

Document Name	rcs_status_icon
Icon aspect ratio (width:height)	3:4 or 4:3
Icon maximum dimensions	240x320
Icon minimum dimensions	60x80
Icon file type	gif (Graphics Interchange Format, both static and animated), jpeg (Joint Photographic Experts Group) or png (Portable Network Graphics) as defined in [Presence_Content]
Document maximum size	200 kilobytes (kB)

Table 39: Characteristics of the icon

Note 1: Fixing the icon document name will ensure that for RCS usage, a single icon is stored in the network and no unnecessary resources are required for the storage of multiple icons. Without this, the situation could occur that multiple icons are stored without possibility to manage them after a switch to a new client. Furthermore the fixing of the icon name will allow clients that are aware of the SIP URI of their contact to build the URI needed for the retrieval of the icon even if the contact is offline.

Note 2: 200kB is not a mandatory size. It is only defined as a maximum and smaller sizes are acceptable

The other parameters are fixed to allow the client implementations to know what to expect.

3.7.4.2.2.3 Location Information

RCS clients shall not include a “from” attribute in the <place-type> and <time-offset> elements. RCS clients shall ignore it when received. RCS clients shall provide an "until" attribute in those elements and set it as specified in section 3.7.4.3.2.4.3.

RCS clients shall not include the optional description attribute in the <time-offset> element as this overlaps with the Location Type. RCS clients shall ignore it when received.

The geographical information will be provided as geographic coordinates. As specified for the “Geographical Location” building block in [Presence2.0_DDS], encoding will use the <*geopriv*>→<*location-info*> and <*geopriv*>→<*usage-rules*> elements.

The mandatory <*usage-rules*> element shall contain only a "*retention-expiry*" element as RCS clients will request the watchers to follow the default handling for the other rules. The RCS client shall set the "retention-expiry" as specified in section 3.7.4.3.2.4.3.

The <*location-info*> published by an RCS presence source will contain geographical information using the GML (Geography Markup Language) 3.1.1 Feature Schema (see [GML3.1.1]) which is the mandatory format to be used in the <*location-info*> element. The civic location format shall not be used by RCS presence sources and location information encoded in that way will be ignored by RCS clients when received.

RCS presence sources will within the <*location-info*> element represent an exact position by providing a GML <*point*> element and an inaccurate position as a <*circle*> element, both referring to the EPSG::4326 spatial reference schema as described in [RFC5491]. The coordinates of either the centre of this circle or the exact position will be represented with a single GML <*pos*> element with the actual coordinates as value. The radius of the circle will be represented in meters, which will be indicated by setting the unit of measure attribute of the radius element to the value of EPSG::9001 as described in [RFC5491]. An RCS client shall ignore any other type of data provided in the <*location-info*> element.

The EPSG format requires that the coordinate representation is defined by the coordinate supplier. RCS presence sources will always provide the coordinates in WGS 84 (latitude, longitude) decimal notion as described in [RFC5491], providing the latitude and longitude as “double”-encoded decimal numbers (as specified in [GML3.1.1]) representing the degrees, separated by a space starting with the latitude. Negative values represent Southern and Western hemisphere respectively.

3.7.4.2.3 *Service*

See section 2.6.1.2.5.

3.7.4.2.4 *Device*

The Device part of presence is out of scope for RCS.

3.7.4.2.5 *Example Document*

The above leads to following example document:

```
<?xml version=”1.0” encoding=”UTF-8”?>
<presence xmlns=”urn:ietf:params:xml:ns:pidf”
            xmlns:op=”urn:oma:xml:prs:pidf:oma-pres”
            xmlns:opd=”urn:oma:xml:pde:pidf:ext”
            xmlns:opd11=”urn:oma:xml:pde:pidf:ext:1.1”
            xmlns:pdm=”urn:ietf:params:xml:ns:pidf:data-model”
            xmlns:rpid=”urn:ietf:params:xml:ns:pidf:rpid”
            xmlns:gp=”urn:ietf:params:xml:ns:pidf:geopriv10”
            xmlns:caps="urn:ietf:params:xml:ns:pidf:caps"
            xmlns:gml="http://www.opengis.net/gml"xmlns:gs="http://www.opengis.net/pidflo/1.0"
            entity=”tel:+1234578901”>

  <tuple id="a2">
      <status><basic>open</basic></status>
      <op:service-description>
          <op:service-id>org.3gpp.urn:urn-7:3gpp-service.ims.icsi.mmtel</op:service-id>
          <op:version>1.0</op:version>
      </op:service-description>
      <caps:servcaps>
          <caps:audio>true</caps:audio>
          <caps:duplex>
              <caps:supported>
                  <caps:full/>
              </caps:supported>
          </caps:duplex>
      </caps:servcaps>
      <contact>tel:+1234578901</contact>
  </tuple>
  <tuple id=”a1”>
      <status><basic>open</basic></status>
      <op:service-description>
          <op:service-id>org.3gpp.cs-videotelephony</op:service-id>
          <op:version>1.0</op:version>
      </op:service-description>
      <contact>tel:+1234578901</contact>
  </tuple>

  <tuple id=”a12”>
      <status><basic>open</basic></status>
      <op:service-description>
          <op:service-id>org.gsma.videoshare</op:service-id>
          <op:version>1.0</op:version>
      </op :service-description>
      <contact>tel:+1234578901</contact>
  </tuple>
  <tuple id=”a123”>
      <status><basic>open</basic></status>
      <op:service-description>
          <op:service-id>org.gsma.videoshare</op:service-id>
          <op:version>2.0</op:version>
      </op :service-description>
      <contact>tel:+1234578901</contact>
  </tuple>
  <tuple id=”a132”>
      <status><basic>open</basic></status>
      <op:service-description>
          <op:service-id>org.openmobilealliance:IM-Session</op:service-id>
          <op:version>1.0</op:version>
      </op :service-description>
      <contact>tel:+1234578901</contact>
  </tuple>

  <pdm:person id=”a1233”>
      <op:overriding-willingness>
          <op:basic>open</op:basic>
      </op:overriding-willingness>
      <rpid:status-icon       opd:etag=”26362”>http://xcap.gsma.org/xcap-ap/service/org.openmobilealliance.pres-
      content/users/sip:1234578901@gsma.org/oma_status-icon/rcs_status_icon</rpid:status-icon>
      <opd11:link opd11:label=”my blog” opd11:priority=”0.8”>
          http://example.com/~alice
      </opd11:link>
      <rpid:place-type opd:until=”2009-11-28T21:00:00Z”>
          <rpid:other>Herentals, Belgium</rpid:other>
      </rpid:place-type>
      <rpid:time-offset opd:until=”2009-11-28T21:00:00Z”>+120</rpid:time-offset>
      <gp:geopriv>
          <gp:location-info>
              <gs:Circle srsName="urn:ogc:def:crs:EPSG::4326">
                <gml:pos>51.1644 4.7880</gml:pos>
                <gs:radius uom="urn:ogc:def:uom:EPSG::9001">10</gs:radius>
              </gs:Circle>
          </gp:location-info>
          <gp:usage-rules>
              <gp:retention-expiry>2009-11-28T21:00:00Z</gp:retention-expiry>
          </gp:usage-rules>
      </gp:geopriv>
      <pdm:note>I’ll be PAG</pdm:note>
  </pdm:person>
</presence>
```

Table 40: Example Presence Document

3.7.4.3 Presentity Side Handling

3.7.4.3.1 *Publication Methods*

3.7.4.3.1.1 Overview

An RCS client publishes its presence information using two different methods:

1. SIP PUBLISH requests
2. Permanent Presence State Publication (that is, a permanent document maintained through XCAP)

The method to be used depends on the information to be published:

SIP PUBLISH requests are used for following data:

- Service Capabilities

Permanent Presence State publication applies to the following attributes of Social Presence Information:

- Portrait icon
- Free text
- Favourite link
- Willingness (that is the overriding-willingness element)
- Location Information

3.7.4.3.1.2 Permanent Presence State Publication

The RCS Client shall support Permanent Presence State publication by manipulating the Permanent Presence State via an XDM Client (XDMC) using the permanent presence state application as defined in [Presence2.0_TS]. An RCS client shall update the permanent presence state document in such a way that elements in the document that are not changed or are even unknown to the RCS client (for example, because they were included by a client supporting a future RCS release), are not altered. To avoid inconsistencies between attributes and the actual element value, unknown attributes of changed elements shall be removed from the updated document.

This can be achieved both through a direct, conditional update of only the changed element itself or through a retrieval of the complete document followed by a client local update of the changed elements. This update should then be used in a conditional replace request for the entire permanent presence state document. The choice between both methods is left to client implementation and could depend on the amount of updated elements. In both cases, whenever the document is modified any expired information will be removed (for example Location Information with an “until” attribute indicating a time in the past).

The RCS Presence Server shall use the Permanent Presence State as input for Presence Information processing. RCS Presence Server should subscribe/fetch the permanent presence state document from Presence XDM when applying the composition policy.

3.7.4.3.2 *Presence Information Handling*

3.7.4.3.2.1 Willingness

When the Service Provider provisioning parameter indicates that willingness is enabled, at the presentity side, the RCS client will always include an <*overriding-willingness*> element in the permanent presence document. This element will have a <*basic*> sub-element set to either “*open*” or “*closed*” depending on what was indicated by the user as his current status. If willingness is disabled through the provisioning parameter, no “<*overriding-willingness*>” element will be included in the permanent presence document.

3.7.4.3.2.2 Status Icon

The status icon shall be stored, updated, deleted and retrieved according to the OMA Presence and XDM 2.0 procedures. For the storage itself, the Presence Content XDMS as defined in [Presence_Content] shall be used including the application usage and document type that it introduces. RCS will only make use of the Presence Content XDMS for the storage of the status icon. Therefore the usage as defined in section 5.1.12.1 of [Presence_Content] is the only one that is applicable including all its associated restrictions. After storing, updating or deleting the icon, the presentity's client should publish an updated presence document including the *etag* attribute in the <*status-icon*> element as described in [Presence2.0_DDS] in sections 7.11.1.3 and 7.20.

3.7.4.3.2.3 Link

The RCS client will limit the length of the label to the maximum length that is provided through a Service Provider provisioning setting.

3.7.4.3.2.4 Location

3.7.4.3.2.4.1 Ending Location Information Sharing

When the user indicates that they do not want to share their location information with the contacts allowed to see their information anymore, the client can fulfil this request by removing the location information from the Permanent Presence State document.

3.7.4.3.2.4.2 Obtaining Location Information

See section 3.10.4.4.

3.7.4.3.2.4.3 Managing Location Information

An RCS presence source is not required to include all location elements specified in section 3.7.4.2.2.3 in the permanent presence state document (that is, all elements are optional to be provided).

The length of the descriptive text that the RCS client includes in the Permanent Presence State document shall not be longer than the maximum that was provided as a Service Provider provisioning setting.

The maximum time a location update remains available to watchers is controlled by a Service Provider provisioning setting. RCS presence sources will set the "*until*" attribute and the "*retention-expiry*" element (see section 3.7.4.2.2.3) in accordance to this provisioning setting (that is, set it to the current time increased with the value of the setting). Furthermore RCS presence sources shall remove expired location information from the published presence document and from any locally cached copy of that document whenever they update other elements in the document.

Clients offering the user the choice to provide an inaccurate position to their contacts (for example, city level or even country level) can do so by providing a *CircleByCenterPoint* element instead of an exact position using coordinates and text reflecting this inaccuracy (for example, the city centre instead of the exact street). Whether the client does this and how it determines the position of the centre, the radius and the text value (that is, the <*place-type*> element) that will be shared, is considered to be client implementation and thus out-of-scope for RCS.

As an option to the user, clients may also offer the possibility to regularly update their position without user intervention. Whether or not this is done is again considered to be a client implementation issue and thus out-of-scope for RCS. Since such an implementation could result in a high load on the network and the clients of the contacts with whom location is shared, some Service Provider control is required. This will be realized through a Service Provider provisioning setting controlling the minimum duration between location updates. An

RCS client shall ensure that the time between two consecutive location updates is larger than this provisioned minimum.

Note: Even though a maximum update frequency could be derived from the provided minimum duration setting, it has been an explicit choice not to provision a frequency, as no updates would be necessary if the device has not moved. Again the decision on when an update is needed is left to the client implementation and thus out-of-scope for RCS provided the client complies with the provisioned minimum interval between updates.

3.7.4.3.2.5 Nickname

The *application/watcherinfo+xml* body in the watcher information notification may contain a display name for the watcher in the display-name attribute as specified in [RFC3858]. In this case, if the telephone number that is derived from the (SIP or tel) URI that is provided for that watcher is not found in the phone book of the client, the RCS client will include the display name in notifications shown to the user. At the same time it will always include the watcher’s telephone number to minimize the risk of false identifications.

If no display name is received (for example because the subscription is initiated from an RCS-e 1.2 network), the client shall only present the E.164 number to the user.

If the watcher’s telephone number is found in the phone book, behaviour shall be as specified in section 2.5 (that is, the received display name shall not be used, but rather the information that is part of the phone book).

An RCS client shall be able to deal with display names up until a maximum length of 200 characters.

3.7.4.3.3 *Multidevice Handling*

If one of the user’s clients changes the (shared) permanent presence state document, the other clients of the user will receive the update as part of a presence notification which will contain information about their own presentity. Such an update will be received immediately when the client is online at the time of the changes. If this is not the case, the client will receive the update when it comes online. Clients shall take the updated social presence information into account and update the presence information that they store locally in the client accordingly. To get the notifications that are necessary to provide this behaviour, the client shall include the own identity in the “*rcs*” list which is part of the Shared XDMS’s “*resource-lists*” document (see section 3.7.4.5.2).

When a user decides that they do not want to receive a certain service on one of their secondary clients (see section 2.9.1.4), the given secondary client will not indicate the capability for that service in the services section of the presence document if such a capability is defined for the service (see section 2.6.1.2.5).

3.7.4.4 Watcher Side Handling

When presence information of a presentity is requested by a watcher a SUBSCRIBE request is initiated (event package ‘*presence’*) according to [Presence]. The watcher should be able to use the tel URI to identify the presentity, see section 2.5.

The support of RLS is mandatory for the clients and servers. Client shall conform to section 5.2.2.1 of the technical specification of [PRESENCE] and in addition to section 5.7.1 and 5.8 in [PRESENCEIG], section 5.1 in [XDMIG] and section 5.1.6 in [RLSXDM]. The XML documents shall follow the templates following later in this section.

3.7.4.4.1 *Caching Presence Information*

The caching of presence information is a client procedure.

The RCS client must be able to locally store the most up-to-date presence information (that have been received through notifications) of all of the user's contacts. This locally stored information must be handled as a persistent cache (that is the data shall not be erased when the terminal is switched-off).

3.7.4.4.2 *Presence Information Handling*

3.7.4.4.2.1 General Processing Rules to Facilitate Forwards Compatibility

To maintain enough flexibility and not to impose potentially sub-optimal technical choices on future RCS releases, the presence parsing for social presence information in an RCS client should be sufficiently robust. Therefore the following guidelines should be taken into account in RCS presence parsing:

- Unknown or unsupported elements could be present in the document. In that case they should be ignored.
- When using RLS subscriptions, information could be contained on presentitys that were not known to be part of the presence list (for example because the list was updated by another client or application). If the unexpected presentity is a known contact, the client should treat this contact as being presence enabled (see section 3.7.4.4.4) and try to retrieve an updated presence list from the network (see section 3.7.4.5.3).
- The Watcher shall follow the procedures defined in section 6.2 "Default Watcher Processing" of [Presence2.0_DDS].

3.7.4.4.2.2 Willingness

When the service provider provisioning parameter indicates that willingness is disabled, on reception of a NOTIFY request, the watcher RCS client will ignore any “<*overriding-willingness*>” in the received presence document(s). If willingness is enabled the client will interpret any “<*overriding-willingness*>” element included/not included in the received presence document(s) as specified in section 3.7.4.2.2.

3.7.4.4.2.3 Status Icon

The link to the status icon that is received in the presence document of the contact will be processed as described in [Presence2.0_TS] section 5.2.5.3. When the *etag* attribute of the *status-icon* element does not match that of the cached icon, the client will download the updated icon. To do that it will handle the link that it received in the presence document as defined in [XDM2.0_Core] section 6.1.1.1 and more specifically the third paragraph: it will replace the XCAP root part of the link with the own XCAP root of the watcher. After downloading the icon, the RCS client shall cache it along with the *etag* to be able to process future notifies on the status of the contact as defined in [Presence2.0_TS] section 5.2.5.3.

3.7.4.4.2.4 Link

If an RCS client receives a document containing multiple <*link*> elements, then it shall only consider the one with the highest priority and use that as the value of the <*link*> element in the processing.

An RCS watcher shall be able to deal with labels with a length of maximum 200 characters.

3.7.4.4.2.5 Location Information

It is considered to be a client implementation decision how received location information from a contact will be handled (for example, display only the text, use an individual map for each contact and so on. This is thus considered to be out of scope for RCS. Clients should at least provide a means to display any descriptive text (that is, the content of the <*place-type*> element) that they might receive.

An RCS client should take into account that a received presence document might not contain location information (for example, because the presence source does not provide it or privacy was enabled).

An RCS client shall be able to deal with *place-type* information with a length of maximum 200 characters.

An RCS client shall not display to the user information contained in location elements for which the "*until*" attribute (for the <*time-offset*> and <*place-type*> elements) or the <*retention-expiry*> element (for the geolocation information) indicate a time in the past. Furthermore it shall not cache the expired information locally any longer.

3.7.4.4.3 *Nickname Handling*

If the user has provided a nickname, an RCS client shall include it as the display name as part of the identity information provided in the *P-Preferred-Identity* and *From* header field of the SIP SUBSCRIBE request used when subscribing to the user's Resource List Server (RLS) document. The RCS client shall ensure that the length of the used display name is not larger than the maximum size that was provisioned by the Service Provider.

3.7.4.4.4 *Multidevice Handling*

For the most part the watcher functionality on the different clients of the same user can function independently of each other. Only with the authorization there might be some interaction as this may trigger unexpected notifications (see section 3.7.4.5.9). An RCS client of this release will provide compatibility with clients of future RCS releases acting as one or more of the other devices of the user. To achieve this it will display the presence information provided in a presence notification if it refers to a known contact, regardless of whether that contact can be found in the "*rcs*", "*rcs_basic_spi_only*", "*rcs_poll*" or "*rcs_poll_basic_spi_only*" lists of the Shared XDMS's "*resource-lists*" document (see section 3.7.4.5.2).

3.7.4.5 Subscriptions and Authorization

3.7.4.5.1 *Overview*

Presence invitations are subject to reactive authorization to guarantee user privacy. This will allow the invited user (presentity) to accept, block or ignore an invitation to establish a presence relationship.

The presence authorization for basic social presence information shall be symmetric. This means the inviting user automatically authorizes the invited user to see their basic social presence information. The invited user by accepting the presence invitation request both authorizes the inviting user to see their basic social presence information and subscribes to the inviting users presence information.

The RCS presentity shall be able to configure the presence authorization rules, which require the support in the RCS client and in the RCS Presence Server of [PresenceXDM]. The RCS client shall store a presence authorization document that follows [PresenceXDM] and the template rules described in section 5.8 in [PRESENCEIG].

In order for a presentity to be able to authorize the subscription of a watcher, the presentity needs to know which watcher(s) are trying to subscribe to the presence of the presentity. The RCS client and the Presence Server shall thus support section 5.3.1 and 5.4.4 of [Presence].

When the subscription is authorized successfully, the Presence Server sends the presentity's presence document to the watcher by using the NOTIFY method as defined in [Presence]. The format of the presence notification follows the Presence Data Model as describe above and it contains the information the watcher is allowed to see according to the configured presence rules.

The contacts with whom the RCS user share presence information can be defined as either VIP contacts or non-VIP contacts (see section 3.7.1.4.9). For VIP contacts, presence information changes are received in real time, using a subscription to the corresponding

“VIP contacts” buddy list in RLS. For non-VIP contacts the client will poll the corresponding “non-VIP contacts” list in RLS to retrieve presence information changes.

Contrary to the general concept for basic social presence information sharing the authorization for location information is not necessarily mutual: User A can get the location information from User B without having to provide his location information. Furthermore, the user can control whether the information that he/she is capable of sharing social presence information is public or not.

3.7.4.5.2 *XML Document Structure*

The Presence XDMS shall contain the following authorization rules following, where possible, the recommendations in [PRESENCEIG]:

- ”*allow own*” rule – allows subscriptions to own presence data
- ”*confirm unlisted*” rule – allows reactive authorization for contacts not yet allowed or blocked
- ”*blocked contacts*” – contains those contacts that the user has blocked (points to ”*blocked contacts*” list in Shared XDMS)
- ”*granted contacts*” rule – will be used as the rule to provide all social presence information (that is, the Basic Social Presence Information and geolocation information)
- “*basic_spi_only_granted_contacts*” rule – will be used by the contacts with whom no location information is being shared.

The RLS XDMS shall for an RCS user contain two entries; one referencing the “*oma_buddylist*” list and one referencing the “*rcs_poll_buddylist*” list, both in Shared XDMS. The service URI referencing the “*oma_buddylist*” allows subscribing with one RLS subscription to the presence information of both the VIP contacts with whom only social presence information is shared and those VIP contacts that are also allowed to see the location information. The RCS client will at start-up subscribe to changes to this list by issuing a SUBSCRIBE request to the RLS targeting this list with an expire value >0 (pre-configured in client).

In addition to information on the VIP contacts, the service URI referencing the “*rcs_poll_buddylist*” allows the RCS client with one subscription request to retrieve presence information also from the non-VIP contacts with whom only social presence information is shared and those non-VIP Contacts that are also allowed to see the location information. The RCS client will, only on user request or also on regular basis issue a “poll” SUBSCRIBE (that is with expires=0) to this list to obtain the presence information for the contacts in this list.

The maximum amount of poll operations on the non-VIP Contacts buddy list during a certain time period can in the client be configured subject to Service Provider policies (see Annex A).

The Shared XDMS shall contain the following lists provided and managed by the RCS client:

- “*rcs*” list: This list includes all VIP contacts with which basic Social Presence and location information is shared. Commonly referred in RCS from both the “*oma_buddylist*” and “*oma_grantedcontacts*” lists as the contacts that are allowed to see your presence are also your buddies (symmetric).
  To provide the behaviour described in section 3.7.4.3.3, the “*rcs*” list will contain the own identity of the user. The client shall not allow the user to remove that entry.
- “*rcs_basic_spi_only*” list: This list includes all VIP contacts with which only basic Social Presence information is shared. Commonly referred in RCS from both the “*oma_buddylist*” and “*rcs_basic_spi_only_granted_contacts*” lists as the contacts that are allowed to see your presence are also your buddies (symmetric).

- “*rcs_poll*” list: This list includes all non-VIP contacts with which basic Social Presence and location information is shared. Commonly referred in RCS from both the “*rcs_poll_buddylist*” and “*oma_grantedcontacts*” lists as the contacts that are allowed to see your presence are also your buddies (symmetric). As a difference with the “*rcs*” list, the “*rcs_poll*” list will not contain the own identity of the user.
- “*rcs_poll_basic_spi_only*” list: This list includes all non-VIP contacts with which only basic Social Presence information is shared. Commonly referred in RCS from both the “*rcs_poll_buddylist*” and “*rcs_basic_spi_only_granted_contacts*” lists as the contacts that are allowed to see your presence are also your buddies (symmetric).
- “*oma_buddylist*” list: Contains a reference to the “*rcs*” and the “*rcs_basic_spi_only*” lists where the actual VIP Contacts (or buddies) are stored. The “*oma_buddylist*” is explicitly used from the RLS document.
- “*rcs_poll_buddylist*” list: Contains a reference to the “*rcs_poll*” and the “*rcs_poll_basic_spi_only*” lists where the actual non-VIP Contacts are stored. The “*rcs_poll_buddylist*” is explicitly used from the RLS document.
- “*oma_grantedcontacts*” list: This list includes all contacts you have authorized to see your basic social presence and location information. Contains a reference to the “*rcs*” and “*rcs_poll*” lists.
- “*rcs_basic_spi_only_grantedcontacts*” list: This list includes all contacts you have authorized to see only your basic social presence information. Contains a reference to the “*rcs_basic_spi_only*” and the “*rcs_poll_basic_spi_only*” lists
- “*oma_blockedcontacts*” list: Contains a reference to the “*rcs_blockedcontacts*” list where the actual permanently blocked contacts are stored and to the “*rcs_revokedcontacts*” list with the revoked users that are temporarily being blocked.
- “*rcs_blockedcontacts*” list: Contains all permanently blocked contacts
- “*rcs_revokedcontacts*” list: Contains all revoked contacts that are currently being blocked.

Note: The “*rcs_revokedcontacts*” list is not intended to be shown to the end user. It is managed automatically.

Note: A contact should be in one list only. To ensure this, the RCS client shall check the other lists for an occurrence of the contact when adding it to a list. If the contact occurs somewhere else, the client will remove that entry. A contact will always be added to the new list before being removed from the old one. This applies both when removing a presence relation (see section 3.7.4.5.5) and when changing a contact from being a VIP Contact to a being a non-VIP Contact or vice versa (see section 3.7.4.5.8).

For RCS, the template definitions below will be used for the different XDM documents related to presence subscriptions and authorizations.

Presence XDMS:
AUID: org.openmobilealliance.pres-rules
Document name: pres-rules
Template

```
<?xml version="1.0" encoding="UTF-8"?>
<cr:ruleset
    xmlns:ocp="urn:oma:xml:xdm:common-policy"
    xmlns:op="urn:oma:xml:prs:pres-rules"
    xmlns:pr="urn:ietf:params:xml:ns:pres-rules"
    xmlns:cr="urn:ietf:params:xml:ns:common-policy">
    <cr:rule id="wp_prs_allow_own">
        <cr:conditions>
          <cr:identity>
              <cr:one id="tel:+1234578901"/>
          </cr:identity>
        </cr:conditions>
        <cr:actions>
          <pr:sub-handling>allow</pr:sub-handling>
        </cr:actions>
        <cr:transformations>
          <pr:provide-services>
              <pr:all-services/>
          </pr:provide-services>
          <pr:provide-persons>
              <pr:all-persons/>
          </pr:provide-persons>
          <pr:provide-devices>
              <pr:all-devices/>
          </pr:provide-devices>
          <pr:provide-all-attributes/>
        </cr:transformations>
    </cr:rule>

    <cr:rule id="wp_prs_unlisted">
        <cr:conditions>
          <ocp:other-identity/>
        </cr:conditions>
        <cr:actions>
          <pr:sub-handling>confirm</pr:sub-handling>
        </cr:actions>
    </cr:rule>
    <cr:rule id="wp_prs_grantedcontacts">
        <cr:conditions>
          <ocp:external-list>
              <ocp:entry anc="http://xcap.gsma.org/resource-
              lists/users/sip:1234578901@gsma.org/index/~~/resource-
              lists/list%5B@name=%22oma_grantedcontacts%22%5D"/>
          </ocp:external-list>
        </cr:conditions>
        <cr:actions>
          <pr:sub-handling>allow</pr:sub-handling>
        </cr:actions>
        <cr:transformations>
          <pr:provide-services>
              <pr:all-services/>
          </pr:provide-services>
          <pr:provide-persons>
              <pr:all-persons/>
          </pr:provide-persons>
          <pr:provide-devices>
              <pr:all-devices/>
          </pr:provide-devices>
          <pr:provide-all-attributes/>
        </cr:transformations>
    </cr:rule>

    <cr:rule id="rcs_basic_spi_only_grantedcontacts">
        <cr:conditions>
          <ocp:external-list>
              <ocp:entry anc="http://xcap.gsma.org/resource-
              lists/users/sip:1234578901@gsma.org/index/~~/resource-
              lists/list%5B@name=%22rcs_basic_spi_only_grantedcontacts%22%5D"/>
          </ocp:external-list>
        </cr:conditions>
        <cr:actions>
          <pr:sub-handling>allow</pr:sub-handling>
        </cr:actions>
        <cr:transformations>
          <pr:provide-services>
              <pr:all-services/>
          </pr:provide-services>
          <pr:provide-persons>
              <pr:all-persons/>
          </pr:provide-persons>
          <pr:provide-devices>
              <pr:all-devices/>
          </pr:provide-devices>
          <pr:provide-note>true</pr:provide-note>
          <pr:provide-status-icon>true</pr:provide-status-icon>
          <pr:provide-unknown-attribute
              ns="urn:oma:xml:pde:pidf:ext:1.1"
              name="link">
              true
          </pr:provide-unknown-attribute>
          <op:provide-willingness>true</op:provide-willingness>
          <pr:provide-unknown-attribute
              ns="urn:oma:xml:prs:pidf:oma-pres"
              name="service-description">
              true
          </pr:provide-unknown-attribute>
        </cr:transformations>
    </cr:rule>

    <cr:rule id="wp_prs_blockedcontacts">
        <cr:conditions>
          <ocp:external-list>
              <ocp:entry anc="http://xcap.gsma.org/resource-
              lists/users/sip:1234578901@gsma.org/index/~~/resource-
              lists/list%5B@name=%22oma_blockedcontacts%22%5D"/>
          </ocp:external-list>
        </cr:conditions>
        <cr:actions>
          <pr:sub-handling>block</pr:sub-handling>
        </cr:actions>
    </cr:rule>
</cr:ruleset>
```

Table 41: Presence Rules Template

Note: If the client is configured to use a presence based capability discovery (as described in section 2.6.1.2, the *rcs_allow_services_anonymous* rule described in Table 21 should be included in this template.

RLS XDMS:
AUID: rls-services
Document name: index
Template:

```
<?xml version="1.0" encoding="UTF-8"?>
<rls-services xmlns="urn:ietf:params:xml:ns:rls-services">
    <service uri="sip:1234578901@gsma.org;pres-list=rcs">
        <resource-list>http://xcap.gsma.com/services/resource-
        lists/users/sip:1234578901@gsma.org/index/~~/resource-
        lists/list%5B@name=%22oma_buddylist%22%5D</resource-list>
        <packages>
          <package>presence</package>
        </packages>
    </service>
    <service uri="sip:1234578901@gsma.org;pres-list=rcs_poll">
        <resource-list>http://xcap.gsma.com/services/resource-
        lists/users/sip:1234578901@gsma.org/index/~~/resource-
        lists/list%5B@name=%22rcs_poll_buddylist%22%5D</resource-list>
        <packages>
          <package>presence</package>
        </packages>
    </service>
</rls-services>
```

Table 42: Presence RLS Template

Shared XDMS:
AUID: resource-lists
Document name: index
Template:

```
<?xml version="1.0" encoding="UTF-8"?>
<resource-lists xmlns="urn:ietf:params:xml:ns:resource-lists"
                  xmlns:xd="urn:oma:xml:xdm:xcap-directory"
                  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
    <!-- The list oma_buddylist contains references to any individual list used according to OMA IG for presence
    subscriptions. -->
    <list name="oma_buddylist">
        <external anchor="http://xcap.gsma.org/resource-
        lists/users/sip:1234578901@gsma.org/index/~~/resource-lists/list%5B@name=%22rcs%22%5D"/>
        <external anchor="http://xcap.gsma.org/resource-
        lists/users/sip:1234578901@gsma.org/index/~~/resource-
        lists/list%5B@name=%22rcs_basic_spi_only%22%5D"/>
    </list>

    <!-- The list rcs_poll_buddylist contains references to individual lists used for RCS non-VIP Contacts -->
    <list name="rcs_poll_buddylist">
        <external anchor="http://xcap.gsma.org/resource-
        lists/users/sip:1234578901@gsma.org/index/~~/resource-lists/list%5B@name=%22rcs_poll%22%5D"/>
        <external anchor="http://xcap.gsma.org/resource-
        lists/users/sip:1234578901@gsma.org/index/~~/resource-
        lists/list%5B@name=%22rcs_poll_basic_spi_only%22%5D"/>
    </list>

    <!-- The list oma_grantedcontacts contains the list of all granted contacts -->
    <list name="oma_grantedcontacts">
        <external anchor="http://xcap.gsma.org/resource-
        lists/users/sip:1234578901@gsma.org/index/~~/resource-lists/list%5B@name=%22rcs%22%5D"/>
        <external anchor="http://xcap.gsma.org/resource-
        lists/users/sip:1234578901@gsma.org/index/~~/resource-lists/list%5B@name=%22rcs_poll%22%5D"/>
    </list>

    <!-- The list rcs_basic_spi_only_grantedcontacts contains the list of all basic SPI Only granted contacts -->
    <list name="rcs_basic_spi_only_grantedcontacts">
        <external anchor="http://xcap.gsma.org/resource-
```

```
          lists/users/sip:1234578901@gsma.org/index/~~/resource-
          lists/list%5B@name=%22rcs_basic_spi_only%22%5D"/>
          <external anchor="http://xcap.gsma.org/resource-
          lists/users/sip:1234578901@gsma.org/index/~~/resource-
          lists/list%5B@name=%22rcs_poll_basic_spi_only%22%5D"/>
     </list>

     <!-- The list oma_blockedcontacts contains the list of all blocked contacts.  -->
     <list name="oma_blockedcontacts">
          <external anchor="http://xcap.gsma.org/resource-
          lists/users/sip:1234578901@gsma.org/index/~~/resource-
          lists/list%5B@name=%22rcs_blockedcontacts%22%5D"/>
          <external anchor="http://xcap.gsma.org/resource-
          lists/users/sip:1234578901@gsma.org/index/~~/resource-
          lists/list%5B@name=%22rcs_revokedcontacts%22%5D"/>
     </list>

     <!-- The list of VIP contacts (buddies) the owner wants to provide all social presence information to. This list
     also includes the owner's own URI -->
     <list name="rcs">
          <display-name>My presence buddies with location sharing</display-name>
          <entry uri="tel:+1234578901"/>
     </list>

     <!-- The list of VIP Contacts (buddies) the owner wants  to provide only basic social presence information to -
     ->
     <list name="rcs_basic_spi_only">
          <display-name>My presence buddies without location sharing</display-name>
     </list>

     <!-- The list of NON-VIP Contacts (buddies) the owner wants to provide all social presence information to -->
     <list name="rcs_poll">
          <display-name>My NON-VIP presence contacts with location sharing</display-name>
     </list>

     <!-- The list of NON-VIP Contacts (buddies) the owner wants  to provide only basic social presence
     information to -->
     <list name="rcs_poll_basic_spi_only">
          <display-name>My NON-VIP presence contacts without location sharing</display-name>
      </list>

     <!-- The list of blocked contacts -->
     <list name="rcs_blockedcontacts">
          <display-name>My blocked contacts</display-name>
     </list>

     <!-- The list of revoked contacts -->
     <list name="rcs_revokedcontacts">
          <display-name>My revoked contacts</display-name>
          <entry uri="tel:+123456" xd:last-modified="2008-12-24T14:32:14Z"/>
     </list>
</resource-lists>
```

Table 43: Presence Shared Lists template

Note: the entry in the "*rcs_revokedcontacts*" list is for illustrative purposes only. It is included as an example since it deviates slightly from the standard list usage. The entry in the "*rcs*" list is also for illustrative purposes only, showing that the user's own URI will be included so the user's clients receive the user's own presence information (see also section 3.7.4.3.3).

3.7.4.5.3 *XML Document Handling*

When first started the RCS client shall check whether the "*pres-rules*", "*rls-services*", "*resource-lists*" and the "*pidf-manipulation*" (permanent presence state) documents exist through a XCAP directory query. If they do not exist, the RCS client shall create them. If the documents exist, the RCS client will check whether they comply with the templates defined in section 3.7.4.5.2 by using the following criteria for the documents:

- For the "*resource-lists*" document, first check whether it contains an "*rcs_basic_spi_only*" list. If not, add the "*rcs_basic_spi_only*" and "*rcs_basic_spi_only_grantedcontacts*" lists to the document and modify the "*oma_buddylist*" list to refer to both the "*rcs*" and the "*rcs_basic_spi_only*" lists.
- Secondly check whether it contains an "*rcs_poll_buddylist*" or an "*rcs_poll*" list. If not, add the "*rcs_poll*", "*rcs_poll_basic_spi_only*" and "*rcs_poll_buddylist*" lists to the document and modify the "*oma_grantedcontacts*" list to refer to both the "*rcs*" and the "*rcs_poll*" lists and the "*rcs_basic_spi_only_grantedcontacts*" list to refer to both the "*rcs_basic_spi_only*" and "*rcs_poll_basic_spi_only*" lists.
- For the "*rls-services*" document, firstly check if the "*rcs*" service URI entry refers to the "*oma_buddylist*" list. If the document refers to the "*rcs*" list instead, the RCS client shall modify it to refer to the "*oma_buddylist*" list
- Secondly, check if it contains an "*rcs_poll*" service URI entry. If not, an "*rcs_poll*" service URI entry with a reference to the "*rcs_poll_buddylist*" in Shared XDMS will be added.
- For the "*pres-rules*" document, check whether it contains the "*rcs_basic_spi_only_granted_contacts*" rule. If not, the RCS client shall add this rule to the document.

Once the documents have been setup in this way, the RCS client shall only modify the "*rcs*", "*rcs_basic_spi_only*", "*rcs_poll*", "*rcs_poll_basic_spi_only*", "*rcs_revokedcontacts*" and "*rcs_blockedcontacts*" lists in the "*resource-lists*" document. Only if the user explicitly requests to recreate the documents according to the possibility described below, the other documents and parts of the "*resource-lists*" document should be modified.

XDM documents can be updated without the involvement of the RCS client of this RCS release. Two types of changes are possible:

1. Shared lists are updated by adding new entries, removing entries or updating entries.
2. Structural changes to the documents (for example to support new options in the presence authorization).

In case 1, in order not to overwrite changes done for example by another client, either a conditional update should be done (per XCAP conditional operations as defined in [RFC4825] section 7.11) or the client should retrieve the latest status of the document before doing the update. An RCS client of this RCS release shall support one of these options when updating XDM documents.

To deal with case 2 (structural changes to a XDM document) could occur when an RCS client of this RCS version is deployed in a future RCS environment, even though the future RCS version should be backward compatible with previous ones. The RCS client shall go to a read-only mode with regards to all XDM documents when it detects such changes. Future RCS versions will indicate this by renaming the "*rcs*" shared list. If the list is not renamed, but structural changes were detected in documents in the presence and RLS XDMS, the RCS client will go to read-only mode only for the updated documents. In that case the RCS client indicates to the user that they should use a client with an updated RCS version to carry out commands that require modifying any of such documents.

Circumstances where the user downgrades from a future RCS release to the use of an RCS client only, (for example the end-user does not have a client with an updated RCS version or there is some blocked situation between the XDMC and XDMS), the RCS client shall offer the user the possibility to remove all information stored in the XDMS's, this then creates new documents based on its current status and RCS release. The removal of the documents shall be based on a retrieval of the complete list of documents using XCAP Directory requests and then removing all listed documents (thus including documents unknown to the RCS client of this RCS release) using relevant operation such as XCAP PUT/DELETE.

Should a device for its own internal use maintain a local copy of the Shared XDMS's "*resource-lists*" document (see section 3.7.4.5.2) or the information contained therein, then it shall verify with the Shared XDMS whether its copy is still up to date in the following situations:

- When the client comes online
- When it receives a notification within the dialog of its RLS subscription indicating that the subscription to a contact is pending or active and according to the locally maintained information, it is not aware that the user is part of the RCS buddy list.
  Note: this situation can occur, when the user invites the contact to share social presence information from another client, or a contact has been added as a VIP-contact from another client.
- When it receives a notification within the dialog of its watcher information subscription indicating that a subscription from a contact changed from the "pending" to the "*active*" or "*terminated*" state when no action was taken to authorize or block that subscription from the client. The state change to "*terminated*" should only be taken into account for this case when the event triggering the state change indicates "*rejected*".
  Note: this situation can occur when the user authorizes or blocks the subscription from another client.
- When it receives a notification within the dialog of its RLS subscription indicating that the subscription to a contact that is presence enabled was terminated with reason "*timeout*" when no action was taken from the client to revoke the presence sharing with that contact.
- When it receives a notification within the dialog of its RLS subscription indicating that the subscription to a contact that is presence enabled was terminated with reason "*noresource*" when no action was taken from the client with that contact.
  Note: this situation can occur, when the user changes a contact from being a VIP contact to being a non-VIP contact from another client.

Note: a device is not required to maintain a local copy of the Shared XDMS's "*resource-lists*" document. If it does not, it can simply display the presence information it receives and it does not need to access the XDMS.

3.7.4.5.4 *Client Procedures, Initiation of Presence Sharing*

When initiating a presence sharing request, the inviting user's RCS client adds the invited user's URI to the "*rcs*" list in Shared XDMS according to the procedures in [Shared-XDM].

When the invited user receives a notification to establish a presence relation, the user can either:

1. Accept the invitation, whereas the RCS client of the invited user adds the inviting User's URI to the "*rcs*" list in Shared XDMS according to the procedures in [SHARED-XDM].
2. Block the invitation, whereas the RCS client of the invited user adds the inviting User's URI to the "*rcs_blockedcontacts*" list in Shared XDMS according to the procedures in [SHARED-XDM].
3. Ignore the invitation, whereas the RCS client of the invited user removes the presence sharing invitation.
4. Not answer the invitation. The presence sharing invitation is pending in the client until either "accepted" (case 1), "blocked" (case 2) or "ignored" (case 3). In the signalling, there is no difference from the "ignore" case.

3.7.4.5.5 *Client Procedures, Removal of Presence Sharing*

When the user decides to end the presence relationship with one of their contacts, they have to use the revoke option on their device. This triggers a notification to the user as defined in section 3.7.1.4.6 asking for confirmation. When this is confirmed, the client will put the user on the "*rcs_revokedcontacts*" list, subsequently remove the user from the "*rcs*" or "*rcs_basic_spi_only*", "*rcs_poll*" or "*rcs_poll_basic_spi_only*" list and remove the contact's presence information from the cache as defined in section 3.7.4.4.1. When putting an entry for the contact in the "*rcs_revokedcontacts*" list the client includes a last modified attribute that indicates the current time in UTC (Coordinated Universal Time).

When a client notices it has been blocked by a contact with whom Social Presence was shared (that is the RLS notify indicates the subscription is in state "*terminated*" and the reason indicates "*rejected*"), it will remove the contact from the "*rcs*" or "*rcs_basic_spi_only*", "*rcs_poll*" or "*rcs_poll_basic_spi_only*" list and remove the contact's cached presence information. Note that for a non-VIP contact (in the "*rcs_poll*" or "*rcs_poll_basic_spi_only*" list) there could be a delay in the detection of this change.

All clients will process the "*rcs_revokedcontacts*" list periodically and remove those contacts that have been included in the list for a sufficiently long period already (for example several days). For that they will compare the last-modified attribute of the entries to the current time. Both the interval at which the list is checked and the period that a contact should remain in this list are Service Provider configurable client parameters defined in Annex A.

With regards to the communication capabilities both clients should fall back to the procedures as defined in section 2.6 for sharing of capabilities between contacts not sharing social presence information.

3.7.4.5.6 *Authorizing XCAP Requests*

XCAP requests need to be authorized by the XDMS. This authorization relies on an assertion of the identity of the requestor of an XCAP request.

The HTTP header fields *X-XCAP-Asserted-Identity* and *X-3GPP-Asserted-Identity* used to contain the asserted identity of a requestor of an XCAP request may depend on operational conditions (type of access used by the terminal, Service Provider policy) for example different Service Providers may apply different algorithms to assert the identity of a requestor of an XCAP request. Thus, for any Authorization check to be carried out by the XDMS, any of both *X-XCAP-Asserted-Identity* and *X-3GPP-Asserted-Identity* header fields are accepted as a valid header field containing the asserted identity of the requestor of the XCAP request inside the Service Provider domain.

To offer a unique inter-Service Provider interface, the *X-3GPP-Asserted-Identity* header field is always conveyed between two Service Provider domains, at the NNI interface.

When the terminal of a watcher requests, via XCAP, some content (for example status-icon, refer to section 3.7.4.4.2.3) associated with the presence document of a presentity, the XDMS of the presentity has to check whether the watcher is authorized to access this content, according to the presentity's presence subscription rules.

As defined in section 3.7.4.5.2, amongst others the "*rcs*" list is granted this permission.

The lists in section 3.7.4.5.2 can contain both SIP URI and tel URI address of authorized watchers in a Service Provider domain. To ensure both cases at the NNI interface, the "*X-3GPP-Asserted-Identity*" of the initiator of an XCAP request should contain both the sip URI and tel URI of this user.

3.7.4.5.7 *Conditional Event Notification*

The support of conditional event notification is strongly recommended for the clients (i.e. Watcher and Watcher Information Subscriber) and for the servers (i.e. Presence Server and RLS) to optimize presence traffic at UNI and NNI.

An RCS client should support subscription with conditional event notification, as defined in section 5.2.6 and section 5.3.2 of [Presence2.0_TS].

An RCS RLS should support subscription with conditional event notification, as defined in section 5.2 of [Presence2.0_RLS_TS].

An RCS Presence Server should support notification with conditional event notification, as defined in section 5.5.3.8, 5.5.3.9 and 5.5.4.2 of [Presence2.0_TS].

An RCS RLS should support notification with conditional event notification, as defined in section 5.4 of [Presence2.0_RLS_TS].

3.7.4.5.8 *Client Procedures, managing of VIP and non-VIP Contacts*

When the user decides to change a user from being a VIP Contact to being a non-VIP Contact (or vice versa) the client will first add the user’s URI to the target list and after this, remove the user’s URI from the list where it was previously stored. That is, when changing a user from being a VIP Contact to a non-VIP Contact, the client will first add the user’s URI to the “*rcs_poll*” (if previously in the “*rcs*” list) or “*rcs_poll_basic_spi_only*” list (if previously in the “*rcs_basic_spi_only*” list) and then remove the URI from the “*rcs*” or “*rcs_basic_spi_only*” list respectively. When changing a user from being a non-VIP Contact to a VIP Contact, the client will first add the user’s URI to the “*rcs*” list (if previously in the “*rcs_poll*” list) or “*rcs_basic_spi_only*” list (if previously in the “*rcs_poll_basic_spi_only*” list) and then remove the URI from the “*rcs_poll*” or “*rcs_poll_basic_spi_only*” list respectively.

3.7.4.5.9 *Multidevice Handling*

Any negative effects of XDM document changes in a multidevice context are countered through the XDM document handling as it is described in section 3.7.4.5.3.

Several situations should be dealt with:

- The user owning multiple clients is invited by a contact to share social presence information.
  All the user’s active clients will receive watcher information notifications both when the contact subscribes for the user’s social presence information (subscription entering the “*pending*” state) and when the user accepts or blocks the “invitation” on one of their clients (subscription going out of the “*pending*” state). When the user accepts the invitation on one of their clients, the other clients will also start receiving the social presence information of the contact.
- The user owning multiple clients invites a contact to share social presence information from one of their clients.
  In this case their other clients will receive presence notifications indicating that a subscription to the contact entered the pending state and notifications including the other user’s social presence information when the contact accepted the “invitation”. If the contact blocks the “invitation”, there will be presence notifications to all the user’s clients indicating that the subscription was terminated. The clients shall use these unexpected notifications as triggers to update the locally stored copy of the Shared XDMS’s “*resource-lists*” document if they cache that kind of information locally.
- The user revokes the presence sharing with a contact from one of their clients.
  Again his other clients that are online will receive unexpected presence notifications indicating that the subscription to the contact’s social presence information was terminated. If they cache the information in the Shared XDMS’s “*resource-lists*” document locally, they shall use this notification as a trigger to verify that the information is still up-to-date.
  Changes are done while the client was offline. A client that caches the information in the Shared XDMS’s “*resource-lists*” document locally should check whether that document has changed when it comes online. Therefore, this will not cause any issues.

- The user owning multiple clients changes a contact from being a VIP contact to being non-VIP contact from one of their clients. His other clients that are online will receive unexpected presence notifications indicating that the subscription to the contact's social presence information was terminated. If they cache the information in the Shared XDMS's "*resource-lists*" document locally, they shall use this notification as a trigger to verify that the information is still up-to-date.
- The user owning multiple clients changes a contact from being a non-VIP contact to being a VIP contact from one of their clients. In this case, their other clients will receive presence notifications indicating that a subscription to the contact has been created and notifications including the other user's social presence information. Again, the clients shall use these unexpected notifications as triggers to update the locally stored copy of the Shared XDMS's "*resource-lists*" document if they cache that kind of information locally.

3.7.4.6 RLS Server Handling

3.7.4.6.1 *Nickname Handling*

A RLS server supporting RCS shall include any display name it received in the *P-Asserted-Identity* and *From* headers of the RLS subscription in the corresponding header of the related backend subscriptions that it sends to the Presence Server.

3.7.4.7 Presence Server Handling

3.7.4.7.1 *Nickname Handling*

A Presence Server supporting RCS shall include any display name it received in the *P-Asserted-Identity* header field of a presence subscription in the display-name attribute of any entry related to that subscription in the *application/watcherinfo+xml* body that is sent to the clients of the served RCS presentity that was the target of the subscription. If the *P-Asserted-Identity* header field does not contain any display name, the display name provided in the *From* header field of the subscription will be used, if any.

3.7.4.8 XDM Server Handling

3.7.4.8.1 *Status Icon*

In the network the retrieval of the information referred to by the link to the status icon will be realized in an architecture as described in [XDM1.1_AD] with the addition of the Cross-Network Proxies and XDM-8 and NNI-1 interfaces defined in [XDM2.0_AD]. The required functionality of the Cross-Network Proxy is limited to the authorization, data transfer and routing of XCAP functionalities. The routing of search requests is not applicable to RCS. For RCS the supported protocols on the NNI-1 interface are limited to XCAP, "*limited XQuery over HTTP*" is not supported.

At the functionality level, this means that the identity provided by the Aggregation Proxy is not only shared on the XDM-4 and enabler specific reference points between the Aggregation Proxy and the Enabler specific XDMS as it is described in [XDM1.1_Core] section 6.4.1, but also on the XDM-8 and NNI-1 interfaces as it is described in [XDM2.0_Core] section 5.1.3. The Integrity and Confidentiality protection of [XDM1.1_Core] section 6.4.2 is extended to the NNI-1 interface as it is described in [XDM2.0_Core] section 5.1.4. Furthermore in addition to the functionality described in [XDM1.1_Core], the Aggregation Proxy shall route requests to the Cross-Network proxy as it is described in [XDM2.0_Core] section 6.3.1.1 and route the Cross-Network Proxy's responses back to the XDM client. The procedures for routing requests to the search proxy that are described in [XDM2.0_Core] section 6.3.1.1 are not applicable for RCS. Finally the functionality of the Cross-Network Proxy as it is described in [XDM2.0_Core] section 6.5 and subsections shall be supported with the exception of all functionality related to the routing of Search Requests and Search Responses.

3.7.5 NNI and IOT considerations

The NNI interfaces for SPI sharing shall behave according to the procedures described in section 2.12 and the documents it refers to.

3.7.6 Implementation guidelines and examples

3.7.6.1 SPI transaction handling

<u>Initiator side</u>

1. An RCS user that wants to Share SPI with a contact selects the contact entry in their local enriched address book.
2. They select in the menu “share” (if available, that is the contact has the SPI service capability) the function “Share Social Presence” and can see by using the SPI general menu the SPI status associated with the contact (“idle”, “pending” “activated”, “terminated”)
3. This SPI general menu, depending on the SPI status, enables them to invite the contact to share SPI with following options
    - “VIP contact”: YES / NO (default NO)
    - “Authorize Location Sharing”: YES / NO (default NO)
      Note: at any moment, for these 2 options, when the SPI status becomes “active”, the general Share SPI menu offers the user the possibility to change their choices
    - “Nickname” text field: free user text
4. Then the user can follow the SPI status evolution the SPI status by selecting the contact and activating the SPI general menu
    - “pending”: the contact has not yet accepted to share SPI with them
    - “active”: the contact has accepted to share SPI with them
    - “terminated”: The contact, after acceptation, has decided to revoke sharing Presence Information

<u>Callee side</u>

1. The RCS user is triggered by a pop up SPI menu that a distant user has invited them to share their Social Presence Information
    - If the user already has a contact entry for the inviting user in the local address book, then the name assigned to the contact entry in the local address book of the user appears in this SPI menu
    - If the user is not present in the local address book, then the “nickname” of the inviting user (if any provided) and their E.164 address appear in the menu instead
2. The SPI pop up menu proposes allows actions through buttons and fields to be filled
    - “Accept”: YES/NO
    - “VIP contact”: YES / NO (default NO)
    - “Authorize Location Sharing”: YES / NO (default NO)
      Note: at any moment, for the latter 2 options, when the SPI status becomes “active” the general Share SPI menu offers the user the possibility to change their choice
3. Then the user can follow the SPI status evolution by selecting the contact and activating the SPI general menu
    - “active”
    - “terminated”: The contact, after acceptation, has decided to revoke sharing Presence Information

SPI status "active"

At any moment, in the "active state" the user can choose for a contact selected in the address book:

- To modify SPI sharing parameters: VIP contact, Geolocation Sharing authorisation
- To revoke SPI sharing

3.7.6.2 *Availability handling*

The user can choose how they appear to their contacts: "Available" or "Not Available".

3.7.6.3 *Free Text handling*

The user enters some free text possibly including emoticons. They are blocked when the length of the text reaches the limit fixed by the Service Provider.

3.7.6.4 *Icon handling*

The user is asked to choose an image in the local file system of the device from a sub set of the images that are candidate to be part of the user SPI (filter based on file size: the size of the icon must not exceed what is authorized by the Service Provider).

3.7.6.5 *URL label*

The user is asked to enter a URL and an associated free text. The user may be assisted by the application to enter the information depending on the Service Provider settings.

3.7.6.6 *Geolocation handling*

In a manual mode, user manually picks a position (x, y) on a map or user requests for an update of their position (x, y) information. Then, geolocation information is given by RCS client towards authorized enriched contacts as soon as it has been made available on the RCS client by the user.

In automatic mode, update of location coordinate information (x, y) is automatically made and given to the authorized enriched contacts on a regular basis.

Manual mode and automatic mode are further detailed below.

3.7.6.6.1 *Display Modes*

Three displays modes are possible:

1. Text: a user is located and the result is given to their authorized enriched contacts under a declarative text format (Paris, La Défense). The declarative text is always manually edited by the user.
2. Map: a user is located and the result is given as coordinate information (x, y) to his authorized enriched contacts and displayed under a map format. When the user is displayed as a dot on a map, their location information can also be displayed as text in other screens. For example, if a user has updated his location to a position in the centre of London on a map, some screens without a map may display his location using the declarative text edited by the user (for example, "London, UK").
3. A combined display of text and a map

3.7.6.6.2 *Update Information*

Declarative location text information is always manually edited/updated by the user.

The Geolocation information update regarding coordinate information (x, y) can be either:

- Manual
    - The user can select their location manually on a map, by either entering text that is then processed to provide location (as coordinate information (x,y)) on a map (for example Google Maps) or, for example, by dragging and dropping a "pin" on a map

  - to the desired location. This user-chosen location can be different from the user's actual location.
  - Triggering their actual current location (based, for example, on a GPS signal from the device or a mobile network-based location). For example, they click on the location update button, and coordinate information (x,y) is automatically filled)
- Automatic
  - (User A decides that they want their authorized contacts to be informed regarding their coordinate position (x,y) on a regular basis). Location coordinate information (x, y), and any update is automatically made and given to authorized enriched contacts on a regular basis.

Other recommendations for implementation from the end user's perspective (these are only meant as examples and not actual specifications):

- For Fully Automatic update, the user shall be able to choose the level of accuracy for their location
  - Country
  - City
  - Street (most accurate location)
- In addition to having a map displayed per contact inside the address book (at -1 or -2 navigation levels), there might be the possibility to have a consolidated map with all contact location information (within the scope defined : country, city or street). The starting position of the map is the user's current position, if available. See also section 3.10.

3.8 IP Voice Call (IR.92 and IR.58)

3.8.1 Feature description

This feature provides an IP Voice Call service on an RCS device. An IP Voice Call interoperates with other RCS devices including VoLTE/VoHSPA as defined in [PRD-IR.92] and [PRD-IR.58] and with CS/PSTN (Public Switched Telephone Network) voice calls. The voice call is provided via IP Voice when the access network allows it, and may be provided via CS voice when IP Voice is not available, depending on the device and network capabilities.

The minimum set of supplementary services provided is described in [PRD-IR.92].

At any time, either user can terminate the IP Voice Call.

3.8.2 Interaction with other RCS features

IP Voice Call must use a separate SIP session which is not shared with Standalone messaging (section 3.2), Chat (section 3.3), Group Chat (section 3.4), File Transfer (section 3.5), Content Sharing (section 3.6) or Geolocation PUSH (section 3.10). Interaction with Content Sharing is covered in section 3.6.2. Interaction with Video Call is covered in section 3.9.2.

3.8.3 High Level Requirements

3-8-1 The scope of the requirements for IP Voice Call are those found in [PRD-IR.92] and [PRD-IR.58].

3.8.4 Technical Realization

At a technical level the voice call service shall be based on [PRD-IR.92] and [PRD-IR.58].

Since in RCS a user may register a primary and one or more secondary devices in IMS, incoming SIP requests are forked. This also applies to incoming SIP requests for IP Voice

Calls, so it is expected that they be forked in the same way as other RCS related SIP requests are forked, i.e. in parallel. For voice sessions set up according to [PRD-IR.92] and [PRD-IR.58], the support for early media as described in [PRD-IR.92] and [PRD-IR.58] is required.

Broadband Access clients which support and are configured for IP Voice Call but are not enabled for VoLTE/VoHSPA (and therefore do not make use of the IMS APN as specified in section 2.9.1.4) shall behave as an RCS-AA device as defined in section 2.2.

A device enabled for VoLTE/VoHSPA (and thus using the IMS APN) will behave depending on the access network used. When connecting through an LTE or HSPA network that supports the use of the access control, the RCS-LTE or RCS-HSPA device shall behave as the corresponding device with access control defined in [PRD-IR.92] and [PRD-IR.58]. When not in LTE or HSPA coverage, an RCS-LTE, RCS-HSPA device shall behave as an RCS-CS device as defined in section 2.2. An RCS-CS device shall not offer the IP Voice Call service.

3.8.4.1 Devices enabled for VoLTE/VoHSPA

If the domain selection has selected 3GPP PS access for voice (VoLTE/VoHSPA) this access is used for RCS features as well. If either VoLTE and/or VoHSPA is supported any of these is assumed to be natively implemented and integrated within the device. The IMS registration shall be shared between VoLTE/VoHSPA and RCS.

A device enabled for VoLTE/VoHSPA always uses the IMS APN for accessing RCS services.

3.8.4.2 Devices using CS domain for voice calls

A device may use the CS domain possibly via Circuit Switched Fallback (CSFB) for voice calls when it is not enabled for VoLTE/VoHSPA, or it is enabled for VoLTE/VoHSPA but the current network does not support VoLTE/VoHSPA (e.g. the serving network does not support VoLTE or an IMS roaming agreement is not in place).

A device not enabled for VoLTE/VoHSPA uses the configured APN as described in section Annex A for accessing RCS services.

LTE access can be used for RCS features providing there is no ongoing CS call.

LTE devices not enabled for VoLTE will fall back to CS for voice calls. Once CS fallback occurs, LTE access is dropped, and RCS functionality is provided via 3G/2G access.

3.8.4.3 Flows

Since the voice call UX is well-known, it is not necessary to provide message flows and a reference UX.

3.8.5 NNI and IOT considerations

No specific guidelines apply other than what is already defined in Section 2.12.

3.8.6 Implementation guidelines and examples

From the UX point of view, two possible entry points to the voice service are:

1. Address book/Call-log: A voice call can be initiated with any registered contact – contact oriented initiation.
2. Chat window: From the Chat (one-to-one Chat only) window a voice call can be initiated using the relevant menu item. The experience is identical to the address book/call-log.

Since the voice call UX is well-known, it is not necessary to provide implementation guidelines and examples.

3.9 IP Video Call (IR.94)

3.9.1 Feature description

This feature provides an IP Video Call between two RCS devices with synchronization between the audio and video streams, thus providing lip synch. For audio the IP Voice Call (as described in section 3.8) is used.

The establishment of the IP Video Call session can be achieved in two possible ways:

1. '**Direct launch**', if no previous voice call was established between the contacts.
2. '**Upgrade to IP Video Call'**, if the users were already engaged with each other in an IP Voice Call communication.

From the user experience perspective the RCS user can toggle between front camera ("me"), the rear camera ("what I see") and a file (video stream), at any time when using the IP Video Call service.

Note: The Video Call service in this context is seen as a superset of Video Share use cases as described in 3.6.1.2 offering lip synch in addition.

In all cases, when invited for a video call an RCS user can either:

- Accept the video call establishing a full duplex video call
- Accept only to receive the inviting user's video content establishing a call where the video part runs in simplex mode alongside a full duplex audio call. In this case the accepting user can at any time decide to move the video part to full duplex as well.
- Accept the call as audio only, i.e. decline the video part of the communication. Voice call is established or continues.
- Decline the video call i.e. no communication is established to any of the receiving user's devices when declining the video call. The call may be redirected to a voice or video messaging system however depending on the policies of the receiving user's network.

When the video stream of the IP Video Call is realised in a full duplex mode, at any time, either user can decide to migrate from a full duplex mode to a simplex mode, i.e. deactivate the sending of their video stream. They can later decide to migrate from a simplex mode to a full duplex mode again.

At any time, either user can terminate the IP Video Call (both audio and video stream or only the video stream).

An RCS device may learn and remember that a contact is IP Video Call capable upon receiving a SIP INVITE request for an IP Voice or IP Video Call. Communication with [PRD-IR.94] compliant devices should not be prevented if RCS procedures for service capability discovery are not supported by those devices.

3.9.1.1 Direct Launch

When both parties support video call at any particular point in time (e.g. by the capability exchange described in section 2.6), either user can initiate the setup of a video call. The receiving user determines whether the call will be initiated in full or simplex mode.

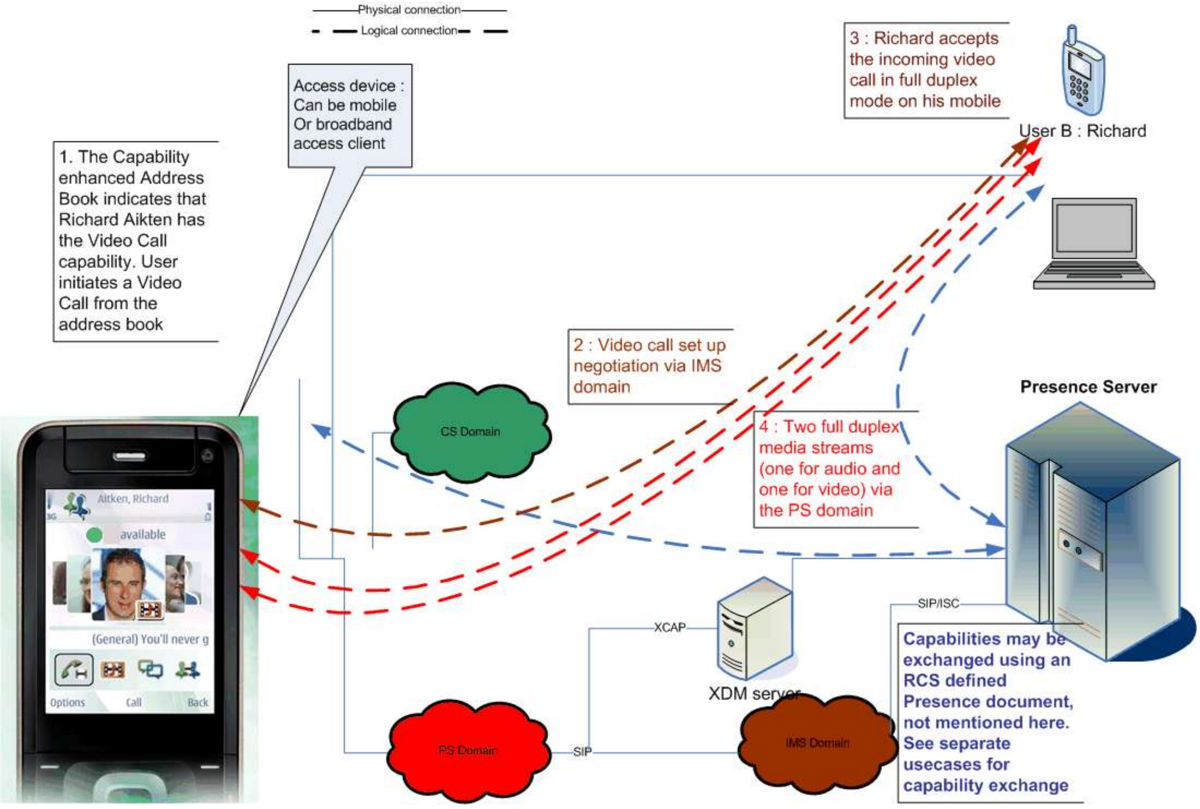

Physical connection
Logical connection
Access device : Can be mobile Or broadband access client
1. The Capability enhanced Address Book indicates that Richard Aikten has the Video Call capability. User initiates a Video Call from the address book
3 : Richard accepts the incoming video call in full duplex mode on his mobile
User B : Richard
2 : Video call set up negotiation via IMS domain
4 : Two full duplex media streams (one for audio and one for video) via the PS domain
Presence Server
CS Domain
XCAP
XDM server
SIP/ISC
Capabilities may be exchanged using an RCS defined Presence document, not mentioned here. See separate usecases for capability exchange
PS Domain
SIP
IMS Domain
Aitken, Richard
available
(General) You'll never g
Options
Call
Back

Figure 85: Full duplex video call

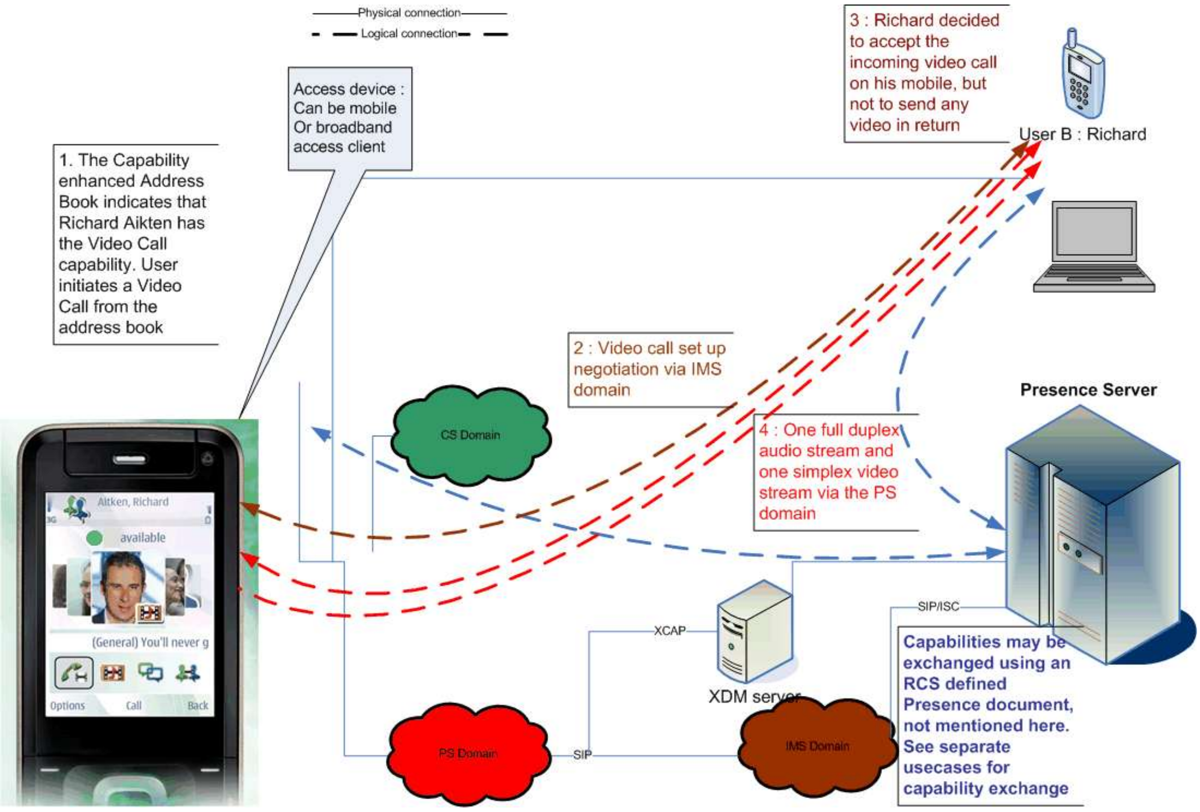

Physical connection
Logical connection
Access device : Can be mobile Or broadband access client
1. The Capability enhanced Address Book indicates that Richard Aikten has the Video Call capability. User initiates a Video Call from the address book
3 : Richard decided to accept the incoming video call on his mobile, but not to send any video in return
User B : Richard
2 : Video call set up negotiation via IMS domain
4 : One full duplex audio stream and one simplex video stream via the PS domain
Presence Server
CS Domain
XCAP
XDM server
SIP/ISC
Capabilities may be exchanged using an RCS defined Presence document, not mentioned here. See separate usecases for capability exchange
PS Domain
SIP
IMS Domain
Aitken, Richard
available
(General) You'll never g
Options
Call
Back

Figure 86: simplex video call

Users could switch between the full duplex and simplex variants of the video during the call. This would result in a new negotiation via the IMS domain for the ongoing call.

Note: multiparty calls are also possible.

3.9.1.2 Upgrade to IP Video Call

As stated in section 3.9.1, a user could also start a video call from an existing IP Voice Call (that is the service described in section 3.8).

When the devices on the call all support video call at a particular point in time, either user can initiate the upgrade to a video call by selecting the corresponding option.

If the voice call was entirely (end-to-end) in the PS domain this initiates a negotiation via the IMS domain and if the other user accepts the upgrade a simplex or duplex video stream is added to the ongoing call.

NOTE: if one end of the call moved to CS, the upgrade may fail, but the voice call would remain in place. If the other party is an RCS user, the party wanting to upgrade may have discovered the fact that video call is no longer available due to the capability exchange described in section 2.6 and should therefore not be offered the possibility to upgrade.

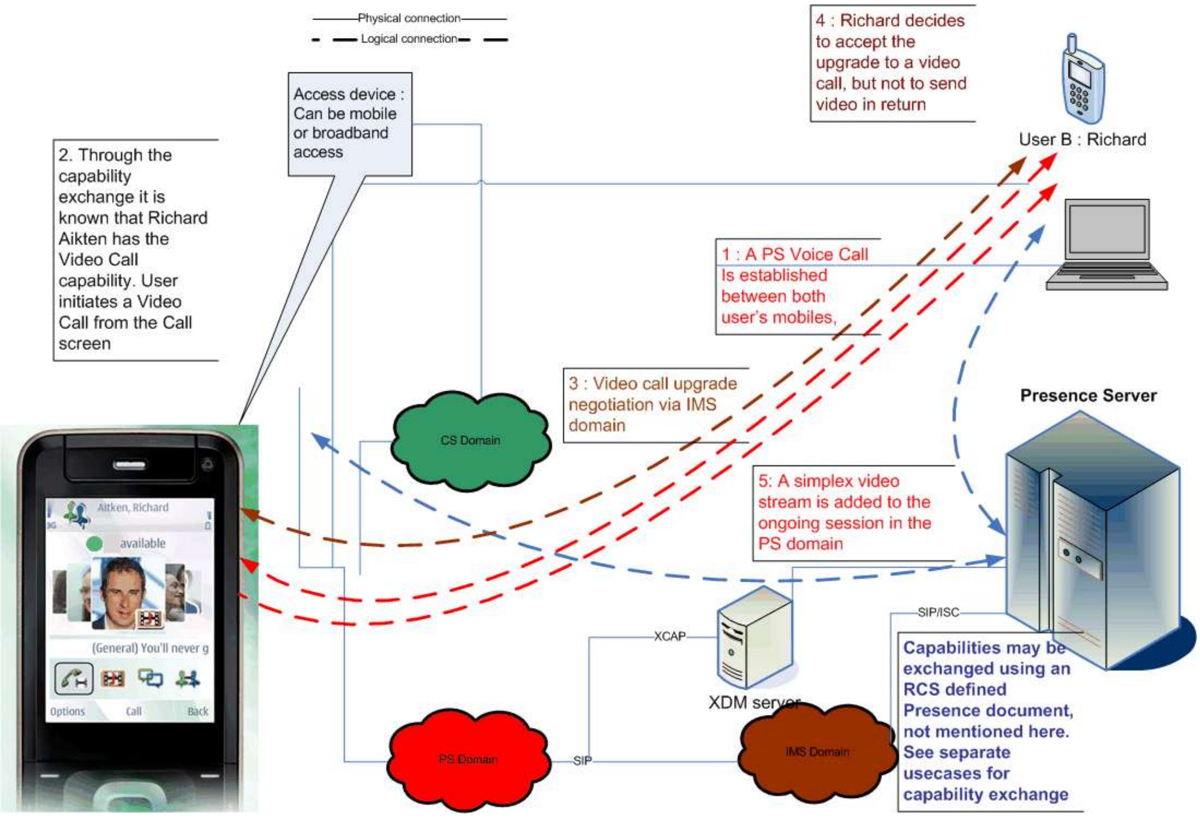

Physical connection
Logical connection
Access device : Can be mobile or broadband access
4 : Richard decides to accept the upgrade to a video call, but not to send video in return
User B : Richard
2. Through the capability exchange it is known that Richard Aikten has the Video Call capability. User initiates a Video Call from the Call screen
1 : A PS Voice Call Is established between both user's mobiles,
3 : Video call upgrade negotiation via IMS domain
Presence Server
CS Domain
5: A simplex video stream is added to the ongoing session in the PS domain
Aitken, Richard
available
(General) You'll never g
Options
Call
Back
XCAP
SIP/ISC
XDM server
Capabilities may be exchanged using an RCS defined Presence document, not mentioned here. See separate usecases for capability exchange
PS Domain
SIP
IMS Domain

Figure 87: Upgrade PS call to video call

Note: The behaviour is the same for the scenario where the user accepted the video call as a full duplex service.

3.9.2 Interaction with other RCS features

3.9.2.1 IP Voice Call

The IP Video call must use the same SIP session as the IP Voice Call (see section 3.8).

The video call service has a strong interaction with the voice call service since both services offer the option for full-duplex real-time communication. That strong relation results in the option to upgrade an existing voice call to a video call as described in section 3.9.1.2. An end-to-end IP Voice Call is upgraded by adding an additional media stream to the ongoing session.

Communication Waiting: when the user is on a voice call and a request for an unrelated video call is received (or vice versa), the device shall handle this video call in the same way as a second voice call coming in. Meaning it will behave differently for the scenario where no call was active and will thus not start ringing loudly and shall use Communication Hold appropriately if the new call is accepted without terminating the ongoing one.

3.9.2.2 Video Share

The IP Video Call and Video Share service capabilities are mutually exclusive: when both ends are capable of using the IP Video Call service (as per [PRD IR.94]), then IP Video Call shall be used as the service to share contents instead of Video Share as described in section 3.6. If one or both ends are not capable of using the IP Video Call service, then Video Share will be used to provide the service. Therefore when performing a capability exchange within a call, if the Video Call capability is set as available, the Video Share capability shall also be made available.

3.9.3 High Level Requirements

3-9-1 In a video call the delay difference between audio and video media shall be unnoticeable (that is lip sync is provided)

3-9-2 The overall delay on both media shall allow for a conversational service

3-9-3 The quality of the video shall be high. At least H.264 level 1.2 shall be supported in suitable circumstances matching the similar requirement in [PRD-IR.94]

3-9-4 It shall be possible to establish a video call without having an active voice call between the parties in the call

3-9-5 It shall be possible to convert an ongoing IP Voice Call (that is as in section 3.8) into an IP Video Call

3-9-6 The receiver shall be able to accept the call in full-duplex mode and in simplex mode in which case no content is sent back to the originating party.

3-9-7 It shall be possible for either party to turn a full duplex video call into a simplex one by terminating the streaming.

3-9-8 If the device has multiple cameras it shall be possible to toggle between them.

3-9-9 The receiver shall be able to reject the video call. This rejection does not affect an ongoing voice call.

3-9-10 Either party shall be able to terminate an active video call

3-9-11 Terminating an active video call shall terminate the communication regardless of whether the call was initiated directly as a video call or initially started as a voice call only.

3-9-12 At least the minimum set of supplementary services defined in [PRD-IR.92] shall be supported

3.9.4 Technical Realization

The IP Video Call service shall be based on [PRD-IR.94]. A VoLTE/VoHSPA enabled device as defined in section 2.2 shall behave as an RCS-LTE or RCS-HSPA device according to the descriptions in [PRD-IR.94]. Broadband access devices shall behave as RCS-AA.

Integration of resource management and SIP is done as per [PRD-IR.94] for RCS-LTE devices, and as per [PRD-IR.94] and [PRD-IR.58] for RCS-HSPA devices. No specific requirements for resource management are required for an RCS-AA device.

For RTP media and RTCP usage, an RCS-AA device shall follow the requirements for NAT traversal as specified in section 2.8.

An RCS-CS device does not support the IP Video Call service.

3.9.4.1 Flows

3.9.4.1.1 *Assumptions*

The following sections describe the relevant message flows and reference UX. Please note that the following assumptions have been made:

- For simplicity, the internal mobile network interactions are omitted in the diagrams shown in the following sections.
- For simplicity RTCP exchanges are omitted in the diagrams. They should be executed as described in [PRD-IR.94] and section 2.8
- The terminal comes with a front and rear camera. If one or both are missing, the user should be notified only with the available options.
- The capability exchange was performed already (as described in section 2.6). Both users are thus aware that the other party supports video call.

3.9.4.1.2 *Direct Launch*

3.9.4.1.2.1 Accept as bidirectional

In this scenario no voice call is ongoing between the users and User A decides to initiate a video call with User B. User B accepts the call as a fully bidirectional video call. This results in two bidirectional RTP/RTCP streams, one for the audio and one for the video.

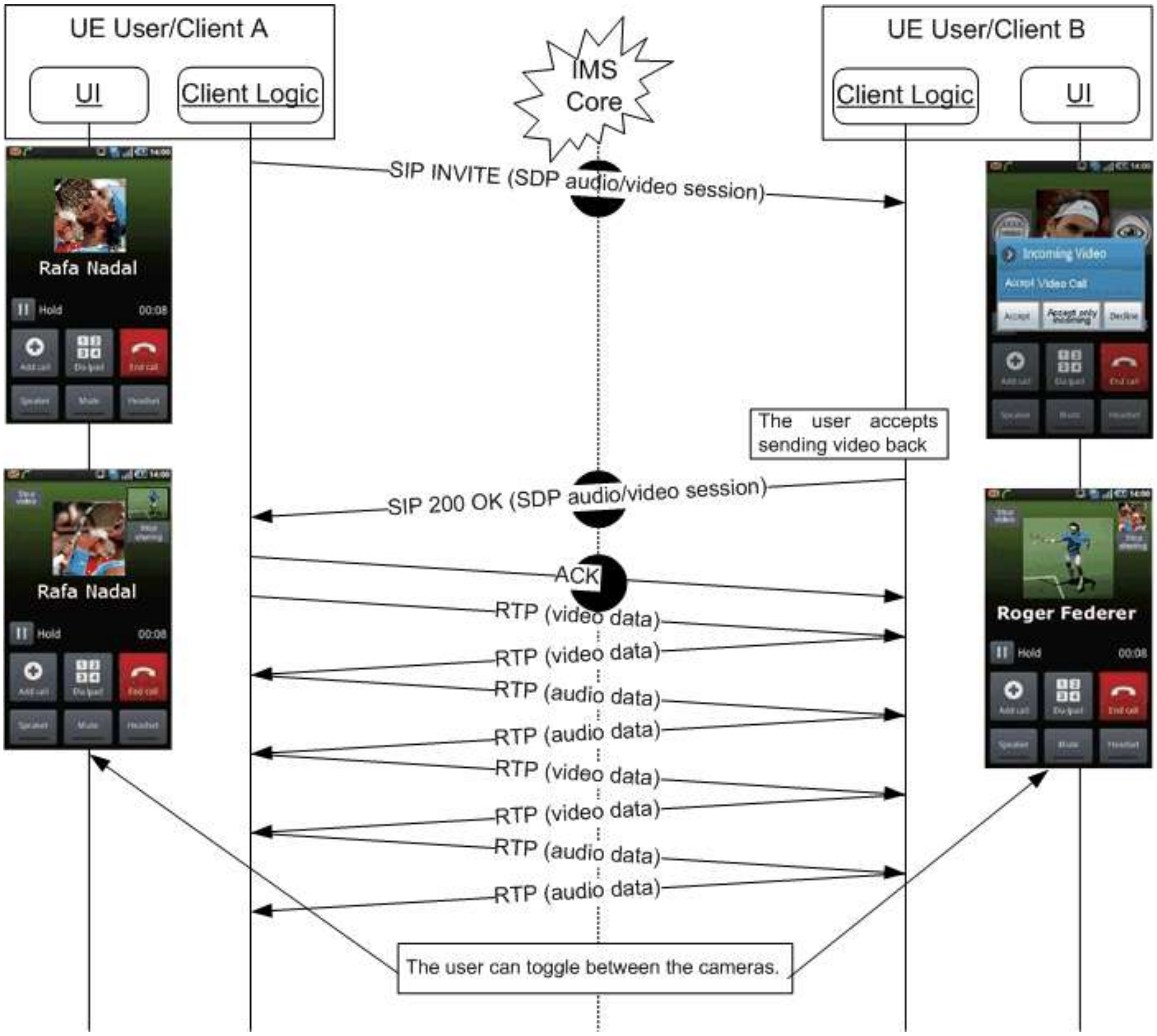


Figure 88: Direct launch of video call - Accept as bidirectional

3.9.4.1.2.2 Accept unidirectional

In this scenario no voice call is ongoing between the users and User A decides to initiate a video call with User B. User B accepts the call, but indicates that they do not want to send video back. This results in two RTP/RTCP streams, one bi-directional for the audio and one uni-directional (from User A to User B) for the video.

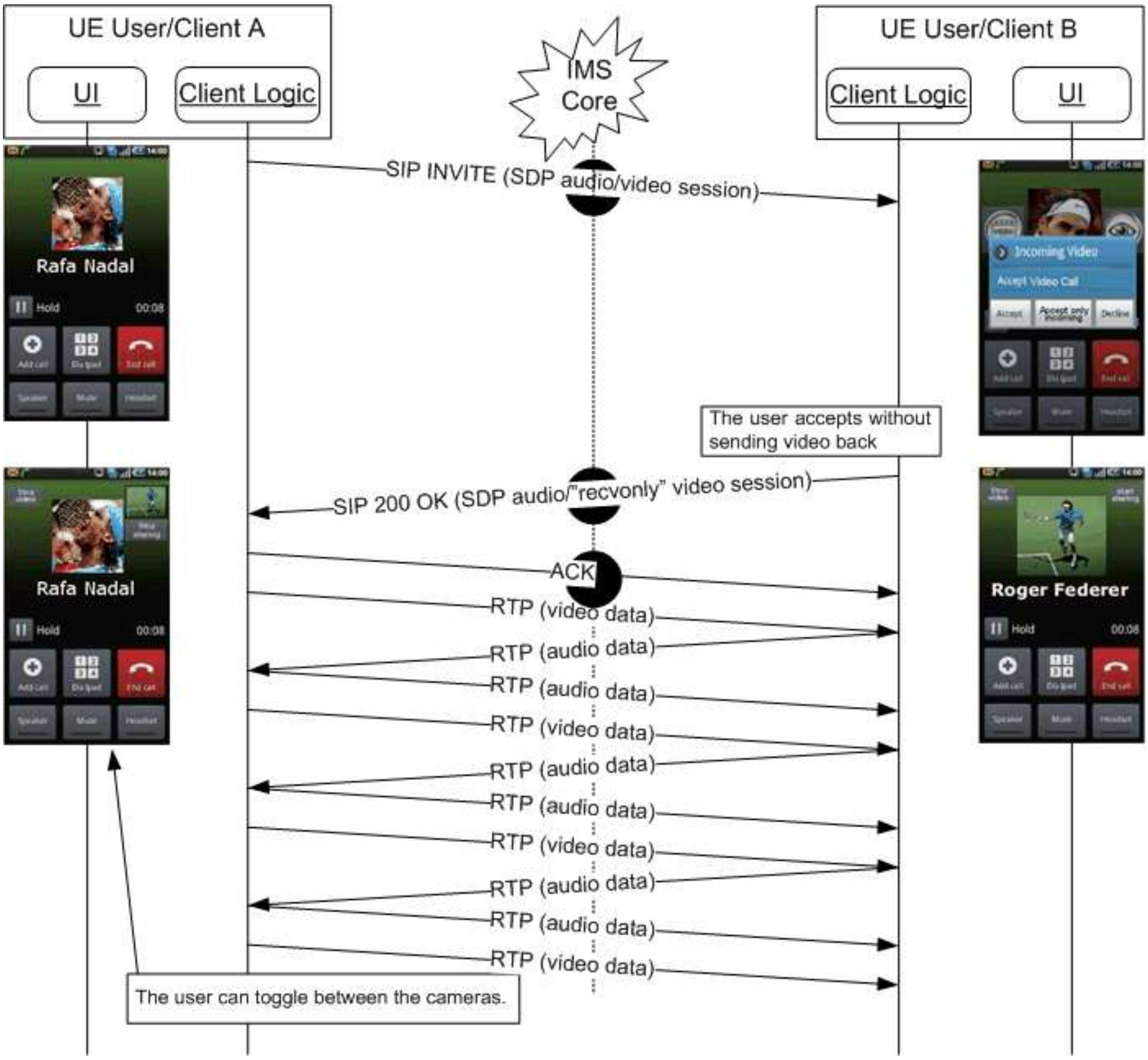


Figure 89: Direct launch of video call - Accept as unidirectional

3.9.4.1.2.3 Decline

In this scenario no voice call is ongoing between the users and User A decides to initiate a video call with User B. User B rejects the call.

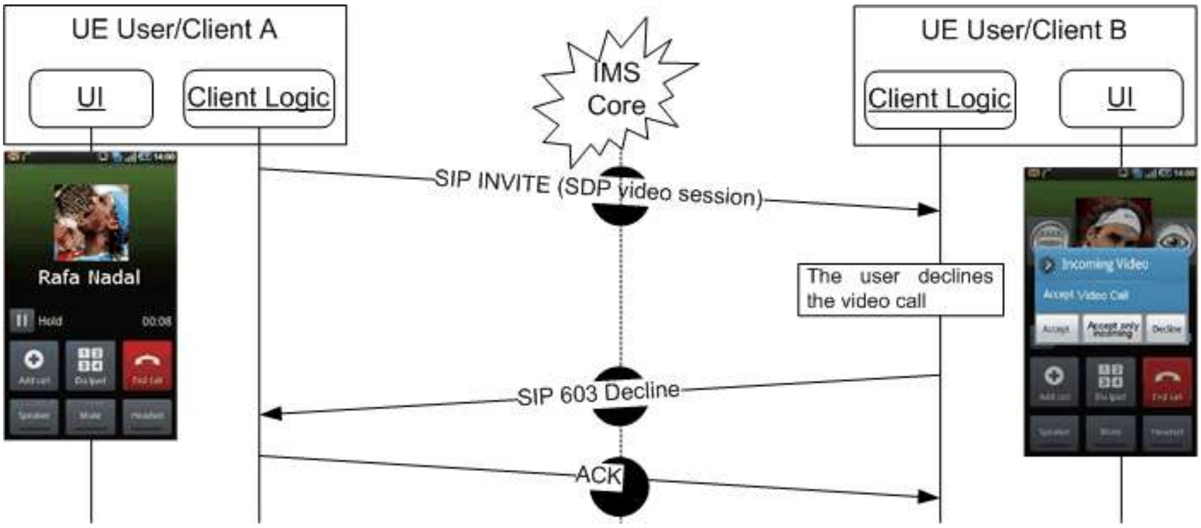


Figure 90: Direct launch of video call – Decline

In this scenario User B’s network could also redirect the call to an announcement or voice/video mail system.

3.9.4.1.3 *Upgrade from PS Call*

3.9.4.1.3.1 Accept

In this scenario a PS voice call is ongoing between the users as specified in section 3.8. As specified in [PRD-IR.94] at the start of this call both terminals have indicated that they are capable of upgrading to a video call and no further capability exchange was done after the call setup indicating that this capability is no longer available.

User A decides to upgrade the ongoing call into a video call. User B accepts the upgrade (and in the illustrated flows decides to send video back). This results in a second RTP/RTCP stream for the video being added to the ongoing call (next to the existing bidirectional audio stream). This video stream can either be bi-directional or uni-directional depending on whether User B accepted to send video back or not. This is similar to the cases illustrated in sections 3.9.4.1.2.1 and 3.9.4.1.2.2.

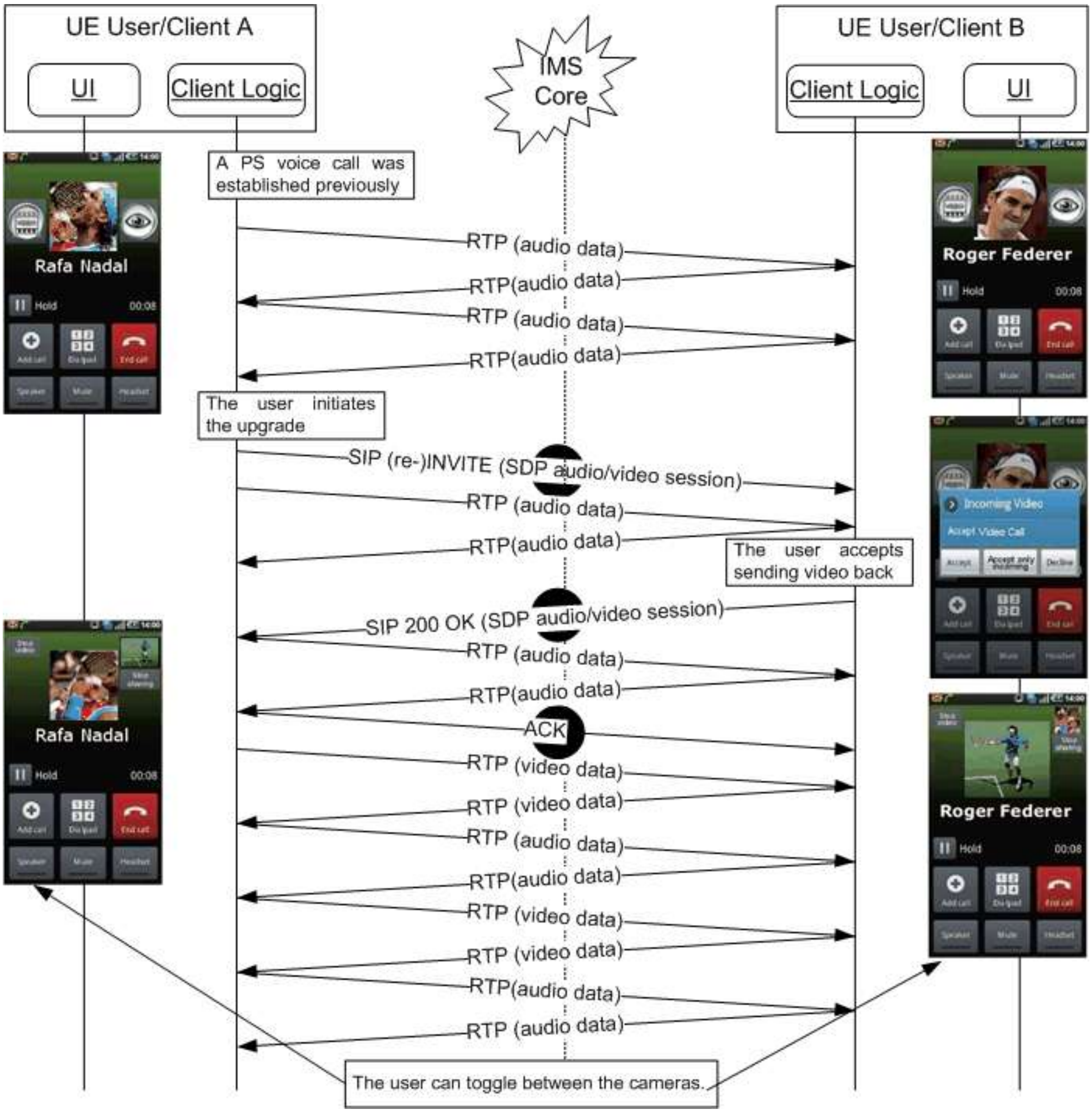


Figure 91: Upgrade PS Voice call to video call

Note: in a multidevice scenario the devices from User B that are not involved in the voice call will not be included in this upgrade flow.

3.9.4.1.3.2 Decline

In this scenario a PS voice call is ongoing between the users as specified in section 3.8. As specified in [PRD-IR.94] at the start of this call both terminals have indicated that they are capable of upgrading to a video call and no further capability exchange was done after the call setup indicating that this capability is no longer available.

User A decides to upgrade the ongoing call into a video call. User B declines the upgrade. The voice call continues unaffected.

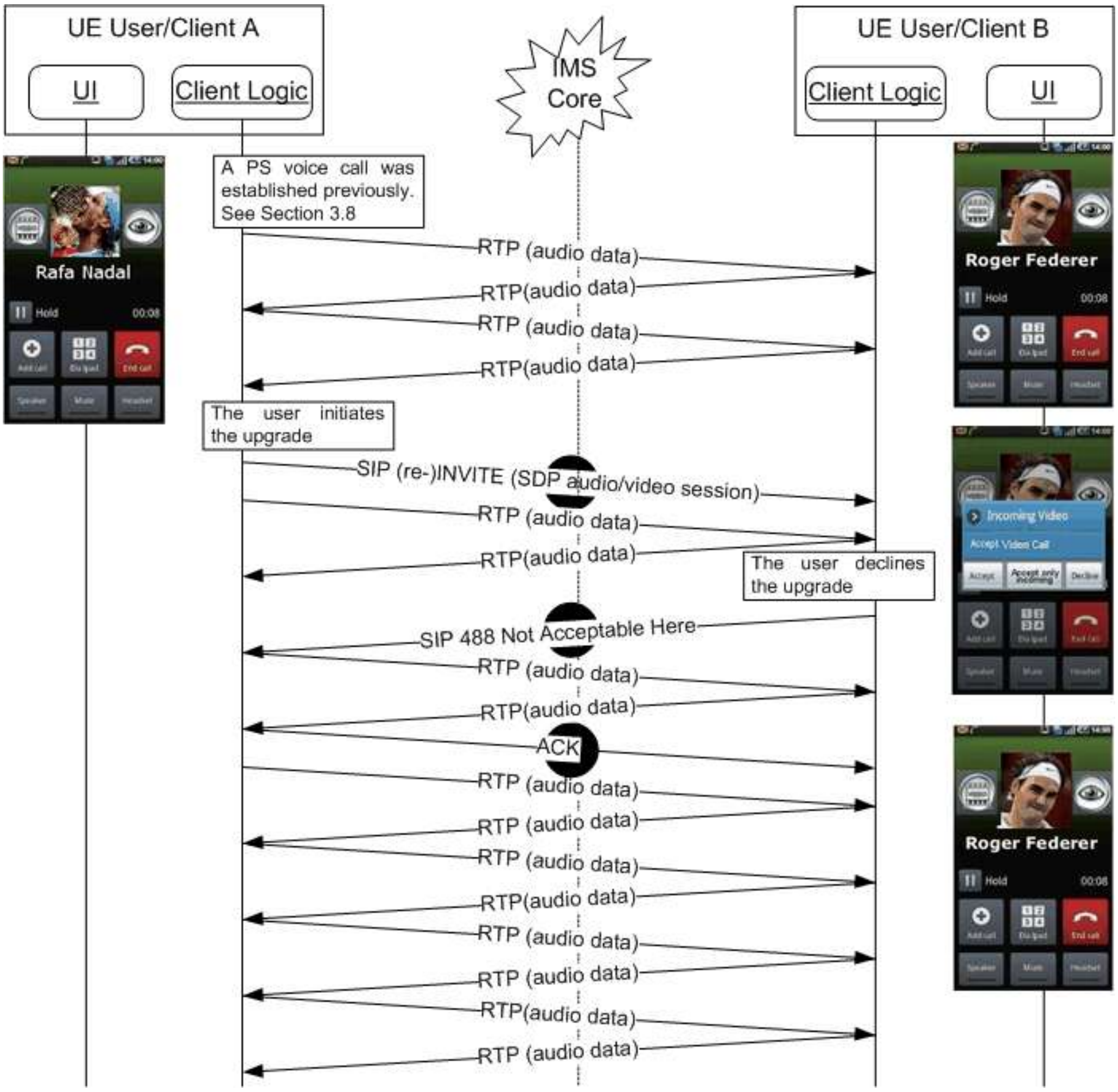


Figure 92: Decline upgrade PS Voice call to video call

3.9.4.1.4 *Switch from unidirectional to bidirectional video*

In this scenario User A and User B are involved in a video call in which User B is not sending video to User A. Then User B decides to start sending a video stream to User A.

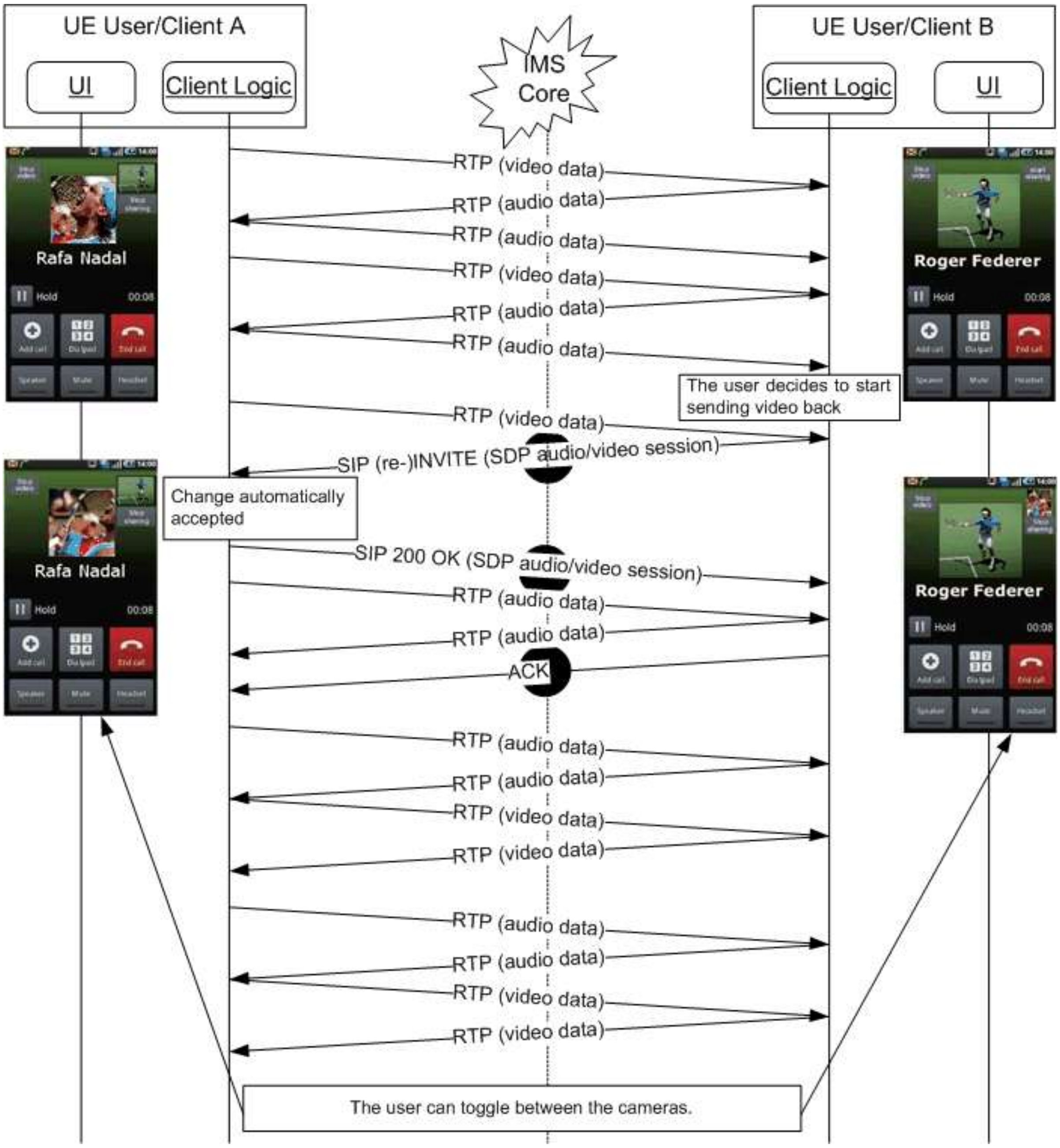


Figure 93: Change from unidirectional video call to bidirectional video call

3.9.4.1.5 *Switch from bidirectional to unidirectional video*

In this scenario User A and User B are involved in a video call in which both users are sending video to each other. Then User B decides to stop sending a video stream to User A.

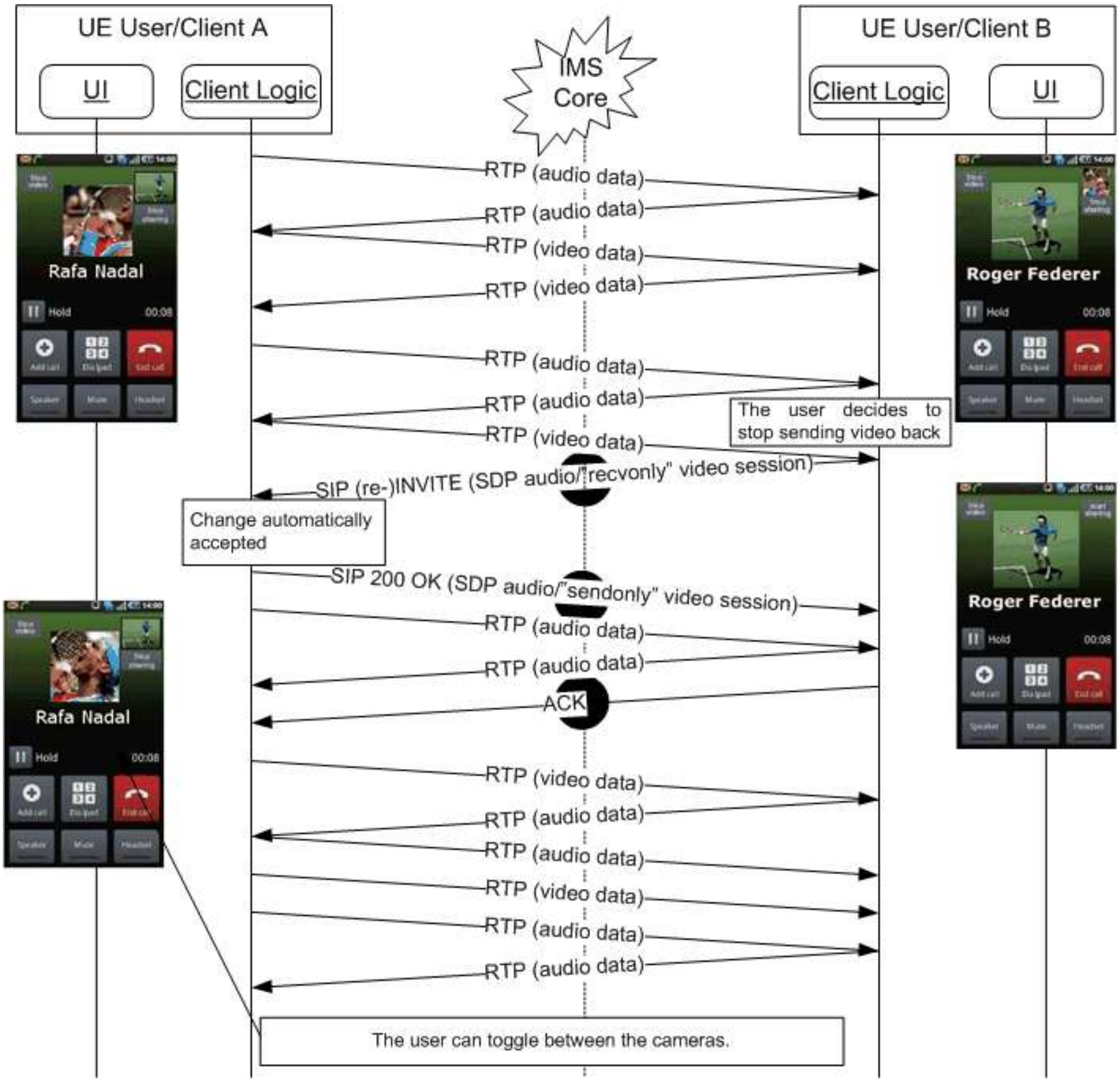


Figure 94: Change from bidirectional video call to unidirectional video call

3.9.4.1.6 *Video call termination*

In this scenario User A and User B are involved in a video call with each other and User A decides to terminate the call.

Note: in this scenario User A is not necessarily the user that started the call.

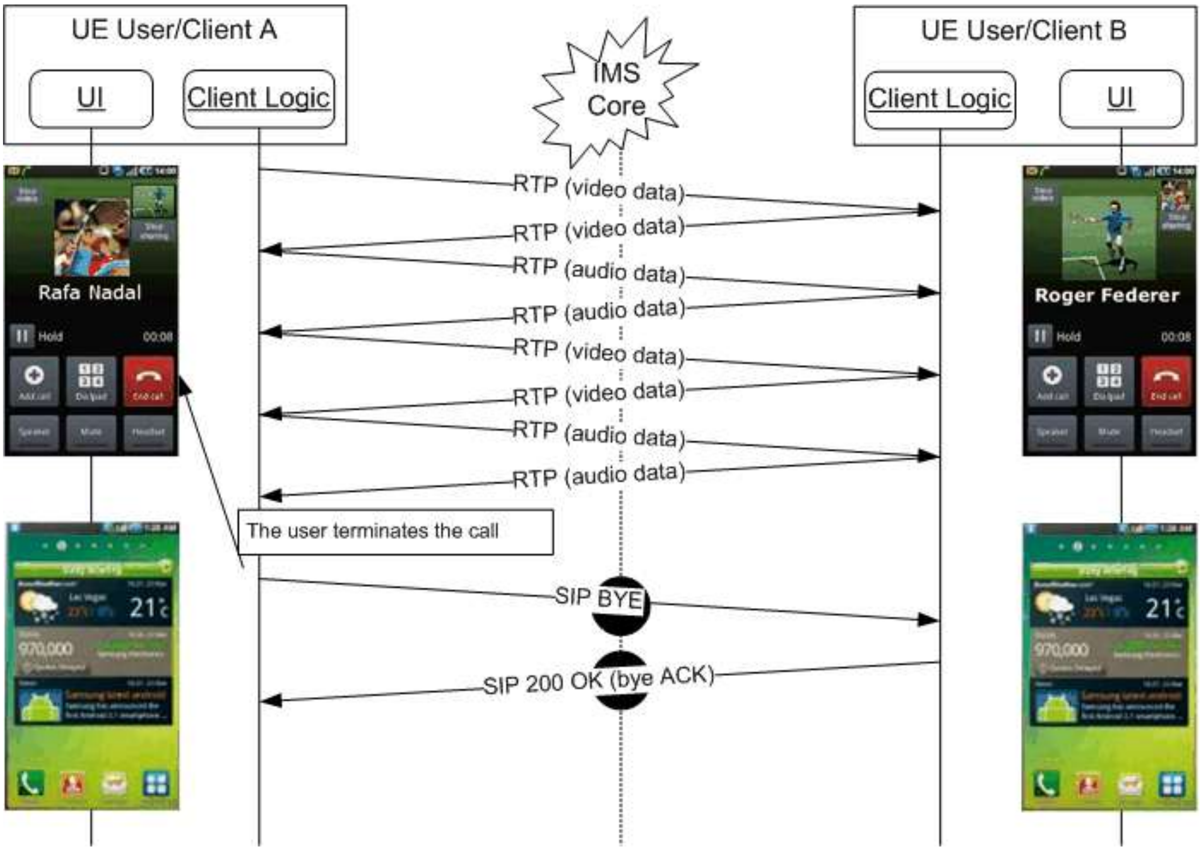


Figure 95: Video call termination

Note: As this terminates the communication between User A and B, there is no need to do a capability exchange to verify whether the termination was or was not voluntary in contrast to the situation for Video Share described in section 3.6.4.

3.9.5 NNI and IOT considerations

The NNI interfaces for content sharing services shall behave according to the procedures described in section 2.12 and the documents it refers to.

3.9.6 Implementation guidelines and examples

From the UX perspective, there are three possible entry points to these services:

1. Address book/Call-log: A video call can be initiated with any registered contact providing the right capabilities are in place – contact oriented initiation.

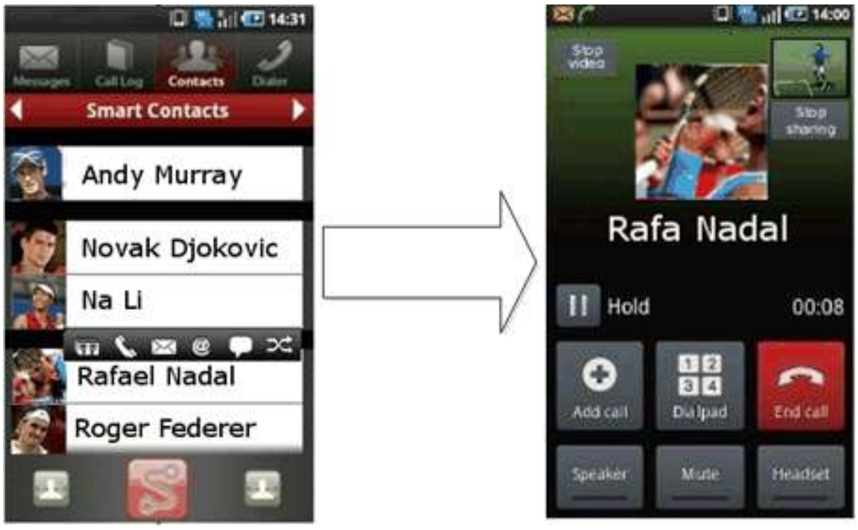


Figure 96: User experience when starting from address book

2. Chat window: From the Chat (one-to-one Chat only) window a video call can be initiated using the relevant menu item. The experience is identical to the address book/call-log. The capability query is initiated when the user opens up the menu in which the available communication options are offered

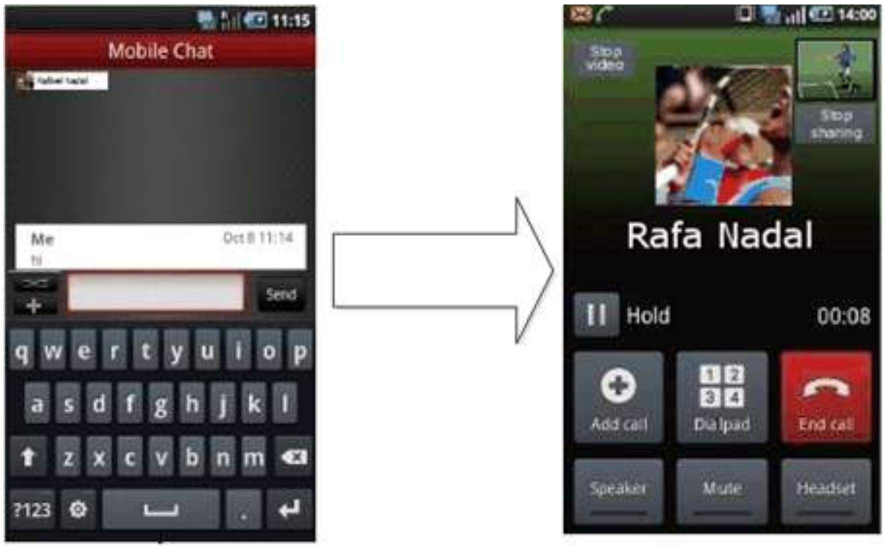


Figure 97: User experience when starting from chat

3. Call screen: an ongoing voice call can be upgraded to a video call.

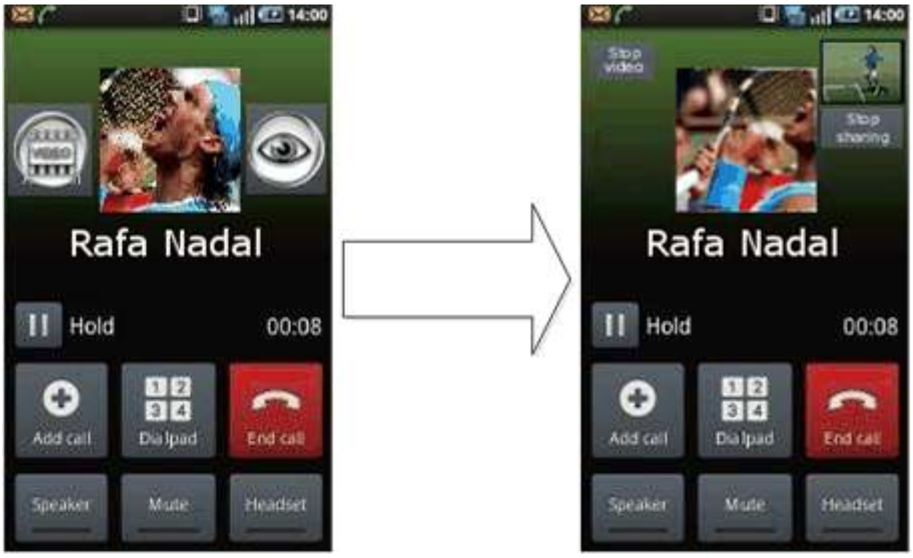


Figure 98: User experience when starting from call screen

Regardless of whether it is an upgrade scenario or a direct call, the receiver will always get 3 options on an incoming video call:

1. Accept
2. Accept only to receive video
3. Decline

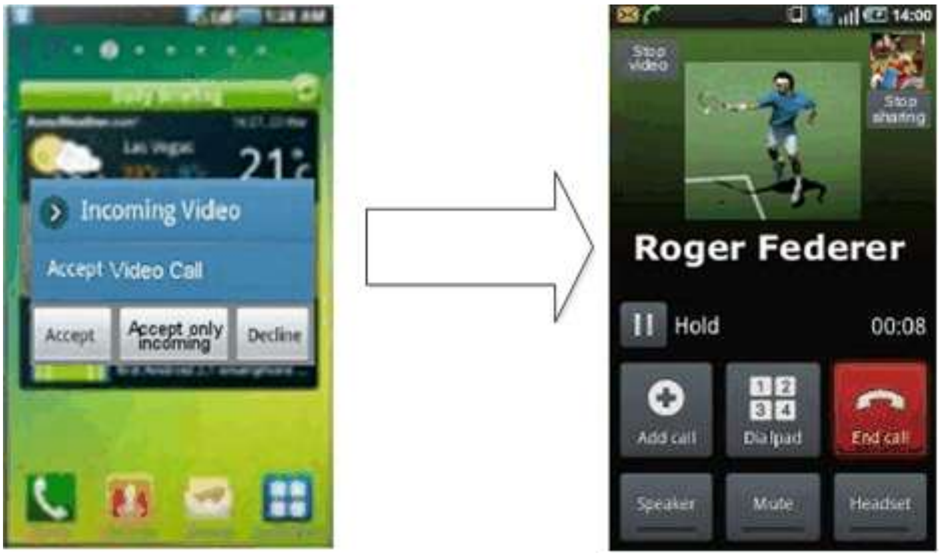


Figure 99: Video call receiver user experience direct video call

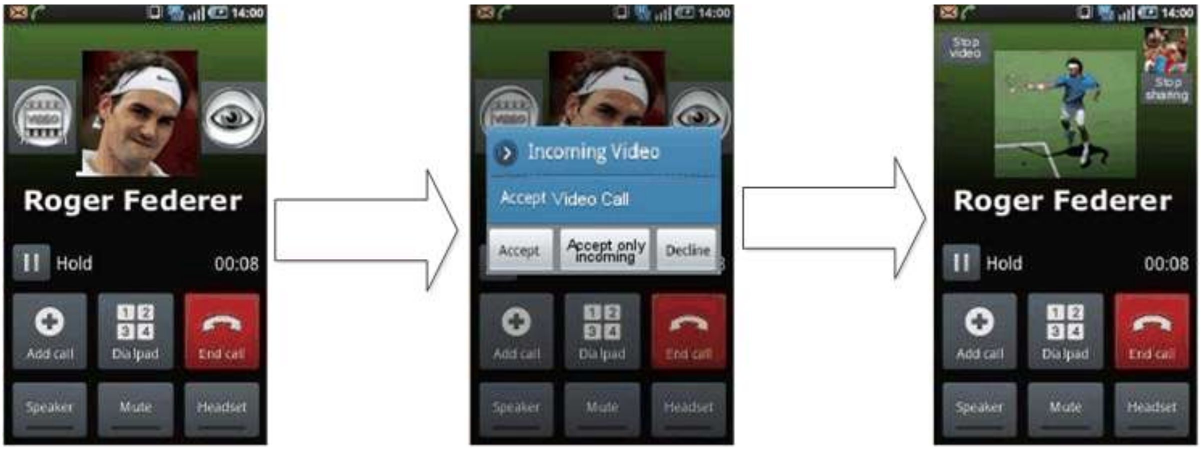


Figure 100: Video call receiver user experience – upgrade from voice call

3.9.6.1 Multidevice handling

When receiving an incoming IP Voice Call with video capabilities indicated as specified in [PRD-IR.94], it is recommended to have the recipient's devices supporting the IP Video Call display a video upgrade indication while it is alerting in order to draw the user's attention to the fact that answering at that device will allow the possibility to upgrade to a video call during the voice call.

3.10 Geolocation services

3.10.1 Feature description

Geolocation services comprise the following 2 features:

1. The "Geolocation PUSH" service that allows an RCS user to push location information (that can be the user location or the location of a suggested meeting point) to another RCS user
2. The "Geolocation PULL" service that allows an RCS user to retrieve the location information about another RCS user

It should be noted that similar services can be provided through the SPI with geolocation presence information (see section 3.7).

Their introduction in RCS 5.0 is justified by the fact that an RCS 5.0 user can have an interest to share geolocation information when SPI geolocation information cannot be used:

- Because SPI service is not offered by the Service Provider (if the 2 users belong to the same Service Provider) or one of the 2 Service Providers (if the 2 users do not belong to the same Service Provider)
- Because SPI is offered by the Service Provider (or the 2 Service Providers if the 2 users do not belong to the same Service Provider), but the 2 users do not want to share social information

3.10.1.1 Geolocation PUSH feature

Locations can be selected by the sender as follows:

- push current location
- push pre-defined location (e.g., the home address, a tool for 'favourite locations might be helpful)
- push a location that is selected on a map

The user can also choose to put additional text information about the location

The full user experience is possible only between two RCS 5.0 users. This is ensured by the RCS Service Discovery scheme.

3.10.1.2 Geolocation PULL feature

This feature is used by an RCS user, the origin RCS user, to retrieve the location information on any other RCS user – i.e. not limiting to users that share SPI with the RCS user

Behaviour at the origin RCS user side:

- When successful, the RCS user is informed with the result: geolocation coordinates (x, y).
- The user can then choose to store the information in the address book or/and show the information on a map

Behaviour at the target RCS user side

- The target user is informed that another RCS user is requesting to retrieve their geolocation
- The target user either authorizes (ALLOW) or refuses (DENY) to share their geolocation
- If the target authorizes (ALLOW) sharing their location, the location is retrieved automatically by the client/device accessing the Location Based Services infrastructure in the network.

Multi device handling for the Geolocation PULL feature:

- The primary device will be the default recipient of the authorization request. If the user replies 'ALLOW', this primary device will provide the user location information

3.10.2 Interaction with other RCS features

3.10.2.1 Geolocation PULL service

Interaction with RCS chat and voice/video call: the feature can be activated in the context of an established voice/video call (single point or multipoint) or in the context of an established RCS chat.

3.10.2.2 Geolocation PUSH service

Interaction with RCS chat and voice/video call: the feature can be activated in the context of an established voice/video call (single point or multipoint) or in the context of an established RCS chat.

3.10.3 High Level Requirements

3.10.3.1 Geolocation PUSH

3-10-1 Geolocation information should be made available to any user (notwithstanding whether at home-PLMN or roaming in visiting-PLMN)

3-10-2 Shall be deployed as point to point service between 2 RCS users having the capability

3-10-3 An RCS user shall have the possibility to communicate geolocation information to a contact that has Geolocation PUSH capability

3-10-4 The service can be accessed from the address book or share menu

3-10-5 The service can be accessed also within a call, a chat or a Group Chat

3-10-6 Geolocation information shall consist of:

- Free text entered by the RCS user (optional)
- coordinates (x,y) (mandatory)

3-10-7 Coordinates can be obtained Manually

- The user referring to a predefined stored location
- Or the user picks the location point on a map.

3-10-8 Coordinates can be obtained Automatically (via one of the localisation methods available in the device and the network)

3-10-9 The user can choose the precision of the location that they want to communicate a Street, City or Country for example

3-10-10 If authorized by the Service Provider (GEOLOCATION VALIDITY parameter in section A.1.7.2), the user has the option to enter a validity time for the geolocation information

3.10.3.2 Geolocation PULL

3-10-11 Geolocation information should be made available to any user (notwithstanding whether at home-PLMN or roaming in visiting-PLMN)

3-10-12 Shall be deployed as point to point service between 2 RCS users having the capability

3-10-13 An RCS user (Emitter side) shall have the possibility to retrieve geolocation information from a contact that has Geolocation PULL capability

3-10-14 The service can be accessed through the address book

3-10-15 The service can be accessed also within a call, a Chat or a Group Chat

3-10-16 The contact (Receiving side) shall have the possibility to accept or to deny the request

3-10-17 There is an expiration period for the authorization granted by the target subscriber. The authorization is on per application (RCS) and per requesting subscriber basis.

3-10-18 The subscriber shall be able to STOP the authorization at any time before the expiration period ends

3-10-19 In case of DENY or STOP, the user shall have the possibility to REVOKE the originator of the Geolocation PULL request. In this case, the originator is put in a Geolocation PULL black list

3-10-20 If the Receiving side accepts the demand, geolocation information provided by the Location Based Services infrastructure in the network consists of: coordinates (x,y)

3-10-21 If authorized by the Service Provider (GEOLOCATION VALIDITY parameter in section A.1.7.2), the user shall have the option to enter a validity time for the geolocation information when the target user is replying to allow PULL operation

3.10.4 Technical Realization

3.10.4.1 Geolocation PUSH service

The RCS File Transfer service (see previous chapter 3.5) is used to convey the geolocation information. See following section 3.10.4.3 for more details on the format.

3.10.4.1.1 *Emitter side*

The Geolocation PUSH service is proposed to the user if the Service Discovery Process has determined that the target RCS user has the Geolocation PUSH service available. See chapter 2.6 and chapter 2.6.4.1 for Service Discovery. An RCS user having the RCS Geolocation PUSH capability must have also the RCS File Transfer capability

If the user has chosen to provide his/her location through automatic localization:

- The RCS user's device is to use OMA SUPL (user plane) technology as the preferred mechanism for obtaining the geolocation (SET initiated primitive);
- If SUPL is not supported by a Service Provider, the RCS user' s device is free to use other locating method(s) rendering the highest possible precision in obtaining geolocation information

The geolocation application interfaces with the RCS File Transfer enabler

The SIP File Transfer uses a specific IARI that allows routing the primitive to the geolocation application in the target device B. The file transfer name has no meaning in this case.

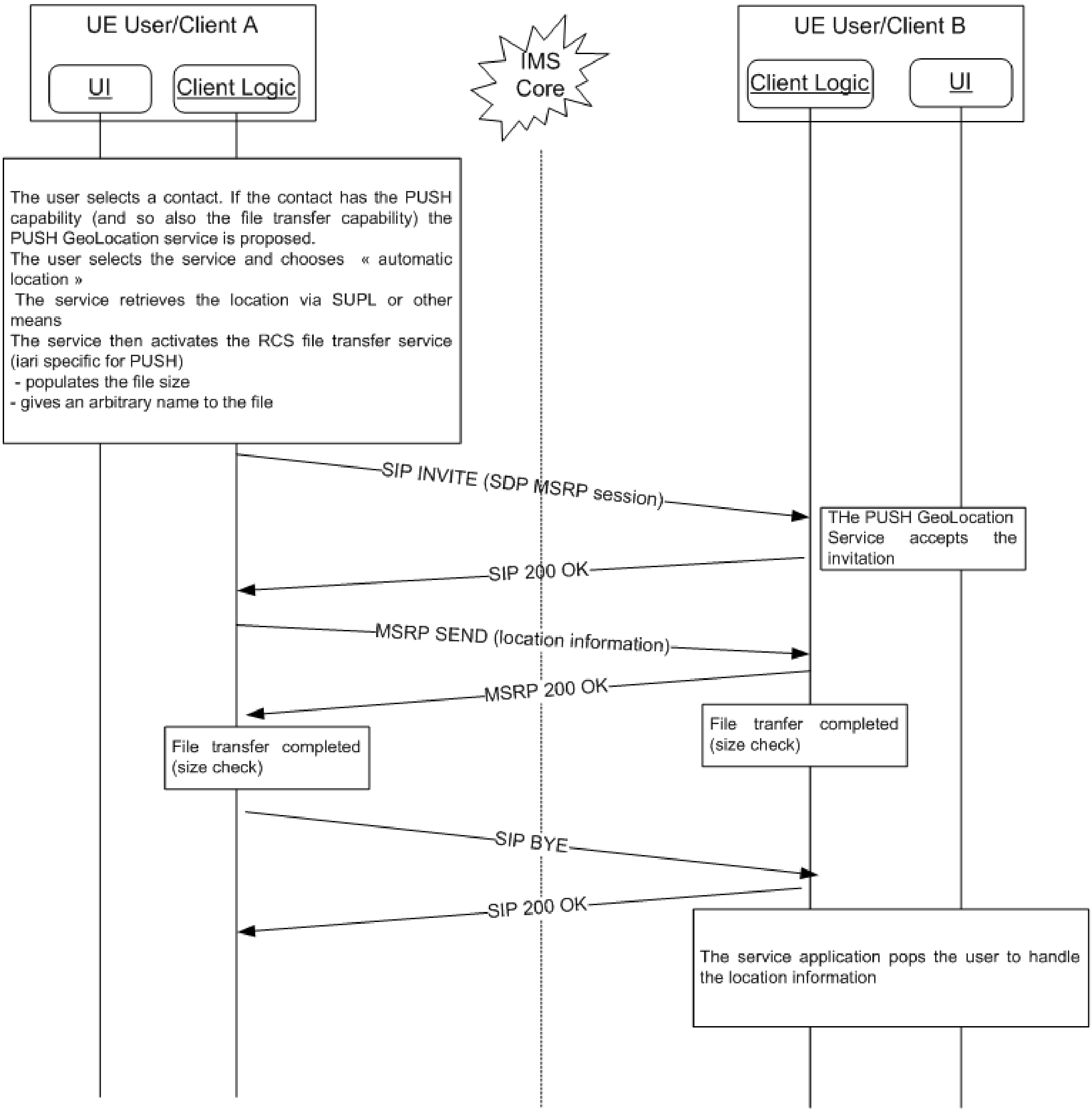
The file type is *application/rcspushlocation+xml*. See the section 3.10.4.3 for more details.

3.10.4.1.2 *Receiving side*

The RCS File Transfer request is routed to the RCS geolocation application (internal routing based on the IARI).

On the receiving side the File Transfer invitation complies with the acceptance rules of RCS File Transfer.

If the transfer is successful, the application triggers the user in a pop up menu to handle the location information.



The user selects a contact. If the contact has the PUSH capability (and so also the file transfer capability) the PUSH GeoLocation service is proposed.
The user selects the service and chooses « automatic location »
The service retrieves the location via SUPL or other means
The service then activates the RCS file transfer service (iari specific for PUSH)
- populates the file size
- gives an arbitrary name to the file

THe PUSH GeoLocation Service accepts the invitation

File tranfer completed (size check)

File transfer completed (size check)

The service application pops the user to handle the location information

Figure 101: Push of geolocation information using RCS File Transfer

3.10.4.2 Geolocation PULL service

This service is realised using the OMA NetAPI_TerminalLocation API [Location_API] and its complement GCOP (GSMA Canadian OneAPI Pilot) Privacy_Service API [PRIVACY-API].

3.10.4.2.1 *Emitter side*

The Geolocation PULL service is proposed to the user if the Service Discovery Process has determined that the target has the service available. See chapter 2.6 and chapter 2.6.4.1 for Service Discovery

The geolocation application interfaces the 2 APIs mentioned in section 3.10.4.2 to obtain authorisation and retrieve location

3.10.4.2.2 *Receiving side*

Authorization request /answer: The authorization request is received by the device through a standard user SMS:

```
The <User_x> wants to use your location. Reply ALLOW or DENY. To
cancel all location authorizations, reply STOP.
```

The target user replies in a MO-SMS (Mobile Originated SMS) message back to the OneAPI system

If user has given their authorization, the OneAPI engages its network enabler (via OMA Mobile Location Protocol, MLP) to query the location of the target mobile from the LBS infrastructure (Location Based Services, i.e. Gateway Mobile Location Centre (GMLC) and Serving Mobile Location Centre (SMLC)). This is to be a network initiated location query (either Control Plane or SUPL) to the target mobile.

3.10.4.3 Location Information format

3.10.4.3.1 *General*

The format of the information re-uses the general structure of the RCS XML Presence data. It uses a subset of RCS SPI data definition adapted to RCS Location information

The following XML schema is defined:

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema targetNamespace="urn:gsma:params:xml:ns:rcs:rcs:geolocation"
        xmlns:xs="http://www.w3.org/2001/XMLSchema"
        xmlns="urn:gsma:params:xml:ns:rcs:rcs:geolocation"
        elementFormDefault="qualified"
        attributeFormDefault="unqualified">
    <xs:element name="rcsenvelope">
        <xs:complexType>
            <xs:sequence>
                <xs:element name="rcspushlocation">
                    <xs:complexType>
                        <xs:sequence>
                            <xs:any namespace="##other" processContents="lax"
                            minOccurs="0" maxOccurs="unbounded"/>
                            <xs:element name="timestamp">
                                <xs:simpleType>
                                    <xs:restriction base="xs:dateTime"/>
                                </xs:simpleType>
                            </xs:element>
                        </xs:sequence>
                        <xs:attribute name="id" type="xs:ID" use="required"/>
                    </xs:complexType>
                </xs:element>
                <xs:any namespace="##other" processContents="lax" minOccurs="0"
                maxOccurs="unbounded"/>
            </xs:sequence>
            <xs:attribute name="entity" type="xs:anyURI" use="required"/>
        </xs:complexType>
    </xs:element>
</xs:schema>
```

Table 44: Geolocation PUSH Envelope XML schema

3.10.4.3.2 *RCSPushLocation data model*

Attribute	Specification	Comment
Person: `<rcsenvelope>` -> `<rcspushlocation>`	Table 44	Each client only publishes one <rcsenvelope> and one <rcspushlocation> element.

Descriptive Location Text <rcspushlocation> -> <place-type> -> <other>	Table 44, [RFC4480] and [Presence2.0_DDS]	The application may provide a descriptive text describing his location. See following chapter section for more information on the handling of the expiry of this information Note: Support for the enumerated values defined in [RFC4589] is thus out of scope for RCS. It is out of scope of RCS how a client will handle these enumerated values when received nevertheless.
Time Zone <rcspushlocation> -> <time-offset>	Table 44, [RFC4480] and [Presence2.0_DDS]	The geolocation application may use this element to provide information on the current time zone See following chapter section for more information on the handling of the expiry of this information
Geographical Information <rcspushlocation> -> <geopriv> -> <location-info> -> <usage-rules>	Table 44, [RFC5491] and [Presence2.0_DDS]	This element can be used to provide geographical location information. The accuracy of which can be controlled by the user. See following section for more details on its encoding and on the handling of the expiry of this information
Timestamp: <rcspushlocation> -> <timestamp>	Table 44, [RFC4479]	Timestamp when the location information was pushed

Table 45: RCSPushLocation data model attributes

3.10.4.3.3 *RCSPushLocation information*

RCS clients shall not include a “*from*” attribute in the <*place-type*> and <*time-offset*> elements. RCS clients shall ignore it when received.

RCS clients can provide (if authorized by the Service Provider) an "*until*" attribute in those elements. The user will populate the validity time of the information with a value that will not exceed a data configuration value (see section A.1.7.2).
Note: this behaviour deviates from SPI where this element is mandatory

RCS clients shall not include the optional description attribute in the <*time-offset*> element as this overlaps with the Location Type. RCS clients shall ignore it when received.

The geographical information will be provided as geographic coordinates. As specified for the “Geographical Location” building block in [Presence2.0_DDS], encoding will use the <*geopriv*>→<*location-info*> and <*geopriv*>→<*usage-rules*> elements.

The optional <*usage-rules*> element shall contain, if present, only a "*retention-expiry*" element. The RCS client shall set the "*retention-expiry*" to the same value as the “*until*” attribute mentioned above.
Note: this behaviour deviates from SPI where this element is mandatory

The <*location-info*> published by an RCS Geolocation PUSH client will contain geographical information using the GML 3.1.1 Feature Schema (see [GML3.1.1]) which is the mandatory format to be used in the <*location-info*> element. The civic location format shall not be used by RCS and location information encoded in that way will be ignored by RCS clients when received.

RCS client will within the <*location-info*> element represent an exact position by providing a GML <point> element and an inaccurate position as a <*circle*> element, both referring to the EPSG::4326 spatial reference schema as described in [RFC5491].

The coordinates of either the centre of this circle or the exact position will be represented with a single GML <*pos*> element with the actual coordinates as value.

The radius of the circle will be represented in meters, which will be indicated by setting the unit of measure attribute of the radius element to the value of EPSG::9001 as described in [RFC5491].

The text value (that is, the <*place-type*> element) shall not exceed a Service Provider configured value (see section A.1.7.2).

An RCS client shall ignore any other type of data provided in the <*location-info*> element.

The EPSG format requires that the coordinate representation is defined by the coordinate supplier. RCS client will always provide the coordinates in WGS 84 (latitude, longitude) decimal notion as described in [RFC5491], providing the latitude and longitude as “double”-encoded decimal numbers (as specified in [GML3.1.1]) representing the degrees, separated by a space starting with the latitude. Negative values represent Southern and Western hemisphere respectively.

The following gives an example of RCSPushLocation information data:

```
<?xml version=”1.0” encoding=”UTF-8”?>
<rcsenvelope xmlns=”urn:gsma:params:xml:ns:rcs:rcs:geolocation”
        xmlns:rpid=”urn:ietf:params:xml:ns:pidf:rpid”
        xmlns:gp=”urn:ietf:params:xml:ns:pidf:geopriv10”
        xmlns:gml="http://www.opengis.net/gml"xmlns:gs="http://www.opengis.net/pidflo/1.0"
        entity=”tel:+1234578901”>
        <rcspushlocation id=”a1233”>
              <rpid:place-type rpid:until=”2012-03-15T21:00:00-05:00”>
                    <rpid:other>Ft Lauderdale, FL, USA</rpid:other>
              </rpid:place-type>
              <rpid:time-offset rpid:until=”2012-03-15T21:00:00-05:00”>-300</rpid:time-offset>
              <gp:geopriv>
                    <gp:location-info>
                              <gs:Circle srsName="urn:ogc:def:crs:EPSG::4326">
                                        <gml:pos>26.1181289 -80.1283921</gml:pos>
                                        <gs:radius uom="urn:ogc:def:uom:EPSG::9001">10</gs:radius>
                              </gs:Circle>
                    </gp:location-info>
                    <gp:usage-rules>
                              <gp:retention-expiry>2012-03-15T21:00:00-05:00</gp:retention-expiry>
                    </gp:usage-rules>
              </gp:geopriv>
              <timestamp>2012-03-15T16:09:44-05:00</timestamp>
        </rcspushlocation>
</rcsenvelope>
```

Table 46: Example of location information data

3.10.4.4 Obtaining Location Information

A client using cellular access shall rely on the SUPL enabled terminal (SET) initiated collaboration that is specified in [SUPL] or other locating methods available from the device or network based solutions for obtaining its position. A-GPS shall be used if it has the appropriate receiver and sufficient coverage (that is, GPS satellites are visible). If it does not have this kind of receiver or if GPS positioning is not possible, a client using cellular access shall rely solely on network based positioning for obtaining its position information. In this case the positioning calculation mode is radio technology dependent, for example, for GSM (Global System for Mobile Communications)/W-CDMA (Wideband Code Division Multiple Access) networks the Location ID mode shall be used. The clients shall use the proxy mode defined in [SUPL] relying on the alternative client authentication mechanism for authentication. Support for network initiated SUPL collaboration, non-proxy mode or other authentication mechanisms described in [SUPL] is in RCS out of scope for both clients and networks, as it is not required to support the RCS use cases. The same is therefore also valid for the functions supporting this functionality (for example, the SUPL Initiation Function).

BA clients using non-cellular access can obtain location information through a regular GPS receiver if they have one available

3.10.5 NNI and IOT considerations

The NNI interfaces for geolocation services shall behave according to the procedures described in section 2.12 and the documents it refers to.

3.10.6 Implementation guidelines and examples

3.10.6.1 Geolocation PUSH

The Geolocation PUSH feature can be selected by an RCS user whenever it makes sense to share her/his location information with other RCS users, i.e.:

- From the general “share menu” or
- Inside a call / video call
- Or inside a Chat or a Group Chat

At the receiver side, a “pop up” menu advertises the user that an RCS user is communicating some location information

3.10.6.2 Geolocation PULL

The Geolocation PULL feature can be selected by an RCS user in same circumstance as the Geolocation PUSH feature, i.e.:

- From the general “share menu” or
- Inside a call / video call
- Or inside a chat or a Group Chat

At the receiver side, no specific behaviour is required for the client implementation, only standard SMS is used:

- The user is triggered by a standard SMS requesting in clear text their authorization to share their localization with the user identified by the caller number.
- The user gives their authorization by answering their decision in a clear SMS text to a dedicated E.164 number that was communicated in the SMS that was received

Annex A: Managed objects and configuration parameters

This Annex provides the full details on the RCS data model including an overview of all configuration parameters. These parameters will be set using the mechanisms described in section 2.3.

The aim of this section is to provide a complete configuration data model for reference by both Service Providers and OEMs.

A.1. Management objects parameters overview

This section provides an overview of the configuration parameters used for RCS. These parameters can either come from an existing management object (like for instance the OMA defined objects for Presence, Messaging and so on) or may be RCS specific. In the latter case they will be formally defined in section A.2.

A.1.1. Presence related configuration

A.1.1.1. *OMA Presence Provisioning parameters*

OMA Presence Client provisioning parameters are defined in [PRESENCE2MO]. Table 47 lists the OMA Presence parameters applicable to RCS.

Configuration parameter	Description	RCS usage
CLIENT-OBJ-DATA-LIMIT	maximum size of the MIME object in SIP PUBLISH request	Optional parameter It is mandatory and becomes relevant only if DEFAULT DISCOVERY MECHANISM is set to PRESENCE or PRESENCE PROFILE is set to 1
CONTENT-SERVER-URI	HTTP URI of the content server to be used for content indirection	Not Used
SOURCE-THROTTLE-PUBLISH	minimum time interval (in seconds) between two consecutive publications	Optional parameter It is mandatory and becomes relevant only if DEFAULT DISCOVERY MECHANISM is set to PRESENCE or PRESENCE PROFILE is set to 1

MAX-NUMBER-OF-SUBSCRIPTIONS-IN-PRESENCE-LIST	Limits the number of back-end subscriptions allowed for a presence list. This parameter applies to the “rcs” list (as described in section 3.7.4.5)	Optional parameter It is mandatory and becomes relevant only if PRESENCE PROFILE is set to 1
SERVICE-URI-TEMPLATE	syntax of the service URI	Optional parameter It is mandatory and becomes relevant only if PRESENCE PROFILE is set to 1, and has then a value of “<xui>;pres-list=<id>” according to section 5.5.1 in [PRESENCEIG]
RLS-URI	SIP URI of the RLS to be used by the Watcher when subscribing to a Request-contained Presence List	Optional parameter

Table 47: RCS usage of OMA presence configuration parameters

A.1.1.2. RCS Specific Provisioning parameters

The RCS 5.0 specification includes the following additional presence related configuration parameters:

Configuration parameter	Description	RCS usage
PRESENCE PROFILE	This parameter allows enabling or disabling the usage of the social information via presence. If set to 0, the usage of the social information via presence feature is disabled. If set to 1, the social information via presence feature is enabled. This parameter will consequently influence the inclusion of the tag associated with social information via presence in OPTIONS exchanges.	Mandatory parameter
AVAILABILITY AUTHORISATION	This parameter controls the use of Availability status feature by the device (“Allowed” or “Not Allowed” as described in section 3.7)	Optional parameter It is mandatory and becomes relevant only if PRESENCE PROFILE is set to 1
FAVOURITE LINK CONTROL	This parameter controls how the user can set the favourite link information: automatic mode, full manual mode or a combination of those for the Favourite link where in the first case the user is can only set the favourite link from a list of predefined URLs	Optional parameter It is mandatory and becomes relevant only if PRESENCE PROFILE is set to 1

FAVOURITE LINK URLS	A list of pre-defined Favourite link URLs	Optional parameter It is mandatory and becomes relevant only if FAVOURITE LINK CONTROL is set to “Auto” or “Auto+Man”
FAVOURITE LINK LABEL MAX LENGTH	This parameter allows the control of the maximum length of the label assigned to a favourite link (with a maximum value of 200 Characters)	Optional parameter It is mandatory and becomes relevant only if PRESENCE PROFILE is set to 1
ICON MAX SIZE	This parameter allows the control of the maximum size of the picture provided in the status-icon (with a maximum value of 200kB).	Optional parameter It is mandatory and becomes relevant only if PRESENCE PROFILE is set to 1
NOTE MAX SIZE	Maximum length of presence tagline at presentity side. The reason to have at presentity side a configurable attribute on the RCS client to control the maximum size of the Note is to make the end user aware of what the limit is (when typing the content of the Note/free text). Avoiding enforcement of this limit at network / watcher side would lead to truncating the note. This value should have a lower value than the one defined at watcher side in the OMA Presence Implementation guideline [PRESENCEIG].	Optional parameter It is mandatory and becomes relevant only if PRESENCE PROFILE is set to 1
LOCATION TEXT MAX LENGTH	This parameter allows the control of the maximum length of the text describing the current location (with a maximum value of 200 characters-	Optional parameter It is mandatory and becomes relevant only if PRESENCE PROFILE is set to 1
LOCATION VALIDITY	This parameter allows controlling the maximum time during which a location information should be considered valid	Optional parameter It is mandatory and becomes relevant only if PRESENCE PROFILE is set to 1
MAX LOCATION UPDATE	This parameter controls the minimum duration between consecutive location updates	Optional parameter It is mandatory and becomes relevant only if PRESENCE PROFILE is set to 1

PUBLISH EXPIRY TIME	This parameter allows setting the default expiry time for a SIP PUBLISH as described in section 2.6.1.2.2	Optional parameter It is mandatory and becomes relevant only if DEFAULT DISCOVERY MECHANISM is set to PRESENCE is set to 1
VIP CONTACTS POLL MAX FREQUENCY	This parameter controls the maximum number of poll operations on the non-VIP contacts list during a certain period of time	Optional parameter It is mandatory and becomes relevant only if PRESENCE PROFILE is set to 1

Table 48: RCS additional presence related configuration parameters

A.1.2. XDM related configuration

A.1.2.1. OMA XDM Provisioning parameters

OMA XDM Client provisioning parameters are defined in [XDMMO]. The following table lists the OMA XDM parameters applicable to RCS. The mandatory parameters become optional if no functionality depending on XDM is deployed (that is no Presence based capability check as described in section 2.6.1.2 and no Social Presence as described in section 3.7) or PS Voice or Video calls as described in section 3.8 and 3.9)), or if the device is VoLTE or VoHSPA enabled. VoLTE or VoHSPA devices would use the default XCAP Root URI value as defined in [PRD-IR.92] or [PRD-IR.58] respectively, but the default value could still be overwritten with the OMA XDM parameter.

Configuration parameter	Description	RCS usage
XCAP Root URI	The root of all XCAP (XML configuration access protocol) resources (which points to the Aggregation Proxy address). This is used when accessing via XCAP.	Mandatory parameter
XCAP Authentication user name	HTTP digest “username”, for accessing an XDMS (XDM server) using the XCAP protocol	Optional parameter It is mandatory and becomes relevant only if XCAP Authentication Type is set to “Digest”
XCAP Authentication Secret	HTTP digest password	Optional parameter It is mandatory and becomes relevant only if XCAP Authentication Type is set to “Digest”

XCAP Authentication type	Authentication method for XDMS over XCAP. Possible values: Early IMS (IP Multimedia Subsystem) or Digest Note: The Early IMS value is a specific RCS value that is not defined in OMA. The support is provided according to of section 6.3 of [3GPP TR 33.978] and sections 6.3 and 6.4 in [XDM1.1_Core]. That means that in the HTTP GET request to the Aggregation Proxy the client shall supply the "*X-3GPP-Intended-Identity*" header to indicate the user identity.	Mandatory parameter

Table 49: RCS usage of OMA XDM configuration parameters

A.1.2.2. RCS Specific Provisioning parameters

The RCS 5.0 specification includes the following additional XDM related configuration parameters:

Configuration parameter	Description	RCS usage
REVOKE TIMER	This parameter allows setting the duration during which a contact should remain in the “rcs_revokedcontacts” list (as described in section 3.7.4.5)	Optional parameter It is mandatory and becomes relevant only if PRESENCE PROFILE is set to 1

Table 50: RCS additional XDM related configuration parameters

A.1.3. Chat related configuration

A.1.3.1. OMA SIMPLE IM Provisioning parameters

OMA SIMPLE IM client provisioning parameters are defined in [RCS5-SIMPLEIM-ENDORS]. Following table only lists which of those SIMPLE IM application parameters are applicable.

Configuration parameter	Description	RCS usage
PRES-SRV-CAP	flag used for the Messaging Server to indicate the Presence publish capability of a Presence information element of the Messaging Server on behalf of the SIMPLE IM Client	Not Used. Always set to the OMA value indicating that the capability is not supported in the network
MAX_AD-HOC_GROUP_SIZE	Maximum number of Participants allowed for an Ad-hoc Group Chat session	Optional parameter It is mandatory and becomes relevant only if CONF-FCTY-URI is set to a value different from “sip:foo@bar”

CONF-FCTY-URI	SIP URI used for setting up an Ad-hoc Group or 1-1 Chat session. Presence of a dummy URI ("sip:foo@bar") in the CONF-FCTY-URI parameter implies that the RCS Group Chat service is to be disabled in the client	Optional parameter It is mandatory and becomes relevant only if CHAT AUTH is set to 1
EXPLODER-URI	SIP URI used for sending SIP MESSAGE e.g. Sending SIP MESSAGE to an Ad hoc Group	Not Used, populated with "sip:foo@bar"
CONV-HIST-FUNC-URI	SIP URI for the SIMPLE IM user's conversation history storage	Not Used, populated with "sip:foo@bar"
DEFERRED-MSG-FUNC-URI / MSG-STORE-URI	SIP URI used for the SIMPLE IM User's message-store account for deferred messaging	Not Used, populated with "sip:foo@bar"
DELETE-URI	SIP URI used when message(s) are to be deleted	Not Used, populated with "sip:foo@bar"

Table 51: RCS usage of OMA SIMPLE IM configuration parameters

A.1.3.2. OMA CPM Provisioning parameters

OMA CPM does not include any formal provisioning parameter definition. Therefore the parameters for CPM are defined as RCS specific in section A.1.3.3. Furthermore following SIMPLE IM Parameters (see section A.1.3.1) will be applicable also for CPM services:

- MAX_AD-HOC_GROUP_SIZE
- CONF-FCTY-URI
- EXPLODER-URI
- DEFERRED-MSG-FUNC-URI / MSG-STORE-URI
  Note: in case standalone messaging is enabled (see section A.1.3.3), this parameter can be set to a value different from sip:foo@bar in which case 1-to-Many standalone messaging can be used.

A.1.3.3. RCS Specific Provisioning parameters

The RCS 5.0 specification includes the following additional Chat related configuration parameters:

Configuration parameter	Description	RCS usage
CHAT AUTH	This parameter Enables/Disables the Chat service. If set to **0** the chat service is disabled. When set to **1** it is enabled.	Mandatory Parameter
STANDALONE MGS AUTH	This parameter Enables/Disables the Standalone Messaging Service. If set to **0** the service is disabled. When set to **1** it is enabled.	Mandatory Parameter

IM CAP ALWAYS ON	This parameter configures the client to support store and forward when presenting the Chat capability status for all the contacts. If set to **1**, the Chat capability for all RCS contacts will be always reported as available. Otherwise (**0**), the capability will be reported based on the algorithm presented in section 2.7.1.1. For example, this can be used by Service Providers that are implementing the store and forward functionality for chat on both the terminating side for its own subscribers, and the originating side for communication with subscribers belonging to other Service Providers do not have the store and forward feature.	Optional parameter (It is mandatory if CHAT AUTH is set to 1 and CONF-FCTY-URI or CONF-FCTY-CLOSED-URI is set)
IM WARN SF	If IM CAP ALWAYS ON is set to enabled (use of store and forward), a new parameter is used called IM WARN SF for UI purposes only. If the IM WARN SF parameter is set to (**1**) then, when chatting with contacts which are offline (Store and Forward), the UI must warn the user of the circumstances (by showing a message on the screen for instance). Otherwise (**0**), there will not be any difference at UX level between chatting with an online or offline (Store and Forward) user	Optional parameter (It is mandatory if CHAT AUTH is set to 1 and CONF-FCTY-URI or CONF-FCTY-CLOSED-URI is set and IM CAP ALWAYS ON is set to 1)
IM CAP NON RCS	This parameter configures the client to support chat with non-RCS contacts. If set to **1**, the Chat capability for all contacts will be always reported as available whether they are RCS enabled or not. Otherwise (**0**), the capability will be reported based on the setting for IM CAP ALWAYS ON and algorithm presented in section 2.7.1.1. For example, this can be used by Service Providers that are implementing the interworking of chat to SMS/MMS	Optional parameter It is mandatory if CHAT AUTH and CONF-FCTY-URI is set is set and IM CAP ALWAYS ON is set to 1
IM WARN IW	If IM CAP NON RCS is set to enabled (use of interworking), a new parameter is used called IM WARN IW for UI purpose only. If IM WARN IW parameter is set to (**1**) then, when chatting with non-RCS contacts (Interworking), the UI must warn the user of the circumstances. Otherwise (**0**), there will not be any difference at UX level between chatting with an online RCS or a non-RCS (SMS/MMS) user.	Optional parameter It is mandatory if CHAT AUTH and CONF-FCTY-URI is set is set to 1 and IM CAP NON RCS is set to 1
IM SMS FALLBACK AUTH	This parameter controls whether the client automatically proposes to fall back to SMS if there is an error in transmitting a chat invite or message. If set to **0** this fallback is disabled. When set to **1** the user is proposed to send as SMS instead if there is an error.	Optional parameter (It is mandatory if CHAT AUTH is set to 1)
IM SESSION AUTO ACCEPT	This parameter controls whether the client automatically accepts incoming session invitations (**1**) or whether acceptance depends on a user action (**0**) as defined through the IM SESSION START parameter. Automatic accept should only be used in a single device environment or in case session forking on the AS is used.	Optional parameter (It is mandatory if CHAT AUTH is set to 1)

IM SESSION START	This parameter defines the point in a chat when the receiver sends the 200 OK back to the sender confirming that the MSRP session can be established: **0** (RCS 5.0 default): The 200 OK is sent when the receiver consumes the notification by opening the chat window. **1** (RCS Release 2-4 default): The 200 OK is sent when the receiver starts to type a message to be sent back in the chat window. **2**: The 200 OK is sent when the receiver presses the button to send a message (that is the message will be buffered in the client until the MSRP session is established). Note: as described in section 3.3.4, the parameter only affects the behaviour for a 1-to-1 session if no session between the parties has been established yet.	Optional parameter (It is mandatory if CHAT AUTH is set to 1)
IM SESSION AUTO ACCEPT GROUP CHAT	This parameter controls whether the client automatically accepts incoming Group Chat session invitations (**1**) or whether acceptance depends on a user action (**0**) as defined through the IM SESSION START parameter. Automatic accept should only be used in a single device environment or if session forking on the AS is used.	Optional parameter (It is mandatory if CHAT AUTH is set to 1)
FIRST MSG IN INVITE	This parameter controls whether an RCS client may include a CPIM body containing an initial message in the SIP INVITE request for setting up a session. When set to **0** such a message may not be included and the client should wait for the MSRP session to be established to send the message. When set to **1** the initial message in the chat shall be included in a CPIM body in the INVITE request. Note: a client shall be able to handle CPIM bodies in incoming SIP INVITE requests whatever value this parameter is set to.	Optional parameter (It is mandatory if CHAT AUTH is set to 1)
IM SESSION TIMER	This parameter controls the time during which a Chat session is allowed to be idle before it's closed. When set to **0**, there shall be no timeout. The recommended value is 3 (three) minutes.	Optional parameter (It is mandatory if CHAT AUTH is set to 1)
MAX CONCURRENT SESSIONS	This parameter controls the number of sessions that are allowed to be handled by a device. A device may not initiate or accept a new session when the current number of active sessions is equal to this maximum number. A client will therefore have to close an existing session before initiating or accepting a new one. When set to 0 this limit does not apply Note: this device parameter applies only to the device. If a limit of active sessions across multiple devices is required for a user, then a parameter setting in the IMS network (HSS) for that user is required to be used.	Optional parameter (It is mandatory if CHAT AUTH is set to 1)
MULTIMEDIA IN CHAT	This parameter controls whether or not non-text (e.g. including images) messages are allowed within the chat session. When set to **0** multimedia content may not be sent over the MSRP session associated with the chat session. The client shall also indicate this in the SDP negotiation at session set up. When set to **1**, such content may be sent and received over this MSRP channel. Note: When set to 0, non-text content can then be sent in a separate File Transfer session	Optional parameter (It is mandatory if CHAT AUTH is set to 1)

MAX SIZE 1-to-1 IM	This parameter controls the maximum size of the content sent within a 1-to-1 chat session	Optional parameter (It is mandatory if CHAT AUTH is set to 1)
MAX SIZE GROUP IM	This parameter controls the maximum size of the content sent within an ad-hoc Group Chat session	Optional parameter (It is mandatory if CHAT AUTH is set to 1)
MAX SIZE STANDALONE	This parameter controls the maximum size of a message sent as a CPM Standalone message	Optional parameter (It is mandatory if STANDALONE MESSAGING TECHNOLOGY is set to 1)
MESSAGE STORE URL	The URL used to access the Message Store The parameter is optional and if not configured, means that the Service Provider is not deploying a Message Store server.	Optional parameter
MESSAGE STORE USER / PASSWORD	The credentials to access the Network-based Common Message Store server. It is an optional parameter even if MESSAGE STORE URL is configured. If it is not provided and MESSAGE STORE URL is configured, the credentials for SIP have to be used.	Optional parameter
MESSAGE STORE AUTH	This parameter controls the authentication mechanism used to access the Network-based Common Message Store. **0**: Plain User Name password **1**: SASL based authentication	Optional parameter, It is Mandatory if a MESSAGE STORE URL is provided
CHAT MESSAGING TECHNOLOGY	This parameter allows selecting what technology is used for the chat service described in sections 3.3 and 3.4 If this parameter is set **0**, SIMPLE IM as specified in [RCS5-SIMPLEIM-ENDORS] will be used. This is the default value if the parameter is not provided. If this parameter is set **1**, CPM as specified in [RCS5-CPM-CONVFUNC-ENDORS].	Optional Parameter (It is mandatory if CHAT AUTH is set to 1)

Table 52: RCS additional Chat related configuration parameters

A.1.4. File Transfer related configuration

As there are no OMA defined parameters for File Transfer, the RCS 5.0 specification includes only RCS specific parameters. There are described in the following table:

Configuration parameter	Description	RCS usage
PROVIDE FT	This parameter allows to enable (1) or disable (0) File Transfer	Mandatory Parameter
FT MAX SIZE	This is a file transfer size limit in Kilobyte (KB). If a file is bigger than FT MAX SIZE, the transfer will be cancelled automatically. Please note that if it is set to **0**, this limit will not apply.	Optional parameter, It is Mandatory if a PROVIDE FT is set to 1

FT WARN SIZE	This is a file transfer size limit in KB to warn the user that a file transfer may end up in significant charges. Please note that if it is set to **0**, the user will not be warned.	Optional parameter, It is Mandatory if a PROVIDE FT is set to 1

Table 53: RCS additional File Transfer related configuration parameters

A.1.5. Content Sharing related configuration

As there are no OMA defined parameters for content sharing, the RCS 5.0 specification includes only RCS specific parameters. There are described in the following table:

Configuration parameter	Description	RCS usage
PROVIDE VS	This parameter allows to enable (1) or disable (0) Video Share	Mandatory Parameter
PROVIDE IS	This parameter allows to enable (1) or disable (0) Image Share	Mandatory Parameter
ALLOW VS SAVE	This parameter allows a Service Provider to configure whether a Video Share session initiated by the RCS client can be saved or not. When set to (-1) the inclusion of the attribute defined in section 3.6.4.1.3 is up to user preference, when set to (0) the attribute will never be included, which is also the default handling if not provided, when set to (1) the attribute will always be included.	Optional Parameter
VS MAX DURATION	This parameter enables the Service Provider of the inviting user's RCS client to control the maximum duration time of a Video Share session that the inviting user's RCS client is authorized to handle.	Optional parameter, It is Mandatory if a PROVIDE VS is set to 1
IS MAX SIZE	Maximum authorized size of the content that can be sent within an Image Share session. This parameter enables the Service Provider of the inviting user's RCS client to control the maximum size of the content that the inviting user's RCS client is authorized to send in an Image Share session	Optional parameter, It is Mandatory if a PROVIDE IS is set to 1

Table 54: RCS additional content sharing related configuration parameters

A.1.6. IMS Core / SIP related configuration

A.1.6.1. VoLTE/VoHSPA Enabled device configuration

In a device enabled for VoLTE/VoHSPA (see section 2.2), the default IMS settings as defined in [PRD-IR.92] or [PRD-IR.58] are expected to be used, so the IMS Core/SIP related configuration would not be required.

For example, the own SIP or tel URI will not be configured through the management object referred to in section A.1.6.2, but rather be received in the 200 OK response to the SIP REGISTER request and the SIP Proxy is provided in Protocol Configuration Options (PCO) information received during Packet Data Protocol (PDP) context activation.

A.1.6.2. RCS endorsement of 3GPP IMS Management Object (MO)

Basic IMS/SIP client parameters are defined in 3GPP TS "IMS 3GPP IMS Management Object (MO)" [3GPP TS 24.167]. They do not directly depend on RCS, but correct settings of these parameters are essential for RCS operation. They are populated by the Service Provider according to the deployment conditions of the IMS core network providing access to RCS services.

Also, it should be noted that:

- Both a SIP and a tel URI may be configured for a user with following clarifications:
  - The configured values should not be used in the non-REGISTER transactions; instead the client uses one of the SIP or tel URIs provided in the P-Associated-URI header field returned in the 200 OK to the SIP REGISTER request as described in [3GPP TS 24.229]
  - The user's own tel URI and/or SIP URI identities are configured through the Public_User_Identity parameters defined in [3GPP TS 24.167][29].
  - The public identity used for IMS registration is built according to the procedure defined in [3GPP TS 24.229].
  - When the device has either ISIM or USIM present and the RCS client has access to the ISIM or USIM, it does not rely on the SIP URI and tel URI configuration parameters.
  - If the device has neither ISIM nor USIM present or is not able to access to it, a SIP URI must be configured. This URI is used for REGISTER transactions.
  - Configuration of the tel URI is optional
- The SIP proxy is configured through the parameters hosted by the LBO_P-CSCF_Address sub-tree defined in [3GPP TS 24.167]. When the P-CSCF address has an "FQDN" type, the SIP transport protocol can be selected by the RCS client thanks to DNS SRV requests. When the P-CSCF address has an "IP Address" type, the SIP transport protocol should be selected based on Service Provider customized settings.

A.1.6.3. RCS Specific Provisioning parameters

The RCS 5.0 specification includes the following additional IMS Core/SIP related configuration parameters:

Configuration parameter	Description	RCS usage
IMS Mode Authentication Type	Specifies the type of authentication support for SIP. Note: In "IETF" Digest authentication is assumed. Accepted values are: • Early IMS • IMS AKA • SIP DIGEST (without TLS)	Mandatory Parameter, NOTE: a VoLTE enabled device always uses IMS AKA when in cellular PS access and can ignore this parameter
Realm	Realm to use for authentication (Digest mode only)	Optional parameter It is Mandatory if a IMS Mode Authentication Type is set to Digest

[29] The private identity (*Private_User_Identity*), public identity (*Public_User_Identity_List/<X>/Public_User_Identity*) and domain (*Home_network_domain_name*) objects mentioned in [3GPP TS 24.167] are defined as read-only and these parameters should be obtained by the UE using the procedures described [3GPP TS 24.229]. This specification makes and exception to that definition and considers them writable during the autoconfiguration process (OMA-DM or the alternative HTTP mechanism).

Realm User Name	Realm username to use for authentication (Digest mode only)	Optional parameter It is Mandatory if a IMS Mode Authentication Type is set to Digest
Realm User Password	Realm user password to use for authentication (Digest mode only)	Optional parameter It is Mandatory if a IMS Mode Authentication Type is set to Digest
tel or SIP URI – international	Specifies whether telephone numbers in international format shall in outgoing SIP requests be sent as tel URIs [RFC3966]or as SIP URIs with “user”-parameter set to “phone” as defined in [RFC3261] See Section 2.3.3	Mandatory Parameter
tel or SIP URI - for non- international format	Specifies whether telephone numbers in non-international format shall in outgoing SIP requests be sent as tel URIs [RFC3966] or as SIP URIs with “user”-parameter set to “phone” as defined in [RFC3261] See Section 2.5	Mandatory Parameter
Register Q-value	Q-value in Contact parameter in SIP Register Required in a multi-terminal deployment to control forking of incoming SIP requests Recommended value: 0.5	Mandatory Parameter

Table 55: RCS additional IMS Core/SIP related configuration parameters

A.1.7. Geolocation related configuration

A.1.7.1. OMA SUPL Provisioning parameters

RCS uses SUPL [SUPL] for providing localization social presence information.

SUPL Client provisioning parameters are defined in OMA Management Object for SUPL [SUPLMO]. RCS may use this object for provision of the required parameters for accessing the H-SLP (Home SUPL Location Platform).

Following table lists the OMA SUPL parameters applicable to RCS. The mandatory parameters become optional if no functionality depending on SUPL is deployed (that is Social Presence as described in section 3.7 or the location functionality described in section 3.10).

Configuration parameter	Description	RCS usage
Addr	The address of the H-SLP	Mandatory parameter
AddrType	The type of the address provided in Addr.	Optional parameter

Table 56: RCS usage of OMA SUPL configuration parameters

A.1.7.2. RCS Specific Provisioning parameters

The RCS 5.0 specification includes the following additional geolocation related configuration parameters

Configuration parameter	Description	RCS usage
PROVIDE GEOLOC PUSH	This parameter allows to enable (1) or disable (0) the Geolocation PUSH service	Mandatory Parameter
PROVIDE GEOLOC PULL	This parameter allows to enable (1) or disable (0) the Geolocation PULL service	Mandatory Parameter
GEOLOCATION TEXT MAX LENGTH	This parameter allows the control of the maximum length of the text describing the current location (with a maximum value of 200 characters	Optional parameter It is mandatory and becomes relevant only if the Geolocation PULL or Geolocation PUSH service is available for the device
GEOLOCATION VALIDITY	This parameter allows controlling the maximum time during which a location information should be considered valid	Optional parameter. If present, it indicates A maximum value the user is authorized to enter

Table 57: RCS additional geolocation related configuration parameters

A.1.8. Configuration related with Address book Back-up/Restore

The RCS 5.0 specification does not include any additional address book back-up/restore related configuration parameters.

A.1.9. Configuration related to secondary devices

A.1.9.1. General

With the Introduction of the broadband secondary device in RCS, there are features in a broadband RCS device that require configuration:

- Control of service delivery:
  Control of service delivery: in a broadband RCS device, as specified in section 2.11.2, this user control facility is itself controlled by the Service Provider that may define the set of services subject to this function
- SMS over IP:
  As specified in [PRD-IR.92], when sending a short message from the RCS Broadband Access (BA) client, the address of the Service Provider's SMS-C needs to be supplied in the SIP request containing the short message, see [3GPP TS 24.341] chapter 5.3.1.
- MMS:
  Before sending a multimedia message from the RCS client, and when retrieving the multimedia message, the addresses of the Service Provider's HTTP proxy and MMS-C (Multimedia Messaging Service Centre) needs to be configured.

A.1.9.2. Specific RCS Configuration parameters for Control of service delivery

Network authorization for user controlling delivery of

- Voice Calls
- Video Calls

- Chat
- Sending SMS
- File Transfer
- Video Sharing
- Image Sharing
- Geolocation PUSH
  Note: Geolocation PULL is provided on the primary device only and as such not subject to control of service delivery

A.1.9.3. RCS endorsement of OMA MMS parameters

MMS client provisioning parameters are defined in OMA Management Object for MMS [MMSMO]. RCS BA clients may use this object for provision of the required parameters for accessing the MMS service.

Specifically, the URL to the MMS-C (MMS Proxy-Relay server) shall be provided.

A.1.9.4. RCS endorsement of OMA Connectivity Management Objects parameters

SMS-C Address: a public service identifier (PSI) in form of a tel URI or SIP URI

The NAP (network access point) object defined in [CONNMO] may be used for this purpose.

Specifically the address type field and the address field shall be provided (with SMS-C address information).

HTTP proxy Client provisioning parameters are defined by the “proxy” object in [CONNMO] and further specified in [CONNMOHTTP]. RCS Broadband access clients may use this object for provision of the required parameters for accessing the HTTP proxy.

Specifically, the proxy type, proxy address and the authorization type and credentials (username & password) shall be provided.

A.1.10. Capability discovery related configuration

The RCS 5.0 specification includes the following RCS Specific configuration parameters related to the capability discovery:

Configuration parameter	Description	RCS usage
POLLING PERIOD	This is the frequency in seconds at which to run a periodic capabilities update for all the contacts in the phone’s address book whose capabilities are not available (such as non-RCS users) or are expired (see CAPABILITY INFO EXPIRY parameter). Please note that if set to **0**, this periodic update is not/no longer performed.	Mandatory parameter
POLLING RATE	This parameter allows controlling the maximum rate at which SIP OPTIONS and Presence Fetch operations are performed for all contacts combined. It therefore provides some control over the network load caused when performing a capability discovery for the whole address book.	Optional parameter (It is mandatory if POLLING PERIOD is set to a value greater than 0)

CAPABILITY INFO EXPIRY	When using the capability discovery mechanism and with the aim of minimizing the traffic, an expiry time is set in the capability information fetched using SIP OPTIONS or Presence. When performing a whole address book capability discovery (i.e. polling), a capability query takes place only if the time since the last capability update took place is greater than this expiration parameter	Optional parameter (It is mandatory if POLLING PERIOD is set to a value greater than 0)
CAPABILITY DISCOVERY MECHANISM	This parameter allows selecting the default capability and new user discovery mechanism. If not provided or set to OPTIONS, the default mechanism employed for capability discovery and new users will be OPTIONS. Otherwise (PRESENCE), it will relay of presence-based discovery by default.	Mandatory parameter
CAPABILITY DISCOVERY VIA COMMON STACK	This parameter allows selecting whether the device will fall back to OPTIONS if a discovery using presence fails with an error indicating that the other user does not support a presence based capability check. When set to **1**, this fallback is done. When set to **0** it is not done.	Optional parameter It is mandatory if CAPABILITY DISCOVERY MECHANISM is set to PRESENCE)

Table 58: RCS additional capability discovery related configuration parameters

A.1.11. APN configuration

The RCS 5.0 specification includes the following RCS Specific configuration parameters targeting APN configuration (see sections 2.9.1.4 and 2.13):

Configuration parameter	Description	RCS usage
RCS-E ONLY APN	This is the reference/identifier of the APN configuration which should be used to provide PS connectivity ONLY to RCS as described in section 2.9.1.4.	Mandatory parameter
ENABLE RCS-E SWITCH	As described in section 2.9.1.4 the user shall be able configure to allow or disallow RCS and/or internet traffic in the device settings. If this parameter is set to 1, the setting is shown permanently. 0, the setting is only shown during roaming. -1: RCS Switch is never shown.	Mandatory parameter

Table 59: RCS roaming configuration parameters

A.1.12. End User Confirmation parameters

The RCS 5.0 specification includes the following RCS Specific configuration parameters targeting the End User Confirmation configuration (see section 2.10):

Configuration parameter	Description	RCS usage
END USER CONF REQ ID	This is the URI that is used to identify the sender of the End User Confirmation Requests	Optional Parameter

Table 60: RCS end user confirmation configuration parameters

A.1.13. Multidevice configuration parameters

The RCS 5.0 specification includes the following RCS Specific configuration parameters targeting the multidevice configuration when using the sip.instance approach described in section 2.4.2 and 2.11:

Configuration parameter	Description	RCS usage
uuid_Value	This is the UUID value used for sip.instance, provided deviceID is set to 1	Optional Parameter

Table 61: RCS multidevice configuration parameters

A.1.14. Service Provider specific extensions

A Service Provider may provide Service Provider specific extensions to the configuration parameters. This can be done both at the individual service level and add the global level (e.g. for the configuration of Service Provider specific services). All parameters are optional and if provided may be ignored by clients that are not Service Provider specific.

A.2. RCS Management trees additions

Please note that all the configuration sub trees described in this section have as type property for the root nodes (that is the /<X> root nodes) urn:gsma:mo:rcs:5.0. All RCS specific MOs shall be placed in this RCS subtree.

A.2.1. Services sub tree additions

The RCS 5.0 specification includes the following additions as a new services sub tree, the Services MO sub tree. Please note this sub tree is not included in any other specifications. So no other nodes from those specifications need to be added:

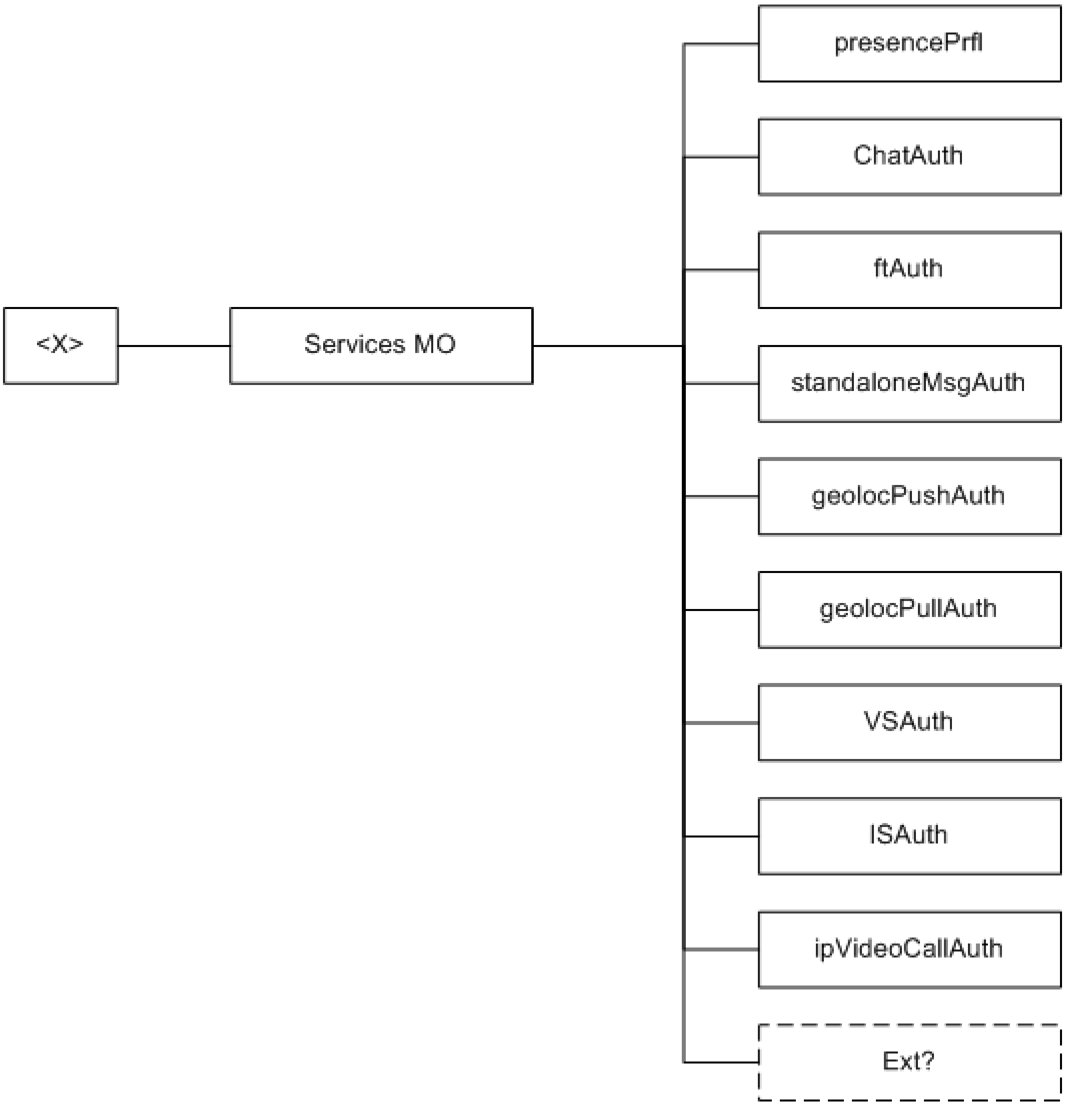


Figure 102: RCS 5.0 additions, Services sub tree

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

```
<characteristic type=”SERVICES”>
        <parm name=”presencePrfl” value=”X”/>
        <parm name=”ChatAuth” value=”X”/>
        <parm name=”ftAuth” value=”X”/>
        <parm name=”standaloneMsgAuth” value=”X”/>
        <parm name=”geolocPullAuth” value=”X”/>
        <parm name=”geolocPushAuth” value=”X”/>
        <parm name=”vsAuth” value=”X”/>
        <parm name=”isAuth” value=”X”/>
        <parm name=”ipVideoCallAuth” value=”X”/>
        <characteristic type=”Ext”/>
</characteristic>
```

Table 62 : Services MO sub tree associated HTTP configuration XML structure

Node: /<x>/ServicesMO

Under this interior node the RCS parameters related to the enabling/disabling of services are placed

Status	Occurrence	Format	Min. Access Types
Required	One	node	Get

Table 63: Services MO sub tree addition presence node

- Values: N/A
- Type property of the node is: *urn:gsma:mo:rcs-services:5.0*
- Associated HTTP XML characteristic type: “SERVICES”

Node: /<x>/ServicesMO/presencePrfl

Leaf node that describes whether or not the social presence functionality is supported

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

Table 64: Services MO sub tree addition parameters (presencePrfl)

- Values: If set to 1, it is supported. If set to 0, it is not supported.
- Post-reconfiguration actions: The client should be reset and should perform the complete first-time registration procedure following a reconfiguration (e.g. OMA-DM/HTTP) as described in section 2.3.1.
- Associated HTTP XML parameter: “presencePrfl”

Node: /<x>/ServicesMO/ChatAuth

Leaf node that represents the authorization for the user to use the chat service

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

Table 65: Services MO sub tree addition parameters (ChatAuth)

- Values: 0, 1
  0- Indicates that chat service is disabled
  1- Indicates that chat service is enabled
- Post-reconfiguration actions: The client should be reset and should perform the complete first-time registration procedure following a reconfiguration (e.g. OMA-DM/HTTP) as described in section 2.3.1.
- Associated HTTP XML parameter ID: “ChatAuth”

Node: /<x>/ServicesMO/ftAuth

Leaf node that represent the authorization for user to use the File Transfer service

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

Table 66: Services MO sub tree addition parameters (ftAuth)

- Values: 0, 1
  0- Indicates that File Transfer service is disabled
  1- Indicates that File Transfer service is enabled
- Post-reconfiguration actions: The client should be reset and should perform the complete first-time registration procedure following a reconfiguration (e.g. OMA-DM/HTTP) as described in section 2.3.1.
- Associated HTTP XML parameter ID: “ftAuth”

Node: /<x>/ServicesMO/standaloneMsgAuth

Leaf node that represents the authorization for user to use the standalone messaging service

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

Table 67: Services MO sub tree addition parameters (standaloneMsgAuth)

- Values: 0, 1
  0- The standalone messaging service is not provided. SMS and MMS is used instead
  1- The standalone messaging service is provided and uses CPM as specified in [RCS5-CPM-CONVFUNC-ENDORS].
- Post-reconfiguration actions: The client should be reset and should perform the complete first-time registration procedure following a reconfiguration (e.g. OMA-DM/HTTP) as described in section 2.3.1.
- Associated HTTP XML parameter ID: “standaloneMsgAuth”

Node: /<x>/ServicesMO/geolocPullAuth

Leaf node that represents the authorization for the user to use the Geolocation PULL service

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

Table 68: Services MO sub tree addition parameters (geolocPullAuth)

- Values: 0, 1
  0- Indicates that Geolocation PULL service is disabled
  1- Indicates that Geolocation PULL service is enabled
- Post-reconfiguration actions: The client should be reset and should perform the complete first-time registration procedure following a reconfiguration (e.g. OMA-DM/HTTP) as described in section 2.3.1.
- Associated HTTP XML parameter ID: “geolocPullAuth”

Node: /<x>/ServicesMO/geolocPushAuth

Leaf node that represents the authorization for the user to use the Geolocation PUSH service

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

Table 69: Services MO sub tree addition parameters (geolocPushAuth)

- Values: 0, 1
  0- Indicates that Geolocation PUSH service is disabled
  1- Indicates that Geolocation PUSH service is enabled
- Post-reconfiguration actions: The client should be reset and should perform the complete first-time registration procedure following a reconfiguration (e.g. OMA-DM/HTTP) as described in section 2.3.1.
- Associated HTTP XML parameter ID: “geolocPushAuth”

Node: /<x>/ServicesMO/VSAuth

Leaf node that represents the authorization for user to use Video Share service

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

Table 70: Services MO sub tree addition parameters (VSAuth)

- Values: 0, 1
  0- Indicates that Video Share service is disabled
  1- Indicates that Video Share service is enabled
- Post-reconfiguration actions: The client should be reset and should perform the complete first-time registration procedure following a reconfiguration (e.g. OMA-DM/HTTP) as described in section 2.3.1.
- Associated HTTP XML parameter ID: “vsAuth”

Node: /<x>/ServicesMO/ISAuth

Leaf node that represents the authorization for user to use Image Share service

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

Table 71: Services MO sub tree addition parameters (ISAuth)

- Values: 0, 1
  0- Indicates that Image Share service is disabled
  1- Indicates that Image Share service is enabled
- Post-reconfiguration actions: The client should be reset and should perform the complete first-time registration procedure following a reconfiguration (e.g. OMA-DM/HTTP) as described in section 2.3.1.
- Associated HTTP XML parameter ID: “isAuth”

Node: /<x>/ServicesMO/ipVideoCallAuth

Leaf node that represents the authorization for user to use IP Video Call service

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

Table 72: Services MO sub tree addition parameters (ipVideoCallAuth)

- Values: 0, 1
  0- Indicates that IP Video Call service is disabled
  1- Indicates that IP Video Call service is enabled
- Post-reconfiguration actions: The client should be reset and should perform the complete first-time registration procedure following a reconfiguration (e.g. OMA-DM/HTTP) as described in section 2.3.1.
- Associated HTTP XML parameter ID: “ipVideoCallAuth”

Node: /<x>/ServicesMO/Ext

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

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	Node	Get

Table 73: Services MO sub tree addition Service Provider Extension Node

- Values: N/A
- Type property of the node is: *urn:gsma:mo:rcs-services:5.0:Ext*
- Post-reconfiguration actions: The client should be reset and should perform the complete first-time registration procedure following a reconfiguration (e.g. OMA-DM/HTTP) as described in section 2.3.1.
- Associated HTTP XML characteristic type: “EXT”

A.2.2. IMS sub tree additions

RCS 5.0 includes the following additions to the IMS MO sub tree

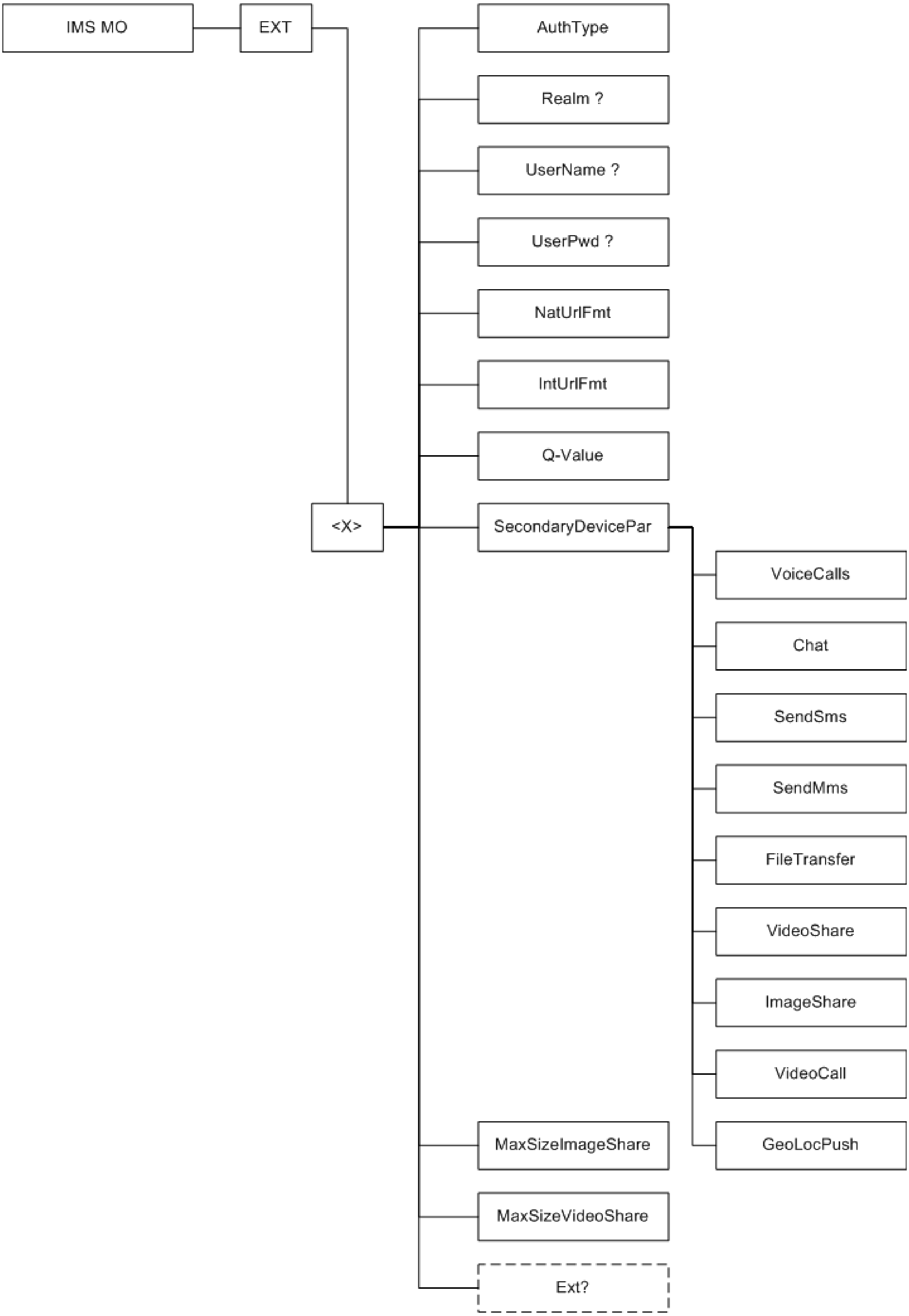


Figure 103: RCS 5.0 additions to the IMS MO sub tree

The associated HTTP configuration XML structure associated with the IMS parameters (both from the IMS MO defined in [3GPP TS 24.167] and the RCS specific parameters (shown in blue)) is presented in the table below

```
<characteristic type="APPLICATION">
    <parm name=”AppID” value=”X”/>
</characteristic>
<characteristic type=”IMS”>
    <parm name=”Name” value=”X”/>
    <characteristic type=”ConRefs”>
        <parm name=”ConRef” value=”X”/>
    </characteristic>
    <parm name=”PDP_ContextOperPref” value=”X”/>
    <parm name=”Timer_T1” value=”X”/>
    <parm name=”Timer_T2” value=”X”/>
    <parm name=”Timer_T4” value=”X”/>
    <parm name=”Private_User_Identity” value=”X”/>
    <characteristic type=”Public_User_Identity_List”>
        <parm name=”Public_User_Identity” value=”X”/>
    </characteristic>
    <parm name=”Home_network_domain_name” value=”X”/>
    <characteristic type=”Ext”>
        <parm name=”NatUrlFmt” value=”X”/>
        <parm name=”IntUrlFmt” value=”X”/>
        <parm name=”Q-Value” value=”X”/>
        <characteristic type=”SecondaryDevicePar”>
            <parm name=”VoiceCall” value=”X”/>
            <parm name=”Chat” value=”X”/>
            <parm name=”SendSms” value=”X”/>
            <parm name=”FileTranfer” value=”X”/>
            <parm name=”VideoShare” value=”X”/>
            <parm name=”ImageShare” value=”X”/>
            <parm name=”VideoCall” value=”X”/>
            <parm name=”GeoLocPush” value=”X”/>
        </characteristic>
        <parm name=”MaxSizeImageShare” value=”X”/>
        <parm name=”MaxTimeVideoShare value=”X”/>
        <characteristic type=”Ext”/>
    </characteristic>
    <characteristic type=”ICSI_List”>
        <parm name=”ICSI” value=”X”/>
        <parm name=”ICSI_Resource_Allocation_Mode” value=”X”/>
    </characteristic>
    <characteristic type=”LBO_P-CSCF_Address”>
        <parm name=”Address” value=”X”/>
        <parm name=”AddressType” value=”X”/>
    </characteristic>
    <parm name=”Voice_Domain_Preference_E_UTRAN” value=”X”/>
    <parm name=”SMS_Over_IP_Networks_Indication” value=”X”/>
    <parm name=”Keep_Alive_Enabled” value=”X”/>
    <parm name=”Voice_Domain_Preference_UTRAN” value=”X”/>
    <parm name=”Mobility_Management_IMS_Voice_Termination” value=”X”/>
    <parm name=”RegRetryBaseTime” value=”X”/>
    <parm name=”RegRetryMaxTime” value=”X”/>
    <characteristic type=”PhoneContext_List”>
        <parm name=”PhoneContext” value=”X”/>
        <parm name=”Public_User_Identity” value=”X”/>
    </characteristic>
    <characteristic type=”APPAUTH”>
        <parm name=”AuthType” value=”X”/>
        <parm name=”Realm” value=”X”/>
        <parm name=”UserName” value=”X”/>
        <parm name=”UserPwd” value=”X”/>
    </characteristic>
</characteristic>
```

Table 74 : IMS sub tree associated HTTP configuration XML structure

Node: /<x>

Under this interior node the RCS parameters related to IMS are placed

Status	Occurrence	Format	Min. Access Types
Required	One	node	Get

Table 75: IMS MO sub tree addition IMS node

- Values: N/A
- Type property of the node is: *urn:gsma:mo:rcs-IMS:5.0*
- Associated HTTP XML characteristic type: “IMS”

Node: /<x>/AuthType

Leaf node that describes the type of IMS authentication for the user

Status	Occurrence	Format	Min. Access Types
Required	One	chr	Get

Table 76: IMS MO sub tree addition parameters (AuthType)

- Values: ‘EarlyIMS’, ‘AKA’, ‘Digest’
- 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 (see section 2.4) using the new parameter.
- Associated HTTP XML characteristic type: “AuthType”

Node: /<x>/Realm

If the IMS mode for authentication is ‘digest’, this leaf node exists and contains the realm URL affected to the user

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	chr	Get

Table 77: IMS MO sub tree addition parameters (Realm)

- Values: <Realm URL>, example: ‘authenticatorY.operatorX.com’
- 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 (see section 2.4) using the new parameter.
- Associated HTTP XML characteristic type: “Realm”

Node: /<x>/UserName

If the IMS mode for authentication is ‘Digest’, this leaf node exists and contains the realm User name assigned to the user for IMS authorization/registration

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	chr	Get

Table 78: IMS MO sub tree addition parameters (UserName)

- Values: <use name assigned to user for IMS authentication/registration purpose>, Example: “Alice”
- 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 (see section 2.4) using the new parameter.
- Associated HTTP XML characteristic type: “UserName”

Node: /<x>/UserPwd

If the IMS mode for authentication is 'Digest', this leaf node exists and contains the User password assigned to the user for IMS authorization/registration

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	chr	Get

Table 79: IMS MO sub tree addition parameters (UserPwd)

- Values: <password assigned to user for IMS authentication/registration purpose>, Example: 'secretxyz'
- 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 (see section 2.4) using the new parameter.
- Associated HTTP XML characteristic type: "UserPwd"

Node: /<x>/NatUrlFmt

This leaf node indicates the format (SIP URI or tel URI) to be used when the callee numbering is dialled in national format

Status	Occurrence	Format	Min. Access Types
Required	One	chr	Get

Table 80: IMS MO sub tree addition parameters (NatUrlFmt)

- Values: 0, 1
  0: tel URI format (example: tel:0234578901;phone-context=<home-domain-name>)
  1: SIP URI format (example: sip:0234578901;phone-context=<home-domain-name>@<home-domain-name>;user=phone)
- Post-reconfiguration actions: The client should be reset and should perform the complete first-time registration procedure following a reconfiguration (e.g. OMA-DM/HTTP) as described in section 2.3.1.
- Associated HTTP XML characteristic type: "NatUrlFmt"

Node: /<x>/IntUrlFmt

This leaf node indicates the format (SIP URI or tel URI) to be used when the callee numbering is dialled in international format

Status	Occurrence	Format	Min. Access Types
Required	One	chr	Get

Table 81: IMS MO sub tree addition parameters (IntUrlFmt)

- Values: 0, 1
  0: tel URI format (example: tel:+32234578901)
  1: SIP URI format (example: sip:+32234578901@<home-domain-name>;user=phone)
- Post-reconfiguration actions: The client should be reset and should perform the complete first-time registration procedure following a reconfiguration (e.g. OMA-DM/HTTP) as described in section 2.3.1.
- Associated HTTP XML characteristic type: "IntUrlFmt"

Node: /<x>/QValue

This leaf node indicates the Q-value to be put in the Contact header of the Register method. This can be useful in case of multidevice for the forking algorithm.

Status	Occurrence	Format	Min. Access Types
Required	One	chr	Get

Table 82: IMS MO sub tree addition parameters (QValue)

- Values: ‘0.1’, ‘0.2’, ‘0.3’, ‘0.4’, ‘0.5’, ‘0.6’, ‘0.7’, ‘0.8’, ‘0.9’, ‘1.0’
- 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 (see section 2.4) using the new parameter.
- Associated HTTP XML characteristic type: “Q-Value”

Node: /<x>/SecondaryDevicePar

Presence of this interior node indicates that the RCS device is a secondary device. This node is not instantiated in case of primary device.

Under this node are instantiated the parameters necessary to control the ability for the user to restrict RCS services on the secondary device. The notion of primary and secondary device is defined in section 2.9.2.2.

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	node	Get

Table 83: IMS MO sub tree addition Secondary Device node

- Values: N/A
- Type property of the node is: *urn:gsma:mo:rcs-IMS:5.0:SecondaryDevice*
- Post-reconfiguration actions: The client should be reset and should perform the complete first-time registration procedure following a reconfiguration (e.g. OMA-DM/HTTP) as described in section 2.3.1.
- Associated HTTP XML characteristic type: “SecondaryDevicePar”

Node: /<x>/SecondaryDevicePar/VoiceCalls

This leaf node is instantiated if the device is an RCS secondary device. It allows the Service Provider to authorize or not the device user to control the voice call delivery on this secondary device. The notion of primary and secondary device is defined in section 2.9.2.2.

Status	Occurrence	Format	Min. Access Types
Required	One	chr	Get

Table 84: IMS MO sub tree addition parameters (VoiceCalls)

- Values: 0, 1
  0- Indicates authorization
  1- Indicates non authorization
- 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 (see section 2.4) using the new parameter.
- Associated HTTP XML characteristic type: “VoiceCall”

Node: /<x>/SecondaryDevicePar/Chat

This leaf node is instantiated if the device is an RCS secondary device. It allows the Service Provider to authorize or not the device user to control the incoming chat session acceptation on this secondary device. The notion of primary and secondary device is defined in section 2.9.2.2.

Status	Occurrence	Format	Min. Access Types
Required	One	chr	Get

Table 85: IMS MO sub tree addition parameters (Chat)

- Values: 0, 1
  0- Indicates authorization
  1- Indicates non authorization

- 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 (see section 2.4) using the new parameter.
- Associated HTTP XML characteristic type: “Chat”

Node: /<x>/SecondaryDevicePar/SendSms

This leaf node is instantiated if the device is an RCS secondary device. It allows the Service Provider to authorize or not the device user to control the restricted SMS service (only possibility to send an SMS on a secondary device) on this secondary device. The notion of primary and secondary device is defined in section 2.9.2.2.

Status	Occurrence	Format	Min. Access Types
Required	One	chr	Get

Table 86: IMS MO sub tree addition parameters (SendSMS)

- Values: 0, 1
  0- Indicates authorization
  1- Indicates non authorization
- 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 (see section 2.4) using the new parameter.
- Associated HTTP XML characteristic type: “SendSMS”

Node: /<x>/SecondaryDevicePar/SendMms

This leaf node is instantiated if the device is an RCS secondary device. It allows the Service Provider to authorize or not the device user to control the restricted MMS service (only possibility to send an MMS on a secondary device) on this secondary device. The notion of primary and secondary device is defined in section 2.9.2.2.

Status	Occurrence	Format	Min. Access Types
Required	One	chr	Get

Table 87: IMS MO sub tree addition parameters (SendMMS)

- Values: 0, 1
  0- Indicates authorization
  1- Indicates non authorization
- 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 (see section 2.4) using the new parameter.
- Associated HTTP XML characteristic type: “SendMMS”

Node: /<x>/SecondaryDevicePar/FileTransfer

This leaf node is instantiated if the device is an RCS secondary device. It allows the Service Provider to authorize or not the device user to control the incoming File Transfer reception on this secondary device. The notion of primary and secondary device is defined in section 2.9.2.2.

Status	Occurrence	Format	Min. Access Types
Required	One	chr	Get

Table 88: IMS MO sub tree addition parameters (FileTransfer)

- Values: 0, 1
  0- Indicates authorization
  1- Indicates non authorization

- 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 (see section 2.4) using the new parameter.
- Associated HTTP XML characteristic type: “FileTransfer”

Node: /<x>/SecondaryDevicePar/VideoShare

This leaf node is instantiated if the device is an RCS secondary device. It allows the Service Provider to authorize or not the device user to control the incoming Video Share session reception on this secondary device. The notion of primary and secondary device is defined in section 2.9.2.2.

Status	Occurrence	Format	Min. Access Types
Required	One	chr	Get

Table 89: IMS MO sub tree addition parameters (VideoShare)

- Values: 0, 1
  0- Indicates authorization
  1- Indicates non authorization
- 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 (see section 2.4) using the new parameter.
- Associated HTTP XML characteristic type: “VideoShare”

Node: /<x>/SecondaryDevicePar/ImageShare

This leaf node is instantiated if the device is an RCS secondary device. It allows the Service Provider to authorize or not the device user to control the incoming Image Share session reception on this secondary device. The notion of primary and secondary device is defined in section 2.9.2.2.

Status	Occurrence	Format	Min. Access Types
Required	One	chr	Get

Table 90: IMS MO sub tree addition parameters (ImageShare)

- Values: 0, 1
  0- Indicates authorization
  1- Indicates non authorization
- 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 (see section 2.4) using the new parameter.
- Associated HTTP XML characteristic type: “ImageShare”

Node: /<x>/SecondaryDevicePar/VideoCall

This leaf node is instantiated if the device is an RCS secondary device. It allows the Service Provider to authorize or not the device user to control the incoming Video Call session reception on this secondary device. The notion of primary and secondary device is defined in section 2.9.2.2.

Status	Occurrence	Format	Min. Access Types
Required	One	chr	Get

Table 91: IMS MO sub tree addition parameters (VideoCall)

- Values: 0, 1
  0- Indicates authorization
  1- Indicates non authorization

- 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 (see section 2.4) using the new parameter.
- Associated HTTP XML characteristic type: “VideoCall”

Node: /<x>/SecondaryDevicePar/GeoLocPush

This leaf node is instantiated if the device is an RCS secondary device. It allows the Service Provider to authorize or not the device user to control the incoming Geolocation PUSH request reception on this secondary device. The notion of primary and secondary device is defined in section 2.9.2.2.

Status	Occurrence	Format	Min. Access Types
Required	One	chr	Get

Table 92: IMS MO sub tree addition parameters (GeoLocPush)

- Values: 0, 1
  0- Indicates authorization
  1- Indicates non authorization
- 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 (see section 2.4) using the new parameter.
- Associated HTTP XML characteristic type: “GeoLocPush”

Node: /<x>/MaxSizeImageShare

Leaf node that represents the maximum authorized size of the content that can be sent in an Image Share session

Status	Occurrence	Format	Min. Access Types
Required	One	Int	Get

Table 93: IMS MO sub tree addition parameters (MaxSizeImageShare)

- Values: <content maximum size in bytes>. Value equals to 0 means no limitation.
- 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 (see section 2.4) using the new parameter.
- Associated HTTP XML characteristic type: “MaxSizeImageShare”

Node: /<x>/MaxTimeVideoShare

Leaf node that represents the maximum authorized duration time for a Video Share session

Status	Occurrence	Format	Min. Access Types
Required	One	Int	Get

Table 94: IMS MO sub tree addition parameters (MaxTimeVideoShare)

- Values: <Timer value in seconds>. Value equals to 0 means no limitation.
- 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 (see section 2.4) using the new parameter.
- Associated HTTP XML characteristic type: “MaxTimeVideoShare”

Node: /<x>/Ext

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

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	node	Get

Table 95: IMS MO sub tree addition Service Provider Extension Node

- Values: N/A
- Type property of the node is: *urn:gsma:mo:rcs-IMS:5.0:Ext*
- Post-reconfiguration actions: The client should be reset and should perform the complete first-time registration procedure following a reconfiguration (e.g. OMA-DM/HTTP) as described in section 2.3.1.
- Associated HTTP XML characteristic type: “Ext”

A.2.3. Presence sub tree additions

RCS 5.0 includes the following additions to the Presence MO sub tree

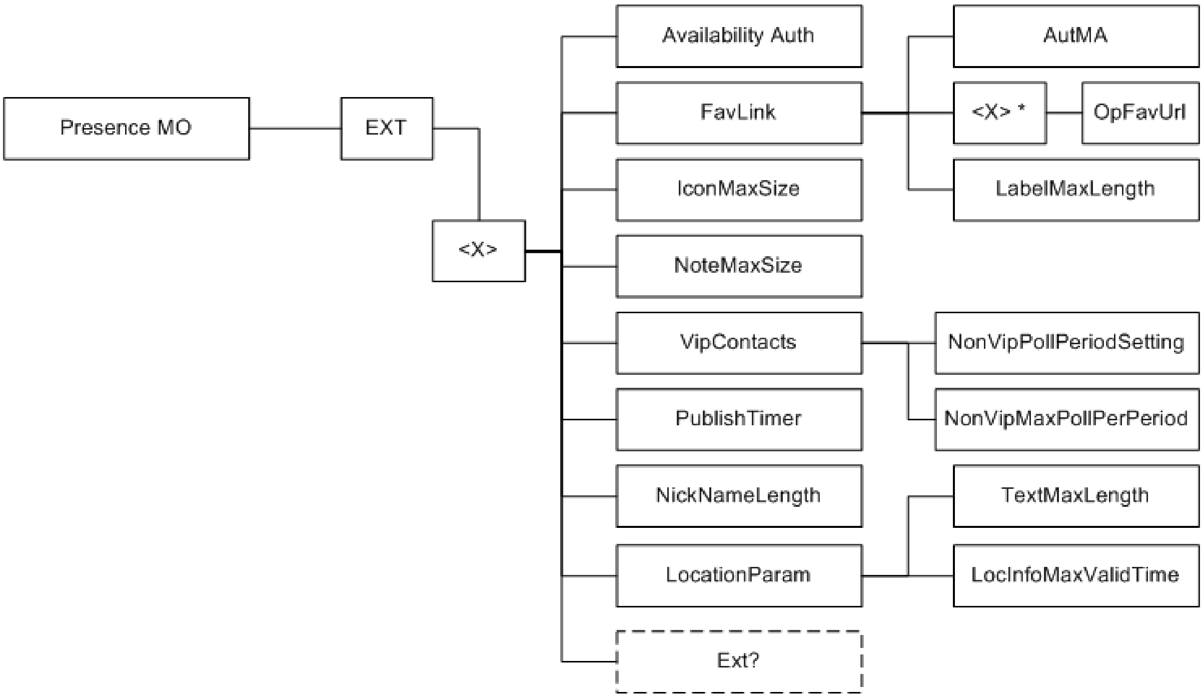


Figure 104: RCS 5.0 additions to the Presence MO sub tree

The associated HTTP configuration XML structure associated with the Presence parameters (both from the Presence MO defined in [PRESENCE2MO] and the RCS specific parameters (shown in blue)) is presented in the table below

```
<characteristic type=”PRESENCE”>
        <parm name=”AvailabilityAuth” value=”X”/>
        <characteristic type=”FAVLINK”>
        <parm name=”AutMa” value=”X”/>
              <characteristic type=”LINKS”>
                    <parm name=” OpFavUrl1” value=”X”/>
                    <parm name=” OpFavUrl2” value=”X”/>
                    <parm name=” OpFavUrl3” value=”X”/>
                    …
              </characteristic>
              <parm name=”LabelMaxLength” value=”X”/>
        </characteristic>
        <parm name=”IconMaxSize” value=”X”/>
        <parm name=”NoteMaxSize” value=”X”/>
        <characteristic type=”VIPCONTACTS”>
              <parm name=”NonVipPollPeriodSetting” value=”X”/>
              <parm name=”NonVipMaxPollPerPeriod” value=”X”/>
        </characteristic>
        <parm name=”PublishTimer” value=”X”/>
        <parm name=”NickNameLength” value=”X”/>
        <characteristic type=”Location”>
              <parm name=”TextMaxLength” value=”X”/>
              <parm name=”LocInfoMaxValidTime” value=”X”/>
        </characteristic>
        <characteristic type=”Ext”/>
        <parm name=”client-obj-datalimit” value=”X”/>
        <parm name=”content-serveruri” value=”X”/>
        <parm name=”source-throttlepublish” value=”X”/>
        <parm name=”max-number-ofsubscriptions-inpresence-list” value=”X”/>
        <parm name=”service-uritemplate” value=”X”/>
        <parm name=”RLS-URI” value=”X”/>
</characteristic>
```

Table 96 : Presence sub tree associated HTTP configuration XML structure

Node: /<x>

Under this interior node the RCS parameters related to Presence are placed

Status	Occurrence	Format	Min. Access Types
Required	One	node	Get

Table 97: Presence MO sub tree addition presence node

- Values: N/A
- Type property of the node is: *urn:gsma:mo:rcs-Presence:5.0*
- Associated HTTP XML characteristic type: “PRESENCE”

Node: /<x>/AvailabilityAuth

Leaf node that describes whether the presence related features are enabled or disabled on the device.

Status	Occurrence	Format	Min. Access Types
Required	One	bool	Get

Table 98: Presence MO sub tree addition parameters (AvailabilityAuth)

- Values: 1, the use of Availability status is authorized. 0, the use of Availability status is not authorized.
- Post-reconfiguration actions: The client should be reset and should perform the complete first-time registration procedure following a reconfiguration (e.g. OMA-DM/HTTP) as described in section 2.3.1.
- Associated HTTP XML parameter ID: “AvailabilityAuth”

Node: /<x>/FavLink

Interior node under which parameters related to the Service Provider provided Favourite Link(s) are located

Status	Occurrence	Format	Min. Access Types
Required	One	node	Get

Table 99: Presence MO sub tree addition Favourite Links node

- Values: N/A
- Type property of the node is: *urn:gsma:mo:rcs-Presence:5.0:favlink*
- Associated HTTP XML characteristic type: “FAVLINK”

Node: /<x>/FavLink/AutMa

Leaf node that determines the Service Provider policy for Favourite Link instantiation in the local presence document of the presentity

Status	Occurrence	Format	Min. Access Types
Required	One	chr	Get

Table 100: Presence MO sub tree addition parameters (AutMa)

- Values: ‘Auto’, ‘Man’, ‘Auto+Man’.
- Post-reconfiguration actions: The client should be reset and should perform the complete first-time registration procedure following a reconfiguration (e.g. OMA-DM/HTTP) as described in section 2.3.1.
- Associated HTTP XML parameter ID: “AutMa”

Node: /<x>/FavLink/<x>

A Placeholder interior node where to place 0 or more OpFavUrl leaf nodes

Status	Occurrence	Format	Min. Access Types
Required	One	node	Get

Table 101: Presence MO sub tree addition Predefined Links node

- Values: N/A
- Type property of the node is: *urn:gsma:mo:rcs-Presence:5.0:favlink:Link-ext*
- Associated HTTP XML characteristic type: “LINKS”

Node: /<x>/FavLink/<x>/OpFavUrl

Leaf node that represent a Favourite URL configured by the Service Provider

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrMore	chr	Get

Table 102: Presence MO sub tree addition parameters (OpFavUrl)

- Values: <a Service Provider defined url>
- 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 (see section 2.4) using the new parameter.
- Associated HTTP XML characteristic type: “OpFavUrl<X>” where <X> is a positive integer value determining the ordering of the different links

Node: /<x>/FavLink/LabelMaxLength

Leaf node that determines the Service Provider policy for Favourite Link instantiation in the local presence document of the presentity

Status	Occurrence	Format	Min. Access Types
Required	One	Int	Get

Table 103: Presence MO sub tree addition parameters (LabelMaxLength)

- Values: an integer that must be less or equal to 200.
  Note: A watcher must be able to display up to 200 characters for this attribute
- Post-reconfiguration actions: The client should be reset and should perform the complete first-time registration procedure following a reconfiguration (e.g. OMA-DM/HTTP) as described in section 2.3.1.
- Associated HTTP XML parameter ID: “LabelMaxLength”

Node: /<x>/IconMaxSize

Leaf node that represent the maximum authorized size for an icon

Status	Occurrence	Format	Min. Access Types
Required	One	Int	Get

Table 104: Presence MO sub tree addition parameters (IconMaxSize)

- Values: <Icon maximum data size in bytes>, the value must be inferior to 204800 (200kB)
- Post-reconfiguration actions: The client should be reset and should perform the complete first-time registration procedure following a reconfiguration (e.g. OMA-DM/HTTP) as described in section 2.3.1.
- Associated HTTP XML parameter ID: “IconMaxSize”

Node: /<x>/NoteMaxSize

Leaf node that represent the maximum authorized size for a note

Status	Occurrence	Format	Min. Access Types
Required	One	Int	Get

Table 105: Presence MO sub tree addition parameters (NoteMaxSize)

- Values: < Note maximum length in characters>
  Note: This should be set to a value that is lower than the one defined at watcher side in the OMA Presence Implementation guideline [PRESENCEIG].
- Post-reconfiguration actions: The client should be reset and should perform the complete first-time registration procedure following a reconfiguration (e.g. OMA-DM/HTTP) as described in section 2.3.1.
- Associated HTTP XML parameter ID: “NoteMaxSize”

Node: /<x>/PublishTimer

Leaf node that indicates the timer value for the Presence Publish refreshment

Status	Occurrence	Format	Min. Access Types
Required	One	Int	Get

Table 106: Presence MO sub tree addition parameters (PublishTimer)

- Values: < Timer value in seconds>
- 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 (see section 2.4) using the new parameter.
- Associated HTTP XML parameter ID: “PublishTimer”

Node: /<x>/NickNameLength

Leaf node that represents the maximum number of characters allowed for the user chosen nickname.

Status	Occurrence	Format	Min. Access Types
Required	One	Int	Get

Table 107: Presence MO sub tree addition parameters (NickNameLength)

- Values: must be less or equal to 200
  Note: An RCS client must be able to handle of up to 200 characters
- 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 (see section 2.4) using the new parameter.
- Associated HTTP XML parameter ID: “NickNameLength”

Node: /<x>/LocationParam

Interior node where Location related parameters are stored

Status	Occurrence	Format	Min. Access Types
Required	One	node	Get

Table 108: Presence MO sub tree addition Location Parameters node

- Values: N/A
- Type property of the node is: *urn:gsma:mo:rcs-Presence:5.0:Location*
- Associated HTTP XML characteristic type: “Location”

Node: /<x>/LocationParam/TextMaxLength

Leaf node that represents the maximum numbers of characters authorized for the textual attribute of the Location information

Status	Occurrence	Format	Min. Access Types
Required	One	Int	Get

Table 109: Presence MO sub tree addition parameters (TextMaxLength)

- Values: must be less or equal to 200.
  Note: A watcher must be able to render of up to 200 characters
- 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 (see section 2.4) using the new parameter.
- Associated HTTP XML parameter ID: “TextMaxLength”

Node: /<x>/LocationParam/LocInfoMaxValidTime

Leaf node that represents the maximum validity duration time for a location item.

This parameter must be taken account by the device presence UA when setting the “until” attribute of the presence items place-type, time-offset and the usage-rule/retention-expiry item value

Status	Occurrence	Format	Min. Access Types
Required	One	Int	Get

Table 110: Presence MO sub tree addition parameters (LocInfoMaxValidTime)

- Values: < Validity time in seconds>, when set to 0 there is no limit to the validity time
- 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 (see section 2.4) using the new parameter.

- Associated HTTP XML parameter ID: “LocInfoMaxValidTime”

Node: /<x>/VipContacts

Interior node where VIP contacts related parameters are stored

Status	Occurrence	Format	Min. Access Types
Required	One	node	Get

Table 111: Presence MO sub tree addition VIP Contacts node

- Values: N/A
- Type property of the node is: *urn:gsma:mo:rcs-Presence:5.0:VipContacts*
- Associated HTTP XML characteristic type: “VIPCONTACTS”

Node: /<x>/VipContacts/NonVipPollPeriodSetting

Leaf node that indicates, in seconds, the period duration for the calculation of the number of Poll operations on the non-VIP Contacts (“rcs_poll”) RLS list authorized during this period

Status	Occurrence	Format	Min. Access Types
Required	One	Int	Get

Table 112: Presence MO sub tree addition parameters (NonVipPollPeriodSetting)

- Values: integer that represents a time value in seconds
- 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 (see section 2.4) using the new parameter.
- Associated HTTP XML parameter ID: “NonVipPollPeriodSetting”

Node: /<x>/VipContacts/NonVipMaxPollPerPeriod

Leaf node that indicates the maximum number of Poll operations on the non-VIP Contacts (“rcs_poll”) RLS list that are authorized for the User Agent during each period (period parameter defined in the previous /VipContacts/NonVipPollPeriodSetting node).

Status	Occurrence	Format	Min. Access Types
Required	One	Int	Get

Table 113: Presence MO sub tree addition parameters (NonVipMaxPollPerPeriod)

- Values: integer that represents the total amount of Poll operations on the non-VIP Contacts list per each period.
- 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 (see section 2.4) using the new parameter.
- Associated HTTP XML parameter ID: “NonVipMaxPollPerPeriod”

Node: /<x>/Ext

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

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	node	Get

Table 114: Presence MO sub tree addition Service Provider Extension Node

- Values: N/A
- Type property of the node is: *urn:gsma:mo:rcs-Presence:5.0:Ext*

- Post-reconfiguration actions: The client should be reset and should perform the complete first-time registration procedure following a reconfiguration (e.g. OMA-DM/HTTP) as described in section 2.3.1.
- Associated HTTP XML characteristic type: “Ext”

A.2.4. XDMS sub tree additions

RCS 5.0 includes the following additions to the XDMS MO sub tree

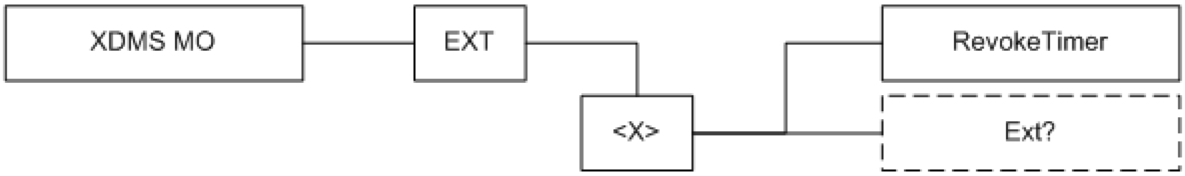


Figure 105: RCS 5.0 additions to the XDMS MO sub tree

The associated HTTP configuration XML structure associated with the XDMS parameters (both from the XDMS MO defined in [XDMMO] and the RCS specific parameters (shown in blue)) is presented in the table below

```
<characteristic type=”XDMS”>
        <parm name=”RevokeTimer” value=”X”/>
        <characteristic type=”Ext”/>
        <parm name=”XCAPRootURI” value=”X”/>
        <parm name=”XCAPAuthenticationUserName” value=”X”/>
        <parm name=”XCAPAuthenticationSecret” value=”X”/>
        <parm name=”XCAPAuthenticationType” value=”X”/>
</characteristic>
```

Table 115 : XDMS sub tree associated HTTP configuration XML structure

Node: /<x>

Under this interior node the RCS parameters related to XDM are placed

Status	Occurrence	Format	Min. Access Types
Required	One	node	Get

Table 116: XDM MO sub tree addition xdm node

- Values: N/A
- Type property of the node is: *urn:gsma:mo:rcs-xdm:5.0*
- Associated HTTP XML characteristic type: “XDMS”

Node: /<x>/RevokeTimer

Leaf node that indicates the duration a contact should remain in the RCS revocation list.

Status	Occurrence	Format	Min. Access Types
Required	One	Int	Get

Table 117: XDMS MO sub tree addition parameters (RevokeTimer)

- Values: < Timer value in seconds>
- 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 (see section 2.4) using the new parameter.
- Associated HTTP XML parameter ID: “RevokeTimer”

Node: /<x>/Ext

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

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	Node	Get

Table 118: XDMS MO sub tree addition Service Provider Extension Node

- Values: N/A
- Type property of the node is: *urn:gsma:mo:rcs-xdm:5.0:Ext*
- Post-reconfiguration actions: The client should be reset and should perform the complete first-time registration procedure following a reconfiguration (e.g. OMA-DM/HTTP) as described in section 2.3.1.
- Associated HTTP XML characteristic type: “Ext”

A.2.5. SUPL sub tree additions

RCS 5.0 includes the following additions to the SUPL MO sub tree:

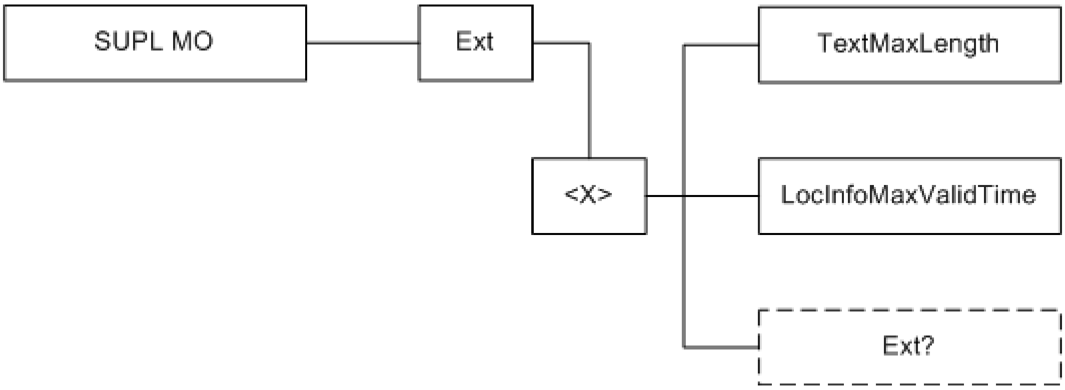


Figure 106 : RCS 5.0 additions to the SUPL MO sub tree

The associated HTTP configuration XML structure associated to the geolocation parameters (both from the SUPL MO defined in [SUPLMO] and the RCS specific parameters (shown in blue)) is presented in the table below

```
<characteristic type=”SUPL”>
        <parm name=”TextMaxLength” value=”X”/>
        <parm name=”LocInfoMaxValidTime” value=”X”/>
        <characteristic type=”Ext”/>
        <parm name=”Addr” value=”X”/>
        <parm name=”AddrType” value=”X”/>
</characteristic>
```

Table 119 : SUPL sub tree associated HTTP configuration XML structure

Node: /<x>

Under this interior node the RCS parameters related to the geolocation configuration are placed.

Status	Occurrence	Format	Min. Access Types
Required	One	node	Get

Table 120: SUPL MO sub tree addition geoloc node

- Values: N/A
- Type property of the node is: *urn:gsma:mo:rcs-supl:5.0*
- Associated HTTP XML characteristic type: “SUPL”

Node: /<x>/TextMaxLength

Leaf node that represents the maximum numbers of characters authorized for the textual attribute of the location information provided in the geolocation PUSH and PULL services

Status	Occurrence	Format	Min. Access Types
Required	One	Int	Get

Table 121: SUPL MO sub tree addition parameters (TextMaxLength)

- Values: must be less or equal to 200.
- 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 (see section 2.4) using the new parameter.
- Associated HTTP XML parameter ID: “TextMaxLength”

Node: /<x>/LocInfoMaxValidTime

Leaf node that represents the maximum validity duration time for a location item

This parameter must be taken account by the device providing the location information when setting the “until” attribute of the items place-type, time-offset and the usage-rule/retention-expiry item value

Status	Occurrence	Format	Min. Access Types
Required	One	Int	Get

Table 122: SUPL MO sub tree addition parameters (LocInfoMaxValidTime)

- Values: < Validity time in seconds>
- 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 (see section 2.4) using the new parameter.
- Associated HTTP XML parameter ID: “LocInfoMaxValidTime”

Node: /<x>/Ext

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

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	Node	Get

Table 123: SUPL MO sub tree addition Service Provider Extension Node

- Values: N/A
- Type property of the node is: *urn:gsma:mo:rcs-supl:5.0:Ext*
- Post-reconfiguration actions: The client should be reset and should perform the complete first-time registration procedure following a reconfiguration (e.g. OMA-DM/HTTP) as described in section 2.3.1.
- Associated HTTP XML characteristic type: “Ext”

A.2.6. IM sub tree additions

RCS 5.0 includes the following additions to the IM MO sub tree

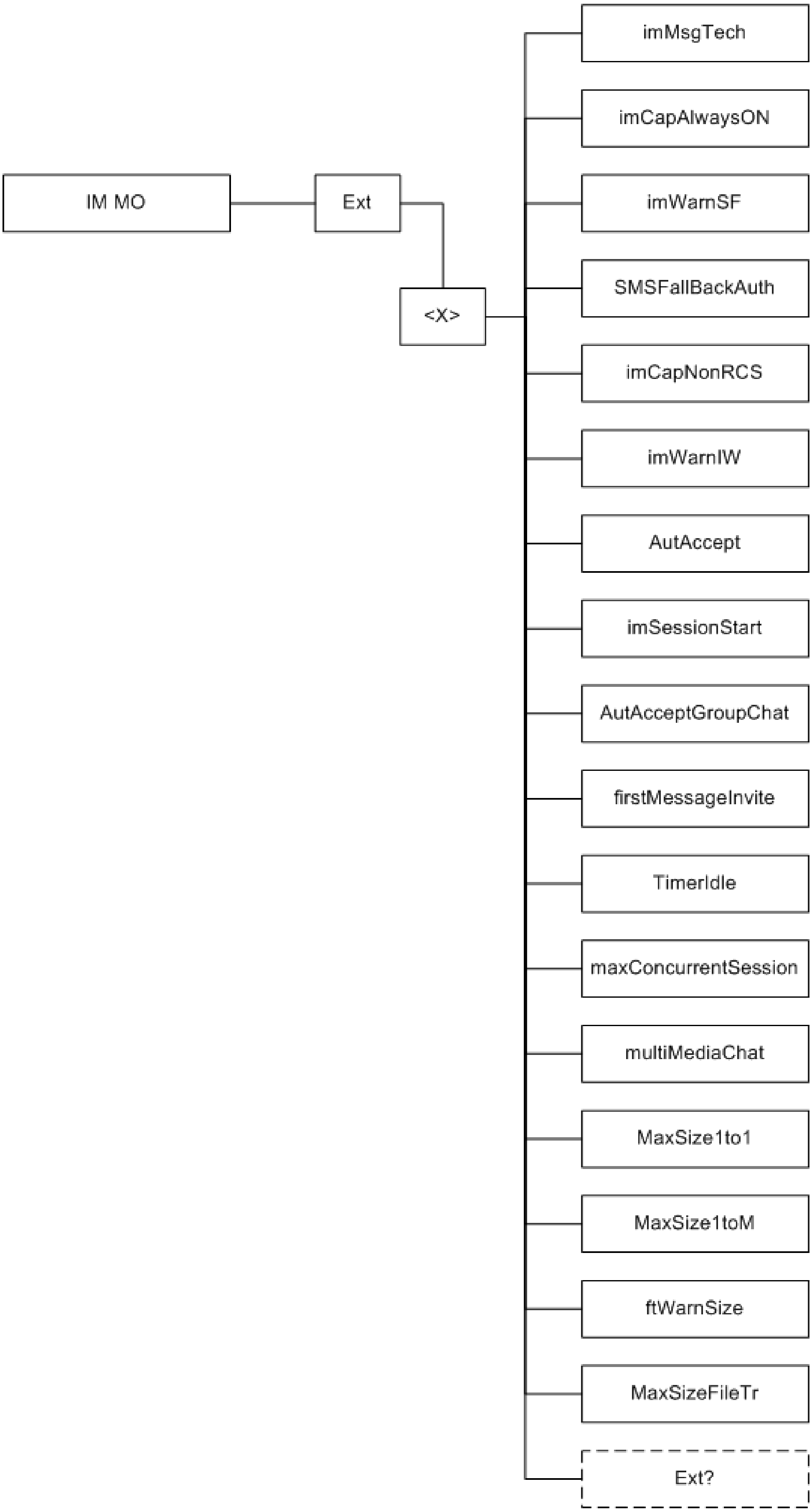


Figure 107: RCS 5.0 additions to the IM MO sub tree

The associated HTTP configuration XML structure associated to the IM parameters (both from the IM MO defined in [RCS5-SIMPLEIM-ENDORS] and the RCS specific parameters (shown in blue)) is presented in the table below

```
<characteristic type=”IM”>
        <parm name=”imMsgTech” value=”X”/>
        <parm name=”imCapAlwaysON” value=”X”/>
        <parm name=”imWarnSF” value=”X”/>
        <parm name=”SmsFallBackAuth” value=”X”/>
        <parm name=”imCapNonRCSE” value=”X”/>
        <parm name=”imWarnIW” value=”X”/>
        <parm name=”AutAccept” value=”X”/>
        <parm name=”AutAcceptGroupChat” value=”X”/>
        <parm name=”imSessionStart” value=”X”/>
        <parm name=”firstMessageInvite” value=”X”/>
        <parm name=”TimerIdle” value=”X”/>
        <parm name=”MaxConcurrentSession” value=”X”/>
        <parm name=”multiMediaChat” value=”X”/>
        <parm name=”MaxSize1to1” value=”X”/>
        <parm name=”MaxSize1toM” value=”X”/>
        <parm name=”ftWarnSize” value=”X”/>
        <parm name=”MaxSizeFileTr” value=”X”/>
        <characteristic type=”Ext”/>
        <parm name=”pres-srv-cap” value=”X”/>
        <parm name=”deferred-msg-func-uri” value=”X”/>
        <parm name=”max_adhoc_group_size” value=”X”/>
        <parm name=”conf-fcty-uri” value=”X”/>
        <parm name=”exploder-uri” value=”X”/>
</characteristic>
```

Table 124 : IM sub tree associated HTTP configuration XML structure

Node: /<x>

Under this interior node the RCS parameters related to the IM configuration are placed.

Status	Occurrence	Format	Min. Access Types
Required	One	node	Get

Table 125: IM MO sub tree addition IM node

- Values: N/A
- Type property of the node is: *urn:gsma:mo:rcs-im:5.0*
- Associated HTTP XML characteristic type: “IM”

Node: /<x>/imMsgTech

Leaf node that describes parameter allows selecting what technology is used for the chat service described in sections 3.3 and 3.4 as well as for the File Transfer service in section 3.5.

Status	Occurrence	Format	Min. Access Types
Optional	One	bool	Get/Replace

Table 126: IM MO sub tree addition parameters (imMsgTech)

- Values: 1, CPM as specified in [RCS5-CPM-CONVFUNC-ENDORS]. 0 (default if not provided), SIMPLE IM as specified in [RCS5-SIMPLEIM-ENDORS].
- Post-reconfiguration actions: The client should be reset and should perform the complete first-time registration procedure following a reconfiguration (e.g. OMA-DM/HTTP) as described in section 2.3.1.
- Associated HTTP XML parameter ID: “imMsgTech”

Node: /<x>/imCapAlwaysON

Leaf node that describes whether the Chat capability needs to be on independently of whether or not the other end is registered. For example this can be used in Service Providers providing the store and forward functionality for Chat

Status	Occurrence	Format	Min. Access Types
Optional	One	bool	Get/Replace

Table 127: IM MO sub tree addition parameters (IMCAPAlwaysOn)

- Values: 1, RCS Messaging Server based store and forward is enabled; 0, it is disabled
- 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 (see section 2.4) using the new parameter.
- Associated HTTP XML parameter ID: “imCapAlwaysOn”

Node: /<x>/imWarnSF

Leaf node that describes whether the UX should alert the user that messages are handled differently when the store and forward functionality is involved.

Status	Occurrence	Format	Min. Access Types
Optional	One	bool	Get/Replace

Table 128: IM MO sub tree addition parameters (imWarnSF)

- Values: 1, the user is made aware via the UX when the messages are deferred using S&F. 0, the user is not aware that messages are deferred.
- 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 (see section 2.4) using the new parameter.
- Associated HTTP XML parameter ID: “imWarnSF”

Node: /<x>/SmsFallbackAuth

Leaf node that represents the authorization for the device to propose automatically a SMS fallback in case of chat initiation failure

Status	Occurrence	Format	Min. Access Types
Optional	One	chr	Get

Table 129: IM MO sub tree addition parameters (SmsFallbackAuth)

- Values: 0, 1
  0- Indicates authorization is ok
  1- Indicates authorization is non ok
- 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 (see section 2.4) using the new parameter.
- Associated HTTP XML parameter ID: “SmsFallbackAuth”

Node: /<x>/imCapNonRCS

Leaf node that describes whether the Chat capability needs to be on independently of whether or not the other end is an RCS contact. For example this can be used in Service Providers providing the interworking functionality for Chat

Status	Occurrence	Format	Min. Access Types
Optional	One	bool	Get/Replace

Table 130: IM MO sub tree addition parameters (IMCAPNonRCS)

- Values: 1, RCS Messaging Server based interworking is enabled; 0, it is disabled

- 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 (see section 2.4) using the new parameter.
- Associated HTTP XML parameter ID: "imCapNonRCS"

Node: /<x>/imWarnIW

Leaf node that describes whether the UX should alert the user that messages are handled differently when the interworking functionality is involved

Status	Occurrence	Format	Min. Access Types
Optional	One	bool	Get/Replace

Table 131: IM MO sub tree addition parameters (IMWarnIW)

- Values: 1, the user is made aware via the UX when the messages are interworked to SMS/MMS. 0, the user is not aware that messages are interworked.
- 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 (see section 2.4) using the new parameter.
- Associated HTTP XML parameter ID: "imWarnIW"

Node: /<x>/AutAccept

Leaf node that represent the automatic/manual chat session answer mode

Status	Occurrence	Format	Min. Access Types
Optional	One	chr	Get

Table 132: IM MO sub tree addition parameters (AutAccept)

- Values: 0, 1
  0- Indicates manual answer mode
  1- Indicates automatic answer mode (default value)
- 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 (see section 2.4) using the new parameter.
- Associated HTTP XML parameter ID: "AutAccept"

Node: /<x>/imSessionStart

Leaf node that describes when the receiver client/device implementation should return the 200 OK initiating the MSRP session associated to a 1-to-1 chat. Please note that this parameter is transparent to the user.

Status	Occurrence	Format	Min. Access Types
Optional	One	Int	Get/Replace

Table 133: IM MO sub tree addition parameters (imSessionStart)

- Values: This parameter can have 3 possible values:
  - 0 (RCS 5.0 default):
    The 200 OK is sent when the receiver consumes the notification by opening the chat window.
  - 1 (RCS Release 2-4 default):
    The 200 OK is sent when the receiver starts to type a message to be sent back in the chat window.

  - 2 (new option):
    The 200 OK is sent when the receiver presses the button to send a message (That is the message will be buffered in the client until the MSRP session is established).

- 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 (see section 2.4) using the new parameter.
- Associated HTTP XML parameter ID: “imSessionStart”

Node: /<x>/AutAcceptGroupChat

Leaf node that represent the automatic/manual Group Chat session answer mode

Status	Occurrence	Format	Min. Access Types
Optional	One	chr	Get

Table 134: IM MO sub tree addition parameters (AutAcceptGroupChat)

- Values: 0, 1
  0- Indicates manual answer mode
  1- Indicates automatic answer mode (default value)
- 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 (see section 2.4) using the new parameter.
- Associated HTTP XML parameter ID: “AutAcceptGroupChat”

Node: /<x>/firstMsgInvite

Leaf node that controls whether the initial message in the chat is sent in a CPIM body of the SIP INVITE request or can only be sent once the MSRP session has been set up

Status	Occurrence	Format	Min. Access Types
Optional	One	bool	Get/Replace

Table 135: IM MO sub tree addition parameters (firstMsgInvite)

- Values: 0, the message is sent in the MSRP, 1, the message is added to the INVITE request as a CPIM body
- 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 (see section 2.4) using the new parameter.
- Associated HTTP XML parameter ID: “firstMessageInvite”

Node: /<x>/TimerIdle

Leaf node that represents the timeout for a chat session in idle mode (when there is no chat user activity)

Status	Occurrence	Format	Min. Access Types
Optional	One	Int	Get

Table 136: IM MO sub tree addition parameters (TimerIdle)

- Values: <Timer value in seconds>
- 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 (see section 2.4) using the new parameter.
- Associated HTTP XML parameter ID: “TimerIdle”

Node: /<x>/MaxConcurrentSession

Leaf node that represent the maximum authorized number of sessions established from the device. Once this number is reached a new session may not be established anymore until another session is torn down.

Status	Occurrence	Format	Min. Access Types
Optional	One	Int	Get

Table 137: IM MO sub tree addition parameters (MaxConcurrentSession)

- Values: <max number of concurrent sessions>, when set to 0 this limit does not apply
- 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 (see section 2.4) using the new parameter.
- Associated HTTP XML parameter ID: "MaxConcurrentSession"

Node: /<x>/multiMediaChat

Leaf node that controls whether or not the device can send and receive other content than text in the chat session

Status	Occurrence	Format	Min. Access Types
Optional	One	bool	Get

Table 138: IM MO sub tree addition parameters (multiMediaChat)

- Values:
  0 (or not provided), the device can only sent and receive text content within the chat . The client should handle the SDP negotiation accordingly
  1, all content allowed by [RCS5-SIMPLEIM-ENDORS] or [RCS5-CPM-CONVFUNC-ENDORS] may be sent in the chat session
- 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 (see section 2.4) using the new parameter.
- Associated HTTP XML parameter ID: "multiMediaChat"

Node: /<x>/MaxSize1To1

Leaf node that represent the maximum authorized size of a content chat message in a 1 To 1 chat session

Status	Occurrence	Format	Min. Access Types
Optional	One	Int	Get

Table 139: IM MO sub tree addition parameters (MaxSize1To1)

- Values: <content maximum size in bytes>
- 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 (see section 2.4) using the new parameter.
- Associated HTTP XML parameter ID: "MaxSize1To1"

Node: /<x>/MaxSize1ToM

Leaf node that represent the maximum authorized size of a chat content message in a Group Chat session

Status	Occurrence	Format	Min. Access Types
Optional	One	Int	Get

Table 140: IM MO sub tree addition parameters (MaxSize1ToM)

- Values: <content maximum size in bytes>

- 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 (see section 2.4) using the new parameter.
- Associated HTTP XML parameter ID: “MaxSize1ToM”

Node: /<x>/ftWarnSize

Leaf node that describes the file transfer size threshold (in KB) when the user should be warned about the potential charges associated to the transfer of a large file.

Status	Occurrence	Format	Min. Access Types
Optional	One	Int	Get/Replace

Table 141: IM MO sub tree addition parameters (ftWarnSize)

- Values: The file size threshold (in KB) or 0 to disable the warning
- 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 (see section 2.4) using the new parameter.
- Associated HTTP XML parameter ID: “ftWarnSize”

Node: /<x>/MaxSizeFileTr

Leaf node that represent the maximum authorized size of a file that can be transfers using the RCS File Transfer service

Status	Occurrence	Format	Min. Access Types
Optional	One	Int	Get

Table 142: IM MO sub tree addition parameters (MaxSizeFileTr)

- Values: The maximum file size threshold (in KB) or 0 to disable the limit
- 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 (see section 2.4) using the new parameter.
- Associated HTTP XML parameter ID: “MaxSizeFileTr”

Node: /<x>/Ext

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

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	Node	Get

Table 143: IM MO sub tree addition Service Provider Extension Node

- Values: N/A
- Type property of the node is: *urn:gsma:mo:rcs-im:5.0Ext*
- Post-reconfiguration actions: The client should be reset and should perform the complete first-time registration procedure following a reconfiguration (e.g. OMA-DM/HTTP) as described in section 2.3.1.
- Associated HTTP XML characteristic type: “Ext”

A.2.7. CPM MO sub tree

RCS 5.0 includes the following additions as a new configuration sub tree, the CPM MO subtree

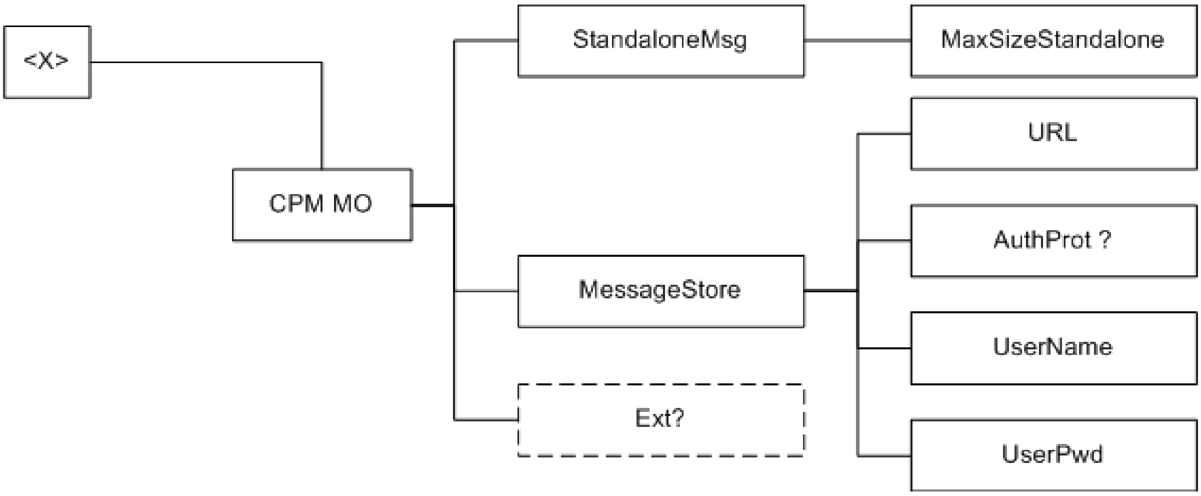


Figure 108: RCS 5.0 additions, CPM MO sub tree

The associated HTTP configuration XML structure associated to the CPM parameters is presented in the table below. Only RCS specific parameters (shown in blue) are included as OMA does not define a CPM MO.

```
<characteristic type=”CPM”>
        <characteristic type=”StandaloneMsg”>
              <parm name=”MaxSizeStandalone” value=”X”/>
        </characteristic>
        <characteristic type=”MessageStore”>
              <parm name=”Url” value=”X”/>
              <parm name=”AuthProt” value=”X”/>
              <parm name=”UserName” value=”X”/>
              <parm name=”UserPwd” value=”X”/>
        </characteristic>
        <characteristic type=”Ext”/>
</characteristic>
```

Table 144 : CPM sub tree associated HTTP configuration XML structure

Node: /<x>/CPMMO

Under this interior node the RCS parameters related to the CPM configuration are placed.

Status	Occurrence	Format	Min. Access Types
Required	One	node	Get

Table 145: CPM MO sub tree addition CPM node

- Values: N/A
- Type property of the node is: *urn:gsma:mo:rcs-cpm:5.0*
- Associated HTTP XML characteristic type: “CPM”

Node: /<x>/CPMMO/StandaloneMsg

Interior node where are filled parameters related to the RCS Text message and Multimedia message service

Status	Occurrence	Format	Min. Access Types
Required	One	node	Get

Table 146: CPM MO sub tree addition Standalone messaging node

- Values: N/A
- Type property of the node is: *urn:gsma:mo:rcs-cpm:5.0:StandaloneMsg*
- Associated HTTP XML characteristic type: “StandaloneMsg”

Node: /<x>/CPMMO/StandaloneMsg/MaxSize

Leaf node that represents the maximum authorized content size of a text or multimedia message

Status	Occurrence	Format	Min. Access Types
Optional	One	Int	Get

Table 147: CPM MO sub tree addition parameters (MaxSize)

- Values: <content maximum size in bytes>
- 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 (see section 2.4) using the new parameter.
- Associated HTTP XML parameter ID: “MaxSize”

Node: /<x>/CPMMO/MessageStore

Interior node where there are filled parameters related to RCS CPM Network-based Common Message Store

Status	Occurrence	Format	Min. Access Types
Optional	One	node	Get

Table 148: CPM MO sub tree addition Message Store node

- Values: N/A
- Type property of the node is: *urn:gsma:mo:rcs-cpm:5.0:MessageStore*
- Associated HTTP XML characteristic type: “MessageStore”

Node: /<x>/CPMMO/MessageStore/Url

Leaf node that represents the URL address of the Network-based Common Message Store server

Status	Occurrence	Format	Min. Access Types
Optional	One	chr	Get

Table 149: CPM MO sub tree addition parameters (Url)

- Values: the URL for accessing the Message Store, if set to an empty string, the Message Store is not available.
- 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 (see section 2.4) using the new parameter.
- Associated HTTP XML parameter ID: “Url”

Node: /<x>/CPMMO/MessageStore/AuthProt

Optional leaf node that can be used to force the RCS agent to use one of the 2 authentication methods defined in [RCS5-CPM-MSGSTOR-ENDORS]. If not instantiated, the RCS agent can use any of the 2 methods

Status	Occurrence	Format	Min. Access Types
Optional	One	chr	Get

Table 150: CPM MO sub tree addition parameters (AuthProt)

- Values: 0, 1
  0- Indicates that the SASL methods must be used by the RCS agent
  1- Indicates that the user name / password method must be used by the RCS agent
- 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 (see section 2.4) using the new parameter.
- Associated HTTP XML parameter ID: "AuthProt"

Node: /<x>/CPMMO/MessageStore/UserName

Leaf node that represents the User Identity information used by the RCS agent to access the subscriber IMAP account on the Message Storage server

Status	Occurrence	Format	Min. Access Types
Optional	One	chr	Get

Table 151: CPM MO sub tree addition parameters (UserName)

- Values: <username assigned to the user for access to his Message Store>
- 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 (see section 2.4) using the new parameter.
- Associated HTTP XML parameter ID: "UserName"

Node: /<x>/CPMMO/MessageStore/UserPwd

Leaf node that represents the ser password associated to his/her User Name Identity information used by the RCS agent to access the subscriber IMAP account on the Message Storage server

Status	Occurrence	Format	Min. Access Types
Optional	One	chr	Get

Table 152: CPM MO sub tree addition parameters (UserPwd)

- Values: <password assigned to the user for access to his Message Store>
- 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 (see section 2.4) using the new parameter.
- Associated HTTP XML parameter ID: "UserPwd"

Node: /<x>/CPMMO/Ext

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

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	Node	Get

Table 153: CPM MO sub tree addition Service Provider Extension Node

- Values: N/A
- Type property of the node is: *urn:gsma:mo:rcs-cpm:5.0:EXT*
- Post-reconfiguration actions: The client should be reset and should perform the complete first-time registration procedure following a reconfiguration (e.g. OMA-DM/HTTP) as described in section 2.3.1.
- Associated HTTP XML characteristic type: "Ext"

A.2.8. Capability discovery MO sub tree

The RCS 5.0 specification includes the following additions as a new configuration sub tree, the capability discovery MO sub tree. Please note this sub tree is not included in any other specifications. So no other nodes from those specifications need to be added:

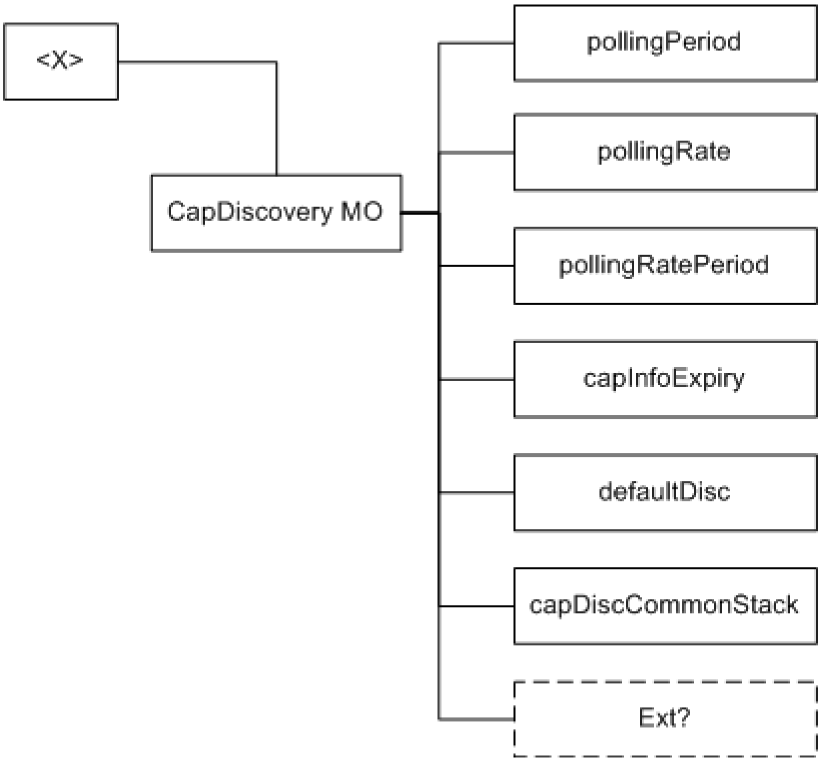


Figure 109: RCS 5.0 additions, capability sub tree

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

```
<characteristic type="CAPDISCOVERY">
        <parm name="pollingPeriod" value="X"/>
        <parm name="pollingRate" value="X"/>
        <parm name="pollingRatePeriod" value="X"/>
        <parm name="capInfoExpiry" value="X"/>
        <parm name="defaultDisc" value="X"/>
        <parm name="capDiscCommonStack" value="X"/>
        <characteristic type="Ext"/>
</characteristic>
```

Table 154 : Capability sub tree associated HTTP configuration XML structure

Node: /<x>/CapDiscoveryMO

Under this interior node the RCS parameters related to capability discovery are placed

Status	Occurrence	Format	Min. Access Types
Required	One	node	Get

Table 155: Capability MO sub tree addition capability discovery node

- Values: N/A
- Type property of the node is: *urn:gsma:mo:rcs-icapdis:5.0*
- Associated HTTP XML characteristic type: “CAPDISCOVERY”

Node: /<x>/CapDiscoveryMO/pollingPeriod

Leaf node that describes the timer in seconds between querying all the contacts in the address book to update the capabilities.

Status	Occurrence	Format	Min. Access Types
Required	One	Int	Get/Replace

Table 156: Capability MO sub tree addition parameters (pollingPeriod)

- Values: The time in seconds. If it is set to 0, the periodic capability update (polling) is not performed
- 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 (see section 2.4) using the new parameter.
- Associated HTTP XML parameter ID: “pollingPeriod”

Node: /<x>/CapDiscoveryMO/pollingRatePeriod

Leaf node that indicates, in seconds, the period duration for the calculation of the authorized number of capability query requests during this period

Status	Occurrence	Format	Min. Access Types
Required	One	Int	Get

Table 157: Capability MO sub tree addition parameters (pollingRatePeriod)

- Values: The period in seconds.
- 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 (see section 2.4) using the new parameter.
- Associated HTTP XML parameter ID: “pollingRatePeriod”

Node: /<x>/CapDiscoveryMO/pollingRate

Leaf node that indicates the maximum capability query operations that are authorized globally for the User Agent during each period (period parameter defined in the previous pollingRatePeriod node).

Status	Occurrence	Format	Min. Access Types
Required	One	Int	Get

Table 158: Capability MO sub tree addition parameters (pollingRate)

- Values: integer that represents the total amount of capability query operations per each period, independently of the number of contacts that have to be query.
- 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 (see section 2.4) using the new parameter.
- Associated HTTP XML parameter ID: “pollingRate”

Node: /<x>/CapDiscoveryMO/capInfoExpiry

Leaf node that describes the validity of the capability information stored in the terminal in seconds

Status	Occurrence	Format	Min. Access Types
Optional	One	Int	Get/Replace

Table 159: Capability MO sub tree addition parameters (capInfoExpiry)

- Values: The time in seconds.
- 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 (see section 2.4) using the new parameter.

- Associated HTTP XML parameter ID: “capInfoExpiry”

Node: /<x>/CapDiscoveryMO/defaultDisc

Leaf node that describes the interworking approach for the capability discover. Please note this is an optional parameter which is only required when the defaultDisc parameter is set to 1.

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

Table 160: Capability MO sub tree addition parameters (defaultDisc)

- Values: 0, the default mechanism employed for capability discovery and new users will be OPTIONS. 1, the default mechanism employed for capability discovery and new users will be Presence
- 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 (see section 2.4) using the new parameter.
- Associated HTTP XML parameter ID: “defaultDisc”

Node: /<x>/CapDiscoveryMO/capDiscCommonStack

Leaf node that describes the default capability and new user discovery mechanism used by the terminal (Presence or Options)

Status	Occurrence	Format	Min. Access Types
Optional	One	bool	Get/Replace

Table 161: Capability MO sub tree addition parameters (capDiscCommonStack)

- Values:
  0, the fallback to SIP OPTIONS mechanism remains disabled.
  1, the fallback to SIP OPTIONS mechanism remains enabled.
- 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 (see section 2.4) using the new parameter.
- Associated HTTP XML parameter ID: “capDiscCommonStack”

Node: /<x>/CapDiscoveryMO/Ext

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

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	Node	Get

Table 162: Capability MO sub tree addition Service Provider Extension Node

- Values: N/A
- Type property of the node is: *urn:gsma:mo:rcs-icapdis:5.0:Ext*
- Post-reconfiguration actions: The client should be reset and should perform the complete first-time registration procedure following a reconfiguration (e.g. OMA-DM/HTTP) as described in section 2.3.1.
- Associated HTTP XML characteristic type: “Ext”

A.2.9. APN Configuration MO sub tree

The RCS 5.0 specification includes the following additions as a new configuration sub tree, the roaming MO sub tree. Please note this sub tree is not included in any other specifications. So no other nodes from those specifications need to be added:

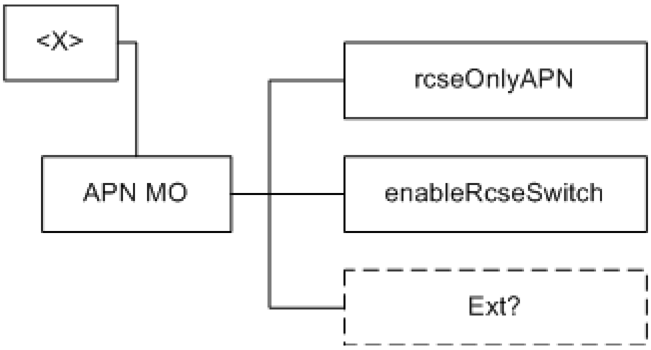


Figure 110: RCS 5.0 additions, roaming sub tree

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

```
<characteristic type="APN">
        <parm name="rcseOnlyAPN" value="X"/>
        <parm name="enableRcseSwitch" value="X"/>
        <characteristic type="Ext"/>
</characteristic>
```

Table 163 : APN sub tree associated HTTP configuration XML structure

Node: /<x>/APNMO

Under this interior node the RCS parameters related to roaming are placed.

Status	Occurrence	Format	Min. Access Types
Required	One	node	Get

Table 164: APN MO sub tree addition node

- Values: N/A
- Type property of the node is: *urn:gsma:mo:rcs-apn:5.0*
- Associated HTTP XML characteristic type: "APN"

Node: /<x>/APNMO/rcseOnlyAPN

Leaf node that describes the APN to be used as the RCS roaming APN (as described in section 2.9.1.4)

Status	Occurrence	Format	Min. Access Types
Required	One	chr	Get/Replace

Table 165: APN MO sub tree addition parameters (rcseOnlyAPN)

- Values: The APN name or the identifier used on the phone for the RCS only APN
- 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 (see section 2.4) using the new parameter.
- Associated HTTP XML parameter ID: "rcseOnlyAPN"

Node: /<x>/APNMO/enableRcseSwitch

Leaf node that describes whether or not to show the RCS enabled/disabled switch permanently as described in section 2.9.1.4

Status	Occurrence	Format	Min. Access Types
Required	One	Int	Get/Replace

Table 166: APN MO sub tree addition parameters (enableRcseSwitch)

- Values:
  1, the switch is shown permanently.
  0, the switch is only shown during roaming.
  -1, the switch is never shown.
- 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 (see section 2.4) using the new parameter.
- Associated HTTP XML parameter ID: “enableRcseSwitch”

Node: /<x>/APNMO/Ext

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

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	Node	Get

Table 167: APN MO sub tree addition Service Provider Extension Node

- Values: N/A
- Type property of the node is: *urn:gsma:mo:rcs-apn:5.0:Ext*
- Post-reconfiguration actions: The client should be reset and should perform the complete first-time registration procedure following a reconfiguration (e.g. OMA-DM/HTTP) as described in section 2.3.1.
- Associated HTTP XML characteristic type: “Ext”

A.2.10. Other RCS Configuration MO sub tree

The RCS 5.0 specification includes the following additions as a new configuration sub tree, containing the remaining RCS configuration parameters. Please note this sub tree is not included in any other specifications. So no other nodes from those specifications need to be added:

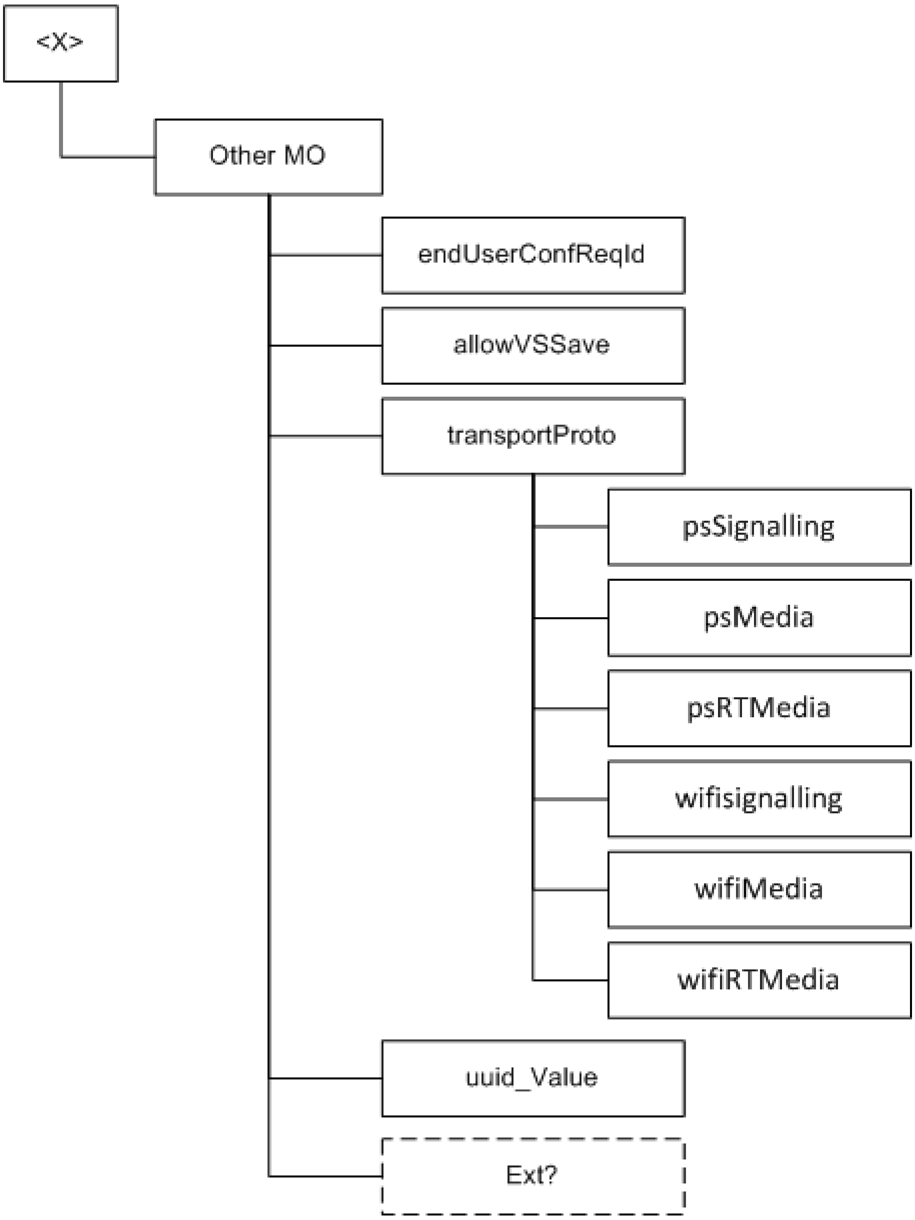


Figure 111: RCS 5.0 additions, other sub tree

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

```
<characteristic type=”OTHER”>
        <parm name=”endUserConfReqId” value=”X”/>
        <parm name=”allowVSSave” value=”X”/>
        <characteristic type=” transportProto”>
              <parm name=”psSignalling” value=”X”/>
              <parm name=”psMedia” value=”X”/>
              <parm name=”psRTMedia” value=”X”/>
              <parm name=”wifiSignalling” value=”X”/>
              <parm name=”wifiMedia” value=”X”/>
              <parm name=”wifiRTMedia” value=”X”/>
        </characteristic>
        <parm name=”uuid_Value” value=”X”/>
        <characteristic type=”Ext”/>
</characteristic>
```

Table 168 : Other sub tree associated HTTP configuration XML structure

Node: /<x>/OtherMO

Under this interior node the RCS parameters which do not fit in the other categories are placed.

Status	Occurrence	Format	Min. Access Types
Required	One	node	Get

Table 169: Other MO sub tree addition node

- Values: N/A
- Type property of the node is: *urn:gsma:mo:rcs-other:5.0*
- Associated HTTP XML characteristic type: “OTHER”

Node: /<x>/OtherMO/endUserConfReqId

Leaf node that describes the identity (*P-Asserted-Identity*) used for sending the end user confirmation request

Status	Occurrence	Format	Min. Access Types
Required	One	chr	Get/Replace

Table 170: Other MO sub tree addition parameters (endUserConfReqId)

- Values: Values: The identity (*P-Asserted-Identity*) used for sending the end user confirmation request
- Post-reconfiguration actions: As the client remains unregistered during configuration, there are no additional actions apart from de-registering using the old configuration and registering back (see section 2.4) using the new parameter.
- Associated HTTP XML parameter ID: “endUserConfReqId”

Node: /<x>/OtherMO/allowVSSave

Leaf node that determines whether or not the SDP attribute and value described in section 3.6.4.1.3 is included in the Video Share invitation

Status	Occurrence	Format	Min. Access Types
Optional	One	Int	Get/Replace

Table 171: Other MO sub tree addition parameters (allowVSSave)

- Values: -1, 0, 1
  -1- Inclusion of the attribute and value is up to the user’s preference
  0- The attribute is never included
  1- The attribute is always included

- 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 (see section 2.4) using the new parameter.
- Associated HTTP XML parameter ID: “allowVSSave”

Node: /<x>/OtherMO/transportProto

Under this interior node the RCS parameters related to roaming are placed.

Status	Occurrence	Format	Min. Access Types
Required	One	node	Get

Table 172: Transport Protocol sub tree node

- Values: N/A
- Type property of the node is: *urn:gsma:mo:rcs-other:5.0:transportProto*
- Associated HTTP XML characteristic type: “transportProto”

Node: /<x>/OtherMO/transportProto/psSignalling

Leaf node that describes the transport protocol used to carry the signalling when connecting over PS cellular access.

Status	Occurrence	Format	Min. Access Types
Required	One	chr	Get/Replace

Table 173: Other MO sub tree addition parameters (psSignalling)

- Values: The possible values are:
  - SIPoUDP
  - SIPoTCP
  - SIPoTLS
- 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 (see section 2.4) using the new parameter.
- Associated HTTP XML characteristic type: “psSignalling”

Node: /<x>/OtherMO/transportProto/psMedia

Leaf node that describes the transport protocol used to carry the media (e.g. Chat, File Transfer and Image Share services) when connecting over PS cellular access.

Status	Occurrence	Format	Min. Access Types
Required	One	chr	Get/Replace

Table 174: Other MO sub tree addition parameters (psMedia)

- Values: The possible values are:
  - MSRP
  - MSRPoTLS
- 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 (see section 2.4) using the new parameter.
- Associated HTTP XML characteristic type: “psMedia”

Node: /<x>>/OtherMO/transportProto/psRTMedia

Leaf node that describes the transport protocol used to carry the real time media (e.g. Video Share) when connecting over PS cellular access.

Status	Occurrence	Format	Min. Access Types
Required	One	chr	Get/Replace

Table 175: Other MO sub tree addition parameters (psRTMedia)

- Values: The possible values are:
  - RTP
  - SRTP
- 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 (see section 2.4) using the new parameter.
- Associated HTTP XML characteristic type: “psRTMedia”

Node: /<x>/OtherMO/transportProto/wifiSignalling

Leaf node that describes the transport protocol used to carry the signalling when connecting over Wi-Fi.

Status	Occurrence	Format	Min. Access Types
Required	One	chr	Get/Replace

Table 176: Other MO sub tree addition parameters (wifiSignalling)

- Values: The possible values are:
  - SIPoUDP
  - SIPoTCP
  - SIPoTLS
- 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 (see section 2.4) using the new parameter.
- Associated HTTP XML characteristic type: “wifiSignalling”

Node: /<x>/OtherMO/transportProto/wifiMedia

Leaf node that describes the transport protocol used to carry the media (e.g. Chat, File Transfer and Image Share services) when connecting over Wi-Fi access

Status	Occurrence	Format	Min. Access Types
Required	One	chr	Get/Replace

Table 177: Other MO sub tree addition parameters (wifiMedia)

- Values: The possible values are:
  - MSRP
  - MSRPoTLS
- 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 (see section 2.4) using the new parameter.
- Associated HTTP XML characteristic type: “wifiMedia”

Node: /<x>/OtherMO/transportProto/wifiRTMedia

Leaf node that describes the transport protocol used to carry the real time media (e.g. Video Share) when connecting over Wi-Fi access.

Status	Occurrence	Format	Min. Access Types
Required	One	chr	Get/Replace

Table 178: Other MO sub tree addition parameters (wifiRTMedia)

- Values: The possible values are:
  - RTP
  - SRTP
- 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 (see section 2.4) using the new parameter.
- Associated HTTP XML characteristic type: "wifiRTMedia"

Node: /<x>/OtherMO/uuid_Value

Leaf node that describes a UUID which is required for the sip.instance multidevice approach as described in sections 2.4.2 and 2.12. In this case the UUID is generated by the Service Provider network following the algorithm described in [RFC4122].

Status	Occurrence	Format	Min. Access Types
Optional	One	chr	Get/Replace

Table 179: Other MO sub tree addition parameters (uuid_Value)

- Values: A string containing the UUID value
- 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 (see section 2.4) using the new parameter.
- Associated HTTP XML characteristic type: "uuid_Value"

Node: /<x>/Ext

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

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	Node	Get

Table 180: Other MO sub tree addition Service Provider Extension Node

- Values: N/A
- Type property of the node is: *urn:gsma:mo:rcs-other:5.0:Ext*
- Post-reconfiguration actions: The client should be reset and should perform the complete first-time registration procedure following a reconfiguration (e.g. OMA-DM/HTTP) as described in section 2.3.1.
- Associated HTTP XML characteristic type: "Ext"

A.2.11. Service Provider Extensions MO sub tree

The RCS 5.0 specification includes the following additions as a new and optional configuration sub tree, the Service Provider extensions MO sub tree. If present this subtree may be ignored by clients that are not aware of any extensions in this tree. Please note this sub tree is not included in any other specifications. So no other nodes from those specifications need to be added:

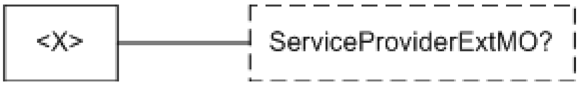


Figure 112: RCS 5.0 additions, Service Provider Extensions sub tree

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

```
<characteristic type=”SERVICEPROVIDEREXT”/>
```

Table 181 : Service Provider Extensions sub tree associated HTTP configuration XML structure

Node: /<X>/ServiceProviderExtMO

Under this interior node the RCS parameters related to Service Provider specific extensions are placed

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	node	Get

Table 182: APN MO sub tree addition node

- Values: N/A
- Type property of the node is: *urn:gsma:mo:rcs-sp:5.0*
- Associated HTTP XML characteristic type: “SERVICEPROVIDEREXT”

A.3. HTTP specific configuration and behaviour

A.3.1. HTTP configuration XML structure

In addition to the parameters and characteristics type correspondences presented in the previous section, it is necessary to define the following mandatory configuration XML elements[30]:

```
<?xml version="1.0"?>
<wap-provisioningdoc version="1.1">
        <characteristic type="APPLICATION">
              <parm name=”AppID” value=”ap2001”/>
              <parm name=”Name” value=”IMS Settings”/>
              <parm name=”AppRef” value=”IMS-Settings”/>
                    …  -- see section A.2.2
        </characteristic>
        <characteristic type="APPLICATION">
              <parm name=”AppID” value=”ap2002”/>
              <parm name=”Name” value=”RCS settings”/>
              <parm name=”AppRef” value=”RCSe-Settings”/>
              <characteristic type=”IMS”>
                    <parm name=”To-AppRef” value=”IMS-Settings”/>
              </characteristic>
              <characteristic type=”SERVICES”>
                    …       -- See section A.2.1
              </characteristic>
              <characteristic type=”PRESENCE”>
                    …       -- See section A.2.3
              </characteristic>
              <characteristic type=”XDMS”>
                    …       -- See section A.2.4
              </characteristic>
              <characteristic type=”SUPL”>
                    …       -- See section A.2.5
              </characteristic>
              <characteristic type=”IM”>
                    …       -- See section A.2.6
              </characteristic>
              <characteristic type=”CPM”>
                    …       -- See section A.2.7
              </characteristic>
              <characteristic type=”CAPDISCOVERY”>
                    …       -- See section A.2.8
              </characteristic>
              <characteristic type=”APN”>
                    …       -- See section A.2.9
              </characteristic>
              <characteristic type=”OTHER”>
                    …       -- See section A.2.10
              </characteristic>
              <characteristic type=”SERVICEPROVIDEREXT”>
                    …       -- See section A.2.11
              </characteristic>
        </characteristic>
</wap-provisioningdoc>
```

Table 183: Complete RCS HTTP configuration XML structure

[30] Please note the AppID’s used in the example are provided for reference only as they have not been reserved.

A.4. Autoconfiguration XML sample

```
<?xml version="1.0"?>
<wap-provisioningdoc version="1.1">
    <characteristic type="VERS">
        <parm name=”version” value=”1”/>
        <parm name=”validity” value=”1728000”/>
    </characteristic>
    <characteristic type="MSG">                  -- This section is OPTIONAL
        <parm name=”title” value=”Example”/>
        <parm name=”message” value=”Hello world”/>
        <parm name=”Accept_btn” value=”X”/>
        <parm name=”Reject_btn” value=”X”/>
    </characteristic>                            -- This section is OPTIONAL
    <characteristic type="APPLICATION">
        <parm name=”AppID” value=”ap2001”/>
        <parm name=”Name” value=”IMS Settings”/>
        <parm name=”AppRef” value=”IMS-Settings”/>
        <characteristic type=”ConRefs”>
            <parm name=”ConRef” value=”X”/>
        </characteristic>
        <parm name=”PDP_ContextOperPref” value=”X”/>
        <parm name=”Timer_T1” value=”X”/>
        <parm name=”Timer_T2” value=”X”/>
        <parm name=”Timer_T4” value=”X”/>
        <parm name=”Private_User_Identity” value=”X”/>
        <characteristic type=”Public_User_Identity_List”>
            <parm name=”Public_User_Identity” value=”X”/>
        </characteristic>
        <parm name=”Home_network_domain_name” value=”X”/>
        <characteristic type=”Ext”>
            <parm name=”NatUrlFmt” value=”1”/>
            <parm name=”IntUrlFmt” value=”1”/>
            <parm name=”Q-Value” value=”0.5”/>
            <characteristic type=”SecondaryDevicePar”>
                <parm name=”VoiceCall” value=”0”/>
                <parm name=”Chat” value=”0”/>
                <parm name=”SendSms” value=”0”/>
                <parm name=”SendMms” value=”0”/>
                <parm name=”FileTranfer” value=”0”/>
                <parm name=”VideoShare” value=”0”/>
                <parm name=”ImageShare” value=”0”/>
                <parm name=”VideoCall” value=”0”/>
                <parm name=”GeoLocPush” value=”0”/>
            </characteristic>
            <parm name=”MaxSizeImageShare” value=”0”/>
            <parm name=”MaxTimeVideoShare” value=”0”/>
            <characteristic type=”Ext”/>
        </characteristic>
        <characteristic type=”ICSI_List”>
            <parm name=”ICSI” value=”0”/>
            <parm name=”ICSI_Resource_Allocation_Mode” value=”X”/>
        </characteristic>
        <characteristic type=”LBO_P-CSCF_Address”>
            <parm name=”Address” value=”X”/>
            <parm name=”AddressType” value=”X”/>
        </characteristic>
        <parm name=”Voice_Domain_Preference_E_UTRAN” value=”X”/>
        <parm name=”SMS_Over_IP_Networks_Indication” value=”X”/>
        <parm name=”Keep_Alive_Enabled” value=”X”/>
        <parm name=”Voice_Domain_Preference_UTRAN” value=”X”/>
        <parm name=”Mobility_Management_IMS_Voice_Termination” value=”X”/>
        <parm name=”RegRetryBaseTime” value=”X”/>
        <parm name=”RegRetryMaxTime” value=”X”/>
-- Continues in the next table --
```

Table 184: Complete RCS autoconfiguration XML structure (1/4)

```
-- Follows from previous table –
        <characteristic type=”PhoneContext_List”>
            <parm name=”PhoneContext” value=”X”/>
            <parm name=”Public_User_Identity” value=”X”/>
        </characteristic>
        <characteristic type=”APPAUTH”>
            <parm name=”AuthType” value=”X”/>
            <parm name=”Realm” value=”X”/>
            <parm name=”UserName” value=”X”/>
            <parm name=”UserPwd” value=”X”/>
        </characteristic>
    </characteristic>
    <characteristic type="APPLICATION">
        <parm name=”AppID” value=”ap2002”/>
        <parm name=”Name” value=”RCS settings”/>
        <parm name=”AppRef” value=”RCSe-Settings”/>
        <characteristic type=”IMS”>
            <parm name=”To-AppRef” value=”IMS-Settings”/>
        </characteristic>
        <characteristic type=”SERVICES”>
            <parm name=”presencePrfl” value=”X”/>
            <parm name=”ChatAuth” value=”X”/>
            <parm name=”ftAuth” value=”X”/>
            <parm name=”standaloneMsgAuth” value=”X”/>
            <parm name=”geolocPullAuth” value=”X”/>
            <parm name=”geolocPushAuth” value=”X”/>
            <parm name=”vsAuth” value=”X”/>
            <parm name=”isAuth” value=”X”/>
            <parm name=”ipVideoCallAuth” value=”X”/>
            <characteristic type=”Ext”/>
        </characteristic>
        <characteristic type=”PRESENCE”>
            <parm name=”AvailabilityAuth” value=”X”/>
            <characteristic type=”FAVLINK”>
                <parm name=”AutMa” value=”X”/>
                <characteristic type=”LINKS”>
                    <parm name=” OpFavUrl1” value=”X”/>
                    <parm name=” OpFavUrl2” value=”X”/>
                    <parm name=” OpFavUrl3” value=”X”/>
                </characteristic>
                <parm name=”LabelMaxLength” value=”X”/>
            </characteristic>
            <parm name=”IconMaxSize” value=”X”/>
            <parm name=”NoteMaxSize” value=”X”/>
            <characteristic type=”VIPCONTACTS”>
                <parm name=”NonVipPollPeriodSetting” value=”X”/>
                <parm name=”NonVipMaxPollPerPeriod” value=”X”/>
            </characteristic>
            <parm name=”PublishTimer” value=”X”/>
            <parm name=”NickNameLength” value=”X”/>
            <characteristic type=”Location”>
                <parm name=”TextMaxLength” value=”X”/>
                <parm name=”LocInfoMaxValidTime” value=”X”/>
            </characteristic>
            <characteristic type=”Ext”/>
            <parm name=”client-obj-datalimit” value=”X”/>
            <parm name=”content-serveruri” value=”X”/>
            <parm name=”source-throttlepublish” value=”X”/>
            <parm name=”max-number-ofsubscriptions-inpresence-list” value=”X”/>
            <parm name=”service-uritemplate” value=”X”/>
            <parm name=”RLS-URI” value=”X”/>
        </characteristic>
-- Continues in the next table --
```

Table 185: Complete RCS autoconfiguration XML structure (2/4)

```
-- Follows from previous table –
            <characteristic type=”XDMS”>
                <parm name=”RevokeTimer” value=”X”/>
                <characteristic type=”Ext”/>
                <parm name=”XCAPRootURI” value=”X”/>
                <parm name=”XCAPAuthenticationUserName” value=”X”/>
                <parm name=”XCAPAuthenticationSecret” value=”X”/>
                <parm name=”XCAPAuthenticationType” value=”X”/>
            </characteristic>
            <characteristic type=”SUPL”>
                <parm name=”TextMaxLength” value=”X”/>
                <parm name=”LocInfoMaxValidTime” value=”X”/>
                <characteristic type=”Ext”/>
                <parm name=”Addr” value=”X”/>
                <parm name=”AddrType” value=”X”/>
            </characteristic>
            <characteristic type=”IM”>
                <parm name=”imMsgTech” value=”X”/>
                <parm name=”imCapAlwaysON” value=”X”/>
                <parm name=”imWarnSF” value=”X”/>
                <parm name=”SmsFallBackAuth” value=”X”/>
                <parm name=”imCapNonRCS” value=”X”/>
                <parm name=”imWarnIW” value=”X”/>
                <parm name=”AutAccept” value=”X”/>
                <parm name=”imSessionStart” value=”X”/>
                <parm name=”AutAcceptGroupChat” value=”X”/>
                <parm name=”firstMessageInvite” value=”X”/>
                <parm name=”TimerIdle” value=”X”/>
                <parm name=”MaxConcurrentSession” value=”X”/>
                <parm name=”multiMediaChat” value=”X”/>
                <parm name=”MaxSize1to1” value=”X”/>
                <parm name=”MaxSize1toM” value=”X”/>
                <parm name=”MaxSizeFileTr” value=”X”/>
                <parm name=”ftWarnSize” value=”X”/>
                <characteristic type=”Ext”/>
                <parm name=”pres-srv-cap” value=”X”/>
                <parm name=”deferred-msg-func-uri” value=”X”/>
                <parm name=”max_adhoc_group_size” value=”X”/>
                <parm name=”conf-fcty-uri” value=”X”/>
                <parm name=”exploder-uri” value=”X”/>
            </characteristic>
            <characteristic type=”CPM”>
                <characteristic type=”StandaloneMsg”>
                        <parm name=”MaxSizeStandalone” value=”X”/>
                </characteristic>
                <characteristic type=”MessageStore”>
                        <parm name=”Url” value=”X”/>
                        <parm name=”AuthProt” value=”X”/>
                        <parm name=”UserName” value=”X”/>
                        <parm name=”UserPwd” value=”X”/>
                </characteristic>
                <characteristic type=”Ext”/>
            </characteristic>
            <characteristic type=”CAPDISCOVERY”>
                <parm name=”pollingPeriod” value=”X”/>
                <parm name=”pollingRate” value=”X”/>
                <parm name=”pollingRatePeriod” value=”X”/>
                <parm name=”capInfoExpiry” value=”X”/>
                <parm name=”defaultDisc” value=”X”/>
                <parm name=”capDiscCommonStack” value=”X”/>
                <characteristic type=”Ext”/>
            </characteristic>
-- Continues in the next table -
```

Table 186: Complete RCS autoconfiguration XML structure (3/4)

```
-- Follows from previous table –
            <characteristic type=”APN”>
                <parm name=”rcseOnlyAPN” value=”X”/>
                <parm name=”enableRcseSwitch” value=”X”/>
                <characteristic type=”EXT”/>
            </characteristic>
            <characteristic type=”OTHER”>
                <parm name=”endUserConfReqId” value=”X”/>
                <parm name=”allowVSSave” value=”X”/>
                <characteristic type=” transportProto”>
                        <parm name=”psSignalling” value=”X”/>
                        <parm name=”psMedia” value=”X”/>
                        <parm name=”psRTMedia” value=”X”/>
                        <parm name=”wifiSignalling” value=”X”/>
                        <parm name=”wifiMedia” value=”X”/>
                        <parm name=”wifiRTMedia” value=”X”/>
                </characteristic>
                <parm name=”uuid_Value” value=”X”/>
                <characteristic type=”Ext”/>
            </characteristic>
            <characteristic type=”SERVICEPROVIDEREXT”/>
      </characteristic>
</wap-provisioningdoc>
```

Table 187: Complete RCS autoconfiguration XML structure (4/4)

Annex B: Additional diagrams

B.1. Chat and store and forward diagrams without Auto-Accept

B.1.1. Chat without store and forward

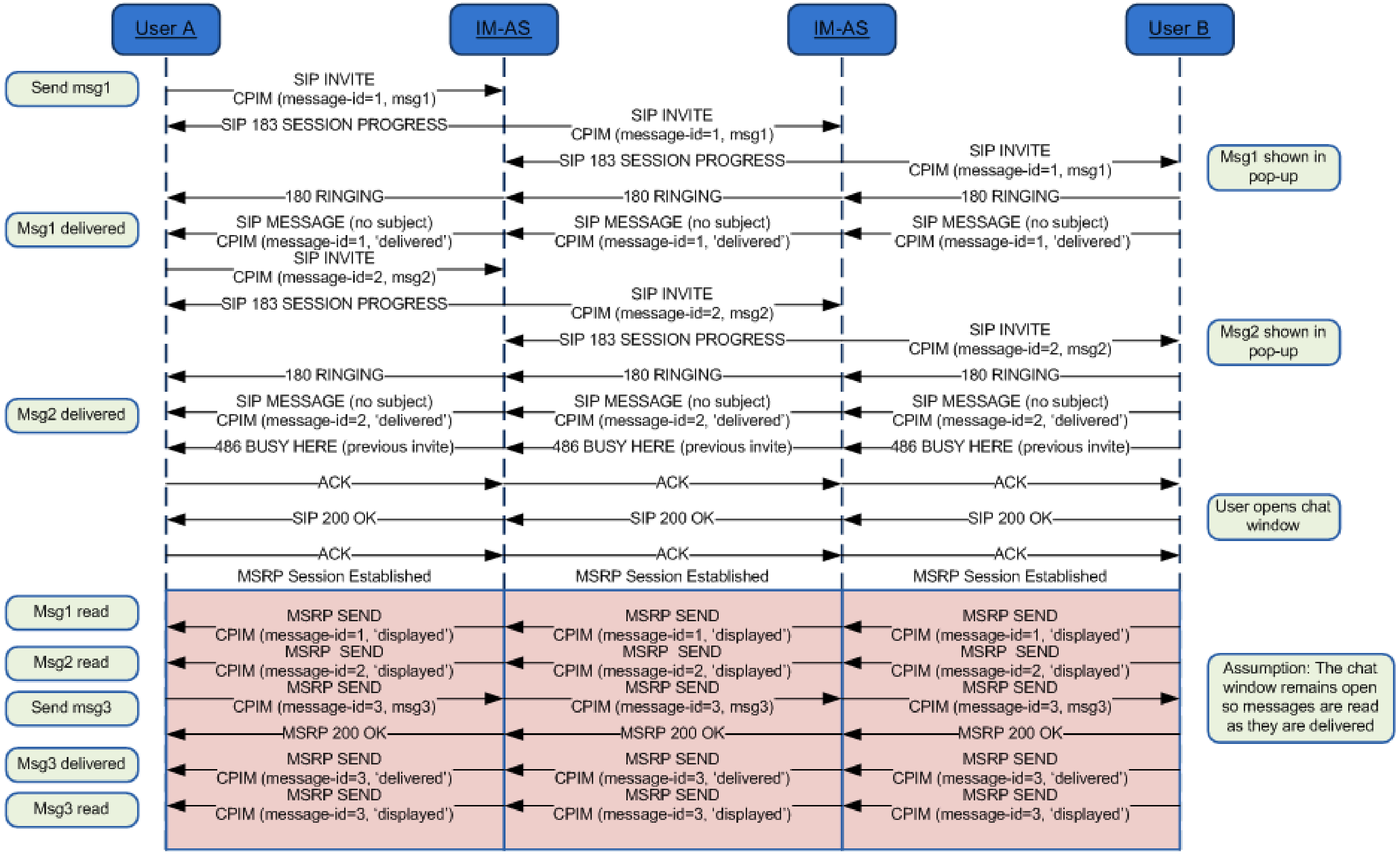

User A
IM-AS
IM-AS
User B
Send msg1
SIP INVITE
CPIM (message-id=1, msg1)
SIP 183 SESSION PROGRESS
SIP INVITE
CPIM (message-id=1, msg1)
SIP 183 SESSION PROGRESS
SIP INVITE
CPIM (message-id=1, msg1)
Msg1 shown in pop-up
180 RINGING
180 RINGING
180 RINGING
Msg1 delivered
SIP MESSAGE (no subject)
CPIM (message-id=1, 'delivered')
SIP MESSAGE (no subject)
CPIM (message-id=1, 'delivered')
SIP MESSAGE (no subject)
CPIM (message-id=1, 'delivered')
SIP INVITE
CPIM (message-id=2, msg2)
SIP 183 SESSION PROGRESS
SIP INVITE
CPIM (message-id=2, msg2)
SIP 183 SESSION PROGRESS
SIP INVITE
CPIM (message-id=2, msg2)
Msg2 shown in pop-up
180 RINGING
180 RINGING
180 RINGING
Msg2 delivered
SIP MESSAGE (no subject)
CPIM (message-id=2, 'delivered')
SIP MESSAGE (no subject)
CPIM (message-id=2, 'delivered')
SIP MESSAGE (no subject)
CPIM (message-id=2, 'delivered')
486 BUSY HERE (previous invite)
486 BUSY HERE (previous invite)
486 BUSY HERE (previous invite)
ACK
ACK
ACK
User opens chat window
SIP 200 OK
SIP 200 OK
SIP 200 OK
ACK
ACK
ACK
MSRP Session Established
MSRP Session Established
MSRP Session Established
Msg1 read
MSRP SEND
CPIM (message-id=1, 'displayed')
MSRP SEND
CPIM (message-id=1, 'displayed')
MSRP SEND
CPIM (message-id=1, 'displayed')
Msg2 read
MSRP SEND
CPIM (message-id=2, 'displayed')
MSRP SEND
CPIM (message-id=2, 'displayed')
MSRP SEND
CPIM (message-id=2, 'displayed')
Assumption: The chat window remains open so messages are read as they are delivered
Send msg3
MSRP SEND
CPIM (message-id=3, msg3)
MSRP SEND
CPIM (message-id=3, msg3)
MSRP SEND
CPIM (message-id=3, msg3)
MSRP 200 OK
MSRP 200 OK
MSRP 200 OK
Msg3 delivered
MSRP SEND
CPIM (message-id=3, 'delivered')
MSRP SEND
CPIM (message-id=3, 'delivered')
MSRP SEND
CPIM (message-id=3, 'delivered')
Msg3 read
MSRP SEND
CPIM (message-id=3, 'displayed')
MSRP SEND
CPIM (message-id=3, 'displayed')
MSRP SEND
CPIM (message-id=3, 'displayed')

Figure 113: Chat flow without store and forward *

*: Check NOTE 1 and 15 in section B.1.14

B.1.2. Store and forward: Receiver offline

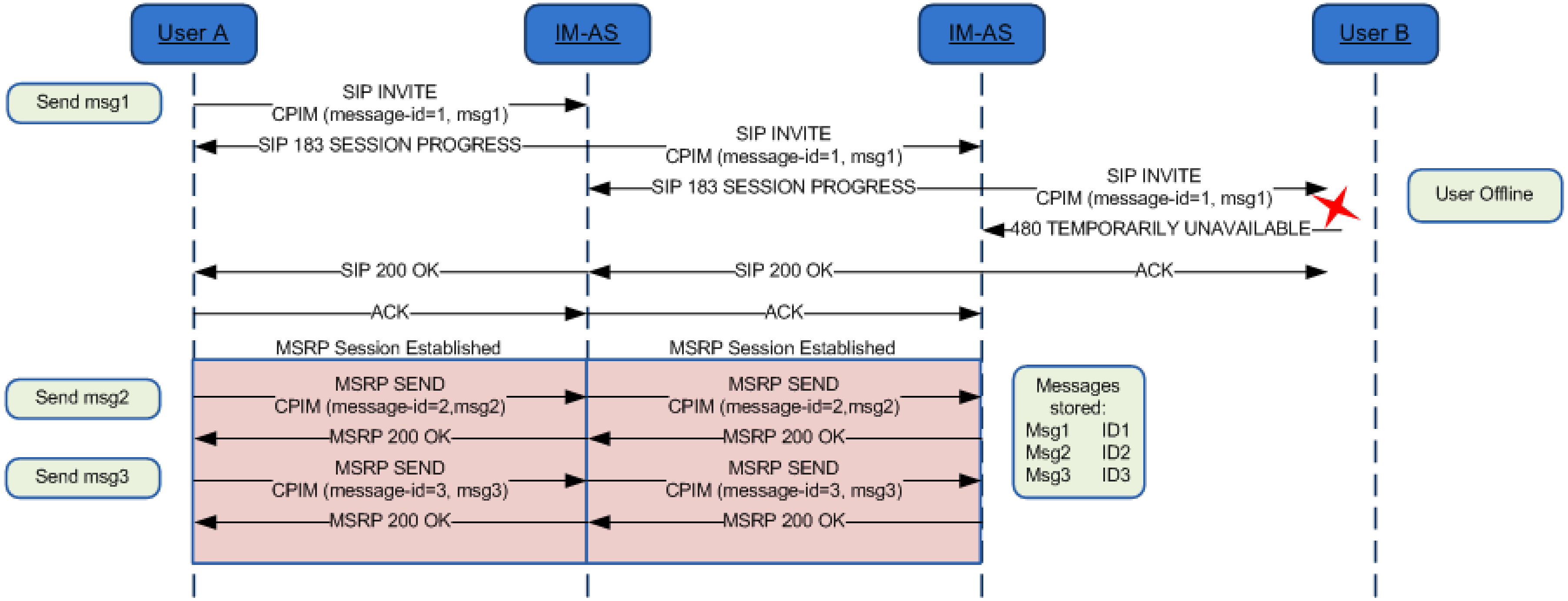


Figure 114: Store and forward: Receiver offline*

*: Check NOTE 1, 6 and 15 in section B.1.14

B.1.3. Store and forward: Message deferred delivery with sender still on an active Chat session

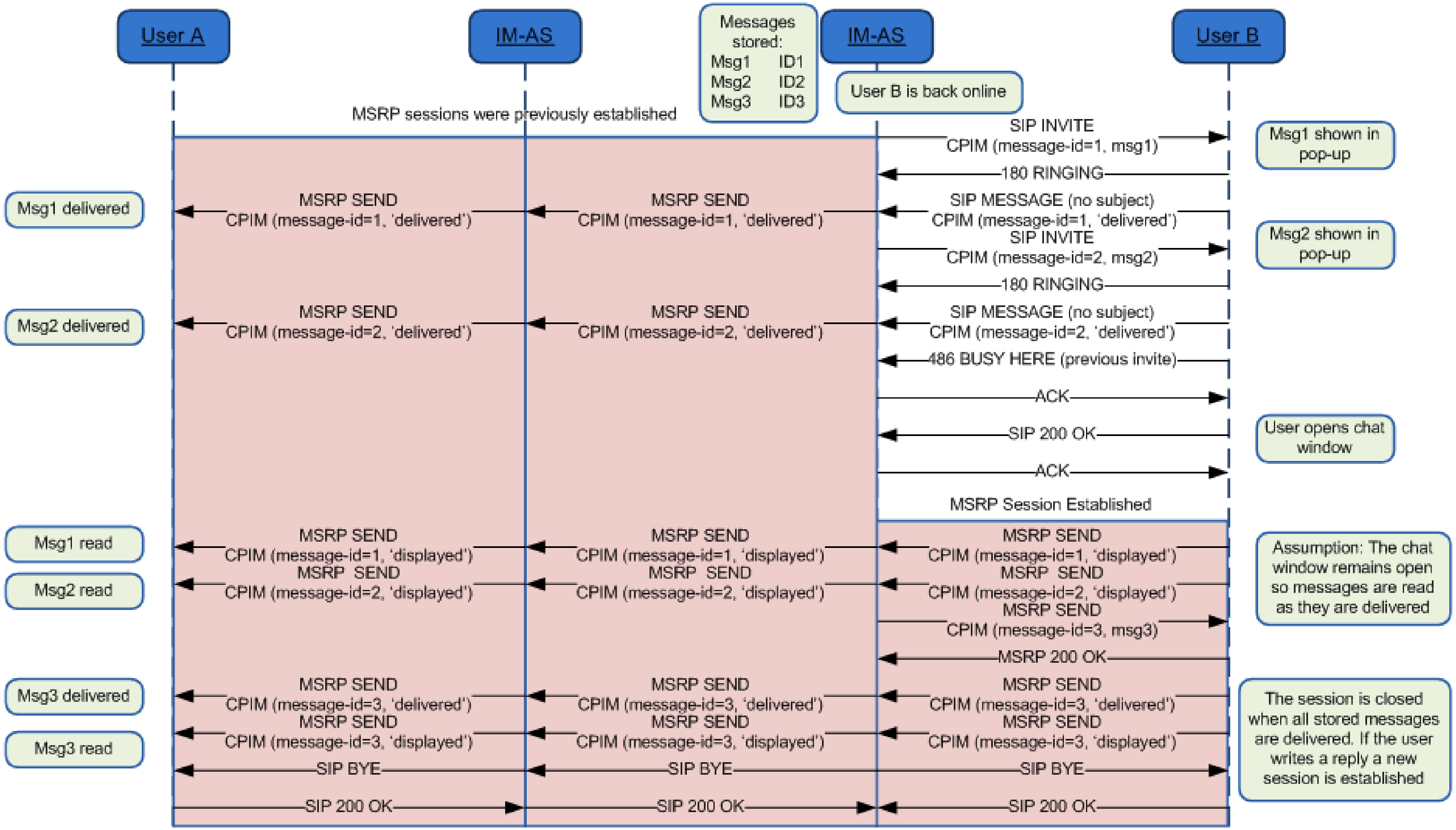

User A
IM-AS
Messages stored:
Msg1 ID1
Msg2 ID2
Msg3 ID3
IM-AS
User B
User B is back online
MSRP sessions were previously established
SIP INVITE
CPIM (message-id=1, msg1)
Msg1 shown in pop-up
180 RINGING
Msg1 delivered
MSRP SEND
CPIM (message-id=1, 'delivered')
MSRP SEND
CPIM (message-id=1, 'delivered')
SIP MESSAGE (no subject)
CPIM (message-id=1, 'delivered')
SIP INVITE
CPIM (message-id=2, msg2)
Msg2 shown in pop-up
180 RINGING
Msg2 delivered
MSRP SEND
CPIM (message-id=2, 'delivered')
MSRP SEND
CPIM (message-id=2, 'delivered')
SIP MESSAGE (no subject)
CPIM (message-id=2, 'delivered')
486 BUSY HERE (previous invite)
ACK
SIP 200 OK
User opens chat window
ACK
MSRP Session Established
Msg1 read
MSRP SEND
CPIM (message-id=1, 'displayed')
MSRP SEND
CPIM (message-id=1, 'displayed')
MSRP SEND
CPIM (message-id=1, 'displayed')
Assumption: The chat window remains open so messages are read as they are delivered
Msg2 read
MSRP SEND
CPIM (message-id=2, 'displayed')
MSRP SEND
CPIM (message-id=2, 'displayed')
MSRP SEND
CPIM (message-id=2, 'displayed')
MSRP SEND
CPIM (message-id=3, msg3)
MSRP 200 OK
Msg3 delivered
MSRP SEND
CPIM (message-id=3, 'delivered')
MSRP SEND
CPIM (message-id=3, 'delivered')
MSRP SEND
CPIM (message-id=3, 'delivered')
The session is closed when all stored messages are delivered. If the user writes a reply a new session is established
Msg3 read
MSRP SEND
CPIM (message-id=3, 'displayed')
MSRP SEND
CPIM (message-id=3, 'displayed')
MSRP SEND
CPIM (message-id=3, 'displayed')
SIP BYE
SIP BYE
SIP BYE
SIP 200 OK
SIP 200 OK
SIP 200 OK

Figure 115: Store and forward: Message(s) deferred delivery with a sender still on an MSRP session*

*: Check NOTES 1, 2, 4, 7, 11 and 15 in section B.1.14

B.1.4. Store and forward: Message deferred delivery with sender online

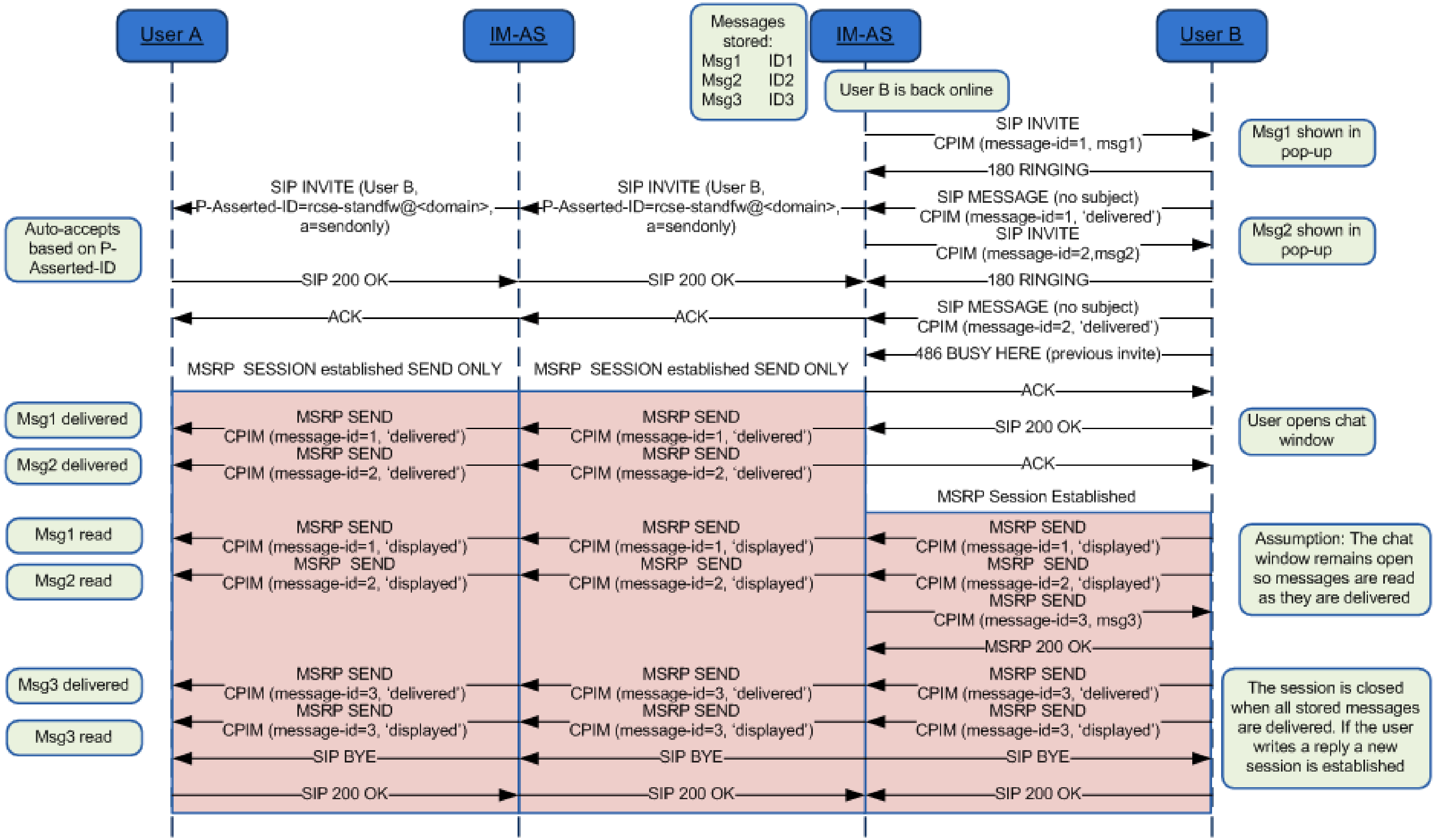

User A
IM-AS
Messages stored:
Msg1 ID1
Msg2 ID2
Msg3 ID3
IM-AS
User B
User B is back online
SIP INVITE
CPIM (message-id=1, msg1)
Msg1 shown in pop-up
180 RINGING
SIP INVITE (User B, P-Asserted-ID=rcse-standfw@<domain>, a=sendonly)
SIP INVITE (User B, P-Asserted-ID=rcse-standfw@<domain>, a=sendonly)
SIP MESSAGE (no subject)
CPIM (message-id=1, 'delivered')
Auto-accepts based on P-Asserted-ID
SIP INVITE
CPIM (message-id=2,msg2)
Msg2 shown in pop-up
SIP 200 OK
SIP 200 OK
180 RINGING
ACK
ACK
SIP MESSAGE (no subject)
CPIM (message-id=2, 'delivered')
486 BUSY HERE (previous invite)
MSRP SESSION established SEND ONLY
MSRP SESSION established SEND ONLY
ACK
Msg1 delivered
MSRP SEND
CPIM (message-id=1, 'delivered')
MSRP SEND
CPIM (message-id=1, 'delivered')
SIP 200 OK
User opens chat window
Msg2 delivered
MSRP SEND
CPIM (message-id=2, 'delivered')
MSRP SEND
CPIM (message-id=2, 'delivered')
ACK
MSRP Session Established
Msg1 read
MSRP SEND
CPIM (message-id=1, 'displayed')
MSRP SEND
CPIM (message-id=1, 'displayed')
MSRP SEND
CPIM (message-id=1, 'displayed')
Assumption: The chat window remains open so messages are read as they are delivered
Msg2 read
MSRP SEND
CPIM (message-id=2, 'displayed')
MSRP SEND
CPIM (message-id=2, 'displayed')
MSRP SEND
CPIM (message-id=2, 'displayed')
MSRP SEND
CPIM (message-id=3, msg3)
MSRP 200 OK
Msg3 delivered
MSRP SEND
CPIM (message-id=3, 'delivered')
MSRP SEND
CPIM (message-id=3, 'delivered')
MSRP SEND
CPIM (message-id=3, 'delivered')
The session is closed when all stored messages are delivered. If the user writes a reply a new session is established
Msg3 read
MSRP SEND
CPIM (message-id=3, 'displayed')
MSRP SEND
CPIM (message-id=3, 'displayed')
MSRP SEND
CPIM (message-id=3, 'displayed')
SIP BYE
SIP BYE
SIP BYE
SIP 200 OK
SIP 200 OK
SIP 200 OK

Figure 116: Store and forward: Message deferred delivery with sender online *

*: Check NOTES 1, 3, 4, 5, 7, 11, 14 and 15 in section B.1.14

B.1.5. Store and forward: Message deferred delivery with sender offline (delivery notifications)

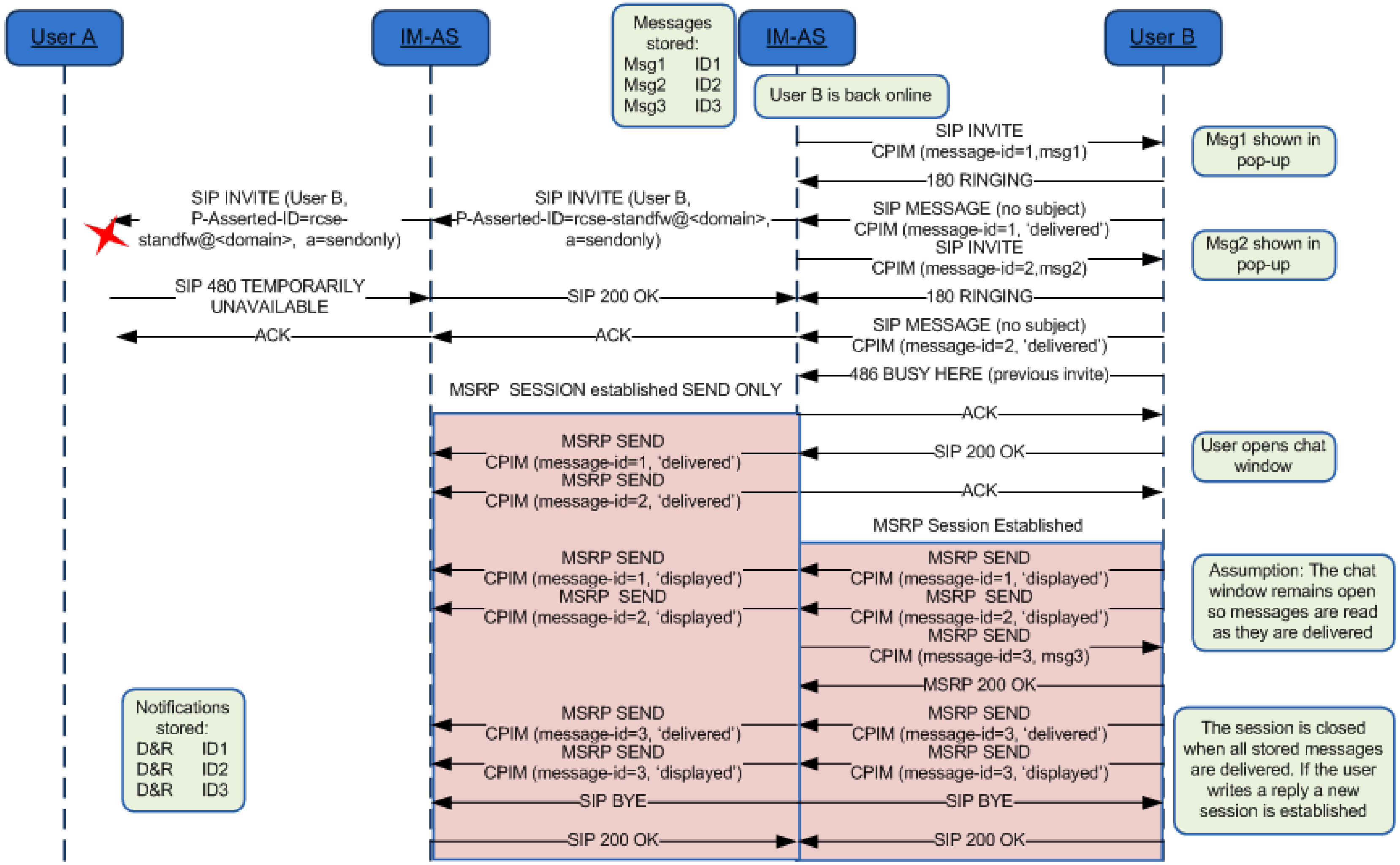

User A
IM-AS
Messages stored:
Msg1 ID1
Msg2 ID2
Msg3 ID3
IM-AS
User B
User B is back online
SIP INVITE CPIM (message-id=1,msg1)
Msg1 shown in pop-up
180 RINGING
SIP INVITE (User B, P-Asserted-ID=rcse-standfw@<domain>, a=sendonly)
SIP INVITE (User B, P-Asserted-ID=rcse-standfw@<domain>, a=sendonly)
SIP MESSAGE (no subject) CPIM (message-id=1, 'delivered')
SIP INVITE CPIM (message-id=2,msg2)
Msg2 shown in pop-up
SIP 480 TEMPORARILY UNAVAILABLE
SIP 200 OK
180 RINGING
ACK
ACK
SIP MESSAGE (no subject) CPIM (message-id=2, 'delivered')
486 BUSY HERE (previous invite)
MSRP SESSION established SEND ONLY
ACK
MSRP SEND CPIM (message-id=1, 'delivered')
SIP 200 OK
User opens chat window
MSRP SEND CPIM (message-id=2, 'delivered')
ACK
MSRP Session Established
MSRP SEND CPIM (message-id=1, 'displayed')
MSRP SEND CPIM (message-id=1, 'displayed')
Assumption: The chat window remains open so messages are read as they are delivered
MSRP SEND CPIM (message-id=2, 'displayed')
MSRP SEND CPIM (message-id=2, 'displayed')
MSRP SEND CPIM (message-id=3, msg3)
MSRP 200 OK
Notifications stored:
D&R ID1
D&R ID2
D&R ID3
MSRP SEND CPIM (message-id=3, 'delivered')
MSRP SEND CPIM (message-id=3, 'delivered')
The session is closed when all stored messages are delivered. If the user writes a reply a new session is established
MSRP SEND CPIM (message-id=3, 'displayed')
MSRP SEND CPIM (message-id=3, 'displayed')
SIP BYE
SIP BYE
SIP 200 OK
SIP 200 OK

Figure 117: Store and forward: Message(s) deferred delivery with a sender offline (delivery notifications)*

*: Check NOTE 1, 5, 7, 11, 14 and 15 in section B.1.14

B.1.6. Store and forward: Notifications deferred delivery

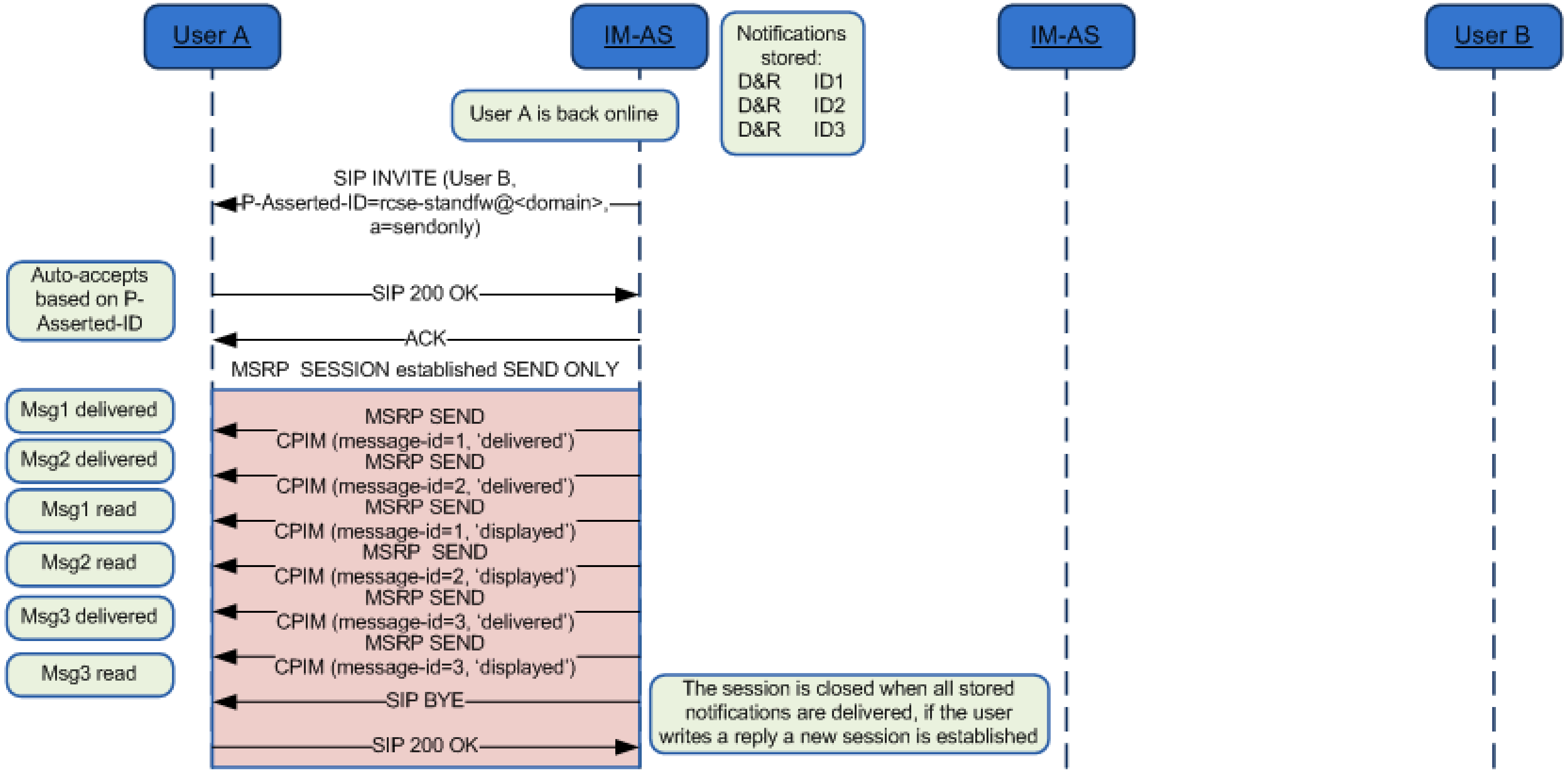

User A
IM-AS
Notifications stored:
D&R ID1
D&R ID2
D&R ID3
IM-AS
User B
User A is back online
SIP INVITE (User B, P-Asserted-ID=rcse-standfw@<domain>, a=sendonly)
Auto-accepts based on P-Asserted-ID
SIP 200 OK
ACK
MSRP SESSION established SEND ONLY
Msg1 delivered
MSRP SEND CPIM (message-id=1, 'delivered')
Msg2 delivered
MSRP SEND CPIM (message-id=2, 'delivered')
Msg1 read
MSRP SEND CPIM (message-id=1, 'displayed')
Msg2 read
MSRP SEND CPIM (message-id=2, 'displayed')
Msg3 delivered
MSRP SEND CPIM (message-id=3, 'delivered')
Msg3 read
MSRP SEND CPIM (message-id=3, 'displayed')
SIP BYE
SIP 200 OK
The session is closed when all stored notifications are delivered, if the user writes a reply a new session is established

Figure 118: Store and forward: Notification(s) deferred delivery*

*: Check NOTES 1, 4, 5, 11, 14 and 15 in section B.1.14

B.1.7. Delivery of displayed notifications in an unanswered chat (without store and forward)

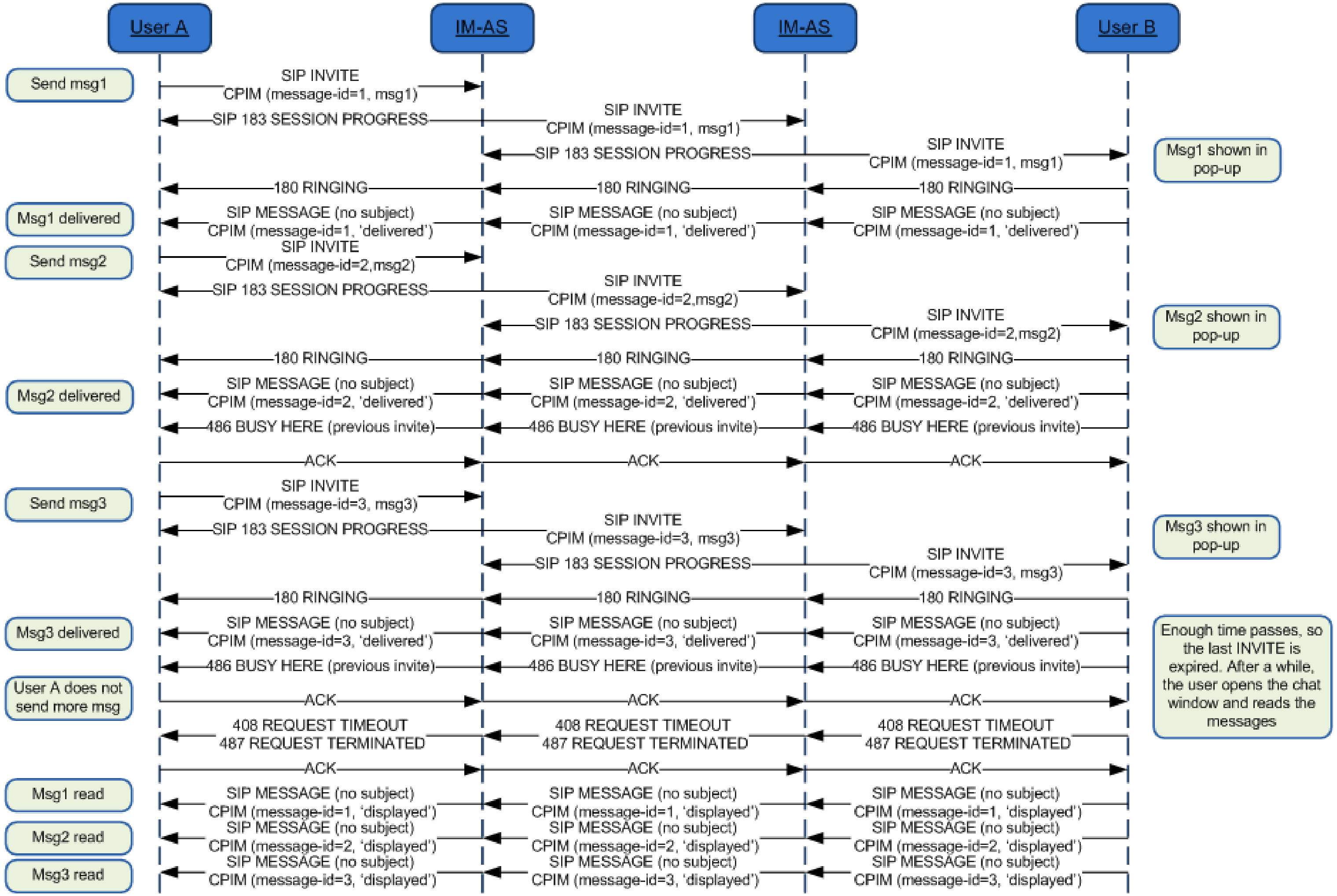

User A
IM-AS
IM-AS
User B
Send msg1
SIP INVITE CPIM (message-id=1, msg1)
SIP 183 SESSION PROGRESS
SIP INVITE CPIM (message-id=1, msg1)
SIP 183 SESSION PROGRESS
SIP INVITE CPIM (message-id=1, msg1)
Msg1 shown in pop-up
180 RINGING
180 RINGING
180 RINGING
Msg1 delivered
SIP MESSAGE (no subject) CPIM (message-id=1, 'delivered')
SIP MESSAGE (no subject) CPIM (message-id=1, 'delivered')
SIP MESSAGE (no subject) CPIM (message-id=1, 'delivered')
Send msg2
SIP INVITE CPIM (message-id=2,msg2)
SIP 183 SESSION PROGRESS
SIP INVITE CPIM (message-id=2,msg2)
SIP 183 SESSION PROGRESS
SIP INVITE CPIM (message-id=2,msg2)
Msg2 shown in pop-up
180 RINGING
180 RINGING
180 RINGING
Msg2 delivered
SIP MESSAGE (no subject) CPIM (message-id=2, 'delivered')
SIP MESSAGE (no subject) CPIM (message-id=2, 'delivered')
SIP MESSAGE (no subject) CPIM (message-id=2, 'delivered')
486 BUSY HERE (previous invite)
486 BUSY HERE (previous invite)
486 BUSY HERE (previous invite)
ACK
ACK
ACK
Send msg3
SIP INVITE CPIM (message-id=3, msg3)
SIP 183 SESSION PROGRESS
SIP INVITE CPIM (message-id=3, msg3)
SIP 183 SESSION PROGRESS
SIP INVITE CPIM (message-id=3, msg3)
Msg3 shown in pop-up
180 RINGING
180 RINGING
180 RINGING
Msg3 delivered
SIP MESSAGE (no subject) CPIM (message-id=3, 'delivered')
SIP MESSAGE (no subject) CPIM (message-id=3, 'delivered')
SIP MESSAGE (no subject) CPIM (message-id=3, 'delivered')
Enough time passes, so the last INVITE is expired. After a while, the user opens the chat window and reads the messages
486 BUSY HERE (previous invite)
486 BUSY HERE (previous invite)
486 BUSY HERE (previous invite)
User A does not send more msg
ACK
ACK
ACK
408 REQUEST TIMEOUT 487 REQUEST TERMINATED
408 REQUEST TIMEOUT 487 REQUEST TERMINATED
408 REQUEST TIMEOUT 487 REQUEST TERMINATED
ACK
ACK
ACK
Msg1 read
SIP MESSAGE (no subject) CPIM (message-id=1, 'displayed')
SIP MESSAGE (no subject) CPIM (message-id=1, 'displayed')
SIP MESSAGE (no subject) CPIM (message-id=1, 'displayed')
Msg2 read
SIP MESSAGE (no subject) CPIM (message-id=2, 'displayed')
SIP MESSAGE (no subject) CPIM (message-id=2, 'displayed')
SIP MESSAGE (no subject) CPIM (message-id=2, 'displayed')
Msg3 read
SIP MESSAGE (no subject) CPIM (message-id=3, 'displayed')
SIP MESSAGE (no subject) CPIM (message-id=3, 'displayed')
SIP MESSAGE (no subject) CPIM (message-id=3, 'displayed')

Figure 119: Delivery of displayed notifications in an unanswered chat (without store and forward)*

*: Check NOTE 1, 10 and 15 in section B.1.14

B.1.8. Store and forward: Handling errors in the receiver's side

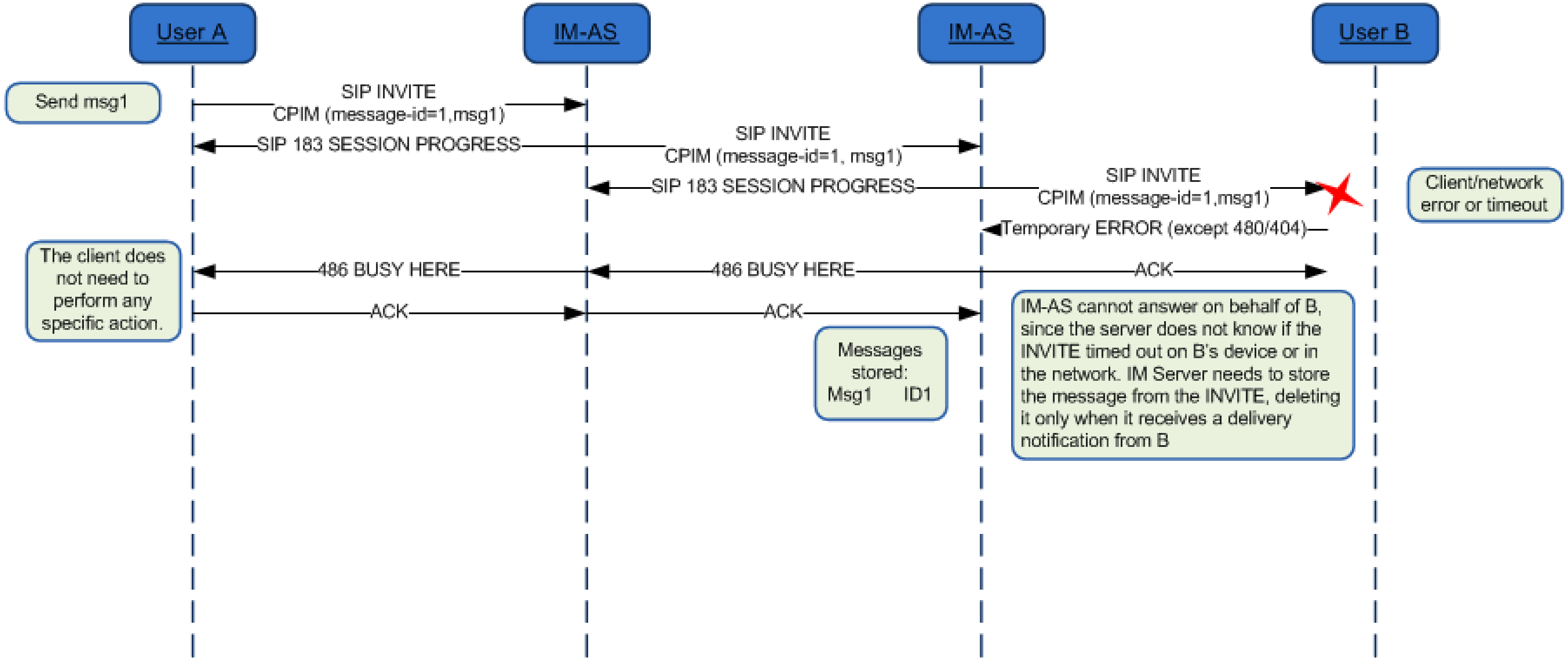

User A
IM-AS
IM-AS
User B
Send msg1
SIP INVITE
CPIM (message-id=1,msg1)
SIP 183 SESSION PROGRESS
SIP INVITE
CPIM (message-id=1, msg1)
SIP 183 SESSION PROGRESS
SIP INVITE
CPIM (message-id=1,msg1)
Client/network error or timeout
Temporary ERROR (except 480/404)
The client does not need to perform any specific action.
486 BUSY HERE
486 BUSY HERE
ACK
ACK
ACK
Messages stored:
Msg1 ID1
IM-AS cannot answer on behalf of B, since the server does not know if the INVITE timed out on B's device or in the network. IM Server needs to store the message from the INVITE, deleting it only when it receives a delivery notification from B

Figure 120: Store and forward: Handling errors in the receiver's side*

*: Check NOTE 15 in section B.1.14

Note: The error messages that are mapped to 486 Busy Here are listed in Table 37.

Also on the path between the IM-ASs (Instant Messaging Application Server i.e. the Messaging Server) similar errors could occur. In that case if the originating Messaging Server supports Store and Forward, it will behave in the same way and store the message.

B.1.9. Race conditions: Simultaneous INVITEs

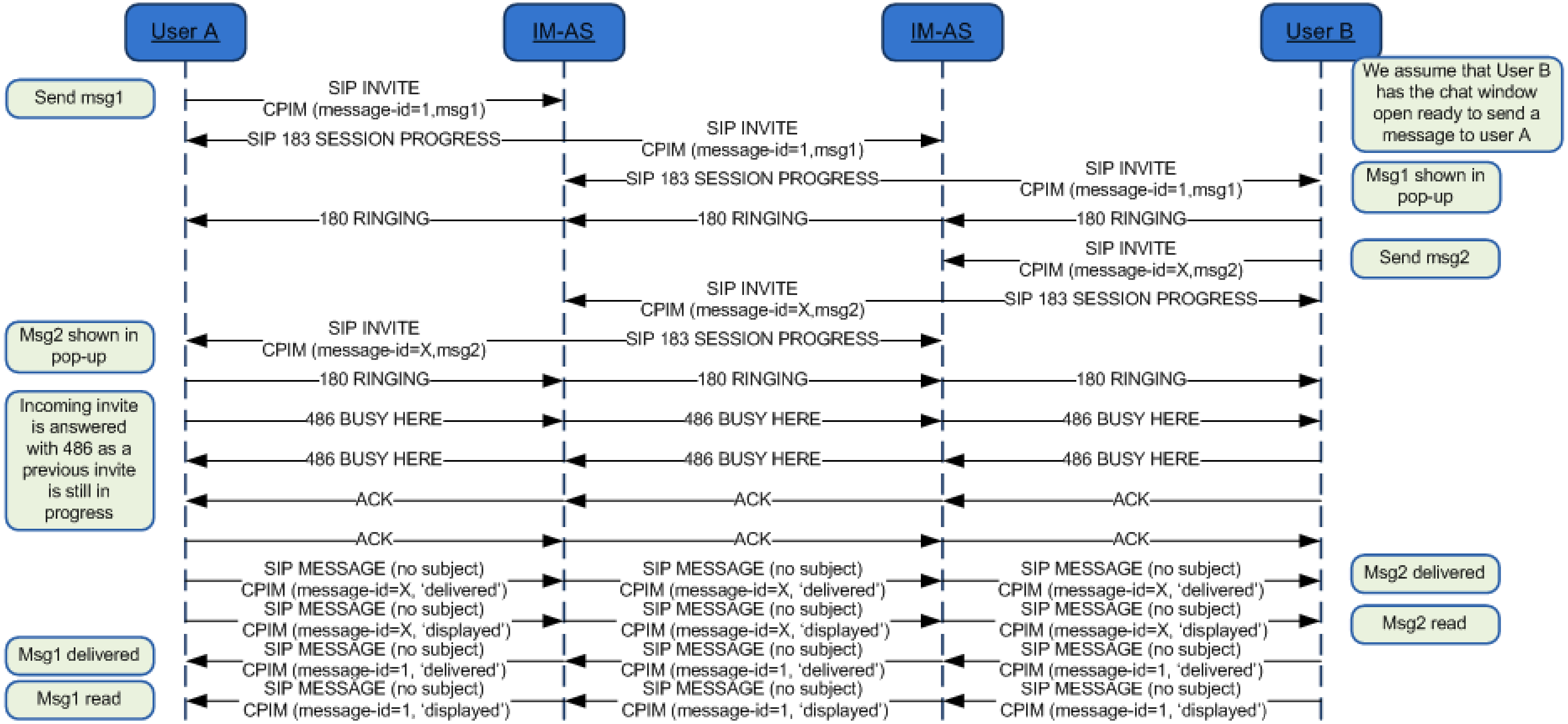

User A
IM-AS
IM-AS
User B
We assume that User B has the chat window open ready to send a message to user A
Send msg1
SIP INVITE CPIM (message-id=1,msg1)
SIP 183 SESSION PROGRESS
SIP INVITE CPIM (message-id=1,msg1)
SIP 183 SESSION PROGRESS
SIP INVITE CPIM (message-id=1,msg1)
Msg1 shown in pop-up
180 RINGING
180 RINGING
180 RINGING
SIP INVITE CPIM (message-id=X,msg2)
Send msg2
SIP INVITE CPIM (message-id=X,msg2)
SIP 183 SESSION PROGRESS
Msg2 shown in pop-up
SIP INVITE CPIM (message-id=X,msg2)
SIP 183 SESSION PROGRESS
180 RINGING
180 RINGING
180 RINGING
Incoming invite is answered with 486 as a previous invite is still in progress
486 BUSY HERE
486 BUSY HERE
486 BUSY HERE
486 BUSY HERE
486 BUSY HERE
486 BUSY HERE
ACK
ACK
ACK
ACK
ACK
ACK
SIP MESSAGE (no subject) CPIM (message-id=X, 'delivered')
SIP MESSAGE (no subject) CPIM (message-id=X, 'delivered')
SIP MESSAGE (no subject) CPIM (message-id=X, 'delivered')
Msg2 delivered
SIP MESSAGE (no subject) CPIM (message-id=X, 'displayed')
SIP MESSAGE (no subject) CPIM (message-id=X, 'displayed')
SIP MESSAGE (no subject) CPIM (message-id=X, 'displayed')
Msg2 read
Msg1 delivered
SIP MESSAGE (no subject) CPIM (message-id=1, 'delivered')
SIP MESSAGE (no subject) CPIM (message-id=1, 'delivered')
SIP MESSAGE (no subject) CPIM (message-id=1, 'delivered')
Msg1 read
SIP MESSAGE (no subject) CPIM (message-id=1, 'displayed')
SIP MESSAGE (no subject) CPIM (message-id=1, 'displayed')
SIP MESSAGE (no subject) CPIM (message-id=1, 'displayed')

Figure 121: Store and forward race conditions: Simultaneous INVITEs*

*: Check NOTE 1 and 15 in section B.1.14

B.1.10. Race conditions: New INVITE after a session is accepted

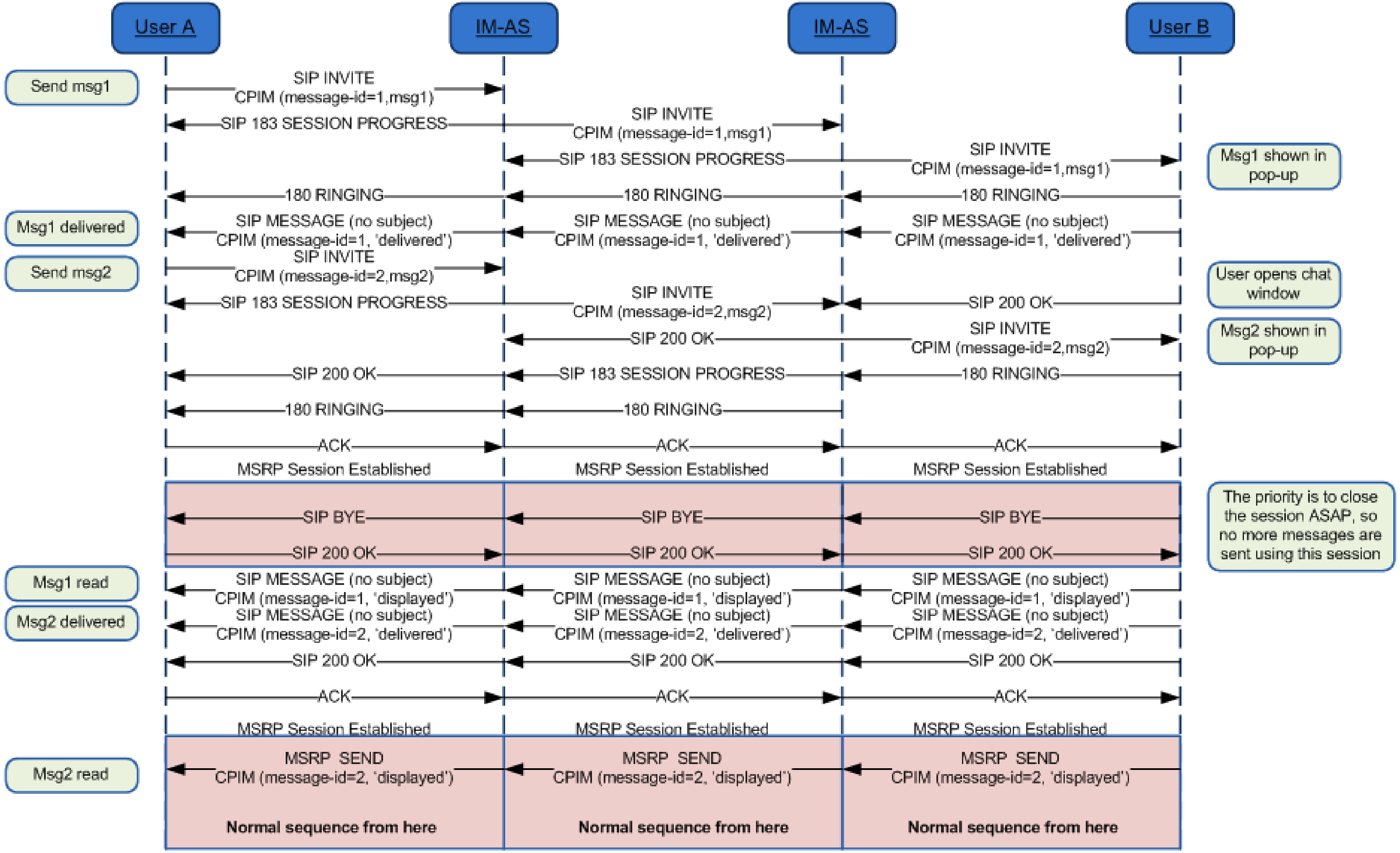


Figure 122: Store and forward race conditions: New INVITE after a session is accepted*

*: Check NOTE 1 and 15 in section B.1.14

B.1.11. Store and forward: Message(s) displayed notifications via SIP MESSAGE with sender offline

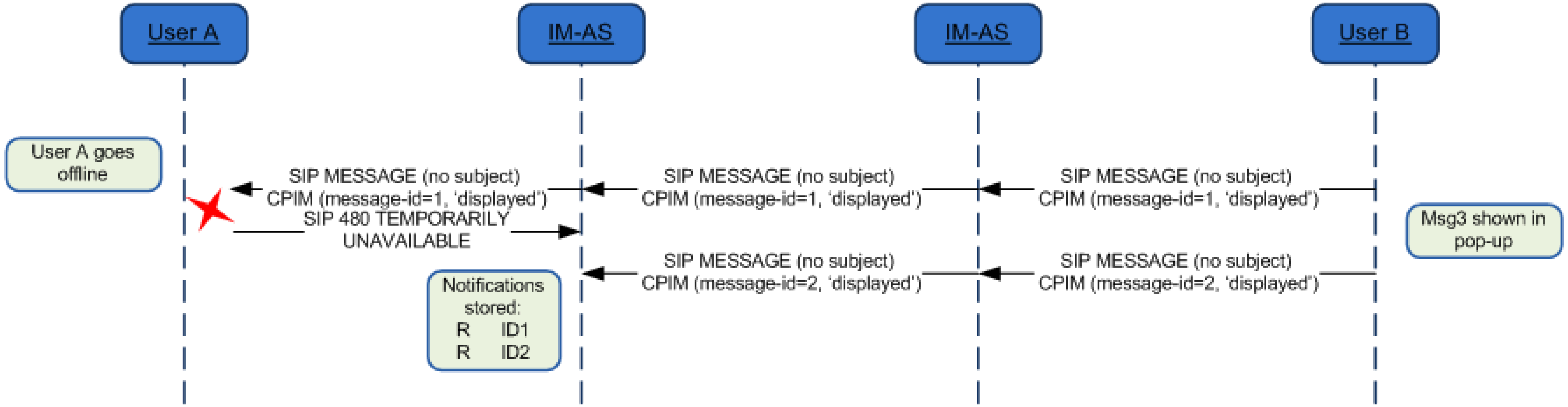

User A
IM-AS
IM-AS
User B
User A goes offline
SIP MESSAGE (no subject) CPIM (message-id=1, 'displayed')
SIP MESSAGE (no subject) CPIM (message-id=1, 'displayed')
SIP MESSAGE (no subject) CPIM (message-id=1, 'displayed')
SIP 480 TEMPORARILY UNAVAILABLE
Msg3 shown in pop-up
SIP MESSAGE (no subject) CPIM (message-id=2, 'displayed')
SIP MESSAGE (no subject) CPIM (message-id=2, 'displayed')
Notifications stored:
R ID1
R ID2

Figure 123: Store and forward: Message(s) displayed notifications via SIP MESSAGE with sender offline*

*: Check NOTES 1, 8, 9, 10 and 15 in section B.1.14

B.1.12. Interworking to SMS/MMS with automatic accept at the IWF

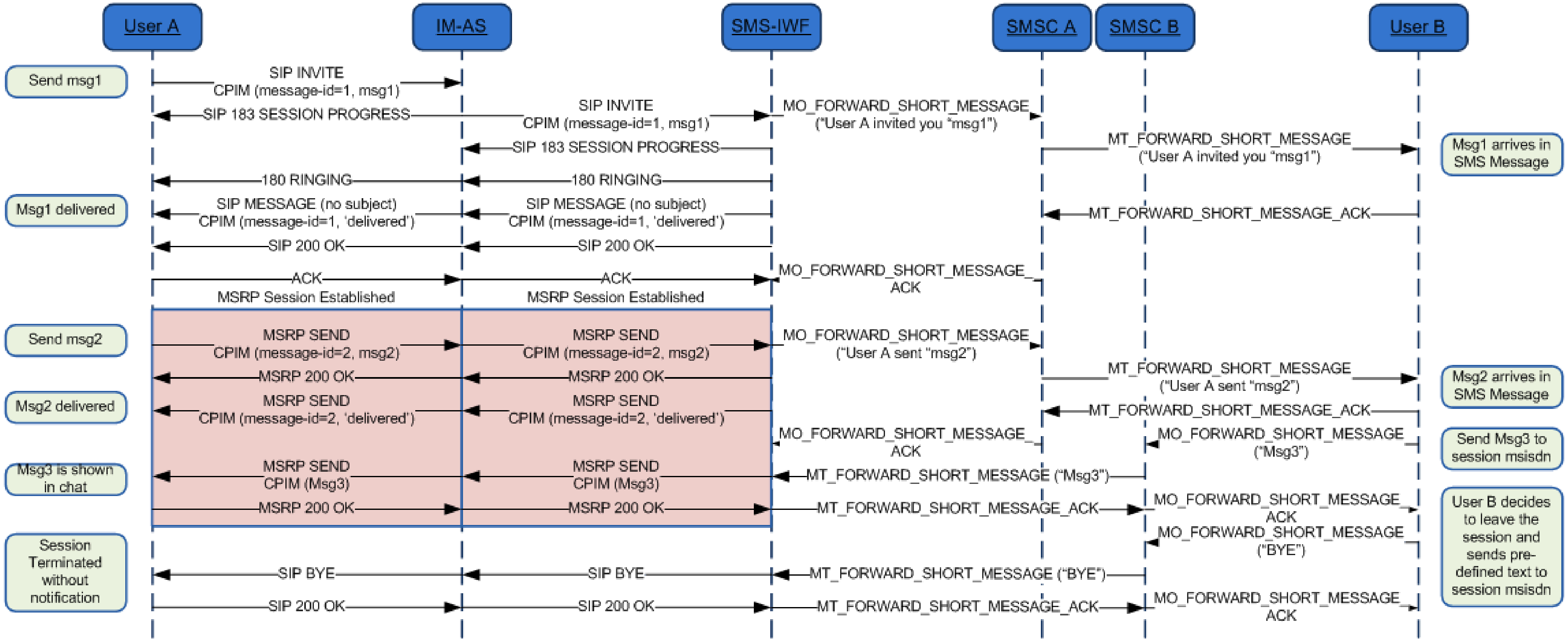

User A
IM-AS
SMS-IWF
SMSC A
SMSC B
User B
Send msg1
SIP INVITE
CPIM (message-id=1, msg1)
SIP 183 SESSION PROGRESS
SIP INVITE
CPIM (message-id=1, msg1)
MO_FORWARD_SHORT_MESSAGE
("User A invited you "msg1")
SIP 183 SESSION PROGRESS
MT_FORWARD_SHORT_MESSAGE
("User A invited you "msg1")
Msg1 arrives in SMS Message
180 RINGING
180 RINGING
Msg1 delivered
SIP MESSAGE (no subject)
CPIM (message-id=1, 'delivered')
SIP MESSAGE (no subject)
CPIM (message-id=1, 'delivered')
MT_FORWARD_SHORT_MESSAGE_ACK
SIP 200 OK
SIP 200 OK
ACK
ACK
MO_FORWARD_SHORT_MESSAGE_ACK
MSRP Session Established
MSRP Session Established
Send msg2
MSRP SEND
CPIM (message-id=2, msg2)
MSRP SEND
CPIM (message-id=2, msg2)
MO_FORWARD_SHORT_MESSAGE
("User A sent "msg2")
MT_FORWARD_SHORT_MESSAGE
("User A sent "msg2")
Msg2 arrives in SMS Message
MSRP 200 OK
MSRP 200 OK
Msg2 delivered
MSRP SEND
CPIM (message-id=2, 'delivered')
MSRP SEND
CPIM (message-id=2, 'delivered')
MT_FORWARD_SHORT_MESSAGE_ACK
MO_FORWARD_SHORT_MESSAGE_ACK
MO_FORWARD_SHORT_MESSAGE
("Msg3")
Send Msg3 to session msisdn
Msg3 is shown in chat
MSRP SEND
CPIM (Msg3)
MSRP SEND
CPIM (Msg3)
MT_FORWARD_SHORT_MESSAGE ("Msg3")
MSRP 200 OK
MSRP 200 OK
MT_FORWARD_SHORT_MESSAGE_ACK
MO_FORWARD_SHORT_MESSAGE_ACK
MO_FORWARD_SHORT_MESSAGE
("BYE")
User B decides to leave the session and sends pre-defined text to session msisdn
Session Terminated without notification
SIP BYE
SIP BYE
MT_FORWARD_SHORT_MESSAGE ("BYE")
SIP 200 OK
SIP 200 OK
MT_FORWARD_SHORT_MESSAGE_ACK
MO_FORWARD_SHORT_MESSAGE_ACK

Figure 124: Interworking: Automatic acceptance on behalf of the SMS/MMS user*

*: Check NOTES 1, 12, 15 and 16 in section B.1.14

B.1.13. Interworking to SMS/MMS with manual accept

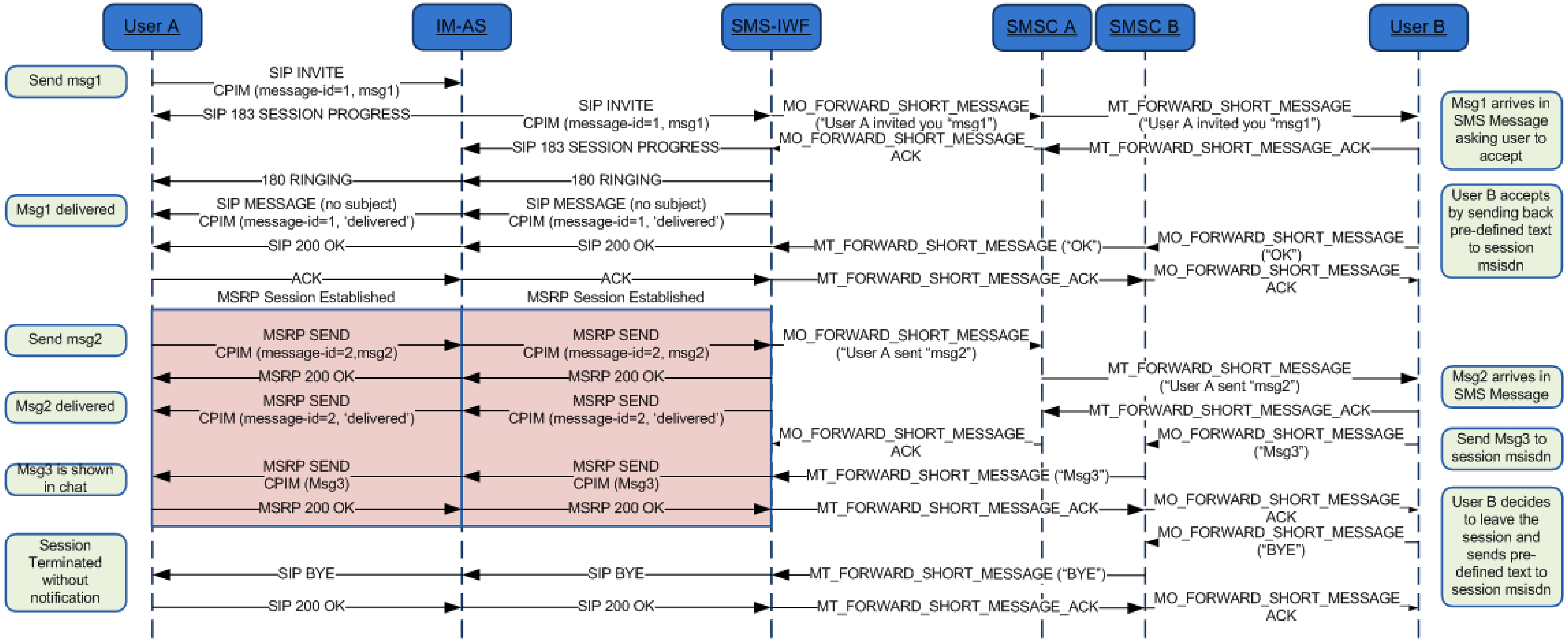

User A
IM-AS
SMS-IWF
SMSC A
SMSC B
User B
Send msg1
SIP INVITE CPIM (message-id=1, msg1)
SIP 183 SESSION PROGRESS
SIP INVITE CPIM (message-id=1, msg1)
MO_FORWARD_SHORT_MESSAGE ("User A invited you "msg1")
MT_FORWARD_SHORT_MESSAGE ("User A invited you "msg1")
Msg1 arrives in SMS Message asking user to accept
SIP 183 SESSION PROGRESS
MO_FORWARD_SHORT_MESSAGE ACK
MT_FORWARD_SHORT_MESSAGE_ACK
180 RINGING
180 RINGING
User B accepts by sending back pre-defined text to session msisdn
Msg1 delivered
SIP MESSAGE (no subject) CPIM (message-id=1, 'delivered')
SIP MESSAGE (no subject) CPIM (message-id=1, 'delivered')
SIP 200 OK
SIP 200 OK
MT_FORWARD_SHORT_MESSAGE ("OK")
MO_FORWARD_SHORT_MESSAGE ("OK")
ACK
ACK
MT_FORWARD_SHORT_MESSAGE_ACK
MO_FORWARD_SHORT_MESSAGE ACK
MSRP Session Established
MSRP Session Established
Send msg2
MSRP SEND CPIM (message-id=2,msg2)
MSRP SEND CPIM (message-id=2, msg2)
MO_FORWARD_SHORT_MESSAGE ("User A sent "msg2")
MSRP 200 OK
MSRP 200 OK
MT_FORWARD_SHORT_MESSAGE ("User A sent "msg2")
Msg2 arrives in SMS Message
Msg2 delivered
MSRP SEND CPIM (message-id=2, 'delivered')
MSRP SEND CPIM (message-id=2, 'delivered')
MT_FORWARD_SHORT_MESSAGE_ACK
MO_FORWARD_SHORT_MESSAGE ACK
MO_FORWARD_SHORT_MESSAGE ("Msg3")
Send Msg3 to session msisdn
Msg3 is shown in chat
MSRP SEND CPIM (Msg3)
MSRP SEND CPIM (Msg3)
MT_FORWARD_SHORT_MESSAGE ("Msg3")
MSRP 200 OK
MSRP 200 OK
MT_FORWARD_SHORT_MESSAGE_ACK
MO_FORWARD_SHORT_MESSAGE ACK
User B decides to leave the session and sends pre-defined text to session msisdn
MO_FORWARD_SHORT_MESSAGE ("BYE")
Session Terminated without notification
SIP BYE
SIP BYE
MT_FORWARD_SHORT_MESSAGE ("BYE")
SIP 200 OK
SIP 200 OK
MT_FORWARD_SHORT_MESSAGE_ACK
MO_FORWARD_SHORT_MESSAGE ACK

Figure 125: Interworking: manual acceptance by the SMS/MMS user*

*: Check NOTES 1, 12, 13, 15 and 16 in section B.1.14

B.1.14. Chat and store and forward diagrams: Notes

Please note the following notes apply to diagrams in section B.1:

- NOTE 1 (B.1.1, B.1.2, B.1.3, B.1.4, B.1.5, B.1.6, B.1.7, B.1.9, B.1.10, B.1.11, B.1.12 and B.1.13): 200 OK responses to SIP MESSAGE and MSRP SEND messages are omitted for clarity.

- NOTE 2 (B.1.3): In a multidevice scenario, if the device public GRUU in a delivery notification received from User B is different from the value for User A's device used in the ongoing MSRP session, a new session with automatic acceptance needs to be set up as specified in section 3.3.4.1.4.
- NOTE 3 (B.1.4): In a multidevice scenario, if the device public GRUU in a delivery notification received after the first INVITE is sent to User A is different from the value in the first one, a new SIP INVITE with the new device public GRUU needs to be sent towards A.
- NOTE 4 (B.1.3, B.1.4 and B.1.6): B could have to handle two incoming INVITEs, one from the Messaging Server on behalf of A to deliver messages and notifications that were stored to be forwarded, and a second one directly from A who happens to want to chat with B at the same time. B should recognize the INVITE from the Messaging Server on behalf of A and not tear it down when the new INVITE directly from A arrives: The INVITE from the Messaging Server has a Referred-By header and no isfocus tag, and the INVITE directly from A does not have a Referred-By header. Please note that the same applies to the case in which the order in which the INVITEs arrive is reversed.
- NOTE 5 (B.1.3, B.1.4, B.1.5 and B.1.6): The session established by the Messaging Server to deliver deferred messages to the destination only allows the receiver (client/device) to send back notifications (that is an INVITE with referred-by header will only allow message/imdn+xml in the CPIM part). If the user replies with a new message, then a separate session shall be established (That is if User B (the receiver) wants to reply, a new INVITE should be used) after all the deferred messages have been delivered.
- NOTE 6 (B.1.2): In the diagram we have represented one of the possible mechanisms to detect that the user is not online (wait for the 480 response), however, there are alternative mechanisms (triggers, 3rd party registration) that can be also used by the Messaging Server for the purpose.
- NOTE 7 (B.1.3, B.1.4 and B.1.5): Note that in the scenario where the MSRP socket is closed between the Messaging Server and the Terminating client (B) in a deferred message delivery (due for instance to a small connectivity loss with the PDP context remaining active) and no re-registration takes place, if there are notifications pending (delivery or displayed) and all the deferred messages have been sent to B already (no need to open a new MSRP session), SIP MESSAGE can be used to confirm the pending delivery/display notifications that could not be sent over MSRP.
- NOTE 8 (B.1.11): Note that the deferred delivery of the display notifications stored to be forwarded in the Messaging Server will be performed as shown in section B.1.6.
- NOTE 9 (B.1.11): In the absence of a Messaging Server (neither in the sender's nor in the receiver's domain) and in the case the display notification fail to be delivered because the sender is offline, these notifications will be discarded and the receiver's client does not need to retry sending them. In any case, the next time User A manages to establish a chat session with User B, all the previous messages pending to receive the displayed notification will be marked as displayed/read.
- NOTE 10 (B.1.7 and B.1.11): In those scenarios where a Messaging Server is not available, neither in the sender's nor in the receiver's network, there is a chance that display notifications carried via SIP MESSAGE may be lost if the original sending client is offline when the receiver sends those display notifications (that is the last three messages in the diagram). To overcome this limitation, a terminal or client implementation should mark all the previous messages as displayed when a new chat message is received from the receiving user.

- NOTE 11 (B.1.3, B.1.4, B.1.5 and B.1.6): The session established by the Messaging Server to deliver deferred messages or notifications should be terminated once the all the messages and notifications have been delivered. In more detail:
    - When delivering deferred messages, the session should be terminated (by sending a BYE) either (whatever is shorter) when the display notification corresponding to the last deferred message has been received by the Messaging Server or, after a timer started on the reception of the delivered notification for the last message expires. This timer is defined by the Service Provider.
- NOTE 12 (B.1.12 and B.1.13): The predefined text for accepting and leaving a session is included for illustration purposes only as it is up to the Service Provider providing the interworking to configure an appropriate an appropriate text and announce that to the SMS/MMS user when appropriate.
- NOTE 13 (B.1.13): If the SMS (or MMS) user does not respond in time, the INVITE will have timed out and the used msisdn may even be assigned to another session. For that reason the Messaging Server should check whether the SMS (or MMS) message comes from a user that is invited to the related session and if that is not the case or the msisdn is not assigned to any session, a message is sent back informing the user that he cannot join the session any longer.
- NOTE 14 (B.1.4, B.1.5 and B.1.6): Whether a Messaging Server sets up a session for the delivery of notifications or sends them using SIP MESSAGE requests is up to its local policy. This could depend on factors such as the number of notifications that were stored or the number of messages for which notifications can be expected (during delivery of stored messages for instance).
- NOTE 15 (B.1.1, B.1.2, B.1.3, B.1.4, B.1.5, B.1.6, B.1.7, B.1.8, B.1.9, B.1.10, B.1.11, B.1.12 and B.1.13): As per [RFC5438], the message-id is conveyed in the messages via the imdn.Message-ID header and in the notifications via the value of the <message-id> element in the body of the IMDN.
- NOTE 16 (B.1.12 and B.1.13): The flows show interworking with SMS, but the flows in the SIP/MSRP part of the figure also apply when interworking with MMS.

B.2. Chat and store and forward diagrams with Automatic Acceptance

B.2.1. Chat without store and forward

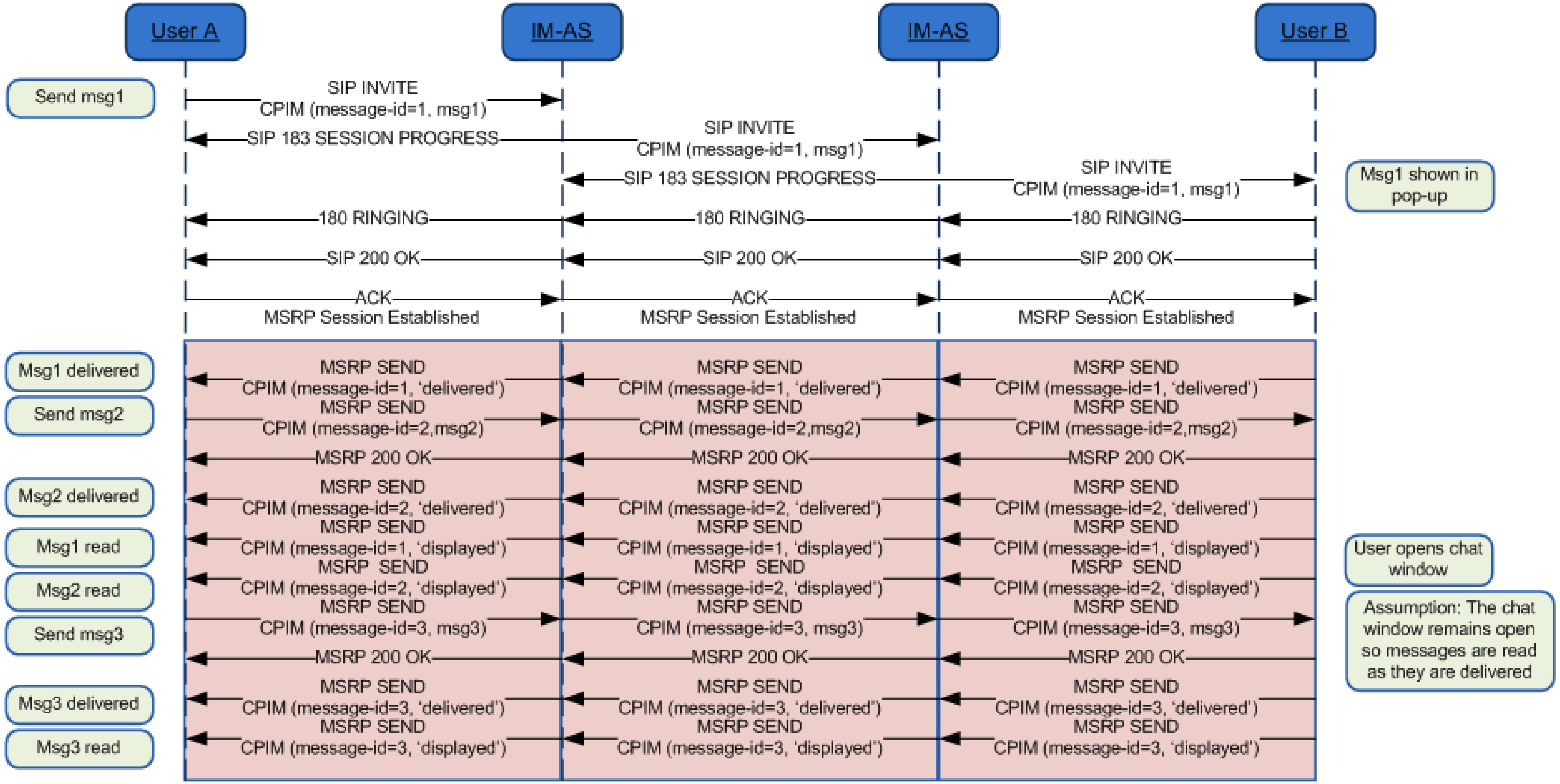


Figure 126: Chat flow without store and forward *

*: Check NOTES 1, 2, 16 and 17 in section B.2.14

B.2.2. Store and forward: Receiver offline

This case is identical to the one without automatic acceptance (see section B.1.2). NOTES 1, 2, 7 and 17 in section B.2.14 apply as well.

B.2.3. Store and forward: Message deferred delivery with sender still on an active Chat session

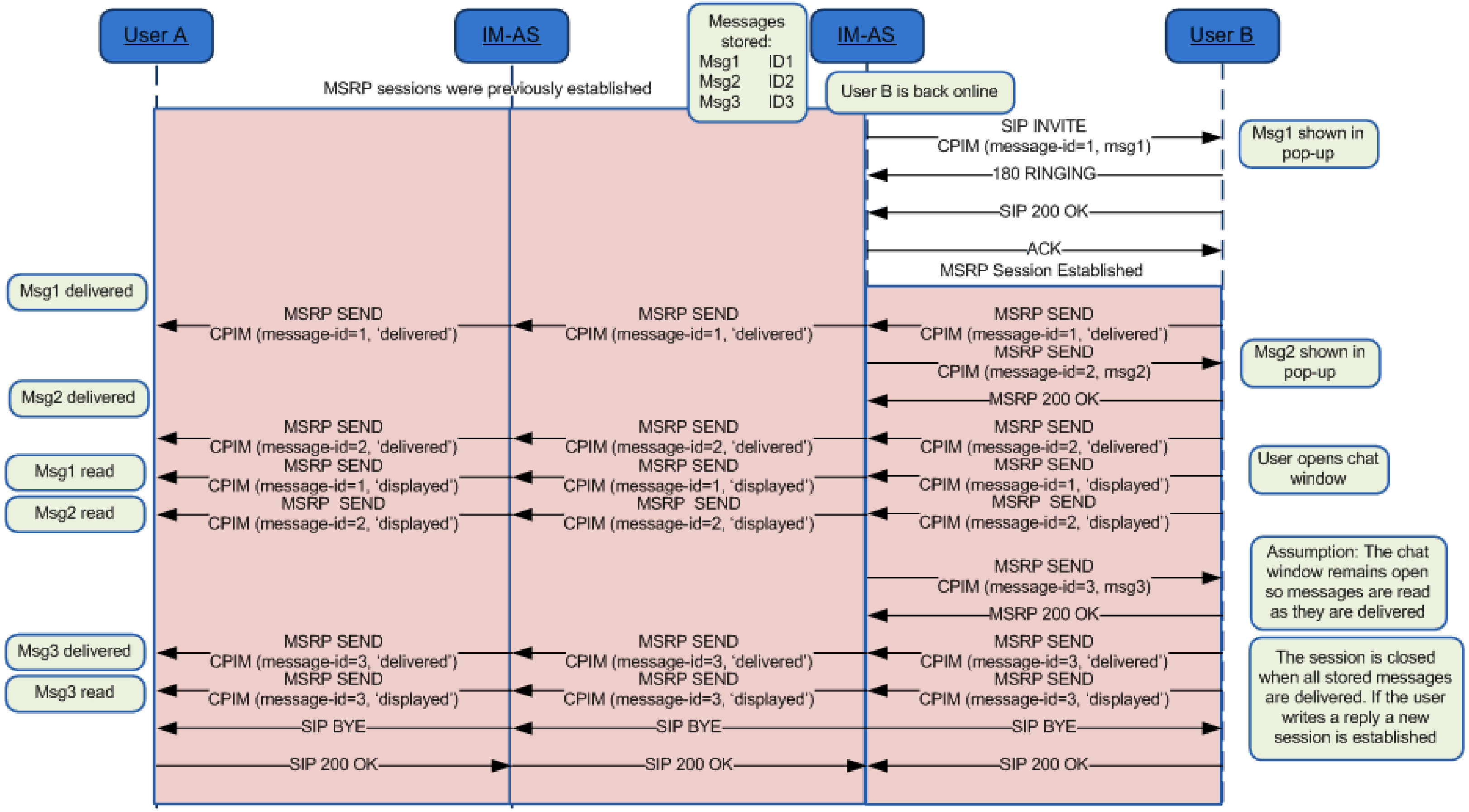

User A
IM-AS
Messages stored:
Msg1 ID1
Msg2 ID2
Msg3 ID3
IM-AS
User B
MSRP sessions were previously established
User B is back online
SIP INVITE
CPIM (message-id=1, msg1)
Msg1 shown in pop-up
180 RINGING
SIP 200 OK
ACK
MSRP Session Established
Msg1 delivered
MSRP SEND
CPIM (message-id=1, 'delivered')
MSRP SEND
CPIM (message-id=1, 'delivered')
MSRP SEND
CPIM (message-id=1, 'delivered')
MSRP SEND
CPIM (message-id=2, msg2)
Msg2 shown in pop-up
MSRP 200 OK
Msg2 delivered
MSRP SEND
CPIM (message-id=2, 'delivered')
MSRP SEND
CPIM (message-id=2, 'delivered')
MSRP SEND
CPIM (message-id=2, 'delivered')
User opens chat window
Msg1 read
MSRP SEND
CPIM (message-id=1, 'displayed')
MSRP SEND
CPIM (message-id=1, 'displayed')
MSRP SEND
CPIM (message-id=1, 'displayed')
Msg2 read
MSRP SEND
CPIM (message-id=2, 'displayed')
MSRP SEND
CPIM (message-id=2, 'displayed')
MSRP SEND
CPIM (message-id=2, 'displayed')
Assumption: The chat window remains open so messages are read as they are delivered
MSRP SEND
CPIM (message-id=3, msg3)
MSRP 200 OK
Msg3 delivered
MSRP SEND
CPIM (message-id=3, 'delivered')
MSRP SEND
CPIM (message-id=3, 'delivered')
MSRP SEND
CPIM (message-id=3, 'delivered')
Msg3 read
MSRP SEND
CPIM (message-id=3, 'displayed')
MSRP SEND
CPIM (message-id=3, 'displayed')
MSRP SEND
CPIM (message-id=3, 'displayed')
The session is closed when all stored messages are delivered. If the user writes a reply a new session is established
SIP BYE
SIP BYE
SIP BYE
SIP 200 OK
SIP 200 OK
SIP 200 OK

Figure 127: Store and forward: Message(s) deferred delivery with a sender still on an MSRP session*

*: Check NOTES 1, 2, 3, 5, 6, 8, 12, 16 and 17 in section B.2.14

B.2.4. Store and forward: Message deferred delivery with sender online

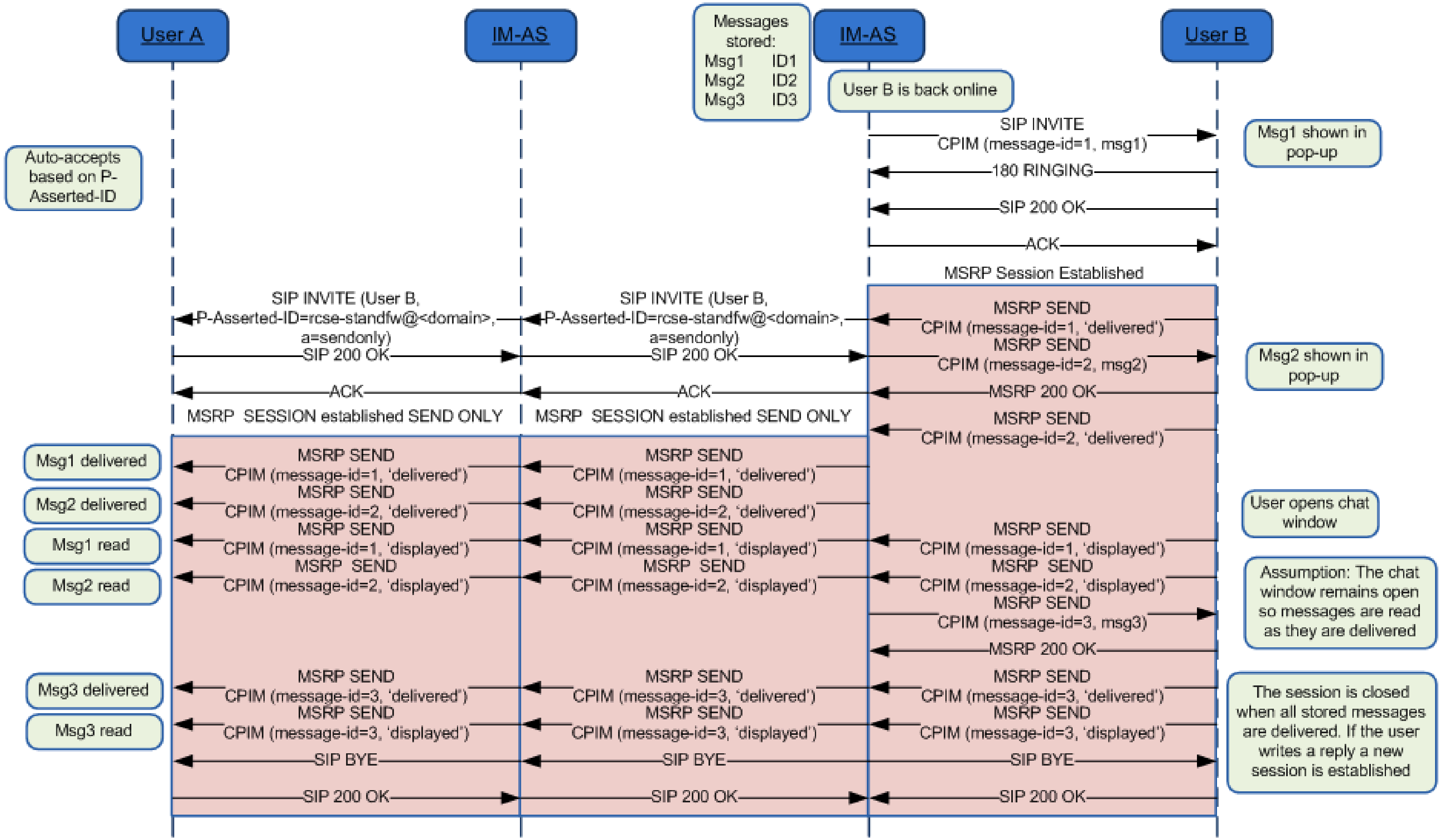

User A
IM-AS
Messages stored:
Msg1 ID1
Msg2 ID2
Msg3 ID3
IM-AS
User B
User B is back online
SIP INVITE
CPIM (message-id=1, msg1)
Msg1 shown in pop-up
180 RINGING
SIP 200 OK
ACK
MSRP Session Established
Auto-accepts based on P-Asserted-ID
SIP INVITE (User B,
P-Asserted-ID=rcse-standfw@<domain>,
a=sendonly)
SIP INVITE (User B,
P-Asserted-ID=rcse-standfw@<domain>,
a=sendonly)
MSRP SEND
CPIM (message-id=1, 'delivered')
SIP 200 OK
SIP 200 OK
MSRP SEND
CPIM (message-id=2, msg2)
Msg2 shown in pop-up
ACK
ACK
MSRP 200 OK
MSRP SESSION established SEND ONLY
MSRP SESSION established SEND ONLY
MSRP SEND
CPIM (message-id=2, 'delivered')
Msg1 delivered
MSRP SEND
CPIM (message-id=1, 'delivered')
MSRP SEND
CPIM (message-id=1, 'delivered')
Msg2 delivered
MSRP SEND
CPIM (message-id=2, 'delivered')
MSRP SEND
CPIM (message-id=2, 'delivered')
User opens chat window
Msg1 read
MSRP SEND
CPIM (message-id=1, 'displayed')
MSRP SEND
CPIM (message-id=1, 'displayed')
MSRP SEND
CPIM (message-id=1, 'displayed')
Msg2 read
MSRP SEND
CPIM (message-id=2, 'displayed')
MSRP SEND
CPIM (message-id=2, 'displayed')
MSRP SEND
CPIM (message-id=2, 'displayed')
Assumption: The chat window remains open so messages are read as they are delivered
MSRP SEND
CPIM (message-id=3, msg3)
MSRP 200 OK
Msg3 delivered
MSRP SEND
CPIM (message-id=3, 'delivered')
MSRP SEND
CPIM (message-id=3, 'delivered')
MSRP SEND
CPIM (message-id=3, 'delivered')
The session is closed when all stored messages are delivered. If the user writes a reply a new session is established
Msg3 read
MSRP SEND
CPIM (message-id=3, 'displayed')
MSRP SEND
CPIM (message-id=3, 'displayed')
MSRP SEND
CPIM (message-id=3, 'displayed')
SIP BYE
SIP BYE
SIP BYE
SIP 200 OK
SIP 200 OK
SIP 200 OK

Figure 128: Store and forward: Message deferred delivery with sender online *

*: Check NOTES 1, 2, 4, 5, 6, 8, 12, 15, 16 and 17 in section B.2.14

B.2.5. Store and forward: Message deferred delivery with sender offline (delivery notifications)

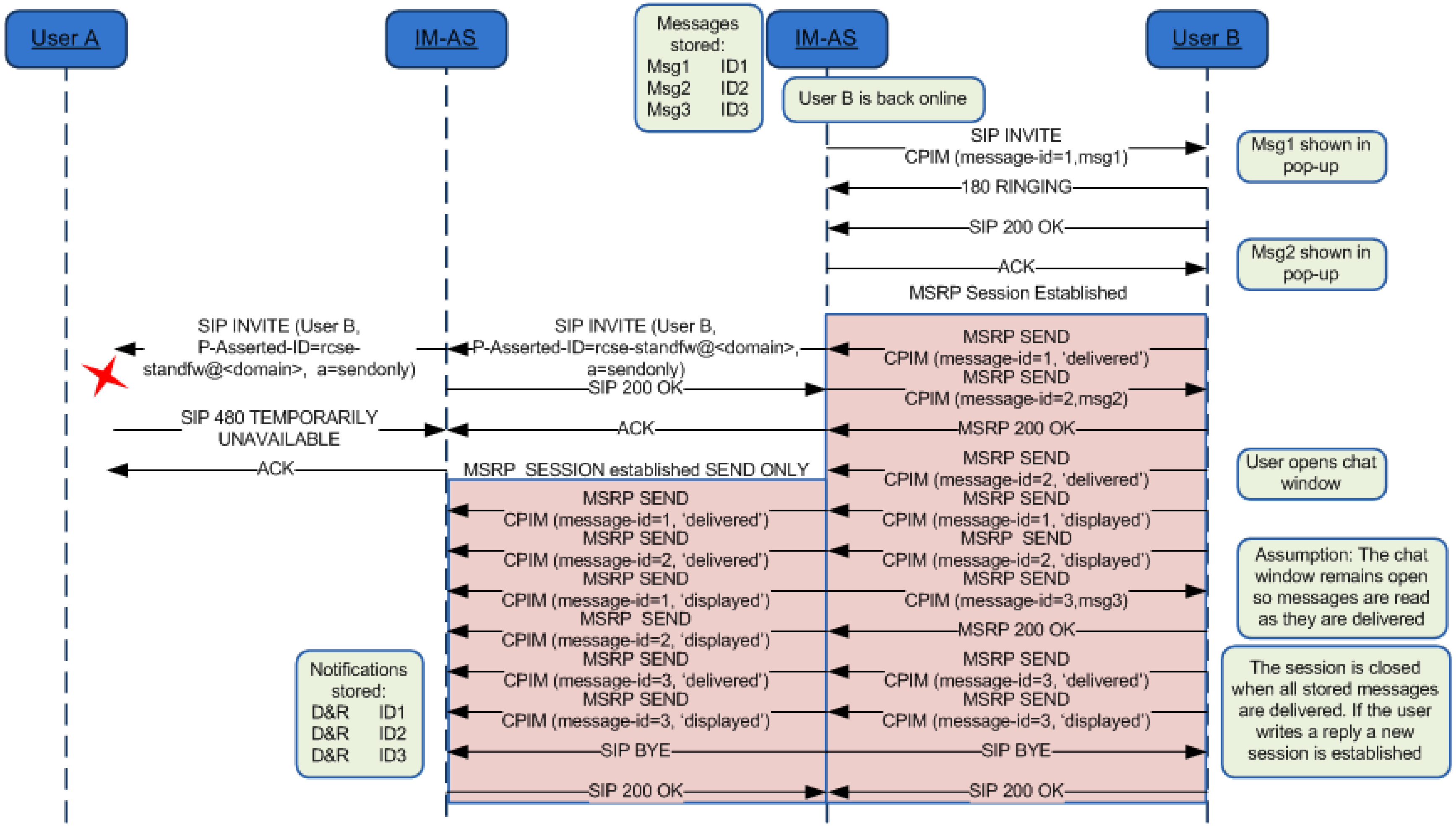

User A
IM-AS
Messages stored:
Msg1 ID1
Msg2 ID2
Msg3 ID3
IM-AS
User B
User B is back online
SIP INVITE
CPIM (message-id=1,msg1)
Msg1 shown in pop-up
180 RINGING
SIP 200 OK
Msg2 shown in pop-up
ACK
MSRP Session Established
SIP INVITE (User B, P-Asserted-ID=rcse-standfw@<domain>, a=sendonly)
SIP INVITE (User B, P-Asserted-ID=rcse-standfw@<domain>, a=sendonly)
MSRP SEND
CPIM (message-id=1, 'delivered')
SIP 200 OK
MSRP SEND
CPIM (message-id=2,msg2)
SIP 480 TEMPORARILY UNAVAILABLE
ACK
MSRP 200 OK
ACK
MSRP SESSION established SEND ONLY
MSRP SEND
CPIM (message-id=2, 'delivered')
User opens chat window
MSRP SEND
CPIM (message-id=1, 'delivered')
MSRP SEND
CPIM (message-id=1, 'displayed')
MSRP SEND
CPIM (message-id=2, 'delivered')
MSRP SEND
CPIM (message-id=2, 'displayed')
Assumption: The chat window remains open so messages are read as they are delivered
MSRP SEND
CPIM (message-id=1, 'displayed')
MSRP SEND
CPIM (message-id=3,msg3)
MSRP SEND
CPIM (message-id=2, 'displayed')
MSRP 200 OK
Notifications stored:
D&R ID1
D&R ID2
D&R ID3
MSRP SEND
CPIM (message-id=3, 'delivered')
MSRP SEND
CPIM (message-id=3, 'delivered')
The session is closed when all stored messages are delivered. If the user writes a reply a new session is established
MSRP SEND
CPIM (message-id=3, 'displayed')
MSRP SEND
CPIM (message-id=3, 'displayed')
SIP BYE
SIP BYE
SIP 200 OK
SIP 200 OK

Figure 129: Store and forward: Message(s) deferred delivery with a sender offline (delivery notifications)*

*: Check NOTE 1, 2, 6, 8, 12, 15, 16 and 17 in section B.2.14

B.2.6. Store and forward: Notifications deferred delivery

This case is identical to the one without automatic acceptance (see section B.1.6). NOTES 2, 5, 6, 12, 15 and 17 in section B.2.14 apply as well.

B.2.7. Delivery of displayed notifications in an unanswered chat (without store and forward)

This case is not applicable in case of automatic acceptance.

B.2.8. Store and forward: Handling errors in the receiver's side

This case is identical to the one without automatic acceptance (see section B.1.8) taking into account NOTE 1 and 17 in section B.2.14.

Note: The error messages that are mapped to 486 Busy Here are listed in Table 37.

Also on the path between the IM-ASs (the Messaging Server) similar errors could occur. In that case if the originating Messaging Server supports Store and Forward, it will behave in the same way and store the message.

B.2.9. Race conditions: Simultaneous INVITEs

Even if somewhat more unlikely in case of automatic acceptance, this case is identical to the one without auto-accept (see section B.1.9). NOTES 1, 2 and 17 in section B.2.14 apply as well.

B.2.10. Race conditions: New INVITE after a session is accepted

Even if somewhat more unlikely in case of automatic acceptance, this case is identical to the one without auto-accept (see section B.1.10). NOTES 1, 2 and 17 in section B.2.14 apply as well.

B.2.11. Store and forward: Message(s) displayed notifications via SIP MESSAGE with sender offline

This case is identical to the one without automatic acceptance (see section B.1.11). NOTES 2, 9, 10, 11 and 17 in section B.2.14 apply as well.

B.2.12. Interworking to SMS/MMS with automatic acceptance at the IWF

This case is identical to the one without automatic acceptance (see section B.1.12). NOTES 1, 2, 13, 17 and 18 in section B.2.14 apply as well.

B.2.13. Interworking to SMS/MMS with manual acceptance

This case is identical to the one without automatic acceptance (see section B.1.13). NOTES 1, 2, 13, 17 and 18 in section B.2.14 apply as well

B.2.14. Chat and store and forward diagrams: Notes

Please note the following notes apply to diagrams in section B.2:

- NOTE 1 (B.2.1, B.2.2, B.2.3, B.2.4, B.2.5, B.2.8, B.2.9, B.2.10, B.2.12 and B.2.13): As said in section B.2, the inclusion of the message in the INVITE request is optional. If not included, the flows would be identical, but the message would be sent in the MSRP session instead as soon as it has been established.
- NOTE 2 (B.2.1, B.2.2, B.2.3, B.2.4, B.2.5, B.2.6, B.2.9, B.2.10, B.2.11, B.2.12 and B.2.13): 200 OK responses to SIP MESSAGE and MSRP SEND messages are omitted for clarity.
- NOTE 3 (B.2.3): In a multidevice scenario, if the device public GRUU in a delivery notification received from User B is different from the value for User A's device used in the ongoing MSRP session, a new session with automatic acceptance needs to be set up as specified in section 3.3.4.1.4.
- NOTE 4 (B.2.4): In a multidevice scenario, if the device public GRUU in a delivery notification received after the first INVITE is sent to User A is different from the value in the first one, a new SIP INVITE with the new device public GRUU needs to be sent towards A.
- NOTE 5 (B.2.3, B.2.4 and B.2.6): B could have to handle two incoming INVITEs, one from the Messaging Server on behalf of A to deliver messages and notifications that were stored to be forwarded, and a second one directly from A who happens to want to chat with B at the same time. B should recognize the INVITE from the Messaging Server on behalf of A and not tear it down when the new INVITE directly from A arrives: The INVITE from the Messaging Server has a Referred-By header and no isfocus tag, and the INVITE directly from A does not have a Referred-By header. Please note that the same applies to the case in which the order in which the INVITEs arrive is reversed.
- NOTE 6 (B.2.3, B.2.4, B.2.5 and B.2.6): The session established by the Messaging Server to deliver deferred messages to the destination only allows the receiver (client/device) to send back notifications (that is an INVITE with referred-by header will only allow message/imdn+xml in the CPIM part). If the user replies with a new message, then a separate session shall be established (That is if User B (the receiver) wants to reply, a new INVITE should be used) after all the deferred messages have been delivered.
- NOTE 7 (B.2.2): In the diagram we have represented one of the possible mechanisms to detect that the user is not online (wait for the 480 response), however, there are alternative mechanisms (triggers, 3rd party registration) that can be also used by the Messaging Server for the purpose.
- NOTE 8 (B.2.3, B.2.4 and B.2.5): Note that in the scenario where the MSRP socket is closed between the Messaging Server and the Terminating client (B) in a deferred message delivery (due for instance to a small connectivity loss with the PDP context remaining active) and no re-registration takes place, if there are notifications pending (delivery or displayed) and all the deferred messages have been sent to B already (no need to open a new MSRP session), SIP MESSAGE can be used to confirm the pending delivery/display notifications that could not be sent over MSRP.
- NOTE 9 (B.2.11): Note that the deferred delivery of the display notifications stored to be forwarded in the Messaging Server will be performed as shown in section B.2.6.

- NOTE 10 (B.2.11): In the absence of a Messaging Server (neither in the sender's nor in the receiver's domain) and in the case the display notification fail to be delivered because the sender is offline, these notifications will be discarded and the receiver's client does not need to retry sending them. In any case, the next time User A manages to establish a chat session with User B, all the previous messages pending to receive the displayed notification will be marked as displayed/read.
- NOTE 11 (B.2.7 and B.2.11): In those scenarios where a Messaging Server is not available, neither in the sender's nor in the receiver's network, there is a chance that display notifications carried via SIP MESSAGE may be lost if the original sending client is offline when the receiver sends those display notifications (that is the last three messages in the diagram). To overcome this limitation, a terminal or client implementation should mark all the previous messages as displayed when a new chat message is received from the receiving user.
- NOTE 12 (B.2.3, B.2.4, B.2.5 and B.2.6): The session established by the Messaging Server to deliver deferred messages or notifications should be terminated once the all the messages and notifications have been delivered. In more detail:
  - When delivering deferred messages, the session should be terminated (by sending a BYE) either (whatever is shorter) when the display notification corresponding to the last deferred message has been received by the Messaging Server or, after a timer started on the reception of the delivered notification for the last message expires. This timer is defined by the Service Provider.
- NOTE 13 (B.2.12 and B.2.13): The predefined text for accepting and leaving a session is included for illustration purposes only as it is up to the Service Provider providing the interworking to configure an appropriate an appropriate text and announce that to the SMS/MMS user when appropriate.
- NOTE 14 (B.2.13): If the SMS (or MMS) user does not respond in time, the INVITE will have timed out and the used msisdn may even be assigned to another session. For that reason the Messaging Server should check whether the SMS (or MMS) message comes from a user that is invited to the related session and if that is not the case or the msisdn is not assigned to any session, a message is sent back informing the user that he cannot join the session any longer.
- NOTE 15 (B.2.4, B.2.5 and B.2.6): Whether a Messaging Server sets up a session for the delivery of notifications or sends them using SIP MESSAGE requests is up to its local policy. This could depend on factors such as the number of notifications that were stored or the number of messages for which notifications can be expected (during delivery of stored messages for instance).
- NOTE 16 (B.2.1, B.2.3, B.2.4 and B.2.5): When there is automatic acceptance and the first message is carried in the initial SIP INVITE, the delivery notification may be either delivered using a SIP MESSAGE or MSRP SEND leaving the choice up to the client implementation. In the diagrams we shown before, we have followed the second option.
- NOTE 17 (B.2.1, B.2.2, B.2.3, B.2.4, B.2.5, B.2.6, B.2.9, B.2.10, B.2.11, B.2.12 and B.2.13): As per [RFC5438], the message-id is conveyed in the messages via the imdn.Message-ID header and in the notifications via the value of the <message-id> element in the body of the IMDN.
- NOTE 18 (B.2.12 and B.2.13): The flows show interworking with SMS, but the flows in the SIP/MSRP part of the figure also apply when interworking with MMS.

B.3. RCS Chat and multidevice

B.3.1. Delivery prior to acceptance

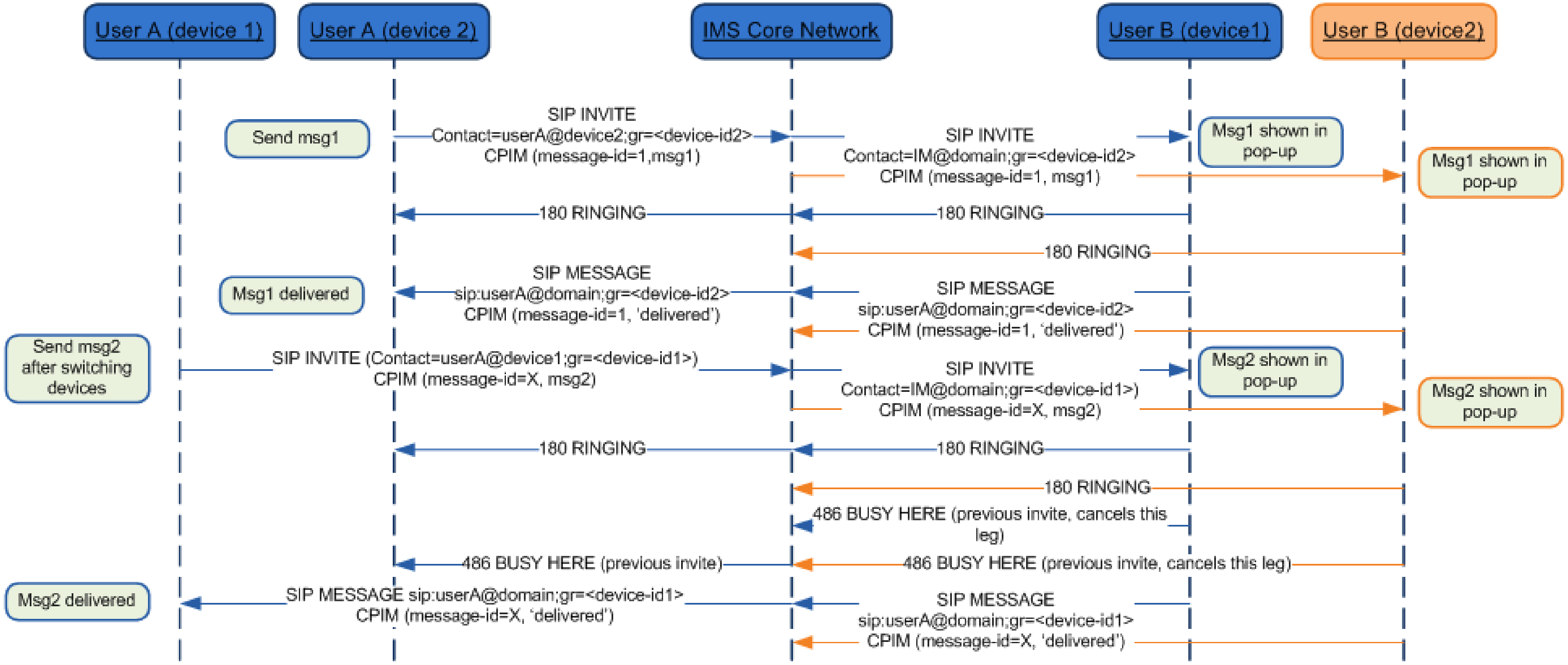

User A (device 1)
User A (device 2)
IMS Core Network
User B (device1)
User B (device2)
Send msg1
SIP INVITE Contact=userA@device2;gr=<device-id2> CPIM (message-id=1,msg1)
SIP INVITE Contact=IM@domain;gr=<device-id2> CPIM (message-id=1, msg1)
Msg1 shown in pop-up
Msg1 shown in pop-up
180 RINGING
180 RINGING
180 RINGING
Msg1 delivered
SIP MESSAGE sip:userA@domain;gr=<device-id2> CPIM (message-id=1, 'delivered')
SIP MESSAGE sip:userA@domain;gr=<device-id2> CPIM (message-id=1, 'delivered')
Send msg2 after switching devices
SIP INVITE (Contact=userA@device1;gr=<device-id1>) CPIM (message-id=X, msg2)
SIP INVITE Contact=IM@domain;gr=<device-id1>) CPIM (message-id=X, msg2)
Msg2 shown in pop-up
Msg2 shown in pop-up
180 RINGING
180 RINGING
180 RINGING
486 BUSY HERE (previous invite, cancels this leg)
486 BUSY HERE (previous invite)
486 BUSY HERE (previous invite, cancels this leg)
Msg2 delivered
SIP MESSAGE sip:userA@domain;gr=<device-id1> CPIM (message-id=X, 'delivered')
SIP MESSAGE sip:userA@domain;gr=<device-id1> CPIM (message-id=X, 'delivered')

Figure 130: Chat and multidevice: Delivery prior to acceptance*

*: Check NOTES 1, 2, 3, 4 and 7 in section B.3.4

B.3.2. Post-acceptance behaviour

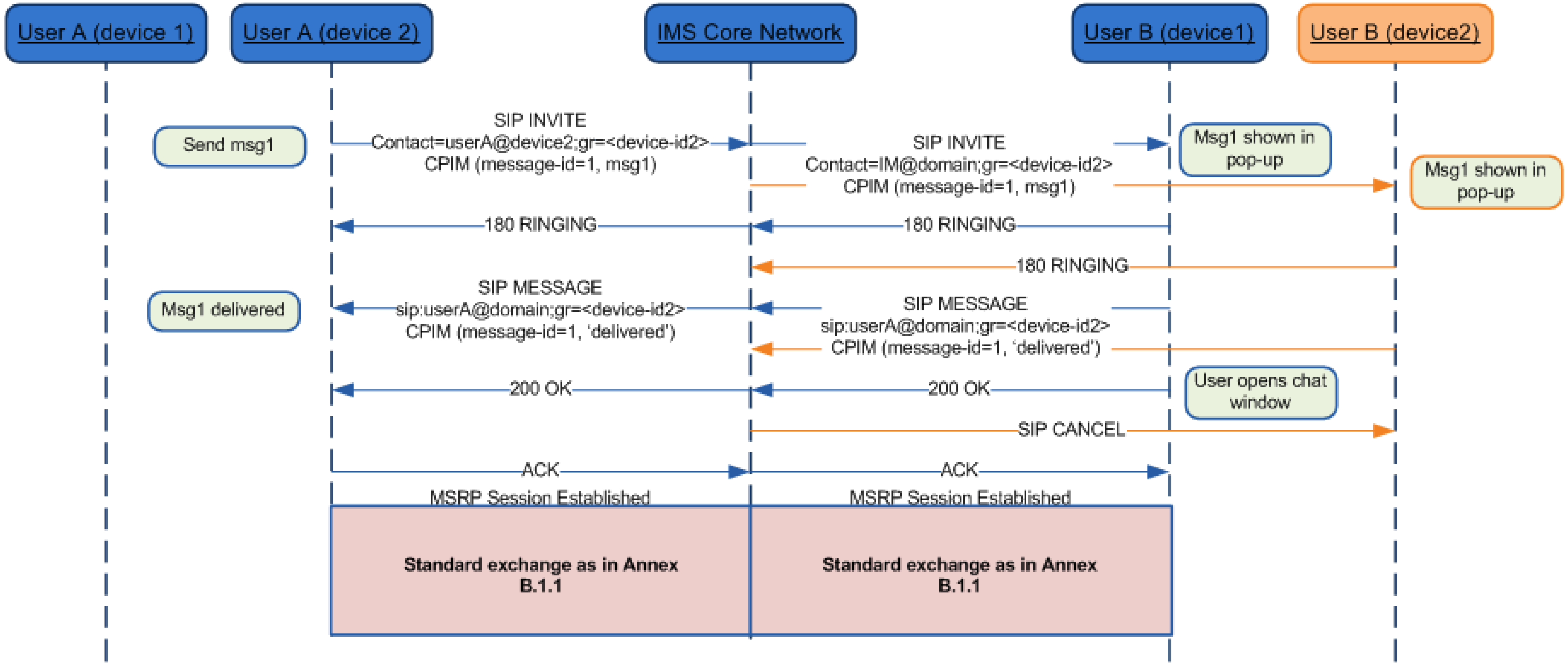

User A (device 1)
User A (device 2)
IMS Core Network
User B (device1)
User B (device2)
Send msg1
SIP INVITE
Contact=userA@device2;gr=<device-id2>
CPIM (message-id=1, msg1)
SIP INVITE
Contact=IM@domain;gr=<device-id2>
CPIM (message-id=1, msg1)
Msg1 shown in pop-up
Msg1 shown in pop-up
180 RINGING
180 RINGING
180 RINGING
Msg1 delivered
SIP MESSAGE
sip:userA@domain;gr=<device-id2>
CPIM (message-id=1, 'delivered')
SIP MESSAGE
sip:userA@domain;gr=<device-id2>
CPIM (message-id=1, 'delivered')
200 OK
200 OK
User opens chat window
SIP CANCEL
ACK
ACK
MSRP Session Established
MSRP Session Established
Standard exchange as in Annex B.1.1
Standard exchange as in Annex B.1.1

Figure 131: Chat and multidevice: Post-acceptance behaviour*

*: Check NOTES 1, 2, 3, 4 and 7 in section B.3.4

B.3.3. Behaviour with automatic acceptance

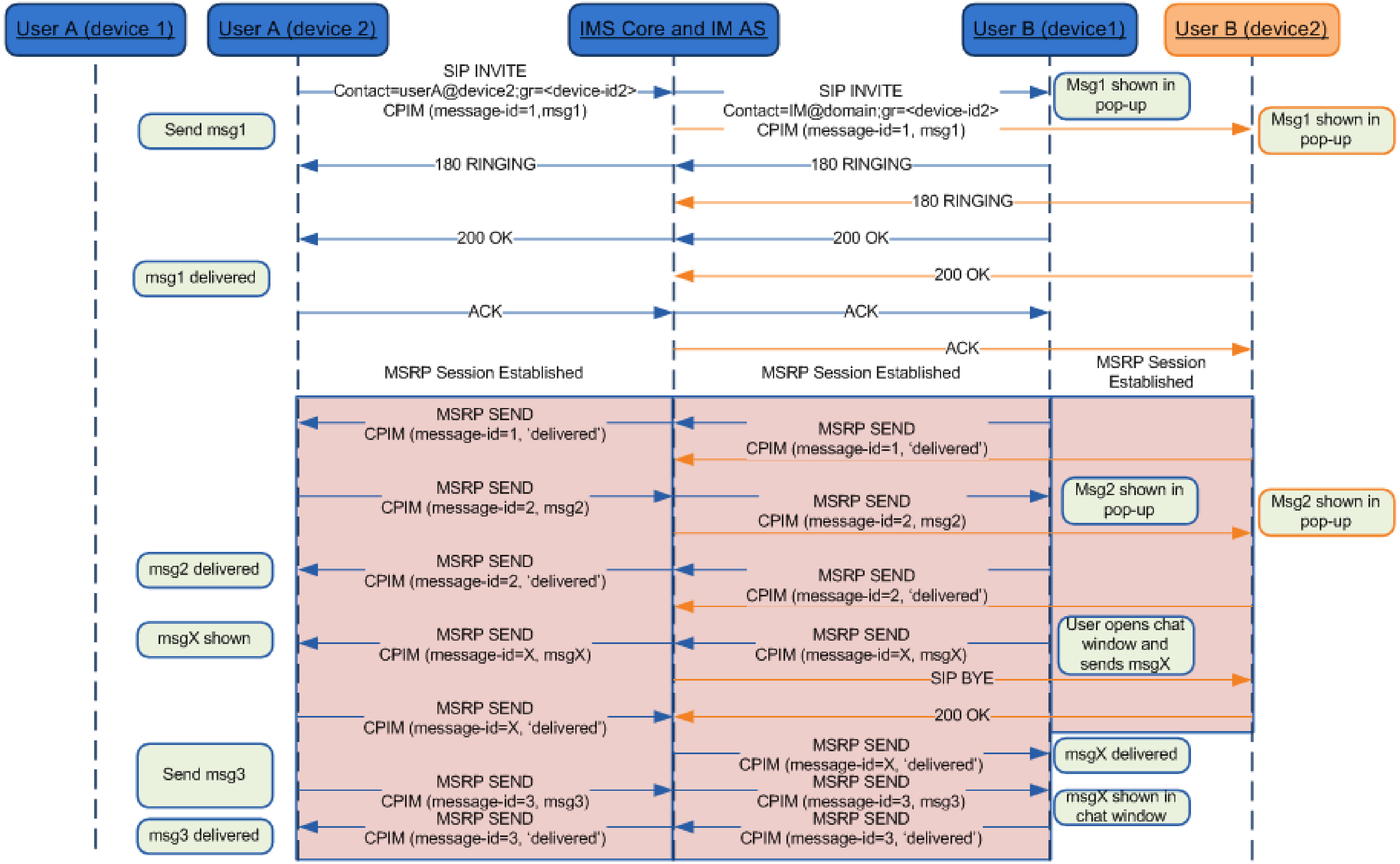

User A (device 1)
User A (device 2)
IMS Core and IM AS
User B (device1)
User B (device2)
SIP INVITE
Contact=userA@device2;gr=<device-id2>
CPIM (message-id=1,msg1)
Send msg1
SIP INVITE
Contact=IM@domain;gr=<device-id2>
CPIM (message-id=1, msg1)
Msg1 shown in pop-up
Msg1 shown in pop-up
180 RINGING
180 RINGING
180 RINGING
200 OK
200 OK
msg1 delivered
200 OK
ACK
ACK
ACK
MSRP Session Established
MSRP Session Established
MSRP Session Established
MSRP SEND
CPIM (message-id=1, 'delivered')
MSRP SEND
CPIM (message-id=1, 'delivered')
MSRP SEND
CPIM (message-id=2, msg2)
MSRP SEND
CPIM (message-id=2, msg2)
Msg2 shown in pop-up
Msg2 shown in pop-up
msg2 delivered
MSRP SEND
CPIM (message-id=2, 'delivered')
MSRP SEND
CPIM (message-id=2, 'delivered')
msgX shown
MSRP SEND
CPIM (message-id=X, msgX)
MSRP SEND
CPIM (message-id=X, msgX)
User opens chat window and sends msgX
SIP BYE
MSRP SEND
CPIM (message-id=X, 'delivered')
200 OK
MSRP SEND
CPIM (message-id=X, 'delivered')
msgX delivered
Send msg3
MSRP SEND
CPIM (message-id=3, msg3)
MSRP SEND
CPIM (message-id=3, msg3)
msgX shown in chat window
msg3 delivered
MSRP SEND
CPIM (message-id=3, 'delivered')
MSRP SEND
CPIM (message-id=3, 'delivered')

Figure 132: Chat and multidevice: Automatic acceptance*

*: Check NOTES 1, 2, 3, 4, 5, 6 and 7 in section B.3.4

B.3.4. RCS Chat and multidevice: Notes

Please note the following notes apply to diagrams in section B.3:

- NOTE 1 (B.3.1, B.3.2 and B.3.3): 200 OK responses to SIP MESSAGE and MSRP SEND messages are omitted for clarity.
- NOTE 2 (B.3.1, B.3.2 and B.3.3): As mentioned in section 2.11.3, the diagrams display the solution in a network supporting the pub-gruu generation. For a network supporting the sip.instance tag only, they would be equivalent with only a change of the mechanism to carry the device identifier (sip.instance instead pub-gruu).
- NOTE 3 (B.3.1, B.3.2 and B.3.3): The diagrams show that “delivered” notifications for messages for which such a notification was sent already, are suppressed by the network. As this cannot always be guaranteed, clients shall be prepared to receive such duplicate notifications and discard them silently. This holds also for display notifications and for notifications related to messages that were not sent by that client.
- NOTE 4 (B.3.1, B.3.2 and B.3.3): The SIP URIs in the diagrams (including those in the contact headers and Request URIs) are shown for illustrative purposes only. Any part of those URIs may thus differ in actual deployments. The details of the URIs are also dependent on the exact location in the network where the message is sent.
- NOTE 5 (B.3.3): The inclusion of the message in the SIP INVITE request is optional, if not supported, the message will be sent in the MSRP session as soon as that is established.
- NOTE 6 (B.3.3): To support this case forking in the terminating side needs to be done at the Messaging Server using the mechanisms defined in section 2.11.2 as forking in the IMS core will lead to a race condition.
- NOTE 7 (B.3.1, B.3.2 and B.3.3): As per [RFC5438], the message-id is conveyed in the messages via the imdn.Message-ID header and in the notifications via the value of the <message-id> element in the body of the IMDN.

Annex C: Special Procedures

C.1. SIP/TCP and NAT traversal

As specified in section 2.8 when using SIP over TCP (or TLS), the client shall rely on the CRLF mechanism defined in [RFC6223]. However [RFC6223] does not provide the means to negotiate the direction in which these keep-alive requests are sent (it's always the party that initiated the SIP request that has to send keep-alive requests) and a device OS's scheduling policy may not always allow the client to meet the timing requirements for sending keep-alive requests. To overcome these limitations for clients running on such platforms a mechanism is provided in this annex which will also be specified in an internet draft that will be submitted to the IETF. This mechanism allows these clients to request to reverse the direction in which the keep-alive requests are sent (that is they will be sent from network to client) by including an 'rkeep' parameter in the Via header of the SIP request that is used in the same way as the 'keep' parameter defined in [RFC6223]. Like the server in [RFC6223], the client can include a proposed frequency (in seconds) of the keep-alive period in the parameter, for instance "rkeep=600". This interval shall not be set to a value smaller than 30 seconds. If the SIP response contains the rkeep parameter in the Via header, the client must assume that the keep-alive requests will be sent and behave accordingly by for example considering the connection as failed when they are not/no longer received.

An Edge Proxy supporting this mechanism, that receives requests that contain an 'rkeep' parameter in the top-most Via header with a period, if any, that is considered acceptable, shall include the 'rkeep' parameter in the top-most Via header when sending a reliable response on that request. Then it shall send double CRLF "ping" requests as defined in [RFC5626] to the client thereby complying to the interval specified by the client, if any and considering the connection as failed when no single CRLF "pong" response is received within 10 seconds. An Edge proxy not supporting this mechanism or answering a request from a client that requested the keep-alive requests to be sent with an unacceptable period, shall not include the 'rkeep' parameter in the responses it sends.

Note 1: it is highly recommended that clients not experiencing such scheduling limitations use the standard 'keep' mechanism defined in [RFC6223] and send the keep-alive requests themselves.

Note 2: Alternatively a Service Provider could decide to rely on client platform specific notification mechanisms

Note 3: The requirement to extend the keep-alive procedures to support network-initiated keep-alives will be brought into the IETF for standardization. The procedures here will be updated once that work is completed. In particular this standardization process should allow the client to detect that the network does not support network-initiated keep-alives.

C.2. Errata for RFC 5438

The following errata have been reported for [RFC5438] in [RFC5438Errata] and is important to be taken into consideration for RCS 5.0 with respect to messaging and chat services:

- Errata ID: 3013
- Status: Held for Document Update
- Type: Technical
- Reported By: Dan Price
- Date Reported: 2011-11-04
- Held for Document Update by: Robert Sparks
- Section 7.2.1.1 says:

From: Bob <im:bob@example.com>

To: Alice <im:alice@example.com>

NS: imdn <urn:ietf:params:imdn>

imdn.Message-ID: d834jied93rf

Content-type: message/imdn+xml

Content-Disposition: notification

Content-length: ...

- It should say:

  From: Bob <im:bob@example.com>

  To: Alice <im:alice@example.com>

  NS: imdn <urn:ietf:params:imdn>

  imdn.Message-ID: d834jied93rf

  Content-type: message/imdn+xml

  Content-Disposition: notification

  Content-length: ...

- Notes:

  None of the examples in this RFC (Request For Comments) comply with the format of CPIM defined in RFC 3862, in which the message metadata headers are separated from the headers of the encapsulated MIME object by a blank line.

Document Management

Document History

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
1.0	19 April 2012	First Version	EMC	Tom Van Pelt / GSMA

Other Information

Type	Description
Document Owner	GSMA RCS Convergence Taskforce
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@gsm.org
Your comments or suggestions & questions are always welcome.