



Rich Communications Suite Release 3 Technical Realisation

2.0

14 February 2011

This is a non-binding permanent reference document of the GSM Association.

Security Classification – NON-CONFIDENTIAL GSMA Material

Copyright Notice

Copyright © 2011 GSM Association

Antitrust Notice

The information contain herein is in full compliance with the GSM Association's antitrust compliance policy.

Table of Contents

1	Introduction	4
1.1	Overview	4
1.2	Scope	4
1.3	Definition of Terms	4
1.4	References	5
2	RCS Architecture	7
3	General	8
3.1	Addressing	8
3.2	Registration	8
3.3	Compatibility and Interworking	8
3.3.1	<i>Single-Device Handling</i>	8
3.3.2	<i>Multi-Device Handling</i>	9
4	Broadband Access (BA)	9
4.1	Multi-Device Handling	10
4.2	Backward Compatibility and Interworking	10
5	Voice	10
6	Social Presence Information	10
6.1	Presence Data Model	10
6.1.1	<i>Person</i>	10
6.1.2	<i>Service</i>	12
6.1.3	<i>Example Document</i>	12
6.2	Presententity Side Handling	14
6.2.1	<i>Link Handling</i>	14
6.2.2	<i>Location handling</i>	14
6.2.3	<i>NICKNAME HANDLING</i>	15
6.3	Watcher Side Handling	16
6.3.1	<i>Link Handling</i>	16
6.3.2	<i>Location Information Handling</i>	16
6.3.3	<i>Capabilities Handling</i>	16
6.3.4	<i>Nickname Handling</i>	17
6.4	Subscriptions and Authorization	17
6.4.1	<i>Overview</i>	17
6.4.2	<i>XML Document Structure</i>	18
6.4.3	<i>XML Document Handling</i>	24
6.4.4	<i>Privacy for RCS Capability</i>	24
6.5	RIs Server Handling	25
6.5.1	<i>Nickname Handling</i>	25
6.6	Presence Server Handling	25
6.6.1	<i>Nickname Handling</i>	25
6.7	Backward Compatibility And Interworking	25
6.7.1	<i>Watcher Side Handling</i>	25
6.7.2	<i>PRESENTITY SIDE HANDLING</i>	27
6.7.3	<i>Interworking between RCS Release 2 and Release 3 networks</i>	28
7	Address Book	28

8	Content Sharing	28
8.1	General	28
8.2	Image Sharing Without Voice Call	29
8.3	Video Sharing Without Voice Call	29
8.4	Video Sharing Live To Legacy Terminal	29
8.5	Video Sharing Deferred To Legacy Terminal.....	29
8.6	Video Sharing Live With Content From A Network Content Server ..	30
8.7	Streaming/Uploading Video from an RCS Release 3 Client to a Network Content Server	30
8.8	Backward Compatibility with RCS Releases 1 & 2 Clients.....	30
9	File Transfer	30
10	Messaging	31
10.1	Architecture.....	31
10.2	Legacy Messaging	31
10.2.1	<i>Introduction</i>	31
10.2.2	<i>SMS Service over Broadband Access</i>	31
10.2.3	<i>MMS Service over Broadband Access</i>	32
10.2.4	<i>Multi-device Handling</i>	32
10.2.5	<i>Handling of Notifications Carried In SMS Messages</i>	32
10.2.6	<i>Compatibility with Earlier RCS Releases</i>	33
10.3	Chat	33
10.3.1	<i>Introduction</i>	33
10.3.2	<i>Compatibility with Earlier RCS Releases</i>	33
11	Network Value Added Services	33
11.1	Introduction	33
11.2	Compatibility with Earlier Releases.....	33
11.2.1	<i>Release 2/1 Client and Release 3 Network</i>	33
11.2.2	<i>Release 3 Client and Release 2/1 Network</i>	33
11.2.3	<i>Release 3 Network and Release 2/1 Network</i>	33
11.2.4	<i>Release 3 Client and Release 2/1 Client</i>	34
Appendix A: Signalling Sequences (Informative)		35
Document Management		36

1 Introduction

1.1 Overview

This document describes architecture and technical details needed for RCS (Rich Communication Suite) Release 3 (R3). Note that in order to get the full picture of RCS technical realisation, it is recommended to read this document in combination with Release 1 (R1) and Release 2 (R2) documents. This is because this document only illustrates the Release 3 specific components and features; it does not include items already documented by Technical Realisation document(s) of earlier release(s).

For general overview of RCS including high-level requirements, please see document [FUNCDESC].

1.2 Scope

The scope of the document includes only the RCS Release 3. For the technical details of RCS Release 1 see [RCSTRR1] and for Release 2 see [RCSTRR2].

1.3 Definition of Terms

Term	Description
AS	Application Server
Basic Social Presence information	The Social Presence information that is offered in RCS Release 1 and Release 2: A free text, a status-icon, a link, the Willingness status which is referred to as Availability Status at a functional level and the service capabilities.
Broadband Access (BA) Client	Non-CS capable client utilizing IP based broadband access (BA) network for RCS services. For example, but not limited to, a PC using WLAN
CS	Circuit Switched (for example "CS Voice" used in the access network such as GSM or UMTS natively supporting the circuit switched voice service)
EAB	Enhanced Address Book
GW	Gateway
IMS	IP Multimedia Subsystem
MGW	Media Gateway, used for performing the conversion between CS and PS voice
MMS-C	Multimedia Messaging Service Centre. The common realisation of the 3GPP defined logical node MMS Relay/Server and OMA defined MMS Proxy-Relay and MMS Server
MMTel	IMS Multimedia Telephony Service, used as the solution for offering the PS Voice service in RCS
Mobile Client	CS capable client utilizing cellular access network for RCS services. For example 2G/3G mobile phone
NAB	Network Address Book
NNI	Network-to-Network Interface, used for inter-operator connectivity
PS	Packet Switched (for example "PS Voice" used in the IP based access networks such as ADSL, WLAN or LTE)
RCS	Rich Communication Suite (provides a feature-rich portfolio of services to unleash the communities hidden in a user's phone book)
Served RCS Presentity	The RCS User on whose behalf the RCS Client acts as Presence Source
SET	SUPL enabled terminal
SMS-C	Short Message Service Centre. The common realisation of the 3GPP defined logical nodes SM-GMSC, SM-IW MSC and SM-SC.

Term	Description
SUPL	Secure user plane location
UNI	User-to-Network Interface, used for access network connectivity

1.4 References

[23.204]	TS 23.204: Support of Short Message Service (SMS) over generic 3GPP Internet Protocol (IP) access; Stage 2, v8.4.0 http://www.3gpp.org
[23.140]	TS 23.140: Multimedia Messaging Service (MMS); Functional description; Stage 2, v6.16.0 http://www.3gpp.org
[24.229]	TS 24.229: Internet Protocol (IP) multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3, v7.13.1 http://www.3gpp.org
[24.341]	TS 24.341: Support of SMS over IP networks; Stage 3, v8.1.0 http://www.3gpp.org
[24.173ENDORSE]	RCS Endorsement of 3GPP TS 24.173 MMTel http://www.gsmworld.com
[26.114ENDORSE]	RCS Endorsement of 3GPP TS 26.114 MMTel Media Handling http://www.gsmworld.com
[GML3.1.1]	OpenGIS® Geography Markup Language (GML) Implementation Specification, Version 3.1.1, OGC 03-105r1 http://www.opengeospatial.org/
[FUNCDESC]	RCS Functional Description http://www.gsmworld.com
[IMENDORSE]	RCS Endorsement of OMA SIP/SIMPLE IM 1.0 http://www.gsmworld.com
[IMAGESHARE]	PRD IR.79 Image Share Interoperability Specification, 1.2, http://www.gsmworld.com/
[IR.65]	PRD IR.65 IMS Roaming & Interworking Guidelines, 3.6, http://www.gsmworld.com/
[IR.84]	PRD IR.84 Video Share Phase 2 Interoperability Specification 1.1 http://www.gsmworld.com/
[IR.90]	PRD IR.90 RCS Interworking Guidelines, 1.0, http://www.gsmworld.com/
[MGMTOBJ]	RCS Management Objects http://www.gsmworld.com/
[OMADS]	DS Protocol, 1.2.1, http://www.openmobilealliance.org/
[OMAMMS]	Multimedia Messaging Service, Client Transactions, Candidate Version 1.3 – 28 Jan 2008 http://www.openmobilealliance.org/
[PRESENCE]	Presence SIMPLE Specification, 1.1, http://www.openmobilealliance.org/
[Presence1.0_DDS]	Presence SIMPLE Data Specification, Approved Version 1.0, 27 June 2008 http://www.openmobilealliance.org/
[Presence2.0_DDS]	Presence SIMPLE Data Specification, Draft Version 2.0, 15 October 2008 http://www.openmobilealliance.org/
[Presence2.1_DDS]	Presence SIMPLE Data Specification, Draft Version 2.1, 25 November 2009 http://www.openmobilealliance.org/
[Presence2.0_TS]	Presence SIMPLE Specification, Draft Version 2.0, 14 October 2008 http://www.openmobilealliance.org/
[Presence_Content]	Presence Content XDM Specification, Draft Version 1.0, 01 October 2008

	http://www.openmobilealliance.org/
[PRESENCEIG]	Implementation Guidelines for OMA Presence SIMPLE v1.1 Presence http://www.openmobilealliance.org/
[PresenceXDM]	Presence XDM Specification, Approved Version 1.1 – 27 Jun 2008 http://www.openmobilealliance.org/
[RCSTRR1]	RCS Technical Realisation Release 1, 15th December 2008 http://www.gsmworld.com
[RCSTRR2]	RCS Technical Realisation Release 2, 31st August 2009 http://www.gsmworld.com
[RFC 3261]	RFC 3261: SIP : Session Initiation Protocol, June 2002 http://www.ietf.org
[RFC3858]	RFC 3858: An Extensible Markup Language (XML) Based Format for Watcher Information, August 2004 http://www.ietf.org
[RFC 3966]	RFC 3966: The tel URI for Telephone Numbers, December 2004 http://www.ietf.org
[RFC 4482]	RFC 4482: CIPID: Contact Information for the Presence Information Data Format, July 2006 http://www.ietf.org
[RFC4589]	RFC 4589: Location Types Registry, July 2006 http://www.ietf.org
[RFC5491]	RFC 5491: GEOPRIV Presence Information Data Format Location Object (PIDF-LO) Usage Clarification, Considerations, and Recommendations, March 2009 http://www.ietf.org
[RLSXDM]	Resource List Server (RLS) XDM Specification Approved Version 1.1 – 27 Jun 2008, http://www.openmobilealliance.org/
[SE.50]	Video Share Phase 2 Service Definition 1.01, http://www.gsmworld.com/
[SharedXDM]	Shared XDM Specification, Approved Version 1.1 – 27 Jun 2008 http://www.openmobilealliance.org/
[SIMPLEIM]	Instant Messaging using SIMPLE, 1.0, http://www.openmobilealliance.org/
[SUPL]	Secure User Plane Location, Approved Version 1.0 – 15 Jun 2007 http://www.openmobilealliance.org/
[TTC_NVAS]	TTC TS-1014 RCSS Stage2 and Stage3 Network Value Added Services http://www.ttc.or.jp/e/publish https://infocentre.gsm.org/cgi-bin/docdisp.cgi?290049
[VIDEOSHARE]	PRD IR.74 Video Share Interoperability Specification, 1.3, http://www.gsmworld.com/
[XDM1.1_AD]	XML Document Management Architecture, Approved Version 1.1, 27 June 2008 http://www.openmobilealliance.org/
[XDM2.0_AD]	XML Document Management Architecture, Candidate Version 2.0, 16 September 2008 http://www.openmobilealliance.org/
[XDM1.1_Core]	XML Document Management (XDM) Specification, Approved Version 1.1, 27 June 2008 http://www.openmobilealliance.org/
[XDM2.0_Core]	XML Document Management (XDM) Specification, Candidate Version 2.0, 16 September 2008 http://www.openmobilealliance.org/
[XDMIG]	Implementation Guidelines for OMA XDM v1.1, http://www.openmobilealliance.org/

2 RCS Architecture

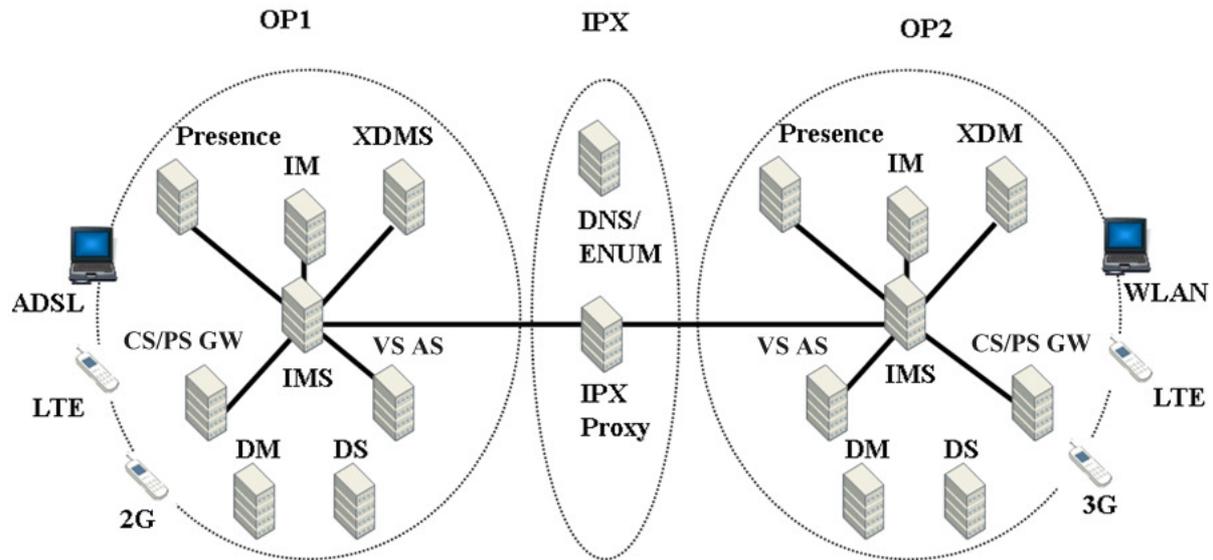


Figure 1: Simplified Example of RCS Architecture

Note: CS/PS GW is used for interworking between CS Voice and PS Voice (MMTel). VS AS indicates a Video Share Application Server, as utilized in [IR.84].

The figure above shows a simplified illustrative example of an overall architecture for RCS Release 3, where two operators offering RCS are exchanging traffic with each other using standard network-to-network Interface, (NNI) mechanisms (IP Packet Exchange (IPX) as an example) as documented in [IR.90]. RCS is offered as an intra-operator service, even though this example shows an inter-operator scenario.

RCS compliant access networks include, but are not limited to, those illustrated in the Figure 1. Thus deploying the RCS service does not mean you have to have a 3G network deployed.

The 2G GPRS/EDGE phone in the Figure 1 relates to the case the RCS device is located under GPRS/EDGE coverage. There are four examples when this could occur:

- The subscriber with a dual-mode 3G/EDGE RCS device, is located under EDGE/GPRS-only coverage of the home 3G operator
- The subscriber with a dual-mode 3G/EDGE RCS device, is roaming under a EDGE/GPRS visited operator's network
- The subscriber has a GPRS/EDGE RCS device only due to having a subscription with a pure 2G operator
- The subscriber has a subscription with a 3G operator but has a GPRS/EDGE RCS device only

There are certain consequences as far as the RCS services are concerned for a Class B (circuit-switched (CS) or packet-switched (PS), one service at a time) RCS device located under GPRS/EDGE coverage. For such device, RCS Video/Image Share will not work. However, all non-call related services will work, for example, RCS Presence, Chat, File-transfer, and Video Share outside of a voice call.

Whilst using, for example, RCS chat, the subscriber might receive a CS call. If such a call is answered the PS activity is suspended (without informing the far side) until the CS call is torn down and the device resumes the PS data activity again. A pure 2G operator wishing to

launch RCS should be aware of these consequences, as well as 3G operators wishing to offer RCS services in their GPRS/EDGE coverage areas. This concerns device vendors as well.

An operator and device vendor can overcome the few limitations mentioned above, by introducing DTM (dual transfer mode) technology in radio network and devices.

3 General

3.1 Addressing

There are no changes in the area of Addressing in Release 3, the text in [RCSTRR1] and [RCSTRR2] is fully applicable.

3.2 Registration

The RCS client shall register all feature tags as per service it supports, in the Contact header of a SIP REGISTER message. For information about the detailed structure of each feature tag related to the RCS Release 1 and RCS Release 2 services, see Chapter 3.2 in [RCSTRR1] and [RCSTRR2] respectively. In RCS Release 3, further feature tags are introduced, due to the inclusion of Video Share Phase 2, which is described in chapter 8. These identifiers are described in [IR.84] section 2.3.2. If it supports this service, the RCS client shall include the ICSI and IARI for Video Share Phase 2 in its registration:

- +g.3gpp.icsi-ref="urn:urn-7:3gpp-service.ims.icsi.mmtel"
- +g.3gpp.iari-ref="urn:urn-7:3gpp-application.ims.iari.gsma-vs"

Note1: The registration of the MMTel ICSI by RCS clients could result in those clients receiving requests for other MMTel services (for example, PS voice calls targeted to a BA client of the same user). An RCS client shall reject any invitations for MMTel services that it does not support.

In addition, in RCS Release 3 the BA Client when used as a primary device will indicate the capability to receive SMS messages over IMS by registering the SMS over IP feature tag in accordance with [24.341]:

- +g.3gpp.smsip

3.3 Compatibility and Interworking

3.3.1 Single-Device Handling

The following table describes combinations where users who only have one **device** (mobile or BA) are using an RCS network. The possible support for these combinations is described in the following table. Every row shows a possible combination.

Example: a Release 2 (R2) mobile is supported in a Release 3 (R3) network.

Table 1: Single device, compatibility & interworking

Details on compatibility are found within dedicated chapters in Technical Realisation per new service

Network Mobile BA

R2	R2		Covered in R2
R2		R2	Not possible, BA only as secondary device not allowed
R2	R3		Covered in R3, details on compatibility and interworking are described per service
R2		R3	Not possible, BA only as secondary device not allowed
R3	R2		Covered in R3, details on compatibility and interworking are described per service
R3		R2	Not possible, only R3 BA allowed as single primary device
R3	R3		Covered in R3, basic case
R3		R3	Covered in R3, BA as single primary device

3.3.2 Multi-Device Handling

The following table describes combinations where users who have **multiple devices** (mobile and BA) are using an RCS network. The possible support for these combinations is described in the following table. Every row shows a possible combination.

Example: a Release 3 mobile with a Release 2 BA is supported in a Release 3 network. BA Client can use Release 2 features.

Table 2: Multiple device, compatibility & interworking

Details on compatibility are found within dedicated chapters in Technical Realisation per new service

Network Mobile BA

R2	R2	R2	Covered in R2 , R2 case with multiple devices
R2	R2	R3	Handled by the R2 network as an R2 BA client
R2	R3	R2	Handled by the R2 network as an R2 Mobile client
R2	R3	R3	Handled by the R2 network as an R2 Mobile & R2 BA client
R3	R2	R2	Handled by R3 network, R2 features are supported
R3	R2	R3	Handled by R3 network, R2 features are supported for Mobile
R3	R3	R2	Handled by R3 network, R2 features are supported for BA
R3	R3	R3	R3 basic case

4 Broadband Access (BA)

In RCS Release 3, the client with the BA may be the primary client in the case where there are no clients with the cellular access, as shown in the figure below. The precondition is that basic telephony services are already available in the BA network. For these services, the local regulations are already fulfilled.

In this case, the SMS and MMS will be delivered to the client with the BA as specified in sub-clause 10.2. With RCS Release 3, the BA client is able to send MMS as well. For details how this is realised, see sub-clause 10.2.3.

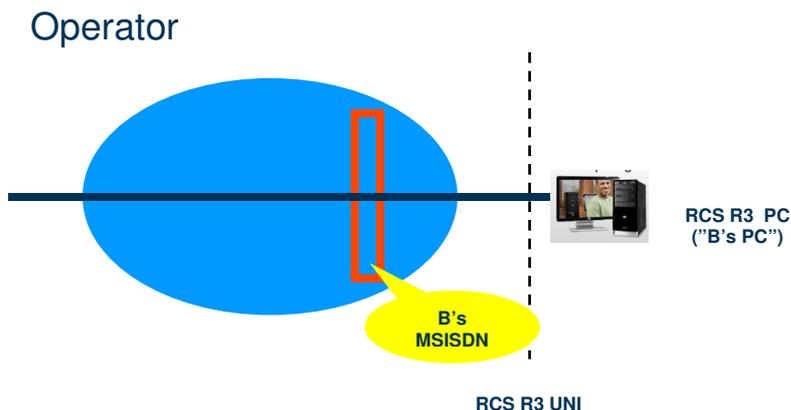


Figure 2: RCS Release 3 BA client used as a primary client

4.1 Multi-Device Handling

A user having both RCS Release 3 BA client and RCS Release 3 mobile client is supported by the RCS Release 3 network where mobile client is primary and BA client is secondary, following the multi-device combinations defined in RCS Release 2 in [RCSTRR2].

Other combinations of multiple devices, like support of multiple mobile clients, are out of scope for RCS Release 3. However, this does not restrict an operator to deploy proprietary solutions to achieve this.

4.2 Backward Compatibility and Interworking

A user having both a RCS Release 3 BA client and a RCS Release 2 mobile client is supported by the RCS Release 3 network where the mobile client is primary and the BA client is secondary.

A RCS Release 3 BA client is supported by the RCS Release 2 network as secondary RCS Release 2 BA client.

A RCS Release 2 BA client is supported by the RCS Release 3 network as secondary client

5 Voice

There are no changes in the area of voice in Release 3; the text in [RCSTRR2] is fully applicable.

6 Social Presence Information

6.1 Presence Data Model

6.1.1 Person

For RCS Release 3 and following, the social presence information provided in the "Person" section of the presence data model defined in [RCSTRR1] is extended with following data:

- A new element for the favourite link containing a label
- Location information

6.1.1.1 Link Enhancements

In RCS Release 3, the possibility is introduced to add a display label to the link that is part of the social presence information. This will be realized using the “Labelled Link” building block that is specified in [Presence2.1_DDS]. The encoding will be using a <link> element as specified in [Presence2.1_DDS] and will include a “label” attribute with a value set to the label provided by the Served RCS presentity and a priority attribute which will for RCS Release 3 always be set to 0.8. Only one such <link> element will be included in the presence document. In case an RCS Release 3 client receives a document containing multiple <link> elements, then it shall only consider the one with the highest priority and use that for the processing described in 6.3.1

Note: the priority of 0.8 was included to allow including links with higher priority in some future RCS release.

Next to the link, also a <homepage> element will be included in the document for backward compatibility with RCS Release 1 and Release 2 (see chapter 6.2.1).

6.1.1.2 Location Information

The location information will consist of three items:

- A descriptive text
- Time zone information
- Geographical Information that can be used on a map.

The descriptive text will be handled as specified in [Presence2.0_DDS] for the “Location Type” building block. As specified for the “Location Type” building block in [Presence2.0_DDS] encoding will use the <other> element including the descriptive text inside of a <place-type> element. RCS Release 3 clients shall not include “from” and “until” attributes. RCS Release 3 clients shall ignore it when received. RCS Release 3 clients shall provide the “until” attribute and set it as specified in chapter 6.2.2.3. As value for the element, RCS Release 3 will only use the free text option. Support for the enumerated values defined in [RFC4589] is thus out-of-scope for RCS Release 3. It is out of scope of RCS Release 3 how a client will handle these enumerated values when received nevertheless.

The time zone information will be handled as specified in [Presence2.0_DDS], for the “Time Zone” building block. As specified for the “Time Zone” building block in [Presence2.0_DDS], encoding will use the <time-offset> element. RCS Release 3 clients shall not include a “from” attribute nor shall they include the optional description attribute as this overlaps with the Location Type. RCS Release 3 clients shall ignore them when received. RCS Release 3 clients shall provide the “until” attribute and set it as specified in chapter 6.2.2.3.

The geographical information will be provided as geographic coordinates. These will be handled as specified in [Presence2.0_DDS] for the “Geographical Location” building block, taking the updates and clarifications of [RFC5491] into account. 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 empty as RCS Release 3 clients will request the watchers to follow the default handling for the other rules. The RCS Release 3 client shall set the “retention-expiry” as specified in chapter 6.2.2.3.

The <location-info> published by a RCS Release 3 presence source 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 Loc format shall not be used by RCS Release 3 presence sources and location information encoded in that way will be ignored by RCS Release 3 clients when received.

RCS Release 3 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]. A RCS Release 3 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 Release 3 presence sources will always provide the coordinates in WGS 84 (latitude, longitude) decimal notation 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 location information will be published as part of the permanent presence state document.

6.1.2 Service

The RCS Release 3 clients shall indicate the service capabilities it supports in the services section of the presence document in accordance with [RCSTRR1] and [RCSTRR2]. In addition, the Release 3 clients shall indicate their support for Video Sharing according to [IR.84] **Error! Reference source not found.** with a service- and media description as defined in [IR.84]**Error! Reference source not found.:**

Service-id: *org.gsma.videoshare*
Version: 2.0
Contact address type: TEL / SIP URI

Note: this means that a RCS Release 3 client shall include both the Video Share 2.0 and the Video Share 1.0 capabilities in order to indicate backwards compatibility.

6.1.3 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:c="urn:ietf:params:xml:ns:pidf:cipid"
  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:gml="http://www.opengis.net/gml"xmlns:gs="http://www.opengis.net/pidflo/1.0"
  entity="tel:+1234578901">
```

```

<tuple id="a0">
  <status><basic>open</basic></status>
  <op:service-description>
    <op:service-id>org.3gpp.cs-speech</op:service-id>
    <op:version>1.0</op:version>
  </op:service-description>
  <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
    service/org.openmobilealliance.pres-
    content/users/sip:1234578901@gsma.org/oma_status-
    icon/rcs_status_icon</rpId:status-icon>
    opD:etag="26362">http://xcap.gsma.org/xcap-ap
    <c:homepage>http://example.com/~alice</c:homepage>
    <opD11:link opD11:label="my blog" opD11:priority="0.8">

```

```

        http://example.com/~alice
    </opd11:link>

    <rpil:place-type opd:until="2009-11-28T21:00:00Z">
        <rpil:other>Herentals, Belgium</rpil:other>
    </rpil:place-type>
    <rpil:time-offset opd:until="2009-11-28T21:00:00Z">+120</rpil: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>

```

6.2 Presentity Side Handling

6.2.1 Link Handling

A RCS Release 3 client will include both the <homepage> element and the <link> element specified in [Presence2.1_DDS]. It will provide the same link in both elements and include the label provided by the Served RCS presentity in the <link> element. The RCS Release 3 client will limit the length of the label to the maximum length that is provided through an operator provisioning setting.

Both the <link> and the <homepage> element will be published as part of the permanent presence state document.

6.2.2 Location handling

6.2.2.1 Ending Location Information Sharing

When the user indicates that he does not want to share his location information with the contacts allowed to see this information anymore, the client can fulfil this request by removing the location information from the Permanent Presence State document.

6.2.2.2 Obtaining Location Information

A client using cellular access shall rely on the SUPL enabled terminal (SET) initiated collaboration that is specified in [SUPL] for obtaining its position. A-GPS shall be used in case 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/W-CDMA 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 Release 3 out of

scope for both clients and networks, as it is not needed to support the RCS Release 3 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

6.2.2.3 Managing Location Information

A RCS Release 3 presence source is not required to include all location elements specified in chapter 6.1.1.2 in the permanent presence state document (that is, all elements are optional to be provided).

The length of the descriptive text that the RCS Release 3 client includes in the Permanent Presence State document will not be longer than the maximum that was provided as an operator provisioning setting.

The maximum time a location update remains available to watchers will be controlled by an operator provisioning setting. RCS Release 3 presence sources will set the "until" attribute and the "retention-expiry" element (see chapter 6.1.1.2) in accordance to this provisioning setting (that is, set it to the current time increased with the value of the setting). Furthermore, RCS Release 3 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 this is done is considered 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 operator control is needed though. This will be realized through an operator provisioning setting controlling the minimum duration between location updates. A RCS Release 3 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 in case the device has not moved. The decision on when an update is needed is left to the client implementation and thus out-of-scope for RCS as long as the client complies with the provisioned minimum interval between updates.

6.2.3 NICKNAME HANDLING

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 Release 3 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 as well in order to minimize the risk of false identifications.

When no display name is received (for example, due to the subscription being initiated from an R2 network), the Release 3 client shall only present the MSISDN to the user.

If the watcher's telephone number is found in the phone book, behaviour shall be as specified in [RCSTRR1] (that is, the received display name shall not be used, but rather the information that is part of the phone book).

A RCS Release 3 client shall be able to deal with display names up until a maximum length of 200 characters.

6.3 Watcher Side Handling

6.3.1 Link Handling

When a RCS Release 3 client receives a presence document from a contact that contains both the <homepage> element and the <link> element, it will check whether both elements refer to the same link. In that case, it will use the <link> element including the label in its presentation towards the end user. If the links differ, it will use the <homepage> element for the presentation and will thus not present the label. In case the document contains multiple <link> elements, the RCS Release 3 client shall only consider the one with the highest priority for this processing. Note: In case only one of the elements is provided, the RCS Release 3 client will use that element in the presentation of the contact's Social Presence Information.

A RCS Release 3 watcher shall be able to deal with labels with a length of maximum 200 characters.

6.3.2 Location Information Handling

It is considered a client implementation decision how received location information from a contact will be handled (for example, displays only the text, use an individual map for each contact and so on. This is considered to be out of scope for RCS. Clients shall provide a means though to display any descriptive text (that is, the content of the <place-type> element) that they might receive.

A RCS Release 3 client should take into account that a received presence document might not contain location information (for example, because it was received from an R2 client, the presence source does not provide it or privacy was enabled).

A RCS Release 3 client shall be able to deal with place-type information with a length of maximum 200 characters.

A RCS Release 3 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.

6.3.3 Capabilities Handling

In RCS Release 3, the capability mechanism introduced in [RCSTRR1] will be improved. In RCS Release 1 and Release 2, there are three operator provisioning settings that control the anonymous fetch operation and that are still applicable in RCS Release 3:

- A setting controlling the watcher's authorization to see the service capabilities
- A setting controlling whether the client is authorized to do an anonymous fetch operation
- A setting controlling whether the client is authorized to use the results of such an operation to display whether or not social presence can be shared with a contact

Those settings are described in chapter 4.9.4 of [RCSTRR1].

An operator wanting to support the “Who I can Invite” feature that is included in the RCS Release 3 scope should authorize the RCS clients of his subscribers to do the anonymous fetch operation and to display the results. Furthermore, for the support of this feature RCS Release 3 introduces additional provisioning settings allowing the operator to control the most important aspects of the user experience and the load on the network:

- A setting controlling the maximum amount of anonymous fetch operations during a certain time period done by a client (that is, for all contacts)
- A setting controlling the maximum interval between anonymous fetch operations 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

These settings will only be used in case the client is provisioned to use anonymous fetch operations.

When the provisioning settings do support the “who I can invite” feature (anonymous fetch operations are authorized and their result are authorized to be shown), the RCS Release 3 client shall highlight the option to invite a contact to share social presence information when a presence document was received as the result of the anonymous fetch operation.

Like in [RCSTRR1] the triggers for a client to initiate an anonymous fetch operation are considered client implementation and thus out-of-scope for RCS as long as the client complies with the provisioned limits.

Note: there might be a conflict between the different provisioning settings (for example, a too low maximum amount of fetch operation combined with a very low maximum interval). In that case, a RCS Release 3 client will prioritize the maximum amount of fetch operations setting over the maximum interval. An operator deploying RCS Release 3 will likely carefully consider the values of these settings and this is not expected to be an issue in practice.

6.3.4 Nickname Handling

If the user has provided a nickname, a RCS Release 3 client shall include it as the display name as part of the identity information provided in the “P-Preferred-Identity” and “From” header of the SIP SUBSCRIBE request used when subscribing to the user's Resource List Server (RLS) document. The RCS Release 3 client shall ensure that the length of the used display name is not larger than the maximum size that was provisioned by the operator.

6.4 Subscriptions and Authorization

6.4.1 Overview

Compared to [RCSTRR1] and [RCSTRR2], RCS Release 3 adds authorization for location information. Contrary to the general concept for social presence information sharing this authorization is not necessarily mutual: user A can get the location information from user B without having to provide his location information. This change impacts all XDM documents

that were used in [RCSTRR1]. The overall subscription and XDM handling mechanisms and concepts do not change though.

Furthermore, the anonymous rule is now managed by the user to allow controlling whether the information that the user is capable of sharing social presence information is public or not.

6.4.2 XML Document Structure

The Presence XML data management server XDMS shall contain the authorization rules that were specified in [RCSTRR1], with following additions and clarifications:

- "granted contacts" rule – will be used as the rule to provide all social presence information (RCS Release 1 and 2 SPI and geo-location 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 a RCS user contain a reference to the "oma_buddylist" list in Shared XDMS instead of directly to the "rcs" list. This allows subscribing with one RLS subscription to the presence information of both the contacts with whom only social presence information is shared and those that are also allowed to see the location information.

The "shared" XDMS shall contain the same lists provided and managed by the RCS client that were introduced in [RCSTRR1] and an additional one. Following enhancements and clarifications should be taken into account compared to [RCSTRR1]:

- "rcs" list: This list includes all contacts with which basic Social Presence and location information is shared. Commonly referred in RCS from both the "buddylist" and "granted contacts" lists, as the contacts that are allowed to see your presence are also your buddies (symmetric).
- "rcs_basic_spi_only" list: This list includes all contacts with which only basic Social Presence information is shared. Commonly referred in RCS from both the "buddylist" and "granted_basic_spi_only_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 buddies are stored. The "oma_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 "rcs" list
- "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 "rcs_basic_spi_only" list

Note: the other lists used in [RCSTRR1] are not mentioned as there are no changes. As in previous releases, a contact should be in one list only. To ensure that the RCS Release 3 client checks 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.

For RCS Release 3, the template definitions below replace the ones provided in [RCSTRR1].

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>

  <! -- This rule allows all service capabilities to be sent for anonymous requests -->
  <! -- in order 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: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:ietf:params:xml:ns:pidf:cipid">
            name="homepage">
                true
        </pr:provide-unknown-attribute>

        <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>

```

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>

</rls-services>
```

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 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"/>
  </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"/>
  </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 buddies the owner wants to provide all social presence information
  to -->
  <list name="rcs">
    <display-name>My presence buddies with location sharing</display-name>
  </list>

  <!-- The list of 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 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>
```

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.

6.4.3 XML Document Handling

When first started the RCS Release 3 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 Release 3 client shall create them. If the documents exist, the RCS Release 3 client will check whether they comply with the templates defined in chapter 6.4.2 by using following criteria for the documents:

- For the “resource-lists” document, check whether it contains a “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
- For the “rls-services” document, check if it refers to the “oma_buddylist” list. If the document refers to the “rcs” list instead, the RCS Release 3 client shall modify it to refer to the “oma_buddylist” list
- For the “pres-rules” document, check whether it contains the “rcs_basic_spi_only_granted_contacts” rule. If not, the RCS Release 3 client shall add this rule to the document.

Once the documents have been setup in this way, the RCS Release 3 client shall only modify the “rcs”, “rcs_basic_spi_only”, “rcs_revokedcontacts” and “rcs_blockedcontacts” lists in the “resource-lists” document. Only if the user requests to recreate the documents according to the possibility offered in chapter 4.10 of [RCSTRR1], the other documents and parts of the “resource-lists” document should be modified.

6.4.4 Privacy for RCS Capability

A user might not want to share with all users that have an entry for him in their phonebook that he is RCS capable and can thus be invited to share social presence. For those users RCS Release 3 introduces the option to disable the sharing of this information with users with whom no social presence information (with or without geo-location information) is shared. When the user enables this setting, the client will change the rule for anonymous subscriptions. Without privacy enabled, this rule would either be the “rcs_allow_services_anonymous” rule provided in the pres-rules template defined in chapter 6.4.2 or the variant introduced in [RCSTRR1] in chapter 4.9.4 if the device is provisioned not to reveal its actual service capabilities. When the user enables the privacy setting, the rule used for the anonymous subscriptions should be replaced with the standard one from [PRESENCEIG]:

```
<! -- This rule blocks all anonymous subscriptions -->
<! -- This rule replaces the rcs default "rcs_allow_services_anonymous" rule -->
<cr:rule id="wp_prs_block_anonymous">
  <cr:conditions>
    <ocp:anonymous-request/>
  </cr:conditions>
  <cr:actions>
    <pr:sub-handling>block</pr:sub-handling>
  </cr:actions>
</cr:rule>
```

Note: as a default RCS Release 3 clients will not have privacy enabled and will thus use the “rcs_allow_services_anonymous” rule defined in chapter 6.4.2 or the one defined in [RCSTRR1] depending on the operator provisioning settings.

When privacy is disabled, the RCS Release 3 client shall change the rule for the handling of anonymous subscriptions back to the one corresponding to the settings with which the client is provisioned by the operator.

In order to correctly deal with this setting, which is shared between all devices of the same user, the RCS Release 3 client shall not store locally on the device whether or not privacy is enabled. Whenever it has to present this setting to the user; it shall rather determine its current state based on the rule for the handling of anonymous subscriptions that is in use at that moment.

6.5 Rls Server Handling

6.5.1 Nickname Handling

A RLS server supporting RCS Release 3 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.

6.6 Presence Server Handling

6.6.1 Nickname Handling

A presence server supporting RCS Release 3 shall include any display name it received in the P-Asserted-Identity header 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. In case the P-Asserted-Identity header does not contain any display name, the display name provided in the From header of the subscription will be used, if any.

6.7 Backward Compatibility And Interworking

6.7.1 Watcher Side Handling

6.7.1.1 Using a RCS Release 2 Client on a RCS Release 3 Network

When used on a RCS Release 3 network, a RCS Release 2 client might receive following presence attributes that were introduced in Release 3:

- The link with label (see chapter 6.3.1)
- The location information (see chapter 6.3.2)
- The Video Share 2.0 capability

As any presence client, the RCS Release 2 client should ignore unknown elements. Therefore, this should cause no issues.

A RCS Release 2 client will not include a display name in its RLS subscription. As this is not against the standards used for RCS Release 2 and according to chapter 6.5.1 that the RLS server should be able to deal with requests without display name, so this should not cause issues when the Release 2 client is used on those networks either.

Furthermore, an anonymous fetch operation to a contact might be blocked due to the contact having requested privacy. This would result in a normal error response to the fetch operation, which like any other error should not cause issues for the Release 2 client.

6.7.1.2 Using a RCS Release 3 Client on a RCS Release 2 Network

When used on a RCS Release 2 network, a RCS Release 3 client might not receive following presence attributes that were introduced in Release 3:

- The link with label (see chapter 6.3.1)
- The location information (see chapter 6.3.2)
- The Video Share 2.0 capability

Since the client should according to the respective chapters be capable of dealing with the absence of this information in the presence document, this should cause no issues.

A RCS Release 3 client will include a display name in its RLS subscription. As this is not against the standards used in RCS Release 2, this should not cause issues when the Release 3 client is used on those networks either. There is no guarantee though that the display name will be relayed further to the presentities.

6.7.1.3 Simultaneous Use of RCS Release 2 and Release 3 Clients

As the subscriptions from different clients are started independently of each other, the only interaction between the clients is through the XDM documents that they share. The introduction of the changes done by a Release 3 client could cause some unexpected side effects for Release 2 clients using the same set of documents.

Once the base set of documents is created according to the templates provided in [RCSTRR1], a Release 2 client manipulates in daily operation only the “rcs”, “rcs_revokedcontacts” and “rcs_blockedcontacts” lists. Those still exist in the templates provided in RCS Release 3. Therefore, these changes themselves will not cause any issues for the Release 2 client in its XDM document manipulation. A side effect of those changes will be however that in its RLS subscription, the Release 2 client will also receive notifications on the status of the contacts in the “rcs_basic_spi_only” list, which is a list unknown to the Release 2 client. According to [RCSTRR2], the Release 2 client presents these unexpected updates to the user if they refer to a known contact. Since due to the address book synchronization, the set of contacts should be the same in all the users' clients, the presence status of the contacts that are on the “rcs_basic_spi_only” list will be presented to the user also in his Release 2 clients therefore this side effect should not be an issue.

Since the “rcs_basic_spi_only” contact list is unknown to the Release 2 client, it will not be able to revoke presence sharing with those users, however despite being able to show their presence information. Depending on the client implementation, the RCS Release 2 client might not offer the option to revoke the sharing as it is aware that the contact is not part of the “rcs” list or it could offer it and try to remove the contact from the “rcs” list. In that latter case, an error will be returned by the network as there is no corresponding entry in the “rcs” list. Likely, this will result in an error being presented to the user. As neither of these behaviours will result in an inconsistent situation and both the revoking of the presence sharing and the combination of clients of two different releases by the same user are expected to be exceptional, this behaviour is considered as being acceptable.

Another exceptional interaction taking place on the XDM documents is in related rule for the handling of anonymous subscriptions. If the operator re-provisions the clients with different setting for the service capability publication (see chapter 4.9.4 of [RCSTRR1]), a Release 2 client might update this rule. Consequently, it may undo the privacy setting that was done by a Release 3 client according to chapter 6.4.4 of this document. Since the user's Release 3 clients will not be aware anymore that privacy was enabled, there is no way to counter this behaviour and the Release 3 will show to the user that privacy is not enabled anymore. Again, this situation should be very exceptional and can be taken into account by operators wanting to update this setting on a network with users using clients of the different releases simultaneously.

6.7.2 PRESENTITY SIDE HANDLING

6.7.2.1 *Using a RCS Release 2 Client on a RCS Release 3 Network*

When used on a RCS Release 3 network, a RCS Release 2 presence source will not publish following presence attributes that were introduced in Release 3:

- The link with label
- The location information
- The Video Share 2.0 capability

This will not cause any issues as this information is not required from the enablers used for Release 3 and any Release 3 clients can deal with the documents that do not contain these elements (see chapter 6.3).

The RCS Release 2 client might receive watcher information notifications containing display names when used on a RCS Release 3 network. As this is supported in the watcher-information format used by the Release 2 client this should cause no issues. The client may either ignore this information or present it to the user. As there is no requirement to support the use of nicknames on Release 2 clients both behaviours are considered acceptable.

The set of XDM documents used by the release 2 client will not follow the templates that are described in chapter 6.4.2. It will rather use those that are described in [RCSTR1]. Both sets of documents provide a consistent behaviour and the changes introduced in Release 3 are only related to the location information feature. Therefore since both are supported by the enablers used in the Release 3 network, this should cause no issues.

6.7.2.2 *Using a RCS Release 3 Client on a RCS Release 2 Network*

When used on a RCS Release 2 network, a RCS Release 3 client might publish following presence attributes that were only introduced in Release 3:

- The link with label
- The location information
- The Video Share 2.0 capability

This will not cause any issues as the publication of this information is supported by the enablers used for Release 2 and any Release 2 clients will ignore this information like any other elements in the document that are unknown to them.

The RCS Release 2 network might not be equipped to support network based positioning using [SUPL]. In that case the RCS Release 3 client will fall back to doing position updates based using a regular GPS receiver if it has one available.

The RCS Release 3 client might not receive watcher information notifications containing display names when used on a RCS Release 2 network. As this is supported in chapter 6.2.3 this should cause no issues.

The set of XDM documents used by the release 3 client will not follow the templates that are described in [RCSTR1] and used by RCS Release 2. It will rather use those that are described in chapter 6.4.2. As both sets of documents provide a consistent behaviour and both are supported by the enablers used in the Release 2 network, this should cause no issues. This means that the Release 3 client will be able to offer privacy for location information even when used on a Release 2 network

6.7.2.3 *Simultaneous Use of RCS Release 2 and Release 3 Presentities*

When the same user uses clients of different releases as a presence source, the additional presence information introduced in Release 3 will not cause issues. According to

[RCSTRR2] Release 2 clients will not manipulate presence elements that they are not supporting. So they will touch neither the geographical information nor the link with the label that are part of the permanent presence state document. Therefore the only issue that could be caused by the Release 2 client is a misalignment between the <homepage> element and the OMA element providing the link with the label that is introduced in release 3. According to chapter 6.3.1, Release 3 clients will deal properly with such misalignments. Release 2 clients will not notice such a misalignment as they do not interpret the OMA element.

The handling of the XDM documents that are manipulated by the clients of both releases has been discussed already in chapter 6.7.1.3.

6.7.3 Interworking between RCS Release 2 and Release 3 networks

Also the interworking between networks of both releases should not cause any issues in the presence area. On the NNI interface, the main differences are

- The new elements in the presence documents that are sent from a Release 3 to a Release 2 network and that are not provided in the other direction
- The display name that may be present in the backend subscriptions that are sent from the Release 3 to the Release 2 network and that is not provided in the other direction

The new elements should be passed transparently to the watchers by the Release 2 RLS server. Those will deal with them properly as discussed in chapters 6.7.1.1 and 6.7.2.2. In the other direction a RCS Release 3 RLS server will have no issues handling documents that do not contain the new elements. It will pass those documents transparently to the watchers that will deal properly with them as described in chapters 6.7.1.2 and 6.7.2.1.

A RCS Release 2 Presence Server should have no issue with a backend subscription containing a display name, as this is part of the standards that it supports. There is no guarantee though that it will pass the display name to the Served RCS presentity in the watcher information notification. According to the description in chapter 6.6.1, a RCS Release 3 presence server should be able to deal with backend subscriptions without display name.

7 Address Book

There are no changes in the area of Address Book in Release 3, the text in [RCSTRR2] is fully applicable.

8 Content Sharing

8.1 General

RCS Release 3 builds on the content sharing functionality supported in RCS Releases 1 and 2, and incorporates the following additional features:

1. One-to-one Content Sharing outside of a voice call between 2 RCS Release 3 users
 - a. Support for Video Sharing and Image Sharing
2. One-to-one Content Sharing with Legacy Terminals – Live
 - a. Support for Video Sharing
3. One-to-one Content Sharing with Legacy Terminals – Deferred
 - a. Support for Video Sharing
4. One-to-one Content Sharing during a voice call, using content stored in the network
 - a. Support for Live Video Sharing

- b. Both endpoints are RCS R3 users

These additional Content Sharing features in RCS Release 3 are based on the following specifications:

1. Video Sharing features: All sections of [IR.84] which are applicable to the additional features are included. The reference architecture required to support the Content Sharing features in RCS Release 3 is described in IR.84 [IR.84] Section 1.1.
2. Image Sharing outside of a Voice Call: [IMENDORSE]

Note: For Release 3, the content sharing features defined in RCS Release 1 and RCS Release 2 shall not be altered. Video Sharing and Image Sharing during a voice call shall thus be realized based on [VIDEOSHARE] and [IMAGESHARE] respectively.

8.2 Image Sharing Without Voice Call

Image Sharing outside of a Voice Call shall utilise file transfer mechanism, as described in [IMENDORSE]. Image Sharing without CS Voice Call shall support the file disposition: "Render". "Render" indicates an immediate display of the transferred image.

Image Sharing during a CS Voice Call shall continue to be based on [IMAGESHARE].

8.3 Video Sharing Without Voice Call

Video Sharing without Voice Call involves the establishment of a Video Sharing session between two RCS R3 terminals without an accompanying voice call. It shall be noted that if a voice call is established between the two endpoints after a Video Sharing session has been established, the voice call shall exist independently from the ongoing Video Sharing session. The Video Sharing session can include packet video with or without packet audio.

A detailed description of this feature can be found in [IR.84] Sections 2.5.1 and 2.5.1.1. Additional information can be found in Sections 2.3.2, 2.4.3.

8.4 Video Sharing Live To Legacy Terminal

Video Sharing Live to a Legacy Terminal involves the streaming of content (video) live from an RCS R3 Client to a non-RCS Terminal through the Video Sharing network infrastructure (as specified in IR.84 Section 1.1). A non-RCS Terminal can be a legacy mobile device or a PC.

IR.84 has defined a new logical entity called Web Portal to enable this use case. This logical entity is shown in Section 1.1, Figure 1 of [IR.84]. Web Portal provides a web interface to facilitate access by a legacy terminal to video being streamed by a RCS R3 terminal. Access to this web interface may require a username and password, for security purposes.

Details of this feature can be found in [IR.84] Section 2.8.5, with additional information in Sections 2.8.1, 2.8.3, 2.3.2, 2.4.3.

8.5 Video Sharing Deferred To Legacy Terminal

Video Sharing Deferred to a Legacy Terminal is a variation of the previous use case and involves the sharing of content (video) from an RCS R3 Client to a non-RCS Terminal in a Deferred manner using the Video Sharing network infrastructure (as specified in IR.84 Section 1.1). 'Deferred' refers to the fact that the video is not streamed live from the originating RCS R3 Client to the Legacy Terminal. Instead, the streamed video is stored temporarily in a file for later retrieval by the Legacy Terminal.

A detailed description of this feature can be found in [IR.84] Section 2.8.5, with additional information in Sections 2.8.1, 2.8.3, 2.3.2, 2.4.3.

8.6 Video Sharing Live With Content From A Network Content Server

This feature is described in [IR.84] Section 2.5.5. Additional information can be found in Sections 2.5.1, 2.3.2, 2.4.3.

When the INVITE request received by the VS-AS contains the +g.3gpp.cs-voice feature tag (that is it is about sharing content from a network content server during a voice call), the VS-AS will include in the INVITE request going out to the invitees only an Accept-Contact header with the +g.3gpp.cs-voice feature tag. For this use case it will thus not include the ICSI feature tag with the MMTEL ICSI and the IARI feature tag with the Video Share IARI. The included contact header will include the +g.3gpp.cs-voice, the ICSI feature tag with as value the MMTEL ICSI and the IARI feature tag with the Video Share IARI as value. This is needed in order to maintain equal forking preferences between clients of previous releases basing on [VIDEOSHARE] and clients basing on [IR.84] allowing to realize the multi-device behaviour for content sharing.

8.7 Streaming/Uploading Video from an RCS Release 3 Client to a Network Content Server

An RCS R3 user can stream/upload video to a Network Content Server. To stream/upload a video to the Network Content Server, the RCS R3 user selects the Content Server as the terminating endpoint, and initiates a normal video sharing session. The Content Server has a unique identity, which may be provisioned on the device. The uploaded video can be shared with other RCS R3 users at a later time, as described in Section 8.6.

This feature is described in [IR.84] Section 2.8.

8.8 Backward Compatibility with RCS Releases 1 & 2 Clients

RCS R1/R2 Clients operating in an RCS R3 network can continue to use the R1/R2 Video Sharing and Image Sharing features without any modification. IR.84 is backwards compatible with IR.74. Specifically, (a) in the case of a video share session during a voice call, the Video Sharing AS in RCS R3 shall be transparent to the signalling [IR.84, Section 1.1] for an RCS R1/R2 Client; and (b) in the case of Image Sharing during a voice call, the RCS R1/R2 Client shall function as in the previous releases.

Image Sharing without a Voice Call to RCS R1/R2 Clients will result in one of the following behaviour depending on R1/R2 terminal implementation:

1. the R1/R2 terminal will reject the image sharing session
2. the R1/R2 terminal will treat the file as an attachment
3. the R1/R2 terminal will render the shared image

9 File Transfer

There are no changes in the area of File Transfer in Release 3, the text in [RCSTRR2] is fully applicable.

10 Messaging

10.1 Architecture

Messaging in RCS includes the messaging services SMS and MMS and the RCS Chat service based on OMA SIMPLE IM Session Mode.

RCS Release 3 adds the possibility for a RCS BA client used as a primary device to receive SMS, send, and receive MMS, including requesting and receiving message status notifications. This in addition to the possibility to send SMS messages defined in RCS Release 2.

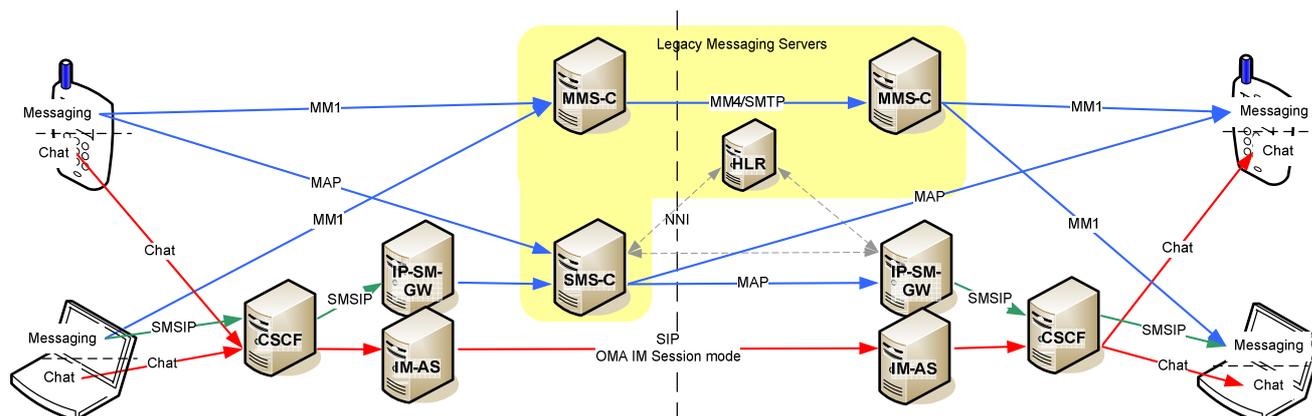


Figure 3: Overall Architecture of Messaging as part of RCS

The SMS service over a BA is realized using 3GPP SMS over IP transport level interworking service as described in [23.204], as in RCS Release 2. In RCS Release 3 the IP-SM-GW also is involved for delivery of SMS to the RCS User's BA Client. This node is placed in the home network of the RCS user and performs bearer level interworking of SMS messages to and from the RCS user's BA device.

For delivery of SMS to mobile access devices, the IP-SM-GW is not involved in RCS Release 3.

The MMS service over a BA is realized using the 3GPP MMS service as defined in [23.140].

The delivery of MMS notifications is based on push messages delivered using the SMS over IP functionality. Note: The MMS-C interface used for these notifications is not shown in the figure above.

10.2 Legacy Messaging

10.2.1 Introduction

Legacy messaging is realized using existing SMS and MMS services using a conversational view in RCS Release 3, as in Release 1 and Release 2.

10.2.2 SMS Service over Broadband Access

The sending and delivery of SMS messages, including status reports, over a BA in RCS Release 3 follows the procedures of 3GPP SMS over IP Transport-level interworking described in [23.204] and [24.341] with the following clarifications;

- The RCS BA client capable of both sending and receiving SMS acts as both "SM-over-IP sender" and "SM-over-IP receiver" as defined in [24.341].

- The SMS-C address is provisioned in the BA client using appropriate Device Management methods.

10.2.3 MMS Service over Broadband Access

The sending and delivery of MMS messages, including delivery and read, reports over a BA in RCS Release 3 uses the MM1 interface as defined in [23.140], which procedures are further defined in [OMAMMS] with the following clarifications;

- The RCS BA client uses the HTTP binding for the MM1 interface.
- Authentication on the MM1 interface is recommended to be based on HTTP Digest. Depending on the environment and the type of client, authentication method(s) are a commercial deployment decision and thus out of scope of this specification. Please also refer to the BA section of this document and [RCSTRR2] where BA authentication is further discussed.
- As a minimum, the procedures in chapters 6.1, 6.2, 6.3, 6.5 and 6.6 of [OMA MMS] are required to be supported.
- The MMS Notifications, Delivery Report and Read Reports are expected to be received as WAP Push messages carried in SMS messages, thus support for OTA Push procedures as referred in [OMA MMS] are required.
- The MMS-C and HTTP proxy addresses are provisioned in the BA client using appropriate Device Management methods.

10.2.4 Multi-device Handling

When a RCS client is used in combination with a mobile device (that is, the RCS Broadband Access client is used as a secondary device), only the mobile device will receive SMS and MMS messages, including SMS Status reports and MMS Delivery and Read Reports. Replies to SMS and MMS messages sent by the RCS Broadband Access client are delivered to the mobile device only.

The use of the SMS service on a Broadband Access client is in this case limited to the procedures for sending SMS over a Broadband Access defined in [RCSTRR2].

The use of the MMS service on a Broadband Access client is in this case limited to sending a MMS as defined in [OMAMMS] and in chapter 7.1.3 above, with the following clarifications;

- A RCS Broadband Access client shall not request a Delivery or Read Report.

Additional functionality, including delivery of SMS and MMS to multiple devices and management of delivery priorities in such case, is out of scope for RCS Release 3, but may be realized using proprietary means.

10.2.5 Handling of Notifications Carried In SMS Messages

The delivery of SMS and MMS message status notifications (SMS Status Reports, MMS Delivery and Read Reports) are carried in SMS messages and follow the normal SMS message delivery. Message status notifications received for messages unknown to that device (the message may have been sent from another of the user's devices) are ignored as already done in today's devices.

Other types of notifications using SMS as a bearer, for example Address Book and Device Management notifications, follow normal SMS delivery, thus they will not be received on the Broadband Access client when used as a secondary device.

10.2.6 Compatibility with Earlier RCS Releases

A RCS R2 Broadband Access client (or RCS R2/R3 mobile client) operating in a RCS R3 network will not receive SMS messages (including MMS notifications) using SMS over IP as this requires an explicit registration of the SMS over IP reception capability in the network as described in section 3.2.

A RCS R3 Broadband Access client operating in a RCS R2 network will not receive SMS messages, as it always will be operating as a secondary device and thus not register the SMS over IP reception capability described in section 3.2. This is not different from RCS Release 3. See also section 4.2.

10.3 Chat

10.3.1 Introduction

The RCS Chat service in Release 3 is as defined [RCSTRR2] with the addition of the possibility to receive a list of invited users (recipient-history-list) in the chat invite as described in [IMENDORSE].

10.3.2 Compatibility with Earlier RCS Releases

A RCS R2 client operating in a RCS R3 network will silently discard the list of invited users in the chat invite if received.

A RCS R3 client operating in a RCS R2 network will not receive a recipient list.

11 Network Value Added Services

11.1 Introduction

The Network Value Added Services are realized using [TTC_NVAS] Chapter 2, 3, 4, 5 and 6. Whenever [TTC_NVAS] refers to [RCS TRR2], RCS Release 3 clients and network elements have to take into account the additions and clarifications provided in this document as well.

11.2 Compatibility with Earlier Releases

If the base RCS service does not have compatibility with earlier releases, the network value added RCS service does not have compatibility with earlier releases.

11.2.1 Release 2/1 Client and Release 3 Network

Release 2 client does not get the NVAS menu and then does not initiate the network value added service. Release 2 client can initiate the base RCS services.

11.2.2 Release 3 Client and Release 2/1 Network

If release 3 client tries to get the NVAS menu from Release 2 network, Release 2 network rejects it. Release 3 client then does not initiate the network value added service.

11.2.3 Release 3 Network and Release 2/1 Network

Release 3 network sends the INVITE including IARI for NVAS to Release 2 network. Then Release 2 network ignores IARI for NVAS and recognizes it as the base RCS service. Then Release 2 network continues to handle it as the base RCS service.

11.2.4 Release 3 Client and Release 2/1 Client

When originating Release 3 client initiates the network value added service, the terminating Release 2 client receives the INVITE including IARI for NVAS. Then the Release 2 client ignores IARI for NVAS and recognizes it as the base RCS service. The Release 2 client continues to handle it as the base RCS service.

Appendix A: Signalling Sequences (Informative)

Note: The following flows are high level to illustrate the behaviour in case of multiple devices

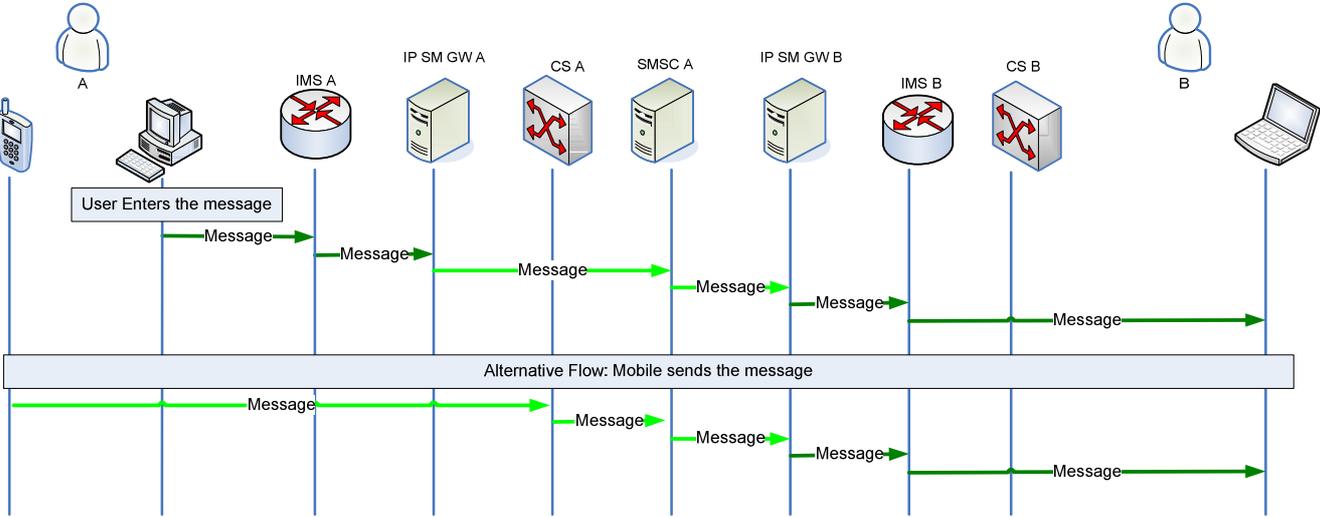


Figure 4: Example high-level flow for SMS to Primary Broadband Access device

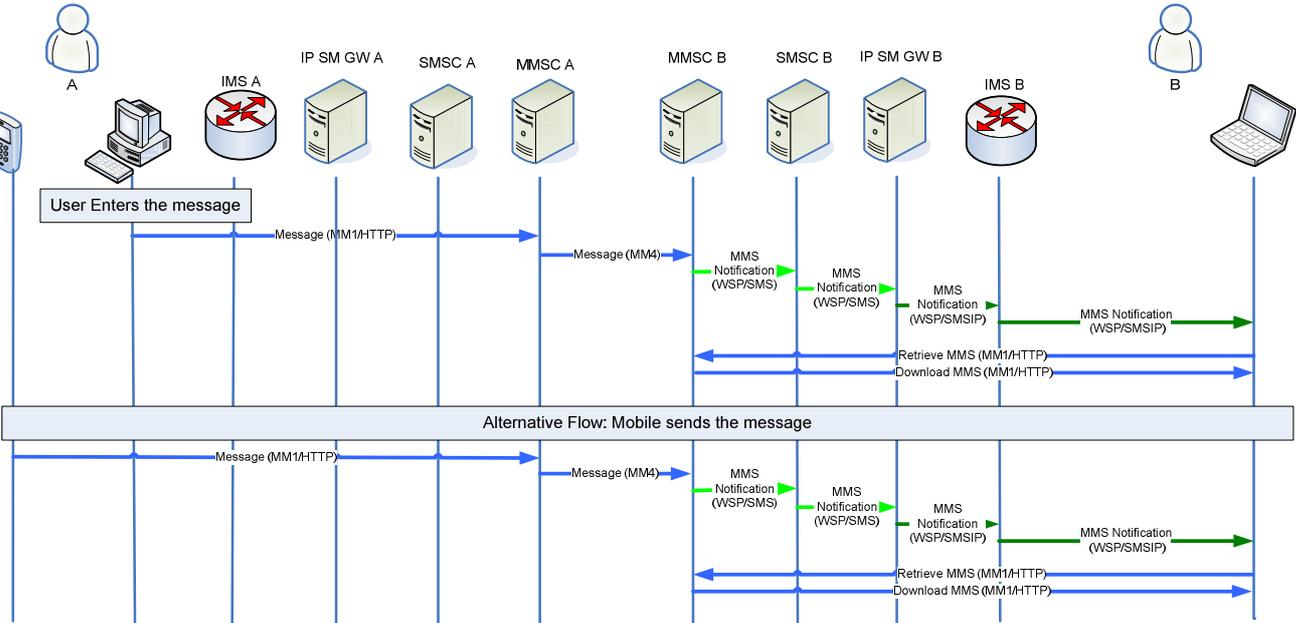


Figure 5: Example high-level flow for MMS to Primary Broadband Access device

Document Management

Document History

Version	Date	Brief Description of Change	Approval Authority	Editor Company /
0.01	5 October 2009	Very first baseline draft for the area responsible distribution	RCS Programme	Tero Jalkanen / TeliaSonera
0.02	12 October 2009	Minor update (chapter alignment with R2 TR for consistency reasons)		
0.03	15 October	Chapter 4 related input added		
0.04	20 October	Modifications to Chapter 4, added input related to Chapter 10 & Appendix A		
0.05	26 October	Added input related to Chapter 6, 8 and 11		
0.06	28 October	Commented version incl. multiple changes around the document		
0.1	29 October	First "real" draft for TG distribution		
0.2	9 November	Second baseline version after incorporating CR: 2009-TR0100 Tel Aviv 2009 TG F2F review		
0.3	27 November	Updated draft with multiple editorial corrections. Also the following CRs are incorporated: <ul style="list-style-type: none"> • 2009-TR0101 • 2009-TR0102 • 2009-TR0103 • 2009-TR0104R1 • 2009-TR0105 • 2009-TR0106R1 • 2009-TR0108 • 2009-TR0109 		
0.4	1 December	Updated with San Francisco TG meeting comments		
0.5	2 December	Final draft version, incorporating CR 2009-TR0110R1		
0.6	11 December	Update on NVAS & Presence 2.1 DDS references review comments received during consistency review See SPEC DOC RCS SPEC R3_006 in https://infocentre.gsm.org/cgi-		

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
		bin/docindex.cgi?34307		
0.7	11 December 2009	Update 0.6 (Approved at Plenary 3/12/09) with front pages for DAG approval. And Infocentre link to TTC RCSS spec	RCS Programme	Dirk Raeymaekers NSN
0.8	14 December 2009	Reference [TTC_RCSS] (in two places) does not exist in reference section. Change to [TTC_NVAS].	RCS Programme	Dirk Raeymaekers NSN
1.0	25 February 2010	Approved by DAG/EMC, removal DAG review sheet	RCS Programme	Dirk Raeymaekers /NSN
1.1	1 December 2010	Update after RCS Paris meeting, incorporated CRs <ul style="list-style-type: none"> RCS3-BF0101R1 In Call Video Share Service Identification RCS2-TR-213R1 Replacement of 'hyper-availability' status by 'availability' status 	RCS Programme	Tero Jalkanen / TeliaSonera
2.0	14 Feb 2011	Submitted to DAG and EMC for approval	EMC	Tero Jalkanen / TeliaSonera

Other Information

Type	Description
Document Owner	Rich Communication Suite Programme
Editor / Company	Tero Jalkanen / TeliaSonera