joyn Implementation Guidelines
Version 3.1
15 February 2017

.

Security Classification – NON CONFIDENTIAL GSMA MATERIAL

Table of Contents

1 Introduction

1.1 Scope

This document provides the highlights of the issues discovered during Interoperability testing (IOT) on the pre-production and production environments of the Operators and contains the guidelines for the Rich Communication Suite (RCS) related protocols implementation in order to achieve seamless interoperability of RCS products and accelerate their time-to-market (TTM).

All clarifications in the current document are related to the respective version of the RCS specification as indicated in the clarification description and all recommendations of the current document would be incorporated into the new versions of the RCS specification.

The guidelines are divided in to six clauses: General and User Interface (UI)/User Experience (UX) issues, Configuration issues, Mobile Operating System (OS) issues, Session Initiation Protocol (SIP)/Session Description Protocol (SDP), Message Session Relay Protocol (MSRP) and Real-Time Protocol (RTP)/Real Time Control Protocol (RTCP) issues. Each clause contains description of issues. These issues are assigned following types:

- Clarification
  Provides further background on functionality already described in the latest version of the RCS specification in order to improve understanding.
- Recommendation
  Includes some suggestions on how the functionality required in the latest version of the RCS specification can be implemented
- Requirement
  Introduces new requirements that will be included in a future update of the RCS specification

The document also includes answers to the frequently asked questions (FAQs).

1.2 Future queries and clarifications

The content of the current document is based on clarification notes provided by the Mobile Network Operators (MNOs) and RCS client manufacturers. These notes were collected during the IOT and accreditation processes on the pre-production and production environments and submitted to the GSMA alone or together with the network traces and self-accreditation declaration forms [5], [6].

The content of the current document is intended to be live and would be updated with new clarifications and recommendations received from the MNOs and RCS client manufacturers.

If you are currently passing through the self-accreditation process please collect and document all the discovered issues and provide together with the declaration form or else send them to the GSMA RCS IOT Team (rcsiot@gsma.com). For more details on self-accreditation procedures refer to [4]

1.3 Definition of Terms

Term	Description
ACS	Autoconfiguration Server
APN	Access Point Name
AS	Application Server
ASO	Arbitrary Slice Ordering

B2BUA	Back-to-Back User Agent
BP	H.264 Baseline Profile
CBP	H.264 Constraint Baseline Profile
CPIM	Common Presence and Instant Messaging
DNS	Domain Name System
EUCR	End User Confirmation Request
FAQs	Frequently asked questions
FQDN	Fully Qualified Domain Name
FMO	Flexible Macroblock Ordering
FT	File Transfer service
FW	Firewall
GPRS	General packet radio service
HSPA	High Speed Packet Access
HTTPS	Hypertext Transfer Protocol Secure
IARI	IMS Application Reference Identifier
IETF	Internet Engineering Task Force
IM	Instant Messaging
IMDN	Instant Message Disposition Notification
IMEI	International Mobile Equipment Identity
IMS	IP Multimedia Subsystem
IMSI	International mobile subscriber identity
IOT	Interoperability testing
IP	Internet Protocol
IS	Image Share service
LTE	Long Term Evolution
MCC	Mobile Country Code
MGCF	Media Gateway Controller Function
MNC	Mobile Network Code
MNO	Mobile Network Operator
MSISDN	Mobile Station International Subscriber Directory Number
MSRP	Message Session Relay Protocol
NAT	Network Address Translation
NDA	Non-Disclosure Agreement
NNI	Network-to-Network Interface
OEM	Original Equipment Manufacturer
OMA	Open Mobile Alliance

OS	Operating system
P-CSCF	Proxy Call Session Control Function
PS	Packet Switched domain
Multi-RAB	Multi Radio Access Bearer
PUP	RCS Pre-Universal Profile
RCS	Rich Communications Suite
RFC	IETF Requests for Comments
RTCP	Real-Time Transport Control Protocol
RTT	Round-Trip delay Time
RTP	Real-Time Transport Protocol
RS	Redundant Slices
SBC	Session Border Controller
SDP	Session Description Protocol
SIP	Session Initiation Protocol
STAP-A	Single-time aggregation packet
TC	Test Case
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TTM	Time-to-market
UA	User Agent
UAC	User Agent Client
UAS	User Agent Server
UDP	User Datagram Protocol
UE	User Equipment
UI	User Interface
UNI	User-to-Network Interface
UUID	Universal Unique Identifier
UX	User eXperience
VoLTE	Voice over Long Term Evolution
VS	Video Share service
WAP	Wireless Application Protocol
XML	eXtensible Markup Language

1.4 Document Cross-References

Ref	Document Number	Title
[1]	RCS5.1	Rich Communication Suite 5.1 Advanced Communications Services

		and Clients specification version 2 http://www.gsma.com/
[2]	RCS IOT 001	RCS IOT joyn Blackbird Test Matrix http://www.gsma.com/
[3]	RCS IOT 002	Guidelines for licensing framework http://www.gsma.com/
[4]	RCS IOT 003	Self-accreditation handbook http://www.gsma.com/
[5]	RCS IOT 004	Self-accreditation declaration form provided by network providers http://www.gsma.com/
[6]	RCS IOT 005	Self-accreditation declaration form provided by RCS client's manufacturers http://www.gsma.com/
[7]	RCS1.2UX	RCS v1.2, User Experience Guidance Document http://www.gsma.com/
[8]	RCS5.0	Rich Communication Suite 5.0 Advanced Communications Services and Clients specification http://www.gsma.com/
[9]	IR.74	Video Share Interoperability Specification 1.2 http://www.gsma.com/
[10]	RFC4575	A Session Initiation Protocol (SIP) Event Package for Conference State, IETF RFC http://tools.ietf.org/html/rfc4575
[11]	RFC3841	Caller Preferences for the Session Initiation Protocol (SIP), IETF RFC http://tools.ietf.org/html/rfc3841
[12]	RFC4122	The Universally Unique IDentifier (UUID) URN Namespace IETF RFC http://tools.ietf.org/html/rfc4122
[13]	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
[14]	3GPP TS 26.114	3GPP TS 26.114 Release 10, 3rd Generation Partnership Project; IP Multimedia Subsystem (IMS); Multimedia telephony; Media handling and interaction http://www.3gpp.org
[15]	DOMAIN	pub.3gppnetwork.org Sub-domain Transfer Process document v0.2
[16]	SIMPLE IM v1.0	Open Mobile Alliance OMA-TS-SIMPLE_IM-V1_0-20120807-A Instant Messaging using SIMPLE www.openmobilealliance.org
[17]	RIG v3.5	RCS Implementation Guidelines v3.5 http://www.gsma.com/
[18]	PDD	joyn Blackbird Product Definition Document http://www.gsma.com/
[19]	3GPP TS 23.228	3GPP TS 23.228 Release 10, 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; IP Multimedia Subsystem (IMS); Stage 2 http://www.3gpp.org
[20]	RFC5438	Instant Message Disposition Notification (IMDN), IETF RFC http://tools.ietf.org/html/rfc5438
[21]	RCS5.2	Rich Communication Suite 5.2 Advanced Communications Services and Client Specification version 5.0 http://www.gsma.com/
[22]	RFC4975	The Message Session Relay Protocol (MSRP) http://tools.ietf.org/html/rfc4975
[23]	RFC6184	RTP Payload Format for H.264 Video http://tools.ietf.org/html/rfc6184

[24]	RCS5.3	Rich Communication Suite 5.3 Advanced Communications Services and Clients specification version 6 http://www.gsma.com/
[25]	IR.92	IMS Profile for Voice and SMS http://www.gsma.com/
[26]	3GPP TS 24.008	3GPP TS 24.008 Release 12, 3rd Generation Partnership Project, Mobile radio interface Layer 3 specification; Core network protocols http://www.3gpp.org
[27]	PRD-RCC.20	Enriched Calling Technical Specification, Version 1.0, 20 July 2015
[28]	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
[29]	RFC3261	SIP: Session Initiation Protocol http://tools.ietf.org/html/rfc3261
[30]	RCC.71	RCS Universal Profile Service Definition Document Version 1.0, 16 November 2016 http://www.gsma.com/
[31]	RFC3840	Indicating User Agent Capabilities in the Session Initiation Protocol (SIP) https://www.ietf.org/rfc/rfc3840.txt
[32]	PDD PRE-UNI	RCS Pre-Universal Profile, Version 1.0, 30 June 2016 http://www.gsma.com/
[33]	PRD-RCC.14	Service Provider Device Configuration, Version 3.0, 21 March 2016 http://www.gsma.com/
[34]	PRD-RCC.15-V1.0	IMS Device Configuration and Supporting Services, Version 1.0, 02 February 2015 http://www.gsma.com/
[35]	PRD-RCC.15-V2.0	IMS Device Configuration and Supporting Services, Version 2.0, 21 March 2016 http://www.gsma.com/
[36]	RCS6.0	Rich Communication Suite 6.0 Advanced Communications Services and Client Specification, Version 7.0, 21 March 2016 http://www.gsma.com/
[37]	IR.51	IMS Profile for Voice, Video and SMS over Wi-Fi http://www.gsma.com/
[38]	SDD-RCC.61	RCS Common Core 2.0 Service Description Document, Version 3.0, 21 March 2016 http://www.gsma.com/
[39]	PRD-RCC.55	RCS Extensibility Terminal API Security, Version 1.0, 15 October 2014 http://www.gsma.com/
[40]	RCC.62	joyn Crane Product Definition Document, Version 3.0, 20 February 2016 http://www.gsma.com/

2 joyn implementation clarifications

2.1 General issues

ID_1_1 Reject_btn parameter

Type	Requirement
Related spec [1] clause	2.3.3.2.3
Applicable joyn release	Blackbird, Crane Priority Release
Related TC [2] ID	N/A
Publish date	04.07.2013
Date modified	15.05.2014

Description

The Reject_btn parameter included in the MSG characteristic that is used to deliver user messages within the autoconfiguration document (described in section 2.3.3.2.3 of [1]) is optional. When not provided a default value of 0 shall be assumed.

ID_1_2 Blushing emotions

Type	Requirement
Related spec [1] clause	3.3.4.1.8
Applicable joyn release	Blackbird, Crane Priority Release
Related TC [2] ID	ID_RCS_7_x_x
Publish date	04.07.2013
Date modified	15.05.2014

Description

To resolve some differences between the joyn UX guidelines and SIMPLE IM, a joyn client shall handle each of the following character sequences as a Blushing emoticon:

:’-) or :”-) or :’) or :”) or :’> or :”> or :-$ or :$.

Since elsewhere the :’-) and :’) may be used for a “crying of happiness” emoticon, it is recommended not to use those combinations when intending to send a Blushing emoticon.

ID_1_3 HTTP Content server URL prefixes

Type	Requirement
Related spec [1] clause	3.5.4.8.4
Applicable joyn release	Blackbird, Crane Priority Release
Related TC [2] ID	RCS_ID_5_1_1
Publish date	17.12.2013
Date modified	15.05.2014

Description

In order to enable the traceability of the HTTP transactions among operators in preproduction or testbed environments in the case operator uses the same server to production environment, the HTTP content server URL prefixes shall follow the format presented below, similar to the scheme used in guideline ID_2_3:

- For Production environment (as defined in [RCS5.1] section 3.5.4.8.4):
  ftcontentserver.rcs.mnc<MNC>.mcc<MNC>.pub.3gppnetwork.org

- For Pre-production environment:
  preprod.ftcontentserver.rcs.mnc<MNC>.mcc<MNC>.pub.3gppnetwork.org
- For Testbed environment:
  testbed.ftcontentserver.rcs.mnc<MNC>.mcc<MNC>.pub.3gppnetwork.org

NOTE: An operator shall not use directly IP server address in the HTTP content server URL in any environment.

ID_1_4 File Transfer over HTTP: sender upload retries in error cases

Type	Clarification
Related spec [1] clause	3.5.4.8.3.1
Applicable joyn release	Blackbird, Crane Priority Release
Related TC [2] ID	RCS_ID_5_1_1
Publish date	07.03.2014
Date modified	07.03.2014

Description

In case of non-successful upload (i.e. error cases other than HTTPS INTERNAL ERROR) with HTTP content server response, the client shall automatically attempt the upload resume procedure (as per 3.5.4.8.3.1 [1]) up to a maximum of 3 times:

- If the get "upload info" request fails with error other than HTTP 404 or 410 then the client shall retry the get "upload info" request.
- If the "resume upload" request fails (content server response other than 200 OK) then the client shall retry by starting the resume upload procedure anew.
- If the "get download info" request fails (content server response other than 200 OK) then the client shall retry by starting the resume upload procedure anew.
- Overall the client shall retry per file upload not more than 3 times until it is considered to be not successful.

In case of non-successful upload due to interrupted transfer, procedures as described in 7.1.1.1 [18] apply.

ID_1_5 Resize video files before transferring

Type	Requirement
Related spec [1] clause	N/A
Applicable joyn release	Blackbird, Crane Priority Release
Related TC [2] ID	N/A
Publish date	15.05.2014
Date modified	25.09.2014

Description

As per 7.1.1 [18], in order to improve the experience when transferring video files, the user should have the possibility to resize a video at point of send within the Chat window that the File Transfer belongs to.

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

- The default resolution shall be 480p encoded at 1200 kbps.
- The resulting size shall be compared to FT WARN SIZE and FT MAX SIZE. The UI shall act correspondingly if the values are reached.

For a pre-recorded video:

- If the resolution is higher than 480p but the file is smaller than FT WARN SIZE the UI warns the user about the resolution of the video.
- if the resolution is higher than 480p and the file is higher than FT WARN SIZE but smaller than FT_MAX_SIZE then the UI warns the user about the resolution and the size.
- if the resolution is higher than 480p and the file is higher than FT MAX SIZE then the UI warns the user about the size and forces the compression or aborts the transfer.

For a live video recording:

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

The video resizing itself shall happen before the File Transfer to the recipient is initiated.

ID_1_6 Support for the FTvHTTP download resume by network

Type	Requirement
Related spec [1] clause	3.5.4
Applicable joyn release	Blackbird, Crane Priority Release
Related TC [2] ID	ID_RCS_5_1_4
Publish date	25.09.2014
Date modified	18.02.2015

Description

A joyn Blackbird network shall always support the FTviaHTTP Download Resume feature.

ID_1_7 Cipher suites support policy for RCS

Type	Recommendation
Related spec [1] clause	2.13.1
Applicable joyn release	Blackbird, Crane Priority Release
Related TC [2] ID	ID_RCS_8_1_1, 8_1_2
Publish date	19.06.2015
Date modified	19.06.2015

Description

As per 2.13.1 [1] it is recommended to enable security mode for signalling and media traffic when it is transported over an unsecure network (e.g. WiFi). In order to ensure the establishment of such secure connections the following cipher suites support policy is recommended for both network and UE implementations:

- Key length for AES should be not lower than 128 bits. If other algorithms are used they should meet that security level.
- DES or RC4 algorithms should not be supported.
- It is recommended to support the current version TLS v1.2.
- SSL v2 or v3 should not be supported.

The minimum recommended cipher suite for RCS signalling and media traffic to be supported by networks and UEs is TLS_RSA_WITH_AES_128_CBC_SHA.

2.2 Configuration issues

ID_2_1 FQDN resolution

Type	Clarification
Related spec [1] clause	2.4.7, A.2.10
Applicable joyn release	Blackbird, Crane Priority Release
Related TC [2] ID	ID_RCS_1_1_1
Publish date	21.02.2012
Date modified	15.05.2014

Description

The FQDN resolution is bearer independent and should be performed by the handset following this process:

1. **Step 1: Autoconfiguration**

   As part of the provisioning process using the autoconfiguration server, the handset gets a FQDN for the P-CSCF.

2. **Step 2: Perform a DNS NAPT SRV query**

   Having obtained the destination domain name the Domain Name System (DNS) is asked to provide matching SIP Server Location Information. One or more NAPTR records may be retrieved and the calling application examines these records to find the best match based on priorities and the desired SIP protocol variant:

```
mnc001.mcc234.3gppnetwork.org. IN NAPTR  50 100 "s" "SIP+D2U"  "" _sip._udp.example.com.
mnc001.mcc234.3gppnetwork.org. IN NAPTR  90 100 "s" "SIP+D2T"  "" _sip._tcp.example.com.
mnc001.mcc234.3gppnetwork.org. IN NAPTR  90 100 "s" "SIPS+D2T" "" _sips._tcp.example.com.
```

   In the above example, “D2U” indicates UDP-based SIP, “D2T” indicates TCP-based SIP, -and “SIPS+D2T” indicates TCP-based encrypted SIP. The presence of these fields indicates what variations of SIP are supported on a given SIP server.

   The "s" flag means the next stage is to look up an "SRV" record.

   Depending on the settings in the XML provided by the autoconfiguration server and the coverage (PS or Wi-Fi), the client will make the choice for the SIP access which they are going to use (SIPoUDP, SIPoTLS or SIPoTCP).

3. **Step 3: Perform a DNS SRV query**

   An example set of SIP server SRV records is as follows:

```
_sip._tcp.example.com.     SRV 0 1 5060    sipserv1.example.com.
_sip._tcp.example.com.     SRV 0 2 5060    sipserv2.example.com.
_sip._udp.example.com.     SRV 0 1 5060    sipserv1.example.com.
_sip._udp.example.com.     SRV 0 2 5060    sipserv2.example.com.
_sips._tcp.example.com.    SRV 0 1 5060    sipserv3.example.com.
_sips._tcp.example.com.    SRV 0 2 5060    sipserv4.example.com.
```

   For each of the variations of the SIP protocols supported the SRV records describe:

   - name of the server;
   - which port number SIP uses; and
   - when there are multiple servers, the weights & priorities to allow rough load balancing.

   The calling network asks the DNS for a SRV record for the host corresponding to the specific service/protocol/domain combination that was returned in Step 2.

   If there are multiple records with the same service/protocol/domain combination, the caller must sort the records based on which has the lowest priority. If there is more than one record with the same priority, the RFC 2782 shall apply.

From the SRV record get the corresponding server name.

There is potential flexibility in this step for the destination operator to receive the SIP traffic on different servers depending on the desired variation of the SIP protocol – TCP, UDP, encrypted, unencrypted.

4. **Step 4: DNS A-query**

   For the server name returned in Step 3, do a standard DNS lookup to finds its IP address This is a normal "A" (address) record lookup:

```
sipserv1.example.com.          IN A    101.1.2.3
sipserv2.example.com.          IN A    101.1.2.4
```

This FQDN resolution procedure shall apply each time the network allocates a new IP address to the Device (example: handover 3G to Wi-Fi) unless IP address change is the result of connectivity regain while the transport protocol remains the same. The client shall store the IP address resulting from the FQDN resolution.

When after connectivity regain the previous client/device registration is valid (registration timer not expired), the client shall use the stored IP address to send an initial REGISTER and to address all subsequent REGISTER and non-REGISTER requests and no FQDN resolution shall be invoked unless connection to the P-CSCF fails. In that case, what is described in ID_2_2 applies.

ID_2_2 P-CSCF redundancy

Type	Requirement
Related spec [1] clause	2.4.7, A.2.10
Applicable joyn release	Blackbird, Crane Priority Release
Related TC [2] ID	ID_RCS_1_x_x
Publish date	04.07.2013
Date modified	15.11.2013

Description

The network operator may deploy the RCS/IMS core in a redundant manner for scalability and high availability reasons. Therefore multiple P-CSCF instances may be available in the network.

The P-CSCF is stateful proxy for the duration of a registration of a user agent. Therefore the P-CSCF discovery and selection procedure need to provide stickiness to the P-CSCF instance selected for the initial registration.

The support of the following procedure is mandated prior to the IMS registration.

RCS/joyn clients receive the P-CSCF address from the auto-configuration server in the LBO_P-CSCF_Address node. Prior to the IMS registration the RCS/joyn client shall handle the address resolution as follows.

- If the P-CSCF AddressType indicates "IPv4" or "IPv6" the RCS/joyn client shall send the initial SIP REGISTER to the address contained in the Address parameter. This IP address shall be used for any subsequent REGISTER and non-REGISTER requests. If the connection to the P-CSCF fails, the RCS/joyn client may consider the configuration as invalid and force a re-configuration via the auto-configuration server.
- If the P-CSCF AddressType indicates "FQDN" the RCS/joyn client shall resolve the FQDN as defined in ID_2_1. If multiple P-CSCF hosts are deployed (e.g. several hosts, up to 4 or more may be deployed) in the network the DNS result will contain multiple SRV or A resource records. In this case the RCS/joyn client shall select one P-CSCF IP address in accordance with the definitions for these DNS resource records.

The RCS/joyn client shall send the initial SIP REGISTER to the selected IP address. The selected IP address shall be stored and used for any subsequent REGISTER and non-REGISTER requests. It should be used together with the port received from the SRV resource record as the topmost route header of SIP transactions initiated by the user agent.

If the connection to the P-CSCF fails (e.g. TCP time-out, connection loss etc.) the RCS/joyn client should select another IP address from the cached DNS search results (if TTL allows) or invoke the FQDN resolution anew. The RCS/joyn client should send an initial registration request to the new selected P-CSCF instance as described in ID_2_1.

It is noted that there are devices on the market already that may not fully comply with the procedure depicted above. OEMs are asked to notify GSMA about these devices. Network operators may take actions in their device provisioning solution to overcome these limitations, e.g. via custom configurations without redundancy.

ID_2_3 Domain prefixes for provisioning

Type	Requirement
Related spec [1] clause	2.3.3.2.1
Applicable joyn release	Blackbird, Crane Priority Release
Related TC [2] ID	RCS_ID_1_1_1
Publish date	22.08.2013
Date modified	15.05.2014

Description

It has been agreed that in order to accelerate Time-To-Market for new joyn releases and at the same time maintain good quality of the current accredited joyn networks and clients Operators should have several network environments. Along with Production environment for commercial use Operators may have Pre-production environment to test resolution of detected issues as well as verify new clients, and there could be also Operators' Testbeds to perform development testing of new joyn releases.

In order to implement that approach all OEMs and client providers are recommended to introduce a mechanism for modification of config domain prefix on a client according to the following config domain prefix values agreed by MNOs:

- Current mechanism for Production environment (*without additional prefix*): config.rcs.mncxxx.mccxxx.pub.3gppnetwork.org
- Proposed value for Pre-production environment (*with additional prefix*): **preprod.**config.rcs.mncxxx.mccxxx.pub.3gppnetwork.org
- Proposed value for Testbed environment (*with additional prefix*): **testbed.**config.rcs.mncxxx.mccxxx.pub.3gppnetwork.org

This recommendation is applicable to device's and client's versions provided for testing only and it is not mandatory for commercial versions.

NOTE*:* an Operator might request from GSMA delegation of the separate subdomains or the parent sub-domain mncxxx.mccxxx.pub.3gppnetwork.org, according to the routine described in [15].

ID_2_4 MSISDN format in configuration request

Type	Clarification
Related spec [1] clause	2.3.3.3.1
Applicable joyn release	Blackbird, Crane Priority Release
Related TC [2] ID	RCS_ID_1_5_1
Publish date	15.11.2013
Date modified	15.11.2013

Description

The MSISDN provided by the client in the configuration request should be in international format. In case that the MSISDN comes with a "+", the following clarifications should be taken into account:

HTTP is the main protocol involved and compliance with the relevant RFCs is suggested. Specifically:

- As per RFC2616 and RFC2396, "+" is a reserved character that should be avoided from being used.
- As per http://www.w3.org/Addressing/URL/4_URI_Recommentations.html, "+" is reserved as shorthand notation for a space and it is likely that is interpreted by the Configuration Server as such. For that reason real plus signs must be encoded.
- As per RFC 3986, percent-encoding is used to represent characters outside the allowed set.

The client should provide the MSISDN value with the plus sign encoded based on percent-encoding i.e. "%2B".

Example: for the msisdn value: +44790000001 the client should send %2B44790000001.

ID_2_5 HTTP request during Wi-Fi Provisioning

Type	Clarification
Related spec [1] clause	2.3.3.3.1
Applicable joyn release	Blackbird, Crane Priority Release
Related TC [2] ID	ID_RCS_1_6_1
Publish date	15.11.2013
Date modified	15.11.2013

Description

The flow in Figure 8 of section 2.3.3.3.1 of [1] may (as mentioned) only be performed in case the client can guarantee that the HTTP request is not routed through the network over a PS connection terminated by another device (e.g. a Wi-Fi to 3G router). Only in that case, a client may start the configuration over Wi-Fi by sending a plain HTTP request. In the more likely case (mobile devices) where the client is not aware of whether or not the request will pass through a device that routes it to the network over a PS connection the device shall start immediately with an HTTPS request when performing the configuration over Wi-Fi.

ID_2_6 Configuration mechanism over PS without Header Enrichment

Type	Clarification
Related spec [1] clause	2.3.3.2
Applicable joyn release	Blackbird, Crane Priority Release
Related TC [2] ID	ID_RCS_1_5_1
Publish date	15.11.2013
Date modified	15.11.2013

Description

In case that the device is connected using a PS data network and the RCS configuration server is unable to successfully identify/verify the identity of the requester (e.g. header enrichment is not implemented by the Service Provider) the configuration mechanism over non-3GPP takes place. Specifically:

- The RCS configuration server shall reply with an HTTP 511 NETWORK AUTHENTICATION REQUIRED error response
- The RCS client starts the SMS based configuration mechanism

ID_2_7 Provisioning for high service availability

Type	Requirement
Related spec [1] clause	2.4.7
Applicable joyn release	Blackbird, Crane Priority Release
Related TC [2] ID	ID_RCS_1_x_x
Publish date	15.11.2013
Date modified	15.05.2014

Description

The priority field given during P-CSCF discovery procedure as defined in ID_2_1 and ID_2_2 determines the precedence of use of the record's data. Clients shall always use the SRV record with the lowest-numbered priority value first and fallback to other records of equal or higher value if the connection to the host fails.

If a service has multiple SRV records with the same priority value, clients shall use the weight field to determine which host to use. The weight value is relevant only in relation to other weight values for the service, and only among records with the same priority value.

In the following example, both the priority and weight fields are used to provide a combination of load balancing and backup service.

_sip._tcp.example.com 86400 IN SRV 10 60 5060 bigbox.example.com.
_sip._tcp.example.com 86400 IN SRV 10 20 5060 smallbox1.example.com.
_sip._tcp.example.com 86400 IN SRV 10 10 5060 smallbox2.example.com.

ID_2_8 Clarification on usage of the FT CAP ALWAYS ON parameter

Type	Clarification
Related spec [1] clause	3.5.4.8.2, A.1.3.3, A.1.4
Applicable joyn release	Blackbird, Crane Priority Release
Related TC [2] ID	ID_RCS_5_5_1
Publish date	15.11.2013
Date modified	15.11.2013

Description

Usage of the FT CAP ALWAYS ON configuration parameter shall be restricted to File Transfer via MSRP area only as it makes little sense in the File Transfer via HTTP case. Consequently client is allowed to perform file transfer via HTTP when the receiver is offline even if FT CAP ALWAYS ON is set to 0 in the provisioning document.

ID_2_9 Clarification on expected client behaviour when validity period has expired

Type	Clarification
Related spec [1] clause	2.3.3
Applicable joyn release	Blackbird, Crane Priority Release
Related TC [2] ID	ID_RCS_1_5_1
Publish date	15.11.2013
Date modified	15.11.2013

Description

If the RCS device/client has received the proper RCS configuration and the configuration period has expired as per the Use Case in section 2.3.3 [1] the RCS device/client shall reattempt autoconfiguration immediately. Waiting for the next reboot could potentially take a long time to happen and there is little sense to wait for an extra time since the validity time has been already provided.

For the same reasons the RCS device/client shall reattempt autoconfiguration immediately in case it has failed registration in IMS with error responses (e.g. 4xx, 5xx). Reboot of the device/client wouldn't help here as well in case that problem was caused by a faulty configuration.

ID_2_10 Clarification on format of the 'token' HTTP parameter

Type	Requirement
Related spec [1] clause	Tables 12, 14, 235,236
Applicable joyn release	Blackbird, Crane Priority Release
Related TC [2] ID	ID_RCS_1_5_x
Publish date	15.11.2013
Date modified	15.05.2014

Description

There have been discovered several typos in [1] with appearance of 'token' HTTP parameter used during provisioning. In particular Table 12 lists the 'token' parameter with a capital T (i.e. Token) whereas Table 15 and Table 18 list it with a lower case t (i.e. token). Since HTTP URIs are to be compared case sensitive, an auto-configuration server may have issues with that.

Similar to that Table 17 lists the 'token' characteristic in all lower case whereas Table 14, Table 235 and Table 236 list it in all uppercase. This can be an issue for those same server and client implementations.

That issue has been already fixed in RCS5.1 specification v3.0 which clarifies that HTTP parameter 'token' shall in all cases be provided in all lower case (i.e. token) and that the TOKEN characteristic in the provisioning document shall always be provided in all upper case (i.e. TOKEN).

Given that the joyn Blackbird Product Definition Document refers to the RCS5.1 specification v2.0, it is recommended to apply case insensitive parsing on both server and client ends.

ID_2_11 Max Message Size

Type	Clarification
Related spec [1] clause	3.3.4.2
Applicable joyn release	Blackbird, Crane Priority Release
Related TC [2] ID	N/A
Publish date	15.11.2013
Date modified	15.11.2013

Description

The maximum size controlled through the MAX SIZE 1-to-1 IM configuration parameter defined in [1], Table 80 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, then the user shall be notified that the message is too large.

The parameter shall count the size of the CPIM body only and not include the size of any header or wrapper of the corresponding SIP INVITE request or MSRP SEND request.

ID_2_12 Client behaviour upon re-start

Type	Clarification
Related spec [1] clause	2.3.3.2.4
Applicable joyn release	Blackbird, Crane Priority Release
Related TC [2] ID	N/A
Publish date	17.12.2013
Date modified	17.12.2013

Description

The non-embedded clients upon restart shall apply the logic described in section 2.3.3.2.4 of [1]. Based on that, new version checking shall not been triggered unless at least one of the two conditions is met.

Regarding error handling procedures, errors generated locally by the client SIP stack due to transaction layer errors (RFC 3261 8.1.3.1 Transaction Layer Errors), shall not be treated by embedded and non-embedded clients as IMS core network errors, but handled as connectivity errors.

ID_2_13 403 Forbidden Response on provisioning request

Type	Clarification
Related spec [1] clause	2.3.3
Applicable joyn release	Blackbird, Crane Priority Release
Related TC [2] ID	RCS_ID_1_1_1, RCS_ID_1_2_1
Publish date	07.03.2014
Date modified	07.03.2014

Description

When receiving a HTTP 403 Forbidden response to a configuration request, a client shall behave in the same way as when a provisioning document was received with version and validity set to 0. It shall thus not only remove the existing configuration, if any, but also remove the RCS specific UX (i.e. the entry points and thus return to vanilla behaviour). A network shall take this behaviour into account when deciding whether to send a HTTP 403 response.

ID_2_14 MAX_AD-HOC_GROUP_SIZE parameter format

Type	Clarification
Related spec [1] clause	Annex A, Tables 163 and 242
Applicable joyn release	Blackbird, Crane Priority Release
Related TC [2] ID	RCS_ID_1_1_1
Publish date	07.03.2014
Date modified	07.03.2014

Description

The RCS5.1 [1] and OMA SIMPLE IM [16] specifications define MAX_AD-HOC_GROUP_SIZE configuration parameter with the dash between ‘AD’ and ‘HOC’ whereas Tables 163 and 242 of [1] provide this parameter without the dash (e.g. max_adhoc_group_size) for the HTTP configuration document. As SIMPLE IM does not provide a mapping to the HTTP configuration there is no conflict and therefore the format to be used while performing HTTP provisioning is without dash - max_adhoc_group_size.

ID_2_15 ACS behaviour when user enters incorrect MSISDN

Type	Recommendation
Related spec [1] clause	2.3.3.3.1.2
Applicable joyn release	Blackbird, Crane Priority Release
Related TC [2] ID	ID_RCS_1_2_x
Publish date	07.03.2014
Date modified	07.03.2014

Description

In order to detail the scenario when a client perform provisioning over non-cellular (e.g. WiFi) access and enters an incorrect MSISDN, meaning it is not the MSISDN from the SIM card, but it could be a valid MSISDN and Autoconfiguration Server (ACS) sends an SMS to the incorrect MSISDN and the client with correct MSISDN is waiting for the SMS from ACS.

After a short period has expired, application asks the phone number for second time and user now sends the correct MSISDN using the same cookie of previous request.

The recommended behaviour of the ACS for that case is as follows:

- Ignore the cookie because it receives a new initial request.

  OR

- Take into account that the parameters may have changed.

NOTE: The main reason for providing the cookie is to allow the ACS to link the requests together. Based on the parameters it can determine that this would be a new initial request there is no previous request that it should link to and as such it must take into account the new values.

ID_2_16 default_sms_app parameter

Type	Requirement
Related spec [1] clause	N/A
Applicable joyn release	Blackbird, Crane Priority Release
Related TC [2] ID	N/A
Publish date	15.05.2014
Date modified	25.09.2014

Description

The default_sms_app parameter as described in sections 2.3.3.2 and 2.3.3.3 of RCS5.2 specification [21] shall be added in the HTTPS request GET parameters. This new parameter is relevant for primary device configuration over both PS and non-PS access. Any change of the SMS application that is translated into a different default_sms_app parameter value shall result in a configuration query towards the Configuration Server For the case that default_sms_app parameter is set to 2 and fully integrated messaging is configured by the Service Provider, the client shall not include the integrated messaging tag in the capability exchange.

ID_2_17 Parameter IM SMS FALLBACK AUTH (SmsFallBackAuth): Values

Type	Clarification
Related spec [1] clause	A.1.3.3, A.2.6
Applicable joyn release	Blackbird, Crane Priority Release
Related TC [2] ID	ID_RCS_1_x_x
Publish date	25.09.2014
Date modified	25.09.2014

Description

The values 0 and 1 of SmsFallBackAuth parameter have opposite meaning in [1] section A.1.3.3 Table 80 and section A.2.6 Table 170.

As defined in [21] the correct meaning for the values in Table 170 are:

0 - Indicates authorization is not granted, i.e. fallback is disabled;

1 - Indicates authorization is granted, i.e. fallback is enabled.

ID_2_18 Parameter IM SMS FALLBACK AUTH (SmsFallBackAuth): Interaction with Fully Integrated Messaging

Type	Recommendation
Related spec [1] clause	A.1.3.3
Applicable joyn release	Blackbird, Crane Priority Release
Related TC [2] ID	ID_RCS_1_x_x
Publish date	25.09.2014
Date modified	25.09.2014

Description

As Fully Integrated Messaging already defines its own rules for resending undelivered joyn messages via SMS including the case where the transmission from the device fails, it is advised that Operator set SmsFallBackAuth parameter to 0 (authorization is not granted, i.e. fallback is disabled) when they enable Fully Integrated Messaging, in order to avoid any undesired interaction between the both fallback mechanisms.

Hence, if the value of MessagingUX parameter is set to 1, then it is recommended that the value of the SmsFallBackAuth parameter is set to 0.

ID_2_19 Parameter Register Q-VALUE (QValue)

Type	Clarification
Related spec [1] clause	A.1.6.3, A.2.2
Applicable joyn release	Blackbird, Crane Priority Release
Related TC [2] ID	ID_RCS_1_x_x
Publish date	25.09.2014
Date modified	25.09.2014

Description

As explicitly stated in [1] section A.1.6.3 Table 80, QValue parameter was Mandatory in RCS 5.0 but is now optional.

The occurrence value in [1] section A.2.2 Table 113 shall therefore be “ZeroOrOne”.

ID_2_20 Parameter DELETE-URI

Type	Clarification
Related spec [1] clause	A.1.3.1
Applicable joyn release	Blackbird, Crane Priority Release
Related TC [2] ID	ID_RCS_1_x_x
Publish date	25.09.2014
Date modified	25.09.2014

Description

The last line of Table 79 in [1] section A.1.3.1 related to DELETE-URI must be ignored.

ID_2_21 Parameters POLLING RATE (pollingRate) and POLLING RATE PERIOD (pollingRatePeriod)

Type	Requirement
Related spec [1] clause	A.1.10
Applicable joyn release	Blackbird, Crane Priority Release
Related TC [2] ID	ID_RCS_1_x_x
Publish date	25.09.2014
Date modified	18.02.2015

Description

When available in the configuration file the POLLING RATE (pollingRate) and POLLING RATE PERIOD (pollingRatePeriod) configuration parameters shall be used during the initial polling of the complete address book at the first time configuration even if POLLING PERIOD (pollingPeriod) is set to 0.

ID_2_22 Generic rules for parameter associated to disabled features

Type	Requirement
Related spec [1] clause	Annex A
Applicable joyn release	Blackbird, Crane Priority Release
Related TC [2] ID	ID_RCS_1_x_x
Publish date	25.09.2014
Date modified	18.02.2015

Description

Several RCS5.1 features are not applicable in joyn Blackbird (e.g. Presence). However, sub-trees or some parameters associated to these features appear with an occurrence of "One" in section A.2 [1] and they should be sent by the Operator.

It is advised that Operator keep these sub-trees or parameters with occurrence of "One" (populated with any authorized value) in their configuration file as they could be considered as mandatory by some Client implementations and a Client SHALL then ignore their content.

Examples of such parameters:

- content of the PRESENCE sub-tree is meaningless when PRESENCE PROFILE (presencePrfl) is set to 0 (not supported) and DEFAULT DISCOVERY MECHANISM (defaultDisc) is set to 0 (the default mechanism employed for capability discovery and new users will be OPTIONS);
- value of the ONE BUTTON VIDEO CALL (oneButtonVideoCall) parameter is meaningless when PROVIDE RCS IP VIDEO CALL (rcsIPVideoCallAuth) is set to 0 (RCS IP Video Call service is disabled).

ID_2_23 Token value upon first time non-cellular configuration

Type	Clarification
Related spec [1] clause	2.3.3.3
Applicable joyn release	Blackbird, Crane Priority Release
Related TC [2] ID	ID_RCS_1_2_x
Publish date	25.09.2014
Date modified	25.09.2014

Description

As per table 12 of section 2.3.3.3.1 of [1], for the case of first time configuration the value of the token HTTP Get parameter should be an empty value and not invalid string. Once successfully configured, in subsequent configuration requests the most recent token value obtained from previous configuration processes shall be reused. If token value is invalid, according to 2.3.3.3.3 of [1] this will result in an HTTP 511 NETWORK AUTHENTICATION REQUIRED error response and for the case that a user retry mechanism is in place, the client shall re-start the configuration process from the beginning.

ID_2_24 Client with access to IMSI and behaviour upon non 3GPP access provisioning

Type	Clarification
Related spec [1] clause	2.3.3.3
Applicable joyn release	Blackbird, Crane Priority Release
Related TC [2] ID	ID_RCS_1_2_x
Publish date	18.02.2015
Date modified	18.02.2015

Description

For the clients with access to IMSI that attempt first time provisioning over non 3GPP access, as per section 2.3.3.3 of [1] the following steps apply:

1. The client shall send provisioning request including the IMSI but not including the MSISDN. The user shall not be asked to insert the MSISDN. If provisioning request fails (e.g. due to lack of network support to retrieve the MSISDN based on IMSI) THEN
2. The client shall send provisioning request including the MSISDN. In that case, the user shall be asked to insert the MSISDN.

The client shall not follow step 2 without attempting step 1.

ID_2_25 HTTP GET parameter terminal_sw_version maximum length

Type	Recommendation
Related spec [1] clause	2.3.3.2.1
Applicable joyn release	Blackbird, Crane Priority Release
Related TC [2] ID	ID_RCS_1_1_x
Publish date	19.06.2015
Date modified	19.06.2015

Description

As per Table 4 of [1] HTTP/HTTPS parameter terminal_sw_version has the maximum length of 10 characters and that can block on the ACS any request from client using the longer software labels.

In order to avoid this is issue it is recommended to extend maximum length of the terminal_sw_version parameter value to 20 characters on both client and network implementations.

ID_2_26 First time Wi-Fi provisioning: checking of radio-cellular network connectivity

Type	Clarification
Related spec [1] clause	2.3.1
Applicable joyn release	Blackbird, Crane Priority Release
Related TC [2] ID	ID_RCS_1_1_x
Publish date	19.06.2015
Date modified	19.06.2015

Description

This clarification applies to a client acting as a primary device.

As long as there is no radio cellular network connectivity (e.g. lack of coverage in indoor situation) available for SMS containing One Time Password receipt by the client, any attempt made by the client to perform a Wi-Fi provisioning procedure when no valid token is available, e.g. first time configuration, will fail. This impacts the customer experience.

Hence, it is required that the client verifies that radio-cellular network connectivity is available prior to performing a first time Wi-Fi provisioning procedure.

ID_2_27 First time Wi-Fi provisioning: retry behaviour transparent to the user

Type	Clarification
Related spec [1] clause	2.3.1
Applicable joyn release	Blackbird, Crane Priority Release
Related TC [2] ID	ID_RCS_1_1_x
Publish date	19.06.2015
Date modified	19.06.2015

Description

This clarification applies to a client acting as a primary device.

During a first-time Wi-Fi provisioning procedure for which no valid token is available when only the IMSI is provided by the client to the network and the network has answered with response different from 403 Forbidden (meaning that the IMSI is sufficient enough to identify the customer – ref to section 2.3.5.1.2 Configuration over non-cellular networks), the client must perform a Wi-Fi provisioning retrying procedure in a transparent way to the

user (e.g. no pop-up requesting the user to enter his/her MSISDN) in case the network did not deliver the SMS (containing one Time Password) for whatever reason as per section 2.3.2.1 [18].

ID_2_28 Group Chat Full Store Forward configuration

Type	Recommendation
Related spec [1] clause	3.4.4
Applicable joyn release	Blackbird, Crane Priority Release
Related TC [2] ID	ID_RCS_1_1_x
Publish date	04.02.2016
Date modified	04.02.2016

Description

From joyn Blackbird version 5.0 onwards the table 33 in [18] mandates the Service Provider to set the configuration GROUP CHAT FULL STORE FORWARD with fixed value "1". In accordance with the definitions in section 3.4.4 of RCC.07 this will cause the joyn Blackbird client to advertise the Group Chat Store and Forward capability via the Full Store and Forward Group Chat IARI tag defined in section 2.6.1.1.2 of [1].

However with the service provider requirement in Table 33 of [18] to set the configuration parameter GROUP CHAT INVITE ONLY FULL STORE FORWARD to value "0", the joyn Blackbird client will ignore the Full Store and Forward Group Chat capability when offering the user contacts for invitation to a Group Chat. This makes the additional feature tag redundant.

With this implementation guideline the table 33 of version 5.0 of [18] is corrected to mandate joyn Blackbird service providers to always set GROUP CHAT FULL STORE FORWARD with the fixed value "0" as it was up to version 4.0 of [18].

Note also, in [24] the configuration parameters GROUP CHAT FULL STORE FORWARD and GROUP CHAT INVITE ONLY FULL STORE FORWARD have been removed from the DM data model and the Full Store and Forward Group Chat IARI tag is no longer used.

ID_2_29 IMS and Transport Protocol Configuration Parameters

Type	Clarification
Related spec [1] clause	A.1.6.1, A.1.6.2, A.2.10
Applicable joyn release	Blackbird, Crane Priority Release
Related TC [2] ID	ID_RCS_1_1_1
Publish date	14.07.2016
Date modified	14.07.2016

Description

This implementation guideline updates section 15.2 of [18] to provide the requirements for the support of client configuration of parameters of the IMS Management Object described in section A.1.6.1 and A.1.6.2 of [1]. In addition it is clarified that the configuration parameters to control the IMS transport protocols for signalling and media in cellular and non cellular access, located in the RCS Configuration MO sub tree defined in section A.2.10 of [1], are applicable for joyn.

Therefore the following configuration parameters need to be added to Table 40 "RCS additional IMS Core/SIP related configuration parameters" in section 15.2 of [18].

Configuration parameter	Description
Timer_T1	Service Provider Configurable The parameter is not applicable for the IMS registration if the configuration parameter ALWAYS USE IMS APN is applicable for the client according to the definitions in section 15.4.1 of [18] and - the value of the configuration parameter ALWAYS USE IMS APN is set to "1", or - the value of the configuration parameter ALWAYS USE IMS APN is set to "0" and RCS uses a cellular connection.
Timer_T2	Service Provider Configurable The parameter is not applicable for the IMS registration if the configuration parameter ALWAYS USE IMS APN is applicable for the client according to the definitions in section 15.4.1 of [18] and - the value of the configuration parameter ALWAYS USE IMS APN is set to "1", or - the value of the configuration parameter ALWAYS USE IMS APN is set to "0" and RCS uses a cellular connection.
Timer_T4	Service Provider Configurable The parameter is not applicable for the IMS registration if the configuration parameter ALWAYS USE IMS APN is applicable for the client according to the definitions in section 15.4.1 of [18] and - the value of the configuration parameter ALWAYS USE IMS APN is set to "1", or - the value of the configuration parameter ALWAYS USE IMS APN is set to "0" and RCS uses a cellular connection.
Private_user_identity	Service Provider Configurable The parameter is not applicable for the IMS registration if the configuration parameter ALWAYS USE IMS APN is applicable for the client according to the definitions in section 15.4.1 of [18] and - the value of the configuration parameter ALWAYS USE IMS APN is set to "1", or - the value of the configuration parameter ALWAYS USE IMS APN is set to "0" and RCS uses a cellular connection.
Public_user_identity	Service Provider Configurable The parameter is not applicable for the RCS IMS registration if the configuration parameter ALWAYS USE IMS APN is applicable for the client according to the definitions in section 15.4.1 of [18] and - the value of the configuration parameter ALWAYS USE IMS APN is set to "1", or - the value of the configuration parameter ALWAYS USE IMS APN is set to "0" and RCS uses a cellular connection.
Home_network_domain_name	Service Provider Configurable The parameter is not applicable for the RCS IMS registration if the configuration parameter ALWAYS USE IMS APN is applicable for the client according to the definitions in section 15.4.1 of [18] and - the value of the configuration parameter ALWAYS USE IMS APN is set to "1", or - the value of the configuration parameter ALWAYS USE IMS APN is set to "0" and RCS uses a cellular connection.

Configuration parameter	Description
LBO_P-CSCF_Address	Service Provider Configurable The parameter is not applicable for the RCS IMS registration if the configuration parameter ALWAYS USE IMS APN is applicable for the client according to the definitions in section 15.4.1 of [18] and the device is attached to the HPLMN and - the value of the configuration parameter ALWAYS USE IMS APN is set to "1", or - the value of the configuration parameter ALWAYS USE IMS APN is set to "0" and RCS uses a cellular connection.
SMS_Over_IP_Networks_Indication	Service Provider Configurable
Keep_Alive_Enabled	Service Provider Configurable The parameter is not applicable for the RCS IMS registration if the configuration parameter ALWAYS USE IMS APN is applicable for the client according to the definitions in section 15.4.1 of [18] and - the value of the configuration parameter ALWAYS USE IMS APN is set to "1", or - the value of the configuration parameter ALWAYS USE IMS APN is set to "0" and RCS uses a cellular connection.
Voice_Domain_Preference_E_UTRAN	Service Provider Configurable Only values "1" and "3" are supported, see section 2.9.1 of [1] and section A.1 of [25]
Voice_Domain_Preference_UTRAN	not provided
Mobility_Management_ IMS_Voice_Termination	not provided
RegRetryBaseTime	Service Provider Configurable
RegRetryMaxTime	Service Provider Configurable
PhoneContext_List	not provided
PS SIGNALLING	Service Provider Configurable Indicates the transport protocol to be used to carry the signalling when connecting over PS cellular access. The configuration parameter is not applicable - if the value of the configuration parameter IMS Mode Authentication Type defined in section A.1.6.2 of [1] is set to "IMS AKA". - if the configuration parameter ALWAYS USE IMS APN is set to value "0" or "1" in accordance with the definitions in section 15.4.1 of [18].
PS MEDIA	Service Provider Configurable Indicates the transport protocol to be used to carry the media (e.g. Chat, File Transfer and Image Share services) when connecting over PS cellular access. The configuration parameter is not applicable - if the value of the configuration parameter IMS Mode Authentication Type defined in section A.1.6.2 of [1] is set to "IMS AKA". - if the configuration parameter ALWAYS USE IMS APN is set to value "0" or "1" in accordance with the definitions in section 15.4.1 of [18].

Configuration parameter	Description
PS RT MEDIA	Service Provider Configurable Indicates the transport protocol to be used to carry the real time media (e.g. Video Share) when connecting over PS cellular access. The configuration parameter is not applicable - if the value of the configuration parameter IMS Mode Authentication Type defined in section A.1.6.2 of [1] is set to "IMS AKA". - if the configuration parameter ALWAYS USE IMS APN is set to value "0" or "1" in accordance with the definitions in section 15.4.1 of [18].
WIFI SIGNALLING	Service Provider Configurable Indicates the transport protocol to be used to carry the signalling when connecting over Wi-Fi The configuration parameter is not applicable - if the value of the configuration parameter IMS Mode Authentication Type defined in section A.1.6.2 of [1] is set to "IMS AKA". - if the configuration parameter ALWAYS USE IMS APN is set to value "1" in accordance with the definitions in section 15.4.1 of [18].
WIFI MEDIA	Service Provider Configurable Indicates the transport protocol to be used to carry the media (e.g. Chat, File Transfer and Image Share services) when connecting over Wi-Fi access. The configuration parameter is not applicable - if the value of the configuration parameter IMS Mode Authentication Type defined in section A.1.6.2 of [1] is set to "IMS AKA". - if the configuration parameter ALWAYS USE IMS APN is set to value "1" in accordance with the definitions in section 15.4.1 of [18].
WIFI RT MEDIA	Service Provider Configurable Indicates the transport protocol to be used used to carry the real time media (e.g. Video Share) when connecting over Wi-Fi access. The configuration parameter is not applicable - if the value of the configuration parameter IMS Mode Authentication Type defined in section A.1.6.2 of [1] is set to "IMS AKA". - if the configuration parameter ALWAYS USE IMS APN is set to value "1" in accordance with the definitions in section 15.4.1 of [18].

ID_2_30 Client Post Re-configuration Actions

Type	Recommendation
Related spec [1] clause	2.3.3.2
Applicable joyn release	Blackbird, Crane Priority Release
Related TC [2] ID	ID_RCS_1_x_x
Publish date	14.07.2016
Date modified	15.12.2016

Description

This implementation guideline corrects the requirements for client post re-configuration actions defined in RCS documents.

The client re-configuration is applied if the client receives in result of the configuration request a response containing a full configuration XML document, as defined

- in section 2.3.3.2 of [1] for Blackbird and Crane Priority Release or
- in section 2.2.2. of [32] for RCS Pre-Universal Profile

The client shall update the locally stored values with the values received in the configuration XML document and apply the new values from this point in time onwards.

In addition, there is a number configuration parameters for which the client needs to apply specific post re-configuration actions to enable a change of value at the time of re-configuration.

For configuration parameters with a post re-configuration action requirement, the client shall determine at the time of processing of the full configuration XML document whether the value of a configuration parameter has been changed by comparing the old value (stored in the client local configuration) with the new value (received in the configuration XML document). If for the applied change of value a post re-configuration is required, the client shall invoke it accordingly.

The post re-configuration actions to be applied for the joyn configuration parameters are summarized in the following table.

Configuration parameter	Reference Document and Section	Node Name in Reference Document	Post Re-configuration action
POLLING PERIOD	Section A.2.8 of [1]	/<x>/CapDiscovery/ pollingPeriod	If the value of pollingPeriod transits from "0" to a positive integer value, then the client shall scan the entire address book to discover RCS capable contacts. If the value of pollingPeriod transits from a non zero value to another non zero value, then the client shall restart the polling period timer with the new received value. If the value of the pollingPeriod transits from a positive integer value to "0", then the client shall stop the polling timer.
POLLING RATE	Section A.2.8 of [1]	/<x>/CapDiscovery/ pollingRate	There is no action required by the client at the time of re-configuration.
POLLING RATE PERIOD	Section A.2.8 of [1]	/<x>/CapDiscovery/ pollingRatePeriod	There is no action required by the client at the time of re-configuration.

Configuration parameter	Reference Document and Section	Node Name in Reference Document	Post Re-configuration action
CAPABILITY INFO EXPIRY	Section A.2.8 of [1]	/<x>/CapDiscovery/ capInfoExpiry	There is no action required by the client at the time of re-configuration. Note, the client should apply the new expiry time for a contacts only at the time of the next capability discovery.
MESSAGING CAPABILITIES VALIDITY	Section 3.4.3.1 of [18]	<x>/joyn/ msgCapValidity	There is no action required by the client at the time of re-configuration.
DELIVERY TIMEOUT	Section 4.3.3 of [18]	<x>/joyn/Messaging/ deliveryTimeout	There is no action required by the client at the time of re-configuration.
FT HTTP CAP ALWAYS ON	Section 4.3.3 of [18]	<x>/joyn/Messaging/ ftHTTPCapAlwaysOn	There is no action required by the client at the time of re-configuration.
IM CAP ALWAYS ON	Section A.2.6 of [1]	<x>/imCapAlwaysON	There is no action required by the client at the time of re-configuration.
IM WARN SF	Section A.2.6 of [1]	<x>/imWarnSF	There is no action required by the client at the time of re-configuration.
IM SMS FALLBACK AUTH	Section A.2.6 of [1]	<x>/ SmsFallbackAuth	There is no action required by the client at the time of re-configuration.
IM SESSION AUTO ACCEPT	Section A.2.6 of [1]	<x>/AutAccept	There is no action required by the client at the time of re-configuration.
IM SESSION START	Section A.2.6 of [1]	<x>/imSessionStart	There is no action required by the client at the time of re-configuration.
IM SESSION TIMER	Section A.2.6 of [1]	<x>/TimerIdle	There is no action required by the client at the time of re-configuration.
MAX CONCURRENT SESSIONS	Section A.2.6 of [1]	<x>/ MaxConcurrentSession	There is no action required by the client at the time of re-configuration.
MAX SIZE 1-to-1 IM	Section A.2.6 of [1]	<x>/MaxSize1To1	There is no action required by the client at the time of re-configuration.
MAX_AD-HOC_GROUP_ SIZE		<x>/ max_adhoc_group_size	There is no action required by the client at the time of re-configuration.
CONF-FCTY-URI		<x>/conf-fcty-uri	There is no action required by the client at the time of re-configuration.
GROUP CHAT AUTH	Section A.2.1 of [1]	/<x>/Services/ GroupChatAuth	If the value transits from "0" to "1" the client shall scan the entire address book to discover group chat capable contacts. If the value of GroupChatAuth transits from "1" to "0", then there is no action required by the client.
MAX SIZE GROUP IM	Section A.2.6 of [1]	<x>/MaxSize1ToM	There is no action required by the client at the time of re-configuration.
FT MAX SIZE	Section A.2.6 of [1]	<x>/MaxSizeFileTr	There is no action required by the client at the time of re-configuration.
FT WARN SIZE	Section A.2.6 of [1]	<x>/ftWarnSize	There is no action required by the client at the time of re-configuration.

Configuration parameter	Reference Document and Section	Node Name in Reference Document	Post Re-configuration action
FT AUT ACCEPT	Section A.2.6 of [1]	<x>/ftAutAccept	There is no action required by the client at the time of re-configuration.
FT HTTP CS URI	Section A.2.6 of [1]	<x>/ftHTTPCSURI	Replace with: There is no action required by the client at the time of re-configuration.
FT HTTP CS USER	Section A.2.6 of [1]	<x>/ftHTTPCSUser	There is no action required by the client at the time of re-configuration.
FT HTTP CS PWD	Section A.2.6 of [1]	<x>/ftHTTPCSPwd	There is no action required by the client at the time of re-configuration.
PROVIDE VS	Section A.2.1 of [1] for blackbird Section A.2.1 of [2] for CPR and PUP [32]	/<x>/Services/VSAuth	There is no action required by the client at the time of re-configuration.
PROVIDE IS	Section A.2.1 of [1] for blackbird Section A.2.1 of [24] for CPR and PUP [32]	/<x>/Services/ISAuth	There is no action required by the client at the time of re-configuration.
VS MAX DURATION	Section A.2.2 of [1] for blackbird Section A.2.2 of [24] for CPR	<x>/MaxTimeVideoShare	There is no action required by the client at the time of re-configuration.
IS MAX SIZE	Section A.2.2 of [1] for blackbird Section A.2.2 of [24] for CPR	<x>/MaxSizeImageShare	There is no action required by the client at the time of re-configuration.
IMS Mode Authentication Type	Section A.2.2 of [1]	<x>/AuthType	The client shall unregister before applying the new configuration and register back using the new parameter.
Realm	Section A.2.2 of [1]	<x>/Realm	The client shall unregister before applying the new configuration and register back using the new parameter.
Realm User Name	Section A.2.2 of [1]	<x>/UserName	The client shall unregister before applying the new configuration and register back using the new parameter.
Realm User Password	Section A.2.2 of [1]	<x>/UserPwd	The client shall unregister before applying the new configuration and register back using the new parameter.
tel or SIP URI – international	Section A.2.2 of [1]	<x>/NatUrlFmt	There is no action required by the client at the time of re-configuration.
tel or SIP URI - for non-international format	Section A.2.2 of [1]	<x>/IntUrlFmt	There is no action required by the client at the time of re-configuration.
RCS-E ONLY APN	Section A.2.9 of [1]	/<x>/APN/rcseOnlyAPN	If the value of rcseOnlyAPN transits from a non empty value to an empty value and the client is roaming and the Data traffic switch is disabled and the client is registered in IMS, then the client shall de-register in IMS and attempt to disconnect the PS bearer which uses the old rcseOnlyAPN value.

Configuration parameter	Reference Document and Section	Node Name in Reference Document	Post Re-configuration action
END USER CONF REQ ID	Section A.2.10 of [1]	/<x>/Other/ endUserConfReqId	There is no action required by the client at the time of re-configuration.
uuid_Value	Section A.2.10 of [1]	/<x>/Other/uuid_Value	The client shall unregister before applying the new configuration and register back using the new parameter.

Configuration parameter	Reference Document and Section	Node Name in Reference Document	Post Re-configuration action
ALWAYS USE IMS APN 3.1	Section A.2.9 of [1]	/<x>/APN/ alwaysUseIMSAPN	If the value of alwaysUseIMSAPN transits from "0" to "1" and the client is registered for RCS in a non-cellular connection, then the client shall de-register in the non-cellular connection and register for the authorized RCS using the IMS APN if no VoLTE services IMS registration exists or the client shall re-register in the existing VoLTE services IMS registration using the IMS APN to add the authorized RCS services. If the value of alwaysUseIMSAPN transits from "1" to "0" and there is a non-cellular connection for the internet access available the client shall de-register the IMS registration over the IMS APN if only used for the authorized RCS services or shall re-register to remove the authorized RCS services if the IMS registration is also used for VoLTE services. The client shall use the non-cellular connection to register in IMS for the authorized RCS services. If the value of alwaysUseIMSAPN transits from "0" to "-1" and the client is registered for RCS and VoLTE services in a cellular connection then the client shall re-register to remove the authorized RCS services. The client shall then use the device's internet connection to register in IMS for the authorized RCS services. If the value of alwaysUseIMSAPN transits from "0" to "-1" and the client is registered only for RCS services in a cellular connection then the client shall de-register and terminate this cellular connection. The client shall then use the device's internet connection to register in IMS for the authorized RCS services. If the value of alwaysUseIMSAPN transits from "1" to "-1" and the client is registered for RCS and VoLTE services then the client shall re-register to remove the authorized RCS services. The client shall then use the device's internet connection to register in IMS for the authorized RCS services. If the value of alwaysUseIMSAPN transits from "1" to "-1" and the client is registered only for RCS services then the client shall de-register and terminate the cellular connection. The client shall then use the device's internet connection to register in IMS for the authorized RCS services.

Configuration parameter	Reference Document and Section	Node Name in Reference Document	Post Re-configuration action
			If the value of alwaysUseIMSAPN transits from "-1" to "0" and the client is registered for RCS services using a cellular connection for internet access, then the client shall de-register. If there is a cellular connection with the IMS APN with an IMS registration for VoLTE services, then the client shall re-register to add the authorized RCS services to this IMS registration. If there is no cellular connection with the IMS APN, then the client shall establish one and register for the authorized RCS services. If the value of alwaysUseIMSAPN transits from "-1" to "1" and the client is registered for RCS services using the device's internet connection, then the client shall de-register. If there is a cellular connection with the IMS APN with an IMS registration for VoLTE services, then the client shall re-register to add the authorized RCS services to this IMS registration. If there is no cellular connection with the IMS APN, then the client shall establish one and register for the authorized RCS services.
PS SIGNALLING	Section A.2.10 of [1]	/<x>/Other/ transportProto/ psSignalling	The client shall unregister if registered in a packet switched access before applying the new configuration and register back using the new parameter.
PS MEDIA	Section A.2.10 of [1]	/<x>/Other/ transportProto/psMedia	There is no action required by the client at the time of re-configuration.
PR RT MEDIA	Section A.2.10 of [1]	/<x>>/Other/ transportProto/ psRTMedia	There is no action required by the client at the time of re-configuration.
WIFI SIGNALLING	Section A.2.10 of [1]	/<x>/Other/ transportProto/ wifiSignalling	The client shall unregister if registered in non-3GPP access before applying the new configuration and register back using the new parameter
WIFI MEDIA	Section A.2.10 of [1]	/<x>/Other/ transportProto/ wifiMedia	There is no action required by the client at the time of re-configuration.
WIFI RT MEDIA	Section A.2.10 of [1]	/<x>/Other/ transportProto/ wifiRTMedia	There is no action required by the client at the time of re-configuration.
Transport Protocols: Signalling Roaming	Section 2.2.1. of [34]	<x>/transportProto/ psSignallingRoaming	The client shall unregister if registered in packet switched access outside of the HPLMN before applying the new configuration and register back using the new parameter. Otherwise, there is no action required by the client apart from storing the new value and applying it from then on.
Transport Protocols: Discrete Media Roaming	Section 2.2.1. of [34]	<x>/transportProto/ psMediaRoaming	There is no action required by the client at the time of re-configuration.

Configuration parameter	Reference Document and Section	Node Name in Reference Document	Post Re-configuration action
Transport Protocols: Real Time Media Roaming	Section 2.2.1. of [34]	<x>/transportProto/ psRTMediaRoaming	There is no action required by the client at the time of re-configuration.
Timer_T1	Section 5.10 of [28]	/<X>/Timer_T1	There is no action required by the client at the time of re-configuration.
Timer_T2	Section 5.11 of [28]	/<X>/Timer_T2	There is no action required by the client at the time of re-configuration.
Timer_T4	Section 5.12 of [28]	/<X>/Timer_T4	There is no action required by the client at the time of re-configuration.
Private_user_ identity	Section 5.13 of [28]	/<X>/Private_user_ identity	There is no action required by the client at the time of re-configuration.
Public_user_ identity	Section 5.16 of [28]	/<X>/ Public_user_identity_List/ <X>/Public_user_identity	There is no action required by the client at the time of re-configuration.
Home_network_ domain_name	Section 5.17 of [28]	/<X>/Home_network_ domain_name	There is no action required by the client at the time of re-configuration.
LBO_P-CSCF_ Address	Section 5.24 of [28]	/<X>/LBO_P-CSCF_Address/<X>/ Address	There is no action required by the client at the time of re-configuration.
Voice_Domain_ Preference_E_ UTRAN	Section 5.27 of [28]	/<X>/Voice_Domain_ Preference_E_UTRAN	See section 5.27 of [28]
Mobility_ Management_ IMS_Voice_ Termination	Section 5.31 of [28]	/<X>/Mobility_ Management_IMS_ Voice_Termination	See section 5.31 of [28]
SMS_Over_IP_ Networks_ Indication	Section 5.28 of [28]	/<X>/SMS_Over_IP_ Networks_Indication	See section A.7 of [25]
Keep_Alive_ Enabled	Section 5.29 of [28]	/<X>/Keep_Alive_ Enabled	The client shall unregister before applying the new configuration and register back using the new parameter.
RegRetryBase Time	Section 5.35 of [28]	/<X>/RegRetryBaseTime	There is no action required by the client at the time of re-configuration.
RegRetryMax Time	Section 5.36 of [28]	/<X>/RegRetryMaxTime	There is no action required by the client at the time of re-configuration.
SS_domain_ setting	Section 5.41 of [28]	/<X>/SS_domain_setting	There is no action required by the client at the time of re-configuration.
PS_domain_IMS_ SS_control_ preference	Section 5.42 of [28]	/<X>/PS_domain_IMS_ SS_control_preference	There is no action required by the client at the time of re-configuration.
CAPABILITY DISCOVERY ALLOWED PREFIXES	Section A.2.8 of [24]	/<x>/CapDiscovery/ CapDiscoveryWhiteList/ <x>/Prefix	There is no action required by the client at the time of re-configuration.
COMPOSER AUTH	Section 2.1.2.1 of [27]	/<x>/Services/ composerAuth	See Section 2.1.2.1 of [27]
SHARED MAP AUTH	Section 2.1.2.1 of [27]	/<x>/Services/ sharedMapAuth	See Section 2.1.2.1 of [27]
SHARED SKETCH AUTH	Section 2.1.2.1 of [27]	/<x>/Services/ sharedSketchAuth	See Section 2.1.2.1 of [27]

Configuration parameter	Reference Document and Section	Node Name in Reference Document	Post Re-configuration action
POST CALL AUTH	Section 2.1.2.1 of [27]	/<x>/Services/ postcallAuth	See Section 2.1.2.1 of [27]
CALL COMPOSER TIMER IDLE	Section 2.1.2.1 of [27]	/<x>/Other/ callComposerTimerIdle	See Section 2.1.2.1 of [27]
MESSAGE STORE URL	Section A.2.7 of [36]	/<x>/CPM/ MessageStore/Url	There is no action required by the client at the time of re-configuration.
MESSAGE STORE USER / PASSWORD	Section A.2.7 of [36]	/<x>/CPM/ MessageStore/ UserName	There is no action required by the client at the time of re-configuration.
	Section A.2.7 of [36]	/<x>/CPM/ MessageStore/UserPwd	There is no action required by the client at the time of re-configuration.
MESSAGE STORE AUTH	Section A.2.7 of [36]	/<x>/CPM/ MessageStore/AuthProt	If the configuration parameter is added to the client configuration then the message store client shall establish a connection to the Common Message Store and login in accordance with the authentication method defined in the value of the configuration parameter. The client shall synchronise with the Common Message Store in accordance with the procedures for synchronization defined in section 4.1.6.7 of [34]. If the configuration parameter is removed from the client configuration, then the client shall remove all data associated with locally stored messages resulting from synchronization with the Common Message Store, e.g. UIDs assigned to messages. If the value of the configuration parameter transits between the allowed values, then there is no additional action required apart from applying it with the next establishment of a connection to the Common Message Store onwards.
MESSAGE STORE EVENT REPORTING	Section A.2.7 of [36]	/<x>/CPM/Message Store/EventRpting	There is no action required by the client at the time of re-configuration.
MESSAGE STORE ARCHIVE AUTH	Section A.2.7 of [36]	/<x>/CPM/Message Store/AuthArchive	There is no action required by the client at the time of re-configuration.
SMS MESSAGE STORE	Section A.2.7 of [36]	/<x>/CPM/Message Store/SMSStore	There is no action required by the client at the time of re-configuration.
MMS MESSAGE STORE	Section A.2.7 of [36]	/<x>/CPM/Message Store/MMSStore	There is no action required by the client at the time of re-configuration.
CHAT REVOKE TIMER	Section A.2.4 of [24]	<x>/RevokeTimer	There is no action required by the client at the time of re-configuration.
MESSAGING FALLBACK DEFAULT	Section 2.5.3.6 of [32]	<x>/msgFBDefault	See section 2.5.3.6 of [30]
RECONNECT GUARD TIMER	Section 2.5.3.6 of [32]	<x>/joyn/Messaging/ reconnectGuardTimer	See section 2.5.3.6 of [30]
CFS TRIGGER	Section 2.5.3.6 of [32]	<x>/joyn/Messaging/ cfsTrigger	See section 2.5.3.6 of [30]

Configuration parameter	Reference Document and Section	Node Name in Reference Document	Post Re-configuration action
FT HTTP FALLBACK	Section A.2.6 of [36]	<x>/ftHTTPFallback	See section A.2.6 of [34]
GEOLOCATION TEXT MAX LENGTH	Section A.2.3 of [1]	<x>/LocationParam/TextMaxLength	There is no action required by the client at the time of re-configuration.
NON RCS CAPABILITY INFO EXPIRY	Section A.2.8 of [24]	/<x>/CapDiscovery/nonRCScapInfoExpiry	There is no action required by the client at the time of re-configuration.
PROVIDE IR94 VIDEO	Section A.2.1 of [36]	/<x>/Services/IR94VideoAuth	If the value of the configuration parameter transits from "0" to "1" and • the device is connected to E-UTRAN and • the device is registered in IMS for MMTEL and • the device supports IR.94 conversational video, then it shall re-register in IMS to add the "video" media feature tag. If the value of the configuration parameter transits from "1" to "0" and • the device is connected to E-UTRAN and • and the device is registered in IMS for MMTEL and for IR.94 conversational video then it shall re-register in IMS to remove the "video" media feature tag.
PROVIDE RCS IP VIDEO CALL	Section A.2.1 of [1]	/<x>/Services/rcsIPVideoCallAuth	If the value of the configuration parameter transits from "0" to "1" and • the device is in in RCS-CS and RCS-AA mode and • the data bearer conditions allow the application of RCS IP Video Call as defined in section 2.7 of [1] then it shall re-register in IMS to add the media feature tags for RCS IP Video Call. If the value of the configuration parameter transits from "1" to "0" and the device is registered in IMS for RCS IP Video Call then it shall re-register in IMS to remove the RCS IP Video Call media feature tags.

Configuration parameter	Reference Document and Section	Node Name in Reference Document	Post Re-configuration action
PROVIDE IR51 VOICE	Section A.2.1 of [36]	/<x>/Services/IR51VoiceAuth	If the value of the configuration parameter transits from "0" to "1" and the device is connected to non cellular access, then the device shall invoke the procedures for PDN and IMS connection establishment and IMS registration, as applicable, to enable Multimedia Telephony and SMS over IP in accordance with the definitions in [35]. If the value of the configuration parameter transits from "1" to "0" and • the device is connected to EPC integrated Wi-Fi and • and the device is registered in IMS for MMTEL then it shall de-register in IMS if the registration is exclusively used for Multimedia Telephony and/or SMS over IP, otherwise the client shall re-register to remove the media feature tags for MMTEL and SMS over IP. The device shall apply service continuity for telephony and short messages via the cellular access.
PROVIDE IR51 VIDEO	Section A.2.1 of [36]	/<x>/Services/IR51VideoAuth	If the value of the configuration parameter transits from "0" to "1" and • the device is connected to EPC integrated Wi-Fi and • the device is registered in IMS for MMTEL and • the device supports conversational video, then it shall re-register in IMS to add the "video" media feature tag. If the value of the configuration parameter transits from "1" to "0" and • the device is connected to EPC integrated Wi-Fi and • and the device is registered in IMS for MMTEL and for conversational video then it shall re-register in IMS to remove the "video" media feature tag.
IR51 SWITCH UX	Section 4.3.2 of [38]	/<x>/UX/IR51SwitchUX	See section 4.3.2 of [36]
RCS MESSAGING DATA OFF	Section A.2.1 of [36]	/<x>/Services/Ext/DataOff/rcsMessagingDataOff	See section A.2.1 of [34]
FILE TRANSFER DATA OFF	Section A.2.1 of [36]	/<x>/Services/Ext/DataOff/fileTransferDataOff	See section A.2.1 of [34]
SMSOIP DATA OFF	Section A.2.1 of [36]	/<x>/Services/Ext/DataOff/smsoIPDataOff	See section A.2.1 of [34]

Configuration parameter	Reference Document and Section	Node Name in Reference Document	Post Re-configuration action
MMS DATA OFF	Section A.2.1 of [36]	/<x>/Services/Ext/ DataOff/mmsDataOff	See section A.2.1 of [34]
CONTENT SHARE DATA OFF	Section A.2.1 of [36]	/<x>/Services/Ext/ DataOff/ contentShareDataOff	See section A.2.1 of [34]
PRE AND POST CALL DATA OFF	Section A.2.1 of [36]	/<x>/Services/Ext/ DataOff/ preAndPostCallDataOff	See section A.2.1 of [34]
VOLTE DATA OFF	Section A.2.1 of [36]	/<x>/Services/Ext/ DataOff/volteDataOff	See section A.2.1 of [34]
IP VIDEO CALL DATA OFF	Section A.2.1 of [36]	/<x>/Services/Ext/ DataOff/ IPVideoCallDataOff	See section A.2.1 of [34]
EXTENSIONS DATA OFF	Section A.2.1 of [36]	/<x>/Services/Ext/ DataOff/ extensionsDataOff	See section A.2.1 of [34]
PROVISIONING DATA OFF	Section A.2.1 of [36]	/<x>/Services/Ext/ DataOff/ provisioningDataOff	See section A.2.1 of [34]
SYNC DATA OFF	Section A.2.1 of [36]	/<x>/Services/Ext/ DataOff/syncDataOff	See section A.2.1 of [34]
ALLOW RCS EXTENSIONS	Section A.2.1 of [36]	/<x>/Services/ allowRCSExtensions	See section 2.4.4.6 of [34]
EXTENSIONS MAX MSRP SIZE	Section A.2.10 of [36]	/<x>/Other/ extensionsMaxMSRP Size	There is no action required by the client at the time of re-configuration.
EXTENSIONS POLICY	Section 9.2 of [39]	/<x>/Other/Ext/APIExt/ extensionsPolicy	There is no action required by the client at the time of re-configuration.
Ext	Section 3.4.3.1 of [18]	<x>/joyn/Ext	There is no re-configuration action required for the content of extension nodes
Ext	Section 4.3.3 of [18]	<x>/joyn/UX/Ext	There is no re-configuration action required for the content of extension nodes
Ext	Section 4.3.3 of [18]	<x>/joyn/Messaging/Ext	There is no re-configuration action required for the content of extension nodes
Ext	Section A.2.1 of [1]	/<x>/Services/Ext	There is no re-configuration action required for the content of extension nodes
Ext	Section A.2.2 of [1]	<x>/Ext	There is no re-configuration action required for the content of extension nodes
Ext	Section A.2.4 of [1]	<x>/Ext	There is no re-configuration action required for the content of extension nodes
Ext	Section A.2.6 of [1]	<x>/Ext	There is no re-configuration action required for the content of extension nodes
Ext	Section A.2.7 of [1]	/<x>/CPM/Ext	There is no re-configuration action required for the content of extension nodes

Configuration parameter	Reference Document and Section	Node Name in Reference Document	Post Re-configuration action
Ext	Section A.2.8 of [1]	/<x>/CapDiscovery/Ext	There is no re-configuration action required for the content of extension nodes
Ext	Section A.2.9 of [1]	/<x>/APN/Ext	There is no re-configuration action required for the content of extension nodes
Ext	Section A.2.10 of [1]	/<x>/Ext	There is no re-configuration action required for the content of extension nodes

Note: joyn defines for a number of configuration parameters a fixed value. By nature, client re-configuration actions do not apply for these parameters. These parameters are not covered in the table above.

ID_2_31 Address Book Scan caused by client re-configuration

Type	Clarification
Related spec [1] clause	N/A
Applicable joyn release	Blackbird, Crane Priority Release
Related TC [2] ID	ID_RCS_1_1_1
Publish date	14.07.2016
Date modified	15.12.2016

Description

This implementation guideline replaces the requirement in the second bullet of the list of requirements starting with "The Device Capability Detection shall" in section 3.1.1 of [18]. Other requirements in this list are no impacted and persist as they are.

The Device Capability Detection shall scan the entire address book

- upon after first service configuration (e.g. out-of-the-factory, new installation, after SIM swap), if a configuration XML document is received with a positive integer version value, i.e. no previous client configuration was present on the client,
- after configuration XML document with a positive integer version was received if the stored value of the client configuration version was "0", "-1", "-2" or "-3",
- if a post re-configuration action of a configuration parameter requires the scan of the entire address book as defined in ID_2_30.

ID_2_32 Version value of the XML configuration document

Type	Clarification
Related spec [1] clause	2.3.3
Applicable joyn release	Blackbird, Crane Priority Release
Related TC [2] ID	ID_RCS_1_x_x
Publish date	14.07.2016
Date modified	14.07.2016

Description

The configuration server indicates in a HTTPS client configuration response that the client configuration is valid via a positive integer value in the "version" parameter of the VERS characteristic as defined in section 2.3.3 of [1].

In accordance with the procedures defined in sections 2.3.3.2.1 and 2.3.3.3.1 of [1], the configuration server shall

- not supply configuration parameters apart from the parameters in the VERS and TOKEN characteristics, if the value of the version parameter in the configuration response is set to the same value as provided by the client in the configuration request,
- set the value of the "version" parameter to a different value than received in the request if a full XML configuration document is supplied in the configuration response. The client shall always parse and apply the full XML configuration in this case and shall not apply additional criteria for the acceptance of the XML configuration document (e.g. not assume ascending order of version values).

ID_2_33 Address Book Scan caused by client re-configuration in Pre-Universal Profile

Type	Clarification
Related spec [1] clause	N/A
Applicable joyn release	Pre-Universal Profile
Related TC [2] ID	ID_RCS_1_x_x
Publish date	15.12.2016
Date modified	15.12.2016

Description

This implementation guideline provides an equivalent to ID_2_31 for the RCS Pre-Universal Profile.

The requirement R3-3-5 in section 2.3.2 of [32] is replaced by the following:

R3-3-5:

The device shall perform a scan of the full contact list and find out which of the contacts are enabled for RCS services

- on first RCS device boot up,
- after installation and/or set up of the RCS application and
- after each client re-configuration with impact to the capabilities discovery.

The requirement R3-4-6 in section 2.3.3.2 of [32] is replaced by the following:

R3-4-6:

To satisfy the requirements of R3-3-5 the client shall scan the entire address book

- after first service configuration (e.g. out-of-the-factory, after SIM swap, new installation) if a configuration XML document is received with a positive integer version value and the configuration parameter RCS DISABLED STATE being absent.
- after a configuration XML document with a positive integer version value and the configuration parameter RCS DISABLED STATE being absent was received and the previously stored value of the version was "0", "-1", "-2" or "-3".
- after a configuration XML document with a positive integer version value and the configuration parameter RCS DISABLED STATE being absent was received and the previously stored value of the rcs_state was "0", "-1", "-2" or "-3".
- after the Master Switch changes the value from "OFF" to "ON" and the client receives a configuration XML document with a positive integer value and the configuration parameter RCS DISABLED STATE being absent in response to the request defined in requirement R16-19-2 of [32].
- after a client instance becomes active in result of a switch of multiple instances (as defined in section 2.2 of [32]) and got a client configuration with a positive integer version value and the configuration parameter RCS DISABLED STATE being absent.

- if a post re-configuration action of a configuration parameter requires the scan of the entire address book as defined in ID_2_30.

ID_2_34 Default Value of MESSGAGE STORE URL configuration parameter

Type	Clarification
Related spec [1] clause	N/A
Applicable joyn release	Pre-Universal Profile
Related TC [2] ID	ID_RCS_1_x_x
Publish date	15.12.2016
Date modified	15.12.2016

Description

The definition for the absence of the configuration parameter MESSAGE STORE URL in Table 75 of [36] is corrected as follows:

If the configuration MESSAGE STORE URL is absent and the configuration parameter MESSAGE STORE AUTH is present, then the default value of MESSAGE STORE URL defined in Table 75 of [36] applies. If both configuration parameters MESSAGE STORE URL and MESSAGE STORE AUTH are absent, then the Service Provider does not deploy a Message Store server.

2.3 Mobile OS issues

ID_3_1 Android

ID_3_1_1 Multiple Client handling on Android™ version prior to 7.0 (embedded and downloadable clients)

Type	Requirement
Related spec [1] clause	N/A
Applicable joyn release	Blackbird, Crane Priority Release
Related TC [2] ID	ID_RCS_1_4_x
Publish date	13.07.2012
Date modified	15.12.2016

Description

In order to prevent having two joyn clients on the same device and, therefore, negative consequences in the user experience, the following mechanism shall be implemented by both joyn embedded and downloadable client implementations.

The mechanism is based on the following principles:

- Identifying Android applications as joyn clients using a Manifest.xml meta-data property
- Identifying if a joyn client is enabled by accessing its Shared Preferences and reading a property from it.
- Accessing a joyn client settings screen by sending an intent using the action defined as a Manifest.xml meta-data property.

ID_3_1_1_1 *Client requirements*

Android joyn clients shall define the following meta-data properties in their Manifest.xml file.

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

Table 1: Android joyn client Manifest meta-data properties

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

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

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

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

        <!-- the following meta-data is used to provide the value of the intent action that can be used by other
        applications to start the joyn client settings screen -->
        <meta-data
              android:name="gsma.joyn.settings.activity"
              android:value="com.vendor.product.MyjoynSettingsActivity" />
         <!-- joyn client shall define a settings property such that it can be open by third party applications using
        an intent which action string corresponds to the meta-data value defined above -->
        <activity
              android:name=".MyjoynSettingsActivity">
              <intent-filter>
                    <action
                    android:name="com.vendor.product.MyjoynSettingsActivity" />
                    <category
                    android:name="android.intent.category.DEFAULT" />
              </intent-filter>
        </activity>
```

Table 2 : Android meta-data usage

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

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

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

The shared preferences shall contain a Boolean property named "*gsma.joyn.enabled*".

This property can have two values:

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

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

ID_3_1_1_2 *Client start-up behaviour*

A joyn client when started for the first time on a device shall:

- Retrieve the list of installed applications from the PackageManager, and identify existing joyn clients by looking for the Boolean meta-data property named "*gsma.joyn.client*", as defined in the previous section.
- For every joyn clients that are found, the client shall open their shared preferences named "*pckgname.gsma.joyn.preferences*" and retrieve the Boolean property "*gsma.joyn.enabled*", as defined in the previous section.
- If an existing joyn client is found with the Boolean property "*gsma.joyn.enabled*" set to "*True*", it means that client is already active on the device. The new client shall inform to the user that there is another joyn client already configured in the device and that as a pre-requisite to use this one, it is necessary to disable it. In the same pop-up the possibility to access the joyn settings of the active joyn application (via intent mechanism) shall be offered. The intent action used to open the active joyn client settings screen shall be retrieved by reading its Manifest meta-data property named "*gsma.joyn.settings.activity*".
- If there is no existing joyn client, or that none of them are enabled, the new joyn client may proceed with provisioning and registration. Once the client is successfully provisioned and registered to the network it shall open its own *"pckgname.gsma.joyn.preferences*" shared preferences and set its own "gsma.joyn.enabled" property to "*True*".
- If the joyn client is disabled (e.g. user switch in settings set to OFF) it shall open its own "*pckgname.gsma.joyn.preferences*" shared preferences and set its own "gsma.joyn.enabled" property to *"False*".

Please note this start-up behaviour shall also apply when:

- There is an attempt to re-activate the disabled client;
- When the disabled client is re-started.

For the downloadable clients, it is possible instead of handling multiple clients based on the procedures described above to apply option 2 of Annex B.2. of [30].

ID_3_1_1_3 *Backward compatibility*

In order to support backward compatibility with implementations not using unique shared preferences (e.g. former joyn Hot Fixes clients) client shall additionally define a publicly readable Shared Preferences with the former name “*gsma.joyn.preferences*” and use it in the similar way as described in RCS Implementation Guidelines v3.5 ID_3_1_1. Client shall check “*gsma.joyn.preferences”* defined in the Manifest by other clients as well.

ID_3_1_2 Multiple Client handling on Android™ version superior or equal to 7.0 (embedded and downloadable clients)

Type	Requirement
Related spec [1] clause	N/A
Applicable joyn release	Blackbird, Crane Priority Release
Related TC [2] ID	N/A
Publish date	15.12.2016
Date modified	15.02.2017

Description

For embedded RCS devices and downloadable applications running on Android™ OS version superior or equal to 7.0, the multiple client handling procedures described in Annex B.1 of [30] for a non RCS device or an embedded RCS device where the stack cannot be used by other applications than the native client shall apply.

ID_3_1_3 Avoiding to use the standard port with Android 4.0.3 and 4.0.4

Type	Recommendation
Related spec [1] clause	N/A
Applicable joyn release	Blackbird, Crane Priority Release
Related TC [2] ID	N/A
Publish date	15.11.2013
Date modified	15.11.2013

Description

There have been issues observed with Android versions 4.0.3 and 4.0.4 on some devices. In particular, SIP messages sent via large TCP segments (e.g. >512 bytes) with well-known port 5060 (inbound or outbound without TLS) could not be sent or received. Although with another port (e.g. 5062) or UDP it is possible.

Please see the descriptions of the following android issues ids:

http://code.google.com/p/android/issues/detail?id=34727

http://code.google.com/p/android/issues/detail?id=32736

To avoid this issue it is recommended on the network side to change the DNS records and network setup to use UDP and TCP with another server port, e.g. port 5062.

Note: The protocols ports should be the same for UDP and TCP.

On the RCS client side it is recommended to avoid the usage of the standard port 5060 and to set another high port for outbound client connections and in the contact header for inbound connections.

ID_3_2 iOS (Apple)

No specific guidelines so far

ID_3_3 Symbian

No specific guidelines so far

ID_3_4 Windows Phone

No specific guidelines so far

2.4 SIP/SDP issues

ID_4_1 Normalization of MSISDNs

Type	Recommendation
Related spec [1] clause	2.5.3.1
Applicable joyn release	Blackbird, Crane Priority Release
Related TC [2] ID	ID_RCS_4_1_14
Publish date	21.02.2012
Date modified	13.07.2012

Description

For outgoing requests no normalization is required for the To header and the Request-URI. The format detailed in section 2.5.3.1 of [1] should be used in case the number is not in international format.

Also, in an outgoing request no normalization is required for the MSISDN in From/P-Preferred-Identity since it will have been provided in the provisioning and during registration in international format already.

For incoming requests the MSISDN in From/P-Asserted-Identity will be in international format unless the international format does not exist for that number and should be matched using the same rules which are used when receiving voice calls.

To avoid issues when roaming though for content sharing it is recommended to use the entry corresponding to that number in the address book in case that is in international format rather than the received Caller-ID.

ID_4_2 Registration procedure intervals

Type	Requirement
Related spec [1] clause	2.4
Applicable joyn release	Blackbird, Crane Priority Release
Related TC [2] ID	ID_RCS_1_1_1
Publish date	16.05.2012
Date modified	16.05.2012

Description

There should be only one initial REGISTER sent to the network. This initial REGISTER should be sent when the RCS software is ready on the device.

In case of RCS implementation architecture design, if only one REGISTER is not feasible on the device, a minimum interval between two REGISTER must be set to prevent Deny of Service threshold activation. The minimum interval shall be set to 1 second. It should be able to configure this duration via a local parameter on the device.

ID_4_3 Session description connection attribute

Type	Clarification
Related spec [1] clause	N/A
Applicable joyn release	Blackbird, Crane Priority Release
Related TC [2] ID	RCS_ID_6_1_3
Publish date	22.08.2013
Date modified	22.08.2013

Description

If a session description provided by Originating or Terminating party during establishment of the session includes “c=” (connection) fields in both session and media levels the address provided in the media level shall have priority as defined in the RFC 4566 and [13].

ID_4_4 OPTIONS during bi-directional Video Share session

Type	Clarification
Related spec [1] clause	3.6.4.3.6
Applicable joyn release	Blackbird, Crane Priority Release
Related TC [2] ID	RCS_ID_6_1_3
Publish date	22.08.2013
Date modified	22.08.2013

Description

After establishment of the bi-directional video share session client MAY send OPTIONS request without feature tags to indicate that there are no capabilities to accept additional sharing sessions. In that case remote client SHALL NOT consider that as request to terminate current sessions due to the fact that BYE was not received. Consequently client which has received such OPTIONS request should not do any actions in that case apart from hiding sharing capabilities for the user.

ID_4_5 FT via HTTP upload/download resume

Type	Clarification
Related spec [1] clause	N/A
Applicable joyn release	Blackbird, Crane Priority Release
Related TC [2] ID	N/A
Publish date	15.11.2013
Date modified	15.11.2013

Description

In order to provide more clarity around the procedures regarding the FT via HTTP upload resume procedure described in PRD GSMA RCS 5.1 version 2 section 3.5.4.8.1.1.1, the following clarifications shall be taken into account:

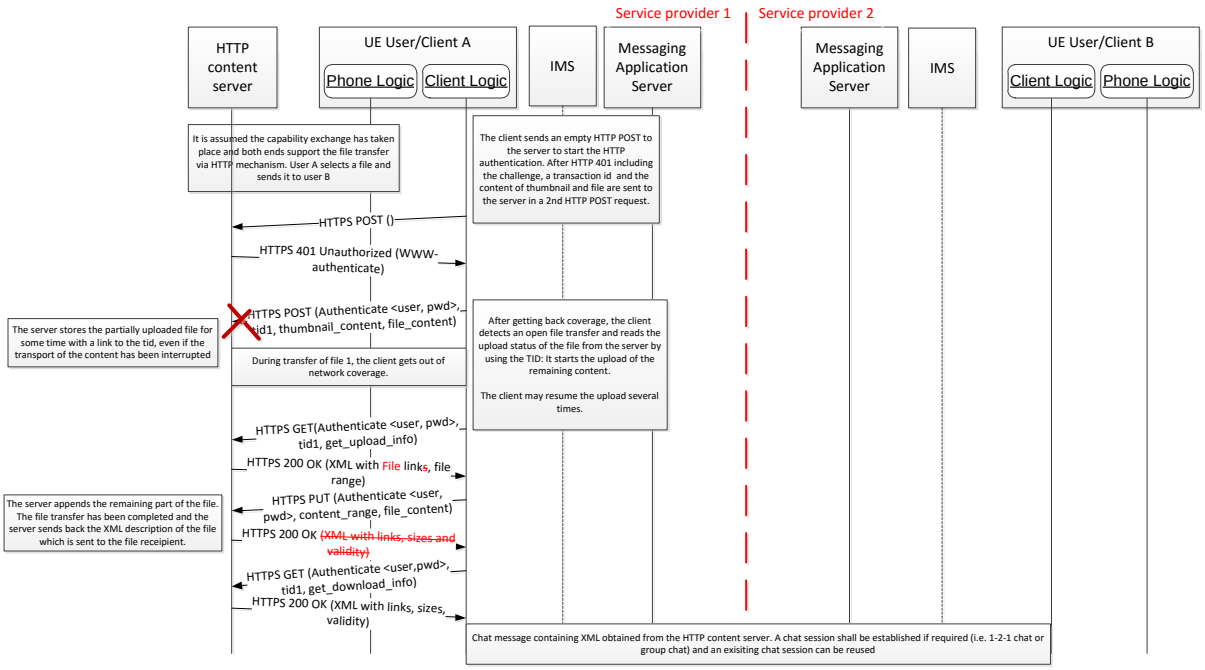
- The content-ranges provided in order to resume the upload of the file always refer to the fragment uploaded so far
- When the server receives the partial file, it shall append the data according to the Content-Range header. In case the upload is successful, a HTTP 200 OK response without body is returned.

- To get the XML description of the complete file to be sent to the file receiver according to 3.5.4.8.3.1 [1], the client sends the following request to the content server:

GET http://< FT HTTP CS URI >?tid=<tid_value>&get_download_info HTTP/1.1

The server sends back a successful HTTP response including the XML description back if the file has been uploaded successfully. In that case the XML includes the file info for the thumbnail (if provided) and the file (as defined in table 59).

An updated figure 75 (PRD GSMA RCS 5.1 version 2 section 3.5.4.8.1.1.1) consistent with the previous comments is provided for reference.



Updated Figure 75: File transfer via HTTP: Resume upload

ID_4_6 SIP User-Agent header

Type	Requirement
Related spec [1] clause	N/A
Applicable joyn release	Blackbird, Crane Priority Release
Related TC [2] ID	N/A
Publish date	15.11.2013
Date modified	15.05.2014

Description

SIP User-Agent sent by the client/device shall comply with [OMA SIMPLE IM v1.0]. According to [OMA SIMPLE IM v1.0] Appendix F:

"User agent and Server headers are used to indicate the release version and product information of the IM Clients and IM Servers. The IM Client and the IM Server shall implement the User-Agent and Server headers, according to rules and procedures of [RFC3261] with the clarifications in this section specific for IM".

User-Agent: **IM-client/OMA1.0 [terminal_vendor/terminal_model-terminal_SW_version] [client_vendor/client_version] [Orange-RCS/ version]**

The parameters **terminal_vendor, terminal_model, terminal_SW_version, client_vendor, client_version** shall be same as used in the http configuration as defined in RCS5.1 specification.

[Orange-RCS/ version] is only added in case Orange-stack is integrated in the client; otherwise it is optional.

Examples native clients:

User-Agent: IM-client/OMA1.0 VND1/Model1-XXXX CLN1/RCS1.0

User-Agent: IM-client/OMA1.0 VND2/Model2-XXXX CLN2-RCS-client1.0

Examples for Android and iPhone App:

User-Agent: IM-client/OMA1.0 APLE/iPhone-7.0 CLN3/RCS1.0.2

User-Agent: IM-client/OMA1.0 VND3/Model3-1.2.3 CLN4/RCS1.0.2

Examples for an Orange-stack based App:

User-Agent: IM-client/OMA1.0 VND5/Model5-1.2.3 CLN5/-RCS1.0.2 Orange-RCS/2.5.8

Note: [client_version] shall be increased in case a new feature is introduced with the new client.

ID_4_7 Clarification on CPIM TO parameter's value used in disposition notifications during Group Chat

Type	Clarification
Related spec [1] clause	3.4.4.1.5
Applicable joyn release	Blackbird, Crane Priority Release
Related TC [2] ID	ID_RCS_7_7_1
Publish date	15.11.2013
Date modified	15.11.2013

Description

According to the section 3.4.4.1.5 [1] when a message has been sent in a Group Chat, the recipient clients should when generating disposition notifications set the CPIM TO header to the identity of the sender of the message. This identity is provided in the CPIM FROM header of the incoming message and may carry the device identifier, which is either a public gruu or a sip.instance value.

Disposition notifications delivered inside the active Group Chat session shall contain CPIM TO headers set to URI found in CPIM FROM of the incoming message and could contain device identifier (e.g. sip.instance) values encoded as defined in section 3.4.4.1.8 of [1].

As not all joyn Blackbird drop 1 networks have implemented ID_4_12, joyn Blackbird drop 1 clients shall not include the device identifier in the Group Chat Message they sent.

NOTE: The lack of device identifier in the sent messages may be a problem in a multi-device group chat environment. As in joyn Blackbird only one device of the user can support Group Chat, the lack of device identifier in Group Chat Messages from joyn Blackbird clients won't cause issues in joyn Blackbird deployments. When in a future evolution of joyn it would be possible to support a multi-device Group Chat experience, either this should not be enabled for users that have a Blackbird client that does not include the device identifier or Group Chat should be disabled on those Blackbird clients.

ID_4_8 Clarification on feature tags in Contact and Accept-Contact headers

Type	Clarification
Related spec [1] clause	3.5.4.8.3.1
Applicable joyn release	Blackbird, Crane Priority Release
Related TC [2] ID	ID_RCS_5_5_1, ID_RCS_5_7_1, ID_RCS_7_7_1
Publish date	15.11.2013
Date modified	15.11.2013

Description

The RCS device/client should insert all tags related to File Transfer service in the Contact header of 1-2-1 chat INVITE which is carrying HTTP file transfer link, including “+g.oma.sip-im” and "+g.3gpp.iari-ref="urn%3Aurn-7%3A3gpp-application.ims.iari.rcs.fthttp".

According to the section 3.5.4.8.3.1 [1] for Accept-Contact there should be multiple of these headers. One Accept-Contact header with the sip-im feature tag and the other Accept-Contact header with the IARI tag for FT via HTTP. That last header shall also contain the ‘required’ and ‘explicit’ parameters.

Similar behaviour is also applicable for Geolocation Push services. The RCS device/client should include in the Contact header of 1-2-1 chat INVITE which is carrying geolocation related data both tags: “+g.oma.sip-im” and "+g.3gpp.iari-ref="urn%3Aurn-7%3A3gpp-application.ims.iari.rcs.geopush". There should be multiple of Accept-Contact headers in INVITE: one Accept-Contact header with the sip-im feature tag and another Accept-Contact header with the IARI tag for Geolocation PUSH and additionally ‘required’ and ‘explicit’ parameters.

The Contact header of the Group Chat INVITE as per [1] shall contain all supported services within a Group Chat (e.g. sip-im, File Transfer via HTTP). The Accept-Contact header of the same INVITE shall only carry sip-im tag.

ID_4_9 Group Chat failed rejoin with non-specified error codes

Type	Requirement
Related spec [1] clause	3.4.4.1.7
Applicable joyn release	Blackbird, Crane Priority Release
Related TC [2] ID	ID_RCS_7_4_1x
Publish date	15.11.2013
Date modified	15.05.2014

Description

In case the RCS device/client fails to rejoin Group Chat it should behave as specified in [1] based on error response code. In RCS5.1 specification behaviour for only 2 error codes is currently defined: 403 Forbidden and 404 Not Found.

Depending on circumstances these 2 error codes above may result in a new Group Chat using the local conference factory. Any other error response is to be handled as what it is, an error preventing the restart of the chat which depending on client implementation may be reported to the user leaving it up to them to take manual action.

ID_4_10 XML body in the INVITE during Geolocation PUSH

Type	Clarification
Related spec [1] clause	3.10.4.1.3.1
Applicable joyn release	Blackbird, Crane Priority Release
Related TC [2] ID	N/A
Publish date	15.11.2013
Date modified	15.11.2013

Description

Section 3.10.4.1.3.1 of [1] states that outside of a voice call the Geolocation XML message body shall be sent as first message in a 1-2-1 Chat. That message should be sent as any first message in a 1-2-1 Chat which could mean sending it as a multipart body of the INVITE request if the device is configured to do that for regular messages.

ID_4_11 Clarification on FT feature tags

Type	Clarification
Related spec [1] clause	3.5
Applicable joyn release	Blackbird, Crane Priority Release
Related TC [2] ID	ID_RCS_5_x_x
Publish date	15.11.2013
Date modified	15.11.2013

Description

In order to avoid any confusion in using various FileTransfer tags please find below some more clarifications for each tag:

- File Transfer +g.3gpp.iari-ref="urn%3Aurn-7%3A3gpp-application.ims.iari.rcse.ft"
  - This tag is used to indicate support for the File Transfer via MSRP service
- File Transfer Thumbnail +g.3gpp.iari-ref="urn%3Aurn-7%3A3gpp-application.ims.iari.rcs.ftthumb"
  - This tag is only relevant in the context of File Transfer via MSRP service. For File Transfer via HTTP a thumbnail may always be uploaded and it is up to the receiving party to decide whether to download
- File Transfer Store and Forward +g.3gpp.iari-ref="urn%3Aurn-7%3A3gpp-application.ims.iari.rcs.ftstandfw"
  - This tag is only relevant in scope of File Transfer via MSRP service as File Transfer via HTTP always provides store and forward functionality
- File Transfer via HTTP +g.3gpp.iari-ref="urn%3Aurn-7%3A3gpp-application.ims.iari.rcs.fthttp"
  - This tag is used to indicate support for the File Transfer via HTTP service and can occur without the urn%3Aurn-7%3A3gpp-application.ims.iari.rcse.ft IARI as that only indicates support for File Transfer via MSRP (rather than File Transfer in general)

ID_4_12 Clarification on forwarding Group Chat Message to legacy clients

Type	Requirement
Related spec [1] clause	3.4.4.1.5
Applicable joyn release	Blackbird, Crane Priority Release
Related TC [2] ID	ID_RCS_7_7_1
Publish date	15.11.2013
Date modified	15.05.2014

Description

When a network forwards a Group Chat Message to a legacy client a joyn Blackbird Messaging Server should next to the behaviour described in section 6.3.4.1 of the joyn Blackbird Product Definition Document [18] (i.e. removing the CPIM/IMDN disposition-notification header and generating the delivery notification on behalf of the legacy client) also remove the device identifier from the CPIM FROM header of the message if present.

ID_4_13 Clarification on File Transfer via HTTP bodies

Type	Clarification
Related spec [1] clause	3.5.4.8.3
Applicable joyn release	Blackbird, Crane Priority Release
Related TC [2] ID	ID_RCS_7_7_1
Publish date	15.11.2013
Date modified	15.11.2013

Description

Both the File Transfer via HTTP XML body returned by the HTTP Content Server and the one that is exchanged between the clients shall correspond to following XML Schema which may be extended further by specific implementations and future versions of this specification. Such extensions shall be ignored by clients that are not aware of them.

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema targetNamespace="urn:gsma:params:xml:ns:rcs:rcs:fthttp"
        xmlns:xs="http://www.w3.org/2001/XMLSchema"
        xmlns="urn:gsma:params:xml:ns:rcs:rcs:fthttp"
        elementFormDefault="qualified"
        attributeFormDefault="unqualified">
    <xs:element name="file">
        <xs:complexType>
            <xs:sequence>
                <xs:element name="file-info" minOccurs="1" maxOccurs="2">
                    <xs:complexType>
                        <xs:sequence>
                            <xs:element name="file-size">
                                <xs:simpleType>
                                    <xs:restriction
                                    base="xs:integer"/>
                                </xs:simpleType>
                            </xs:element>
                            <xs:element name="file-name"
                            minOccurs="0" maxOccurs="1">
                                <xs:simpleType>
                                    <xs:restriction
                                    base="xs:string"/>
                                </xs:simpleType>
                            </xs:element>
                            <xs:element name="content-type">
                                <xs:simpleType>
```

```
                                                <xs:restriction
                                                base="xs:string"/>
                                        </xs:simpleType>
                                </xs:element>
                                <xs:element name="data">
                                        <xs:complexType>
                                                <xs:attribute    name="url"
                                                type="xs:anyURI"
                                                use="required"/>
                                                <xs:attribute name="until"
                                                type="xs:dateTime"
                                                use="required"/>
                                                <xs:anyAttribute
                                                namespace="##other"
                                                processContents="lax"/>
                                        </xs:complexType>
                                </xs:element>
                                <xs:any                 namespace="##other"
                                processContents="lax"
                                minOccurs="0" maxOccurs="unbounded"/>
                        </xs:sequence>
                        <xs:attribute name="type" use="required">
                                <xs:simpleType>
                                        <xs:restriction base="xs:string">
                                                <xs:enumeration
                                                value="file"/>
                                                <xs:enumeration
                                                value="thumbnail"/>
                                        </xs:restriction>
                                </xs:simpleType>
                        </xs:attribute>
                        <xs:attribute name="file-disposition" use="optional">
                                <xs:simpleType>
                                        <xs:restriction base="xs:string">
                                                <xs:enumeration
                                                value="render"/>
                                                <xs:enumeration
                                                value="attachment"/>
                                        </xs:restriction>
                                </xs:simpleType>
                        </xs:attribute>
                        <xs:anyAttribute                namespace="##other"
                        processContents="lax"/>
                </xs:complexType>
        </xs:element>
        <xs:any namespace="##other" processContents="lax" minOccurs="0"
        maxOccurs="unbounded"/>
    </xs:sequence>
  </xs:complexType>
 </xs:element>
</xs:schema>
```

Table 60: File transfer via HTTP message body schema

This schema includes support for a file-disposition attribute which isn't described in [1]. joyn Blackbird clients should ignore this attribute when received and shall not include it in the bodies that they send.

joyn Blackbird clients and content servers may indicate that the XML schema is used in the provided XML as follows:

```
<?xml version="1.0" encoding="UTF-8"?>
<file xmlns="urn:gsma:params:xml:ns:rcs:rcs:fthttp">
        <file-info type="thumbnail" >
                <file-size>[thumbnail size in bytes]</file-size>
                <content-type>[MIME-type for thumbnail]</content-type>
                <data url="[HTTP URL for the thumbnail]" until="[validity of the thumbnail]"/>
        </file-info>
        <file-info type="file">
                <file-size>[file size in bytes]</file-size>
                <file-name>[original file name]</file-name>
                <content-type>[MIME-type for file]</content-type>
                <data url="[HTTP URL for the file]" until="[validity of the file]"/>
        </file-info>
</file>
```

Table 59: HTTP content server response: XML contained in the body

Even if this wasn't described in [1], joyn Blackbird clients shall be able to handle received XML bodies in which this namespace is indicated.

The XML document provided by the HTTP content server with the File Transfer via HTTP upload information content to allow the resume of an interrupted upload shall comply to following schema:

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema targetNamespace="urn:gsma:params:xml:ns:rcs:rcs:fthttpresume"
        xmlns:xs="http://www.w3.org/2001/XMLSchema"
        xmlns="urn:gsma:params:xml:ns:rcs:rcs:fthttpresume"
        elementFormDefault="qualified"
        attributeFormDefault="unqualified">
    <xs:element name="file-resume-info">
        <xs:complexType>
            <xs:sequence>
                <xs:element name="file-range">
                    <xs:complexType>
                        <xs:attribute name="start" type="xs:integer"
                        use="required" />
                        <xs:attribute name="end" type="xs:integer"
                        use="required" />
                        <xs:anyAttribute namespace="##other"
                        processContents="lax"/>
                    </xs:complexType>
                </xs:element>
                <xs:element name="data">
                    <xs:complexType>
                        <xs:attribute name="url" type="xs:anyURI"
                        use="required"/>
                        <xs:anyAttribute namespace="##other"
                        processContents="lax"/>
                    </xs:complexType>
                </xs:element>
                <xs:any namespace="##other" processContents="lax" minOccurs="0"
                maxOccurs="unbounded"/>
            </xs:sequence>
        </xs:complexType>
    </xs:element>
</xs:schema>
```

Table 61: File transfer via HTTP upload information schema

A joyn Blackbird HTTP Content Server may indicate the use of this schema in the File Transfer via HTTP upload information as follows:

```
<?xml version="1.0" encoding="UTF-8"?>
<file-resume-info xmlns="urn:gsma:params:xml:ns:rcs:rcs:fthttpresume">
        <file-range start="[start-offset in bytes]" end="[end-offset in bytes]" />
        <data url="[HTTP upload URL for the file]"/>
</file-resume-info>
```

Table 61: File transfer via HTTP upload information content

Again, joyn Blackbird clients shall be able to handle received upload information bodies in which the use of this namespace is indicated and shall ignore any elements and attributes added based on the extensibility allowed in this schema.

ID_4_14 Client de-registration upon reboot, switch off or termination

Type	Clarification
Related spec [1] clause	2.3 and 2.4
Applicable joyn release	Blackbird, Crane Priority Release
Related TC [2] ID	ID_RCS_1_4_x, ID_RCS_1_5_x, ID_RCS_1_9_x
Publish date	07.03.2014
Date modified	07.03.2014

Description

Assuming that connectivity is available, for the case that:

- Client detects that the device is about to be rebooted or
- Client detects that the device is about to be switched off or
- Client detects that it is being terminated (e.g. upgrade or client being closed by the user)

the client/device shall instantly generate a de-registration request towards the IMS network that is registered as per section 4.5 of 3GPP TS 23.228 [19].

ID_4_15 Group Chat: Conference state event package and user-count element

Type	Clarification
Related spec [1] clause	3.4.4.1.3.1
Applicable joyn release	Blackbird, Crane Priority Release
Related TC [2] ID	N/A
Publish date	15.05.2014
Date modified	15.05.2014

Description

For the conference state event package notification the deleted state for an element of the conference state defined in RFC4575 [10] shall not be used. As a result of that, all users invited upon session (re-)start (SIP INVITE) or added during the session (SIP REFER) shall be included in the conference state event package notification regardless of their status (active, pending, disconnected) until the Group Chat Session is closed.

Based on that, even if a user explicitly leaves a Group Chat upon Group Chat (re-)start (SIP 603 DECLINE) or while Group Chat is active (SIP BYE e.g. SIP;cause=200;text="Call completed"), that status shall remain part of the conference state (and therefore included in every full conference state notification) until the session is closed. Users subscribing to the conference status shall thus be aware of such events regardless when their subscription was received by the Controlling Function during the same active session.

As per RFC4575 [10], user-count represents the number of users participating in the conference at a certain point regardless of their status (active, pending, dis-connected) and can therefore be higher than the maximum-user-count which does not include the users in the disconnected state.

ID_4_16 Additional Client functionality

Type	Clarification
Related spec [1] clause	2.6.1.1.2
Applicable joyn release	Blackbird, Crane Priority Release
Related TC [2] ID	N/A
Publish date	25.09.2014
Date modified	25.09.2014

Description

RCS clients may include additional services and functionality beyond the scope defined in joyn Blackbird. This could either be services defined in the RCS specifications that are not included in joyn Blackbird or entirely proprietary enhancements.

If such functionality requires support from the terminating side beyond the standard joyn Blackbird features, it may only be offered for use towards contacts that support it and therefore needs to rely on the capability exchange. If this additional functionality is defined in the RCS specifications, it is allowed to use the defined identifiers for that service only when the implementation intends to be fully compliant to what is described in the RCS specification. This includes aspects such as using the correct media types, etc. In this case it shall also be possible to disable the functionality through the configuration defined for that purpose in the RCS specifications. This might be required when the functionality is included in a future joyn version and issues are discovered in the implementation.

Additional functionality that is proprietary or that derives from a service defined in the RCS specification without intending to be fully compliant (e.g. a partial implementation), shall use operator specific identifiers as defined in section 2.6.1.1.3 of the RCS 5.1 specification [1]. Again it should be possible to disable such functionality.

ID_4_17 Additional functionality deployed in a network

Type	Clarification
Related spec [1] clause	2.6.1.1.2
Applicable joyn release	Blackbird, Crane Priority Release
Related TC [2] ID	N/A
Publish date	25.09.2014
Date modified	25.09.2014

Description

RCS clients deployed in a network may include additional services and functionality beyond the scope defined in joyn Blackbird (see also ID_4_16). Such functionality shall not be allowed to cross the NNI unless requiring no support on the receiving end beyond the standard joyn Blackbird features or being explicitly covered by a bilateral agreement between Operators. This includes the identifiers exchanged as part of the capability exchange. Given that different implementations may be involved, it is recommended to put such bilateral agreements in place only after extensive interoperability testing between the networks.

ID_4_18 403 Forbidden response for a Conference Chat

Type	Clarification
Related spec [1] clause	3.4.4.1.7
Applicable joyn release	Blackbird, Crane Priority Release
Related TC [2] ID	RCS_ID_7_4_18
Publish date	18.02.2015
Date modified	18.02.2015

Description

A 403 Forbidden Error that is returned from the Messaging Server, when the client is not authorized to recreate the group chat, shall contain a warning header with the warning text set to '127 Service not authorised' as specified in OMA SIMPLE IM [16]. In that case the RCS client shall create a new group chat with new Contribution-ID.

Any other SIP 403 Forbidden response to a non-REGISTER request without warning header, shall be considered as loss of registration due to change of IP, expiration, network problem and handled as in section 2.4.8 of [1].

ID_4_19 Handling of the subscriptions to the conference event package

Type	Clarification.
Related spec [1] clause	3.4.4.3.1
Applicable joyn release	Blackbird, Crane Priority Release
Related TC [2] ID	N/A
Publish date	19.06.2015
Date modified	19.06.2015

Description

For the handling of subscriptions to the conference event package from the participating function to the controlling function the Connection Model defined in section 3.4.5.3 of [24] applies.

ID_4_20 Discovery via OPTIONS message: contact addition or modification

Type	Clarification.
Related spec [1] clause	2.6.2.1
Applicable joyn release	Blackbird, Crane Priority Release
Related TC [2] ID	RCS_ID_4_2_x
Publish date	24.08.2015
Date modified	24.08.2015

Description

As per section 2.6.2 of [1], user discovery via OPTIONS shall be triggered when the user adds a new contact or modifies an existing contact which results in a new IMS identity for the contact.

According to section 2.5.1 of [1] phone numbers and SIP URIs of contacts are applicable to discover RCS users.

Thus any creation or modification of a contact which does not create a new phone number or SIP URI shall not trigger user discovery via OPTIONS message.

ID_4_21 Dual IMS Registration and device instance identification

Type	Clarification.
Related spec clause	2.2.1, 2.2.2, 2.4.2 [1]
Applicable joyn release	Blackbird, Crane Priority Release
Related TC [2] ID	RCS_ID_1_1_1
Publish date	24.08.2015
Date modified	04.02.2016

Description

If the value of the configuration parameter ALWAYS USE IMS APN is set to "-1" joyn Blackbird devices supporting and configured for the use of VoLTE shall apply separate IMS registrations for VoLTE (Multimedia Telephony and SMS) and RCS services according to section 15.4.1 of [18].

In this case the device shall derive the value of the "+sip.instance" header field parameter of the Contact address for the IMS registration for RCS services as defined for non-embedded clients in section 2.4.2 of [1].

In the IMS registration for VoLTE services the “+sip.instance” header field parameter of the Contact address shall contain the IMEI as per [25].

ID_4_22 Removal of Group Chat participant after removal of IMS subscription

Type	Recommendation
Related spec clause	3.4.4.1.7 [1]
Applicable joyn release	Blackbird, Crane Priority Release
Related TC [2] ID	N/A
Publish date	04.02.2016
Date modified	04.02.2016

Description

The Group Chat technical implementation defined in [1] and [18] lacks procedures for the case where a service provider removes the IMS profile of a user being participant in Group Chats. Therefore participants are kept in participant lists of Group Chats after cancellation of their relation to a service provider. In addition new users getting an MSISDN of a previous participant in Group Chats assigned are automatically added to the Group Chat conversations of the predecessor.

Therefore the Messaging Server of joyn networks shall implement the following procedure in addition to the definitions in section 3.4.4.1.7 of [1] and section 6.3.5.5 of [18]

If the Controlling Function re-starts a Group Chat and it receives a SIP 404 Not Found response to the INVITE sent to a participant, it shall remove the corresponding participant from the participant list. The clients of the other participants in the Group Chat are informed via the notification of conference events within their subscription.

The elements of the removed participant's user endpoint in the conference event package shall be set as follows:

- status of the user endpoint element is set to "disconnected"
- disconnection-method of the user endpoint element is set to "departed"

This layout is required to ensure that all clients receiving the notification of the conference event remove the corresponding participant from its local participant list.

ID_4_23 Relating the ongoing call with in-call incoming SIP requests: caller and callee procedures

Type	Clarification
Related spec clause	N/A
Applicable joyn release	Blackbird, Crane Priority Release
Related TC [2] ID	N/A
Publish date	04.02.2016
Date modified	04.02.2016

Description

The procedures that the client shall follow to relate the ongoing call with in-call incoming SIP requests are not described in [1]. In order the client to relate the ongoing call with incoming SIP requests shall follow the following procedures:

Caller procedures

The destination identity of the telephony call that the caller dials or gets from his address book and the originator identity of any in-call incoming request may be in various formats. The client of the caller shall therefore apply the following matching mechanism to determine whether an incoming request relates to the ongoing call:

1. If both the destination identity of the telephony call and the originator identity of the in-call incoming request are phone numbers in international format, the client of the caller shall compare all digits of the provided numbers to determine whether they match.
2. If any of the identities is not in international format, the client of the caller shall apply a smart matching mechanism between the destination identity from the telephony call and the originator identity of the incoming request, e.g. by comparing the 7 digits starting from the end of the number. It is left to the client implementation to apply a smarter matching algorithm to decrease the probability of false matches.

The client shall consider the identities to be in international format if

for a CS or multimedia telephony outgoing call, the digits dialled or taken from the address book start with a “+”.

for an incoming request, the P-Asserted-Identity of the SIP request contains either:

- a tel URI starting with a “+” without phone-context i.e. a global number or
- SIP URI with user part starting with a “+” and user=phone parameter without a phone-context in the user part

Examples:

The destination identity of the outgoing telephony call: +**447123456789** (display string for an international format number)

The originator identity of the incoming request: +**447123456789**
⇨ Matching result: Successful

when the applied smart matching algorithm is based on the 7 digits starting from the end of the number:

The destination identity of the outgoing telephony call: 0712**3456789** (non international format)

The originator identity of the incoming request: +44712**3456789**
⇨ Matching result: Successful

Callee procedures

The originator identity of the telephony call and the originator identity of any in-call incoming request may be provided in various formats both in the home networks and when roaming. The client of the callee shall therefore apply the following matching mechanism to determine whether an incoming request relates to the ongoing call:

1. If both the originator identity of the telephony call and the originator identity of the in-call incoming request are phone numbers in international format, the client of the callee shall compare all digits of the provided numbers to determine whether they match.
2. If any of the originator identities is not in international format, the client of the callee shall apply a smart matching mechanism between the originator identity from the telephony call and the originator identity of the incoming request, e.g. by comparing the 7 digits starting from the end of the number. It is left to the client implementation to apply a smarter matching algorithm to decrease the probability of false matches.

The client shall consider the identities to be in international format if

1. for a CS incoming call, the Type Of Number (TON) of the Calling Party BCD Number is set to “international” as defined in [26].
2. for a multimedia telephony incoming call, the P-Asserted-Identity of the SIP INVITE request contains either:
   - a tel URI starting with a “+” without phone-context i.e. a global number or
   - SIP URI with user part starting with a “+” and user=phone parameter without a phone-context in the user part
3. for an incoming request, the P-Asserted-Identity of the SIP request contains either:
   - a tel URI starting with a “+” without phone-context i.e. a global number or
   - SIP URI with user part starting with a “+” and user=phone parameter without a phone-context in the user part

Examples:

The originator identity of the incoming telephony call: +**447123456789** (display string for an international format number)

The originator identity of the incoming request: +**447123456789**
⇨ Matching result: Successful

When the applied smart matching algorithm is based on the 7 digits starting from the end of the number:

The originator identity of the incoming telephony call: 00644712**3456789** (non international format)

The originator identity of the incoming request: +44712**3456789**
⇨ Matching result: Successful

ID_4_24 Addressing in-call SIP requests towards the other party in the call: caller and callee procedures

Type	Clarification
Related spec clause	N/A
Applicable joyn release	Blackbird, Crane Priority Release
Related TC [2] ID	N/A
Publish date	04.02.2016
Date modified	04.02.2016

Description

The procedures that the client shall follow to address an in-call SIP request towards the other party in the call are not described in [1]. In order the client to address an in-call SIP request towards the other party in the call shall apply the following procedures:

Caller procedures

The destination identity of the telephony call that the caller dials or gets from the address book may be in various formats. The client of the caller shall therefore apply the following principles for addressing the callee when triggers in-call SIP requests:

1. If the destination identity of the telephony call is in international format, the client of the caller shall use this information for addressing in-call SIP requests towards the callee.
2. If the destination identity of the telephony call is not in international format, the client of the caller shall use geo-local numbering of the destination identity of the telephony call for addressing in-call SIP requests towards the callee. If the request fails, the client of the caller shall attempt to correlate the destination identity of the telephony call with his local identity records acquired from incoming SIP requests received in a window prior to the call and/or during the call using a smart matching mechanism between the destination identity from the telephony call and the incoming SIP requests, e.g. by comparing the 7 digits starting from the end of the number. It is left to the client implementation to set the time length of the window and apply a smarter matching algorithm to decrease the probability of false matches.
    a. If there is successful matching, the client of the caller shall use the “matched” destination identity from his local identity records for addressing in-call SIP requests towards the callee.
    b. If there is no successful matching, the client of the caller shall use the destination identity from the telephony call that the caller dials or gets from his address book for addressing in-call SIP requests towards the callee. The client of the caller shall continue applying the smart matching mechanism for any in-call incoming SIP request until it matches the destination identity from the telephony call with the originator identity from an in-call incoming SIP request. Once there is a successful matching it shall from then on use the “matched” originator identity from the SIP request for addressing any future in-call SIP requests towards the callee.

The client shall consider the identities to be in international format if

for a CS or multimedia telephony outgoing call, the digits dialled or taken from the address book start with a “+”.

Examples:

The destination identity of the outgoing telephony call: +447123456789 (display string for an international format number)

The client of the caller uses the destination identity from the telephony call for addressing in-call SIP requests towards the callee.

The smart matching mechanism does not apply.

The destination identity of the outgoing telephony call: 0712**3456789** (non international format).
The client of the caller shall use geo-local numbering of the destination identity of the telephony call for addressing in-call SIP requests towards the callee: tel:07123456789;phone-context=geolocal.<homedomain>, where <homedomain> needs to be replaced with the home network domain name as configured by the device (as per section 2.2.3 of [25])

If the in-call SIP request fails, the client shall apply the smart matching mechanism.

The originator identity of incoming SIP request: +44712**3456789**
⇨ Matching result: Successful

Callee procedures

The originator identity of the telephony call may be provided in various formats both in the home networks and when roaming. The client of the callee shall therefore apply the following principles for addressing the caller when triggers in-call SIP requests:

1. If the originator identity of the telephony call is in international format, the client of the callee shall use this information for addressing in-call SIP requests towards the caller.
2. If the originator identity of the telephony call is not in international format, the client of the callee shall use geo-local numbering of the originator identity of the telephony call for addressing in-call SIP requests towards the caller. If the request fails, the client of the callee shall attempt to correlate the originator identity of the telephony call with his local identity records acquired from incoming SIP requests received in a window prior to the call and/or during the call using a smart matching mechanism between the originator identity from the telephony call and the incoming SIP requests, e.g. by comparing the 7 digits starting from the end of the number. It is left to the client implementation to set the time length of the window and apply a smarter matching algorithm to decrease the probability of false matches.
    a. If there is successful matching, the client of the callee shall use the “matched” originator identity from his local identity records for addressing in-call SIP requests towards the caller.
    b. If there is no successful matching, the client of the callee shall use the originator identity from the telephony call for addressing in-call SIP requests towards the caller. The client of the callee shall continue applying the smart matching mechanism for any in-call incoming SIP request until it matches the originator identity from the telephony call with the originator identity from an in-call incoming SIP request. Once there is a successful matching it shall from then on use the “matched” originator identity from the SIP request for addressing any future in-call SIP requests towards the caller.

The client shall consider the identities to be in international format if

1. for a CS incoming call, the Type Of Number (TON) of the Calling Party BCD Number is set to “international” as defined in [26].

1. for a multimedia telephony incoming call, the P-Asserted-Identity of the SIP INVITE request contains either:

   - a tel URI starting with a “+” without phone-context i.e. a global number or
   - SIP URI with user part starting with a “+” and user=phone parameter without a phone-context in the user part

Examples

The originator identity of the incoming telephony call: +447123456789 (display string for an international format number)

The client of the callee uses the originator identity from the telephony call for addressing in-call SIP requests towards the caller.

The smart matching mechanism does not apply.

When the applied smart matching algorithm is based on the 7 digits starting from the end of the number:

The originator identity of the incoming telephony call: 00644712**3456789** (non international format)
The client of the callee shall use geo-local numbering of the originator identity of the telephony call for addressing in-call SIP requests towards the caller: tel: 006447123456789;phone-context=geolocal.<homedomain>, where <homedomain> needs to be replaced with the home network domain name as configured by the device (as per section 2.2.3 of [25])

If the in-call SIP request fails, the client shall apply the smart matching mechanism.

The originator identity of incoming SIP request: +44712**3456789**
⇨ Matching result: Successful

ID_4_25 Void

ID_4_26 Void

ID_4_27 Void

ID_4_28 Call Composer XML structure

Type	Clarification
Related spec clause	N/A
Applicable joyn release	Crane Priority Release
Related TC [2] ID	N/A
Publish date	04.02.2016
Date modified	15.12.2016

Description

This implementation guideline corrects the structure and encoding of the Call Composer XML elements of [27] as follows:

- In section 2.4.4 of [27] the example in Table 9 is replaced by the following.

```
<?xml version=”1.0” encoding=”UTF-8”?>
<rcsenvelope xmlns=”urn:gsma:params:xml:ns:rcs:rcs:calldata”>
<rcscalldata>
  <subject>this is the subject</subject>
  <importance>[0/1]</importance>
  <location>[coordinates]</location>
  <composerid>[Random generated number to identify the session]</composerid>
  <picture url="[HTTP URL for the file]"/>
</rcscalldata>
</rcsenvelope>
```

- In section 2.4.4 of [27] the definition of the element <picture url> under rcscalldata is replaced by the following:

  <picture> provides the characteristics of the picture file on the FT content server. The element includes an attribute "url" containing the URL of the picture file on the FT content server to be displayed.

- The XML schema defined in section 2.6 of [27] is replaced by the following:

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema
   targetNamespace="urn:gsma:params:xml:ns:rcs:rcs:calldata"
   xmlns="urn:gsma:params:xml:ns:rcs:rcs:calldata"
   xmlns:xs="http://www.w3.org/2001/XMLSchema"
   elementFormDefault="qualified" attributeFormDefault="unqualified">

   <!-- This import brings in the XML language attribute xml:lang -->
   <xs:import namespace="http://www.w3.org/XML/1998/namespace"
       schemaLocation="http://www.w3.org/2001/xml.xsd"/>

 <!-- The root "rcsenvelope" element -->
  <xs:element name="rcsenvelope">
    <xs:complexType>
      <xs:sequence>
        <xs:element name="rcscalldata" type="reasontype" maxOccurs="1"/>
        <xs:any minOccurs="0" maxOccurs="unbounded" processContents="lax"/>
      </xs:sequence>
    </xs:complexType>
  </xs:element>

 <!-- The definition of type "reasontype" is as below -->
  <xs:complexType name="reasontype">
    <xs:sequence>
      <xs:element name="subject" type="xs:string" minOccurs="0" maxOccurs="1"/>
```

```
      <xs:element name="importance" type="xs:boolean" minOccurs="0" maxOccurs="1"/>
      <xs:element name="location" type="xs:string" minOccurs="0" maxOccurs="1"/>
      <xs:element name="composerid" type="xs:string" minOccurs="0" maxOccurs="1"/>
      <xs:element name="picture" minOccurs="0" maxOccurs="1">
        <xs:complexType>
          <xs:attribute name="url" type="xs:anyURI" use="required"/>
          <xs:anyAttribute namespace="##other" processContents="lax"/>
        </xs:complexType>
      </xs:element>
      <xs:element name="note" type="xs:string" minOccurs="0" maxOccurs="1"/>
       <xs:any minOccurs="0" maxOccurs="unbounded" processContents="lax"/>
    </xs:sequence>
  </xs:complexType>
</xs:schema>
```

ID_4_29 Void

ID_4_30 Void

ID_4_31 Void

ID_4_32 Void

ID_4_33 Void

ID_4_34 Primary device/client behaviour when device is not in the SIM Ready State

Type	Recommendation
Related spec [1] clause	2.3.4
Applicable joyn release	Blackbird, Crane Priority Release
Related TC [2] ID	ID_RCS_1_8_4
Publish date	14.07.2016
Date modified	14.07.2016

Description

This recommendation applies to a client acting as a primary device.

If the client detects that the device leaves the SIM Ready State (e.g. power off, physical removal of SIM), it shall instantly generate a de-registration request as stated in ID_4_14, if connectivity is available.

If the device is not in SIM Ready State, a client configuration stored in the client remains valid (in accordance with its validity) but it is in dormant state, i.e. the client does not register in IMS Network.

If the client recovers the SIM Ready State (e.g. user enters PIN, re-insert the SIM Card in the device), then the client shall check if the configuration in the device corresponds to the inserted SIM (comparing the IMSI from client configuration with IMSI from SIM).

If the result of comparing them is that it is not the same, then, the procedures for SIM change apply as per section 2.3.4 of [1]. Otherwise, the device uses the existing client configuration to register in IMS Network.

ID_4_35 Clarification for quotes in XML

Type	Clarification
Related spec [1] clause	N/A
Applicable joyn release	Blackbird, Crane Priority Release
Related TC [2] ID	ID_RCS_6_6_1
Publish date	14.07.2016
Date modified	14.07.2016

Description

In XML version 1.0 literals may come with single or double quotes, see section 2.3 Common Syntactic Constructs of xml version 1.0. Only the start quote and the end quote need to be the same. Therefore a client shall be able to parse XML with both types of quotes.

ID_4_36 Client Handling of Registration Requests

Type	Clarification
Related spec [1] clause	N/A
Applicable joyn release	Blackbird, Crane Priority Release
Related TC [2] ID	N/A
Publish date	14.07.2016
Date modified	14.07.2016

Description

When sending SIP REGISTER requests the client implementation shall respect the requirements of section 10.2 of [29] to enforce only one registration transaction being in progress at a time. This is also applicable for device implementations supporting converged IP communication services, i.e. Multimedia Telephony, SMS over IP and other RCS services and being configured via client configuration to apply separate registration instances, i.e. by means of the configuration parameter ALWAYS USE IMS APN according to section 15.4.1 of [18] (see also ID_4_21). In the latter case the requirement to enforce a single registration transactions spans over the separate instances and is independent from the type of registration which any of client instances performs at the time, i.e. initial registration, re-registration or de-registration.

This client behaviour is essential for IMS Core deployments to ensure the integrity of the user's registration status kept in the network.

ID_4_37 Clarification on the Contact header format when several ICSI and/or IARI values are included

Type	Clarification
Related spec [1] clause	N/A
Applicable joyn release	Blackbird, Crane Priority Release
Related TC [2] ID	N/A
Publish date	15.12.2016
Date modified	15.12.2016

Description

When several IMS Application Reference Identifier (IARI) values or several ICSI values are included in the Contact header in a SIP REGISTER request, consistently with [31], these

IARI values shall be concatenated in a single IARI feature tag using commas, and these ICSI values shall be concatenated into a single ICSI feature tag using commas.

The same format applies if several IARI values are included in the Contact Header in a SIP INVITE or REFER request/response for a Group Chat.

In general, this rule applies to all SIP requests when the IARI and ICSI feature tags are used and more than one IARI or ICSI value is required in a Contact header.

ID_4_38 Stabilization of Group Chat participant management

Type	Clarification
Related spec [1] clause	3.4.4.1.7
Applicable joyn release	Crane Priority Release, Pre-Universal Profile
Related TC [2] ID	N/A
Publish date	15.12.2016
Date modified	15.12.2016

Description

RCS 5.1 Version 2.0 and joyn Blackbird define a procedure for the client to compare the participant list of the resource-list body of a received INVITE with the locally stored participant list when receiving a Group Chat session invitation with a known Group Chat ID, see section 3.4.4.1.7 of [1]. The client is required to invite participants which are not found in the resource-list body but found in the local participant list. This leads to unexpected service behaviour in a Group Chat with offline users with such a client. The procedure defined in this section intends to compensate this client behaviour in the Controlling Function.

If the Controlling Function processes a request for explicit departure as described in section 3.4.4.1.3.1 of [1] then the Controlling Function shall not remove the participant from the locally stored participant list. Instead it shall mark the participant as "departed".

The procedures of the Controlling function to notify the participants in the Group Chat session about voluntarily departure as described in section 3.4.4.1.3.1 of [1] and the additional procedure defined in ID_4_15 applies.

If the Controlling Function processes a request to restart a Group Chat session as described in section 3.4.4.1.7 of [1] and the participant list stored in the Controlling Function contains one or more participants marked as "departed", then the Controlling Function shall restart the Group Chat session for all non-departed participants only.

When inviting a participant to a Group Chat session on restart, the Controlling Function shall add to the resource-list body of the INVITE all participants from the stored participant list, including the participants being marked as "departed".

Subsequently, if the Controlling Function sends a NOTIFY for a client's subscription to the conference event package in result of processing of the SUBSCRIBE request or caused by subsequent changes to the conference event package, then the Controlling Function shall indicate the status of "departed" participants as "disconnected" and include a disconnection-method element with the value "departed", see also ID_4_15.

If the Controlling Function receives a request to add (re-invite) a participant as described in section 3.4.4.1.2 of [1] and the invited participant is marked as "departed" in the stored participant list, then the Controlling Function shall process the request and invite the new participant.

If the participant accepted the invitation to the Group Chat as described in section 3.4.4.1.1 of [1] then the Controlling Function shall remove the "departed" marker.

If the participant rejected the invitation to the Group Chat as described in section 3.4.4.1.1 of [1] or section 3.4.4.1.3.1 of [1] then the Controlling Function shall keep the participant marked as "departed".

The Controlling Function may support housekeeping to remove departed participants from locally stored participant lists. Housekeeping should be applied only after significant number of Group Chat sessions have been set-up for the Group Chat after a participant did voluntarily depart the Group Chat This is required to allow all offline clients to learn the participant's status.

ID_4_39 Client Procedure on restart of a Group Chat

Type	Clarification
Related spec [1] clause	3.4.4.1.7
Applicable joyn release	Blackbird, Crane Priority Release, Pre-Universal Profile
Related TC [2] ID	N/A
Publish date	15.12.2016
Date modified	15.12.2016

Description

A client receiving an invitation for a restarted Group Chat session as defined in section 6.3.5.5 of [18] shall not evaluate the content of the resource-list body of the INVITE request for the management of the local participant list, e.g. update of locally stored participant list.

As a clarification of the description in section 3.4.4.1.3.1 of [1], a client receiving a notification for the conference event package of a Group Chat containing one or more participants with status set to "disconnected" and a disconnection-method set to "departed" shall apply the indication that an user has left the conversation only if the participant was stored in the local participant list at the time of reception.

ID_4_40 RCC.20 endorsement in CPR

Type	Clarification
Related spec [1] clause	N/A
Applicable joyn release	Crane Priority Release
Related TC [2] ID	N/A
Publish date	15.12.2016
Date modified	15.12.2016

Description

The endorsement of RCC.20 in section B.4 of [40] is modified as follows:

- for bullet 2: section 2.1.1 of [27] is void, [27] does not define a rcs_profile configuration request parameter.
- for bullet 3: the reference to section 2.1.2.1 of [27] is replaced by a reference to section 2.1.3.1 of [27].
- for bullet 7: [27] does not specify the use of the MAX RRAM DURATION configuration parameter, thus it is not applicable in CPR.
- for bullet 8: in addition, the references to sections 3.11.4.2.2 and 3.11.4.1 of [36] are replaced by references to sections 3.11.4.2.2 and 3.11.4.1 of [1].

For the definitions of configuration parameters in section B.5 the following applies

- bullet 3 does not apply, [27] does not specify a value of the rcs_profile configuration request parameter

2.5 MSRP issues

ID_5_1 MSRP passive role

Type	Clarification
Related spec [1] clause	2.13.1.3.2
Applicable joyn release	Blackbird, Crane Priority Release
Related TC [2] ID	RCS_ID_5_4_1
Publish date	07.03.2014
Date modified	07.03.2014

Description

Regardless of the negotiated direction for the actual content, a MSRP endpoint taking the passive role in the MSRP session set up shall be prepared to receive an empty MSRP packet to allow the binding of the MSRP session to the TCP connection.

ID_5_2 IMDN.Message-ID length

Type	Recommendation
Related spec [1] clause	B.1.17, B.2.17, B.3.4
Applicable joyn release	Blackbird, Crane Priority Release
Related TC [2] ID	RCS_ID_7_1_1
Publish date	07.03.2014
Date modified	07.03.2014

Description

RFC5438 [20] defines a minimum, but no maximum length for the message-ID which may be a cause for interoperability problems. For joyn Blackbird, the maximum length for the IMDN message-ID shall be 32 characters.

ID_5_3 Network initiated IMDNs Aggregation

Type	Requirement
Related spec [1] clause	3.3.4.1
Applicable joyn release	Blackbird, Crane Priority Release
Related TC [2] ID	N/A
Publish date	15.05.2014
Date modified	25.09.2014

Description

As per 3.3.4.1 [1] (see also RFC5438 [20], section 8.3), the aggregation of network initiated IMDNs may be supported as per local policy in the network. However, it is observed that some clients cannot process incoming aggregated IMDNs correctly. This may cause interoperability issues. Hence, neither the networks nor the clients shall aggregate IMDNs.

ID_5_4 MSRP range-end field in byte-range header for FT and IS

Type	Clarification
Related spec [1] clause	3.5.4
Applicable joyn release	Blackbird, Crane Priority Release
Related TC [2] ID	N/A
Publish date	15.05.2014
Date modified	15.05.2014

Description

joyn Blackbird PDD [18] recommends an MSRP chunk size of 10 KB for MSRP-based FileTransfer (FT) and ImageShare (IS). RFC 4975 [22] requires in section 5.1 and 7.1.1 that chunks larger than 2048 octets need to be interruptible and with that a "*" and not a byte number is included in the range-end field of the byte-range header.

With joyn MSRP chunks of up to 10KB size sent by the client for FT or IS are not required to be interruptible and with that the joyn Blackbird client shall always include a byte number in the range-end field. A joyn Blackbird client shall accept receiving MSRP chunks including both, a "*" or number value in the end-range field.

2.6 RTP/RTCP issues

ID_6_1 Use of the Video profiles

Type	Requirement
Related spec [1] clause	3.6.4.1.4
Applicable joyn release	Blackbird, Crane Priority Release
Related TC [2] ID	RCS_ID_6_1_3
Publish date	04.07.2013
Date modified	25.09.2014

Description

In case the originator of the Video session uses Constraint Baseline Profile (CBP) for the actual stream it shall indicate support for both Baseline Profile (BP) and CBP with profile-level-ids 42900B and 42D00B correspondingly.

NOTE: Unlike what is indicated in RCS 5.1 specification v2.0, for H.264 it is possible to indicate one level **per** profile in the SDP (instead of one level and profile) and therefore it is possible to include both profiles in the SDP.

Originator shall never use Flexible Macroblock Ordering (FMO), Arbitrary Slice Ordering (ASO), Redundant Slices (RS) features of the profile whatever the receiving party selects.

When a receiving party faces the combination of BP and CBP profiles within the same SDP offer it shall select CBP profile.

```
v=0
o=- 1323909835 1323909838 IN IP4 10.0.100.189
s=-
c=IN IP4 10.0.100.189
t=0 0
m=video 4284 RTP/AVP 118 119
```

```
a=sendrecv
a=rtpmap:118 H264/90000
a=fmtp:118 packetization-mode=1;profile-level-id=42d00b
a=rtpmap:119 H264/90000
a=fmtp:119 packetization-mode=1;profile-level-id=42900b
```

Table 3: VideoShare with CBP profile: SDP sample

When the SDP negotiation results in the use of the Baseline Profile, a client shall not send STAP-A packets, even when the packetization-mode has been negotiated. When accepting the use of the Constrained Baseline Profile a client shall support the use of STAP-A packets when packetization-mode 1 was negotiated.

ID_6_2 Extmap local IDs

Type	Requirement
Related spec [1] clause	2.7.1.2.2
Applicable joyn release	Blackbird, Crane Priority Release
Related TC [2] ID	RCS_ID_6_1_3
Publish date	22.08.2013
Date modified	15.05.2014

Description

According to RFC 5285 during establishment of the Video Share session the SDP Answerer MAY update extmap's local identifier initially proposed by the SDP Offerer and in that case the video share sender SHALL further use that negotiated value while sending video-orientation information in RTP packets. Although it is recommended not to change the extmap's local identifier in the SDP answer from the one in the SDP offer because there are no reasons to do that since there should only be one extension in use.

ID_6_3 RTP Extensions

Type	Clarification
Related spec [1] clause	2.7.1.2.2
Applicable joyn release	Blackbird, Crane Priority Release
Related TC [2] ID	RCS_ID_6_1_3
Publish date	22.08.2013
Date modified	22.08.2013

Description

The Video Orientation Coordination information (ROT and CAM bits) SHALL be delivered by Sender of the Video stream using special RTP Extension Headers in accordance with RFC 5285, [14] and RCS5.1 specification. Consequently such information shall never be delivered in RTP Payload extensions.

ID_6_4 H.264 profile-level negotiation

Type	Clarification
Related spec [1] clause	3.6.4.1.4
Applicable joyn release	Blackbird, Crane Priority Release
Related TC [2] ID	RCS_ID_6_1_3
Publish date	22.08.2013
Date modified	22.08.2013

Description

In accordance with RFC 6184 [23] if during establishment of the Video session the Terminating party does not support H.264 profile-level (e.g. 1.3) indicated in the SDP offer that Terminating party SHALL reply with a lower supported level (e.g. 1b) instead of sending a failure report (e.g. 415 Unsupported Media Type) and consequently showing bad user experience (user won't able to start a video session).

ID_6_5 Encoding allowed for the actual video stream based on the SDP negotiation

Type	Clarification
Related spec [1] clause	3.6.4.1.4
Applicable joyn release	Blackbird, Crane Priority Release
Related TC [2] ID	RCS_ID_6_1_3
Publish date	22.08.2013
Date modified	15.05.2014

Description

Independently on the H.264 profile level negotiated over SDP during video session establishment the encoding of the actual stream should be adapted to the currently available bandwidth and might therefore use bitrates lower than the maximum negotiated during session setup. Thereby the H264 bitstream parameter conveyed over RTP packet shall indicate either negotiated profile-level-id during session setup or a lower profile-level-id. For example, if clients negotiated profile level 1b (42900B) then RTP should convey either indication of the same level (e.g. 42900B) or a lower profile level (e.g. 42800A) whereas it shall not indicate higher profile level (e.g. 42800B) since that could cause issues with presenting video on the recipient side.

ID_6_6 Recommendations for encoding based on connectivity

Type	Recommendation
Related spec [1] clause	3.6.4.1.4
Applicable joyn release	Blackbird, Crane Priority Release
Related TC [2] ID	RCS_ID_6_1_3
Publish date	15.05.2014
Date modified	15.05.2014

Description

To improve quality of the video services across different clients it is recommended to use following H.264 profile levels and their parameters depending on the network coverage:

Network coverage	profile-level	profile-level-id in SDP and RTP		video resolution	frame rate	data rate
		BP	CBP			
UMTS	1b	42900B	42D00B	176x144	15	128kb/sec
	1.1	42800B	42C00B	176x144	15	192kb/sec
HSPA/Wi-FI	1.2	42800C	42C00C	320x240	20	384kb/sec
LTE/	1.3	42800D	42C00D	320x240	30	768kb/sec

Table 4: Recommended H.264 profile levels

As it is defined in 3.6.4.1.4 [1] the only mandated profile-level for the devices not supporting LTE should be 1b. As indicated in the above table though, if supported by the client it is recommended to use a higher profile where coverage allows this.

2.7 End User Confirmation Request (EUCR) issues

ID_7_1 Terms and Conditions

Type	Requirement
Related spec [1] clause	2.10
Applicable joyn release	Blackbird, Crane Priority Release
Related TC [2] ID	ID_RCS_10_x_x
Publish date	04.07.2013
Date modified	15.05.2014

Description

End User Confirmation Requests may in a network implementation be used for a variety of use cases that require communication to an end user. A client shall therefore not implement any behaviour related to it apart from what has been described in section 2.10 of [1]. Specifically, an implementation shall not assume that End User Confirmation Requests will be used for providing client-initiated Terms and Conditions to a user: once configured a client shall be fully functional and NOT wait for the first End User Confirmation Request to be accepted before enabling the joyn functionality nor shall it perform any action when a user rejects an End User Confirmation Request. The network may trigger further actions in case user rejects EUCR.

ANNEX A Frequently asked questions

Q1: What is the expected behaviour if TLS/TCP connection gets terminated? Should the client ONLY re-establish the connection OR should the client initiate registration after connection establishment?

The client should re-establish connection. I guess that the same socket will be used, if not reregistration will be needed.

Q2: MSRP: Does the server support sending of the File in ONE chunk?

No problem. IM Server does not limit this. Note that if chunks are big, latency will increase since IM Server does not retransmit the MSRP chunk until it is completely received.

Q3: When should the UE auto-accept a session from the deferred messaging function?

It should accept when P-Asserted-Id is RCS-standfw@domain and only for deferred notifications only (not deferred messages). It will be the a=sendonly session from this PAID with content-type:application/sdp since deferred notifications are sent over MSRP.

Q4: What is the P-Asserted-Identity supposed to be for these 2 scenarios?

Incoming deferred notification:

RCS-standfw@domain.

Incoming deferred IM:

Up to MNO, these messages can be rejected. You will know it is deferred messaging because content-type is multipart/mixed, with a Referred-by header containing the tel-uri of the originator, and a PAID that is a different uri.

Q5: Should the UE auto-accept for deferred IM as well?

No, that is why PAID can be different

Q6: Hiding Identities in CPIM / IMDN. This is a new requirement due to security issues over WIFI. Does this apply to messages carrying IMDN only, and not to messages carrying actual text messages?

Both. To avoid dropping of media part over WI-FI (MSRP over TLS is not ready yet) anonymous@anonymous.invalid will work.

Q7: In case of SIM swap, "backup & restore" of Configuration data should be supported. Up to how many SIM cards should be considered?

There is a proposal to support up to 3 SIMs for backup & restore of configuration.

Q8: A clarification for Store and Forward call flow (RCS spec [1], section B.2.3) is required

User A is Sending Invite to User B.

Since User B is offline, Server has accepted the session on behalf of User B.

User A sends Messages to User B which is stored at server.

User B comes online, Server start sending Deferred Messages to User B.

User B Accepts the session and start receiving the stored message from server and send the Delivery and Display notification to server which in turn send the notification to user A.

After all the stored message has been delivered then server will send the BYE to User B.

Hence, from a Client side handling, we are having difficulty in understanding, what should be the behaviour and when we need to accept-1st call and when we need to accept 2nd incoming call. Are we missing any information that may differ between Session-1 and Session-2 from A's side?

User B at any time may send a new INVITE to user A, and that would cause user A to accept that session and tear down the one it has with the IM Server on behalf of user B. The INVITE will not be rejected with a 486 - it would be the normal procedures where user A's device accepts a new INVITE from the same user, i.e. B, as per b) in section 3.2.4.12 in RCS spec:

Device switching (as per the RCS Release 2 OMA-SIMPLE-IM endorsement):

…

If user B changes from one device B1 to another B2 by just sending a new message to the chat from the new device B2. It will send a new INVITE with the message in the subject field as usual that will go to A's device. When A's device detects a new INVITE session from a user (B) which already has an established session it shall end it and accept the new one. All subsequent messages will be received only by device B2. Device B2 must then store the received messages and display them appropriately. If A still has delivery and displayed reports for Device B1, they should be sent before A's device tears down the old session."

Q9: Passing a fingerprint is only for the case using TLS in Peer-to-Peer Mode and there are no service using MSRP in Peer-to-Peer Mode in RCS. Should a client support 'fingerprint' mechanism? If yes, should a client support all features including 'Identity' and 'Identity-Info' header fields in RFC 4474?

No, the behaviour of the SBC in MSRP is B2BUA, therefore, the client has only to negotiate with the SBC and the mentioned headers do not need to be supported by the client.

Q10: Does the value of the 'Setup' SDP attribute have an impact on the direction of the MSRP traffic?

No. This attribute only indicates which of the end points should initiate the TCP connection establishment (i.e., send the initial TCP SYN).

Once the session is established and when not in recvonly or sendonly modes, any MSRP end-point shall be ready to send or receive MSRP packets.

Q11: What is the need of MSRP SEND empty packets?

MSRP SEND empty packets are used to ensure that the session matching process takes place ASAP. MSRP SEND empty packets should be handled as non-empty packets (i.e. responded with an MSRP 200 OK).

ANNEX B Q&A for Shared Sketch

Category	User Story ID	Requirement ID	Requirement	Questions	Answers
Interactive In-call Services (Sketch Share)	US5-3	R5-3-3	If pre-share sketch editing is supported: The A-Party shall be able to send the sketch to the B-Party as a normal file transfer, if the shared sketch invitation failed for any reason, or if it was not delivered or was rejected by the B-Party.	1) What should be the format of file? 2) "The A-Party shall be able to send the sketch", what does it mean sketch here? Is it complete screenshot or only capturing the sketch area without toolbar and status bar	1) From a functional perspective, sharing prepared sketches as a background image would be ok. (JPG/PNG are ok) 2) capturing the sketch area, no toolbar etc.
Interactive In-call Services (Sketch Share)	US5-6	R5-6-2	Both parties shall be notified if the shared sketch invitation times out before the B-Party has accepted (or rejected) it.	Time-out after how long?	Same time out as already in use for invites e.g. for live video share.
Interactive In-call Services (Sketch Share)	US5-22	R5-22-1	R5-22-1 The most recent version of the sketch shall be automatically saved to both parties' devices when the session ends NOTE 1: Sketch may be saved as a 'flat' image, without separately editable background and drawing layers. NOTE 2: Requirements for integrating In-call shared sketches into the enriched call logs, message threads and/or contact-centric views for both parties are detailed in this Enriched Calling OIG PDD, section 8.	What should be the format of file?	JPG/PNG are ok.

Category	User Story ID	Requirement ID	Requirement	Questions	Answers
Interactive In-call Services (Sketch Share)	US5-29	R5-29-1	If the other party has edited a part of the map that the current party is not viewing, then the current party should be notified (e.g. via a toast message).	What does it mean here by editing map?	The requirement kicks in whenever one party sketches outside the view of the other party. Then, and only in this case, the party who is not able to see the changes on the actual screen shall be notified and offered to navigate to the section where the changes happen. "Editing" in this context means not changing the map, but drawing on top of the map.

Category	User Story ID	Requirement ID	Requirement	Questions	Answers
Interactive In-call Services (Sketch Share)	US5-14	R5-14-4	Either party may be able to redo the last undo action in the sketch. NOTE: **Undo/redo** actions only apply to lines drawn by the current party.	1) No Element is defined XML DTD for "Redo" Action. So Redo would be performed with Drawing action, right? 2) Action means "User A or User B draws the sketch and it is sent to other party as soon as user `detach` the finger from the screen ", is it right? 3) What is undo redo depth? means how many actions to retain in stack for performing undo redo.	1) covered by GSG CR 28 (updated in baseline document RCC.20 CR1002). 2) yes, that is right 3) technically, the depth is multiple times, but we recommend to implement probably 5 undo steps.
Interactive In-call Services (Sketch Share)	US5-14	R5-14-3	Using the erase function shall not delete the sketch background image or map.	Do we need to support erase function in Map? It is contradicting with shared sketch protocol	The functional requirements do ask for erase in map as well. If the technical function does not support erase function, this is a limitation we need to accept. Drawing erase its included in both DTDs DTD 2.9.7.2.1 (shared map) and DTD 2.9.8.3.1

Category	User Story ID	Requirement ID	Requirement	Questions	Answers
Interactive In-call Services (Sketch Share)	US5-12	R5-12-2	Any sketch drawings shall be shown in real-time on both parties' devices.	For showing in real-time, we need to keep capturing and sending points from party A side. Party B will keep receiving the points continuously and will be drawing. Now how party B will know, when new line is started? We are facing very basic issue because of this. Suppose party A has drawn a line on upper side of screen, then start drawing next line at lower side, now problem is- end point of first line is getting joined with start point of second line.	"Real time" in this context means that an action that has been made on one device is visible to the other party when the action has been completed. It is not required to see the ongoing change on the other device while the drawing is made but not yet a completed action.

Category	User Story ID	Requirement ID	Requirement	Questions	Answers
Interactive In-call Services (Sketch Share)	US5-12	R5-12-2	Any sketch drawings shall be shown in real-time on both parties' devices.	1) While sending multiple points (co-ordinates/LatLang), how to differentiate between 2 points? I mean what is the delimiter between point1 and point2. 2) In shared map DTD, point tag is mentioned in DTD where it is not mentioned to encode base64 format , but where as if we see the example at the end of the DTD document we can find the encode = "Base64" attribute in point tag. So we need clarification whether we need to do base64 encoding to point tag or not. (Note: we have points as well as point tag both are different).	1) & 2) covered by GSG CR 28 (updated in baseline document RCC.20 CR1002).
Interactive In-call Services (Sketch Share)			Does shared sketch support both Landscape and Portrait mode?	Does shared sketch support both Landscape and Portrait mode?	Yes, both orientations should be supported, but the canvas shall keep the same original orientation. In this case, changing the orientation is a local on-device zooming in or out function on the screen.

Category	User Story ID	Requirement ID	Requirement	Questions	Answers
Pre-edit	US12-53	R12-53-1	Either party should be able to continue editing a sketch when the sketch sharing session has ended. NOTE: Any edits made to the sketch after the sharing session has ended will only be available to the party editing the sketch.	**Question** **Condition** : Once sketch shared, there exist some drawn lines, post drawn lines and currently session closed. **Action** : party A want to invite again. **Question** : Are drawn lines from previous session (including lines drawn by party B) and post drawn lines treated as a pre-edit? In other words, should all lines moved to party B? (B might close shared sketch, of course **Doubts** : Undoing including lines drawn by party B is available.	The idea was that a sketch is saved after a sketch session is closed. That sketch is saved locally as an image which can be accessed again by that single user. The user can sketch on that image (for the user himself) and by doing that preparing a new sketch that can be used as a background within a next session. If that image is shared as background for a new sketch session, there is no option to remove / edit anything of formerly done drawings. Note: the requirement about pre-editing a sketch is optional same as editing a sketch after it was stored locally.

Category	User Story ID	Requirement ID	Requirement	Questions	Answers
Shared Image Sketch	US12-56	R12-56-1	A separate entry point for a shared image sketch should be provided on the in-call screen (i.e. defaulting to an image background or a blank canvas).	**Question:** In protocol level, there's only two kind of session Shared Sketch/Map. The only difference between Shared Sketch and Shared Image Sketch is just availability of setting background once before session established. Right? **Doubts**: Very less meaning on Shared Image Sketch.	The B party needs to know it is a map share and new parameters like the coordinates and map scale need to be shared.
Bounds Tag	US12-61	R12-61-2	Both parties shall be able to move the map location, independent of the map being viewed by the other party. NOTE: These changes to the map are not visible to the other party.	**Question**: When this Bounds tag will be used? For reserve? Spec is just related requirement, not necessarily needed Bounds tag	See R12-62-2 If the other party has edited a part of the map that the current party is not viewing, then the current party should be able to easily synchronise the map location. The bounds tag is used to implement that requirement. (So that B party can see where on the map A party has edited something. This is needed in case A and B party look at different areas of the map).

Category	User Story ID	Requirement ID	Requirement	Questions	Answers
Handling at Terminating Nodes			*On receipt of the SIP INVITE request the RCS Client shall check if the Enriched Calling services as indicated by the ICSI in the Accept-Contact header are running on the device:* *3) Shall respond with a SIP 603 Decline if the session is not accepted by the user*	IR.92 CR1068 Call Rejection by Busy: If the user rejects an incoming call by invoking User Determined User Busy (UDUB) as described in 3GPP TS 22.030 [x], then the UE must send a SIP 486 (Busy here) response to the network. How the UE should act in case of Enriched Calling service over VoLTE call is declined by the user?	1) Incoming SIP invite for a VoLTE call à in case the user declines that call, UE sends SIP 486 (Busy here). 2) Incoming SIP invite for an Enriched Calling Session à RCS client sends SIP 603 Decline if the user does not accept e.g. a Shared Map invite. In case of call composer over VoLTE there will be two invites. One for the call and one for the Enriched Calling Session.

Document Management

Document History

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
1.0	04.02.2016	First version approved by IOT MNO Group, based on guidelines transferred from joyn Blackbird Implementation Guidelines v1.7 and additional guidelines approved by the IOT MNO Group: - new clarification ID_2_28 on Group Chat Full Store Forward configuration; - changes to the existing ID_4_21 on Dual IMS Registration and device instance identification; - new recommendation ID_4_22 on Removal of Group Chat participant after removal of IMS subscription, to become a requirement 3 months after the publication. New clarifications for Enriched Calling services have been added based on the approved CRs toward RCC.20 and RCC.07 and included into ID_4_23 – ID_4_33. The Annex B has been added to the document with the Q&A section for Shared Sketch	joyn IP Comms IOT MNO	Konstantin Savin / GSMA
2.0	14.07.2016	New guidelines ID_2_29 – ID_2_32 on configuration aspects, new guidelines ID_4_34 – ID_4_36 on SIP/SDP/XML related aspects and correction to the existing clarification ID_4_28 have been incorporated into the document. All changes have been approved by joyn IP Comms IOT MNO Group.	joyn IP Comms IOT MNO	Konstantin Savin / GSMA
3.0	15.12.2016	New guidelines ID_3_1_1-3_1_2 for multiple clients handling on Android, new clarification ID_4_37 on concatenation of ICSI and/or IARI tags, corrected client re-configuration actions in ID_2_30, clarified ID_2_31 on address book scan, new	joyn IP Comms IOT MNO	Konstantin Savin / GSMA

		clarifications ID_2_33 and ID_2_34 on client configuration for RCS pre-universal profile, new guidelines ID_4_38 and ID_4_39 on Group Chat participant management, existing guidelines ID_4_25,26,27,29,30,31, 32,33 considered as no longer relevant and marked as Void, modification to ID_4_28 on call composer XML and new clarification ID_4_40 on RCC.20 endorsement have been incorporated into the document. All changes have been approved by joyn IP Comms IOT MNO Group.		
3.1	15.02.2017	Guideline ID_3_1_2 has been updated to embrace embedded RCS clients. All changes have been approved by joyn IP Comms IOT MNO Group.	joyn IP Comms IOT MNO	Konstantin Savin / GSMA

Other Information

Type	Description
Document owner	IOT Group
Editor / Company	Vodafone Group – IOT Group Lead Oscar Gallego