GSMA RCS IOT joyn Blackbird Implementation Guidelines

Version 1.2

07 March 2014

.

Security Classification – NON CONFIDENTIAL GSMA MATERIAL

Table of Contents

1 Introduction 4
1.1 Scope 4
1.2 Future queries and clarifications 4
1.3 Definition of Terms 4
1.4 Document Cross-References 6
2 RCS implementation clarifications 8
2.1 General issues 8
ID_1_1 Reject_btn parameter 8
ID_1_2 Blushing emotions 8
ID_1_3 HTTP Content server URL prefixes 8
ID_1_4 File Transfer over HTTP: sender upload retries in error cases 9
2.2 Configuration issues 9
ID_2_1 FQDN resolution 9
ID_2_2 P-CSCF redundancy 10
ID_2_3 Domain prefixes for provisioning 11
ID_2_4 MSISDN format in configuration request 12
ID_2_5 HTTP request during Wi-Fi Provisioning 12
ID_2_6 Configuration mechanism over PS without Header Enrichment 13
ID_2_7 Provisioning for high service availability 13
ID_2_8 Clarification on usage of the FT CAP ALWAYS ON parameter 13
ID_2_9 Clarification on expected client behaviour when validity period has expired 14
ID_2_10 Clarification on format of the 'token' HTTP parameter 14
ID_2_11 Max Message Size 15
ID_2_12 Client behaviour upon re-start 15
ID_2_13 403 Forbidden Response on provisioning request 15
ID_2_14 MAX_AD-HOC_GROUP_SIZE parameter format 16
ID_2_15 ACS behaviour when user enters incorrect MSISDN 16
2.3 Mobile OS issues 17
ID_3_1 Android 17
ID_3_2 iOS (Apple) 19
ID_3_3 Symbian 19
ID_3_4 Windows Phone 20
2.4 SIP/SDP issues 20
ID_4_1 Normalization of MSISDNs 20
ID_4_2 Registration procedure intervals 20
ID_4_3 Session description connection attribute 21
ID_4_4 OPTIONS during bi-directional Video Share session 21
ID_4_5 FT via HTTP upload/download resume 21
ID_4_6 SIP User-Agent header 22
ID_4_7 Clarification on CPIM TO parameter's value used in disposition notifications during Group Chat 23
ID_4_8 Clarification on feature tags in Contact and Accept-Contact headers 23
ID_4_9 Group Chat failed rejoin with non-specified error codes 24
ID_4_10 XML body in the INVITE during Geolocation PUSH 24
ID_4_11 Clarification on FT feature tags 25
ID_4_12 Clarification on forwarding Group Chat Message to legacy clients 25
ID_4_13 Clarification on File Transfer via HTTP bodies 26
ID_4_14 Client de-registration upon reboot, switch off or termination 28
2.5 MSRP issues 29
ID_5_1 MSRP passive role 29
ID_5_2 IMDN.Message-ID length 29
2.6 RTP/RTCP issues 29
ID_6_1 Use of the VideoShare profiles 29
ID_6_2 Extmap local IDs 30

ID_6_3 RTP Extensions 30
ID_6_4 H.264 profile-level negotiation 31
2.7 End User Confirmation Request (EUCR) issues 31
ID_7_1 Terms and Conditions 31
ANNEX A Frequently asked questions 32
Document Management 34
Document History 34
Other Information 35

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 latest version of the RCS specification [1] available on the GSMA website and all update recommendations of the current document would be incorporated in 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 [1] in order to improve understanding.
- Recommendation
  Includes some suggestions on how the functionality required in the latest version of the RCS specification [1] can be implemented
- Requirement
  Introduces new requirements that will be included in a future update of the RCS specification [1]

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]. All the test cases were executed using the RCS Test Matrix tool [2]. Detailed information on the IOT and accreditation process could be found in the ‘Guidelines for Licensing Framework’ [3] available on the GSMA website.

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
IMS	IP Multimedia Subsystem
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
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
UX	User eXperience
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 4 http://www.gsma.com/
[2]	RCS IOT 001	RCS IOT joyn Blackbird Drop 1 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_jBBd1 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]	-	RCS v1.2, User Experience Guidance Document http://www.gsma.com/
[8]	-	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]	-	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 v3.0 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

2 RCS implementation clarifications

2.1 General issues

ID_1_1 Reject_btn parameter

Type	Recommendation
Related spec [1] clause	2.2.2.1.2
Related TC [2] ID	N/A
Publish date	04.07.2013
Date modified	04.07.2013

Description

The Reject_btn parameter included in the MSG characteristic that is used to deliver user messages within the autoconfiguration document (described in section 2.2.2.1.2 of [1]) is optional. When not provided a default value of “0” shall be assumed.

ID_1_2 Blushing emotions

Type	Recommendation
Related spec [1] clause	3.2.4.16
Related TC [2] ID	ID_RCS_7_x_x
Publish date	04.07.2013
Date modified	04.07.2013

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	Recommendation
Related spec [1] clause	3.5.4.8.4
Related TC [2] ID	RCS_ID_5_1_1
Publish date	17.12.2013
Date modified	17.12.2013

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	2.3.3.2
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.

2.2 Configuration issues

ID_2_1 FQDN resolution

Type	Clarification
Related spec [1] clause	A.1.5
Related TC [2] ID	ID_RCS_1_1_1
Publish date	21.02.2012
Date modified	21.08.2012

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).

ID_2_2 P-CSCF redundancy

Type	Requirement
Related spec [1] clause	2.1
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	Recommendation
Related spec [1] clause	2.2.2.1.2
Related TC [2] ID	RCS_ID_1_1_1
Publish date	22.08.2013
Date modified	22.08.2013

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
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
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
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	Recommendation
Related spec [1] clause	2.1
Related TC [2] ID	ID_RCS_1_x_x
Publish date	15.11.2013
Date modified	15.11.2013

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
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
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	Recommendation
Related spec [1] clause	Tables 12, 14, 235,236
Related TC [2] ID	ID_RCS_1_5_x
Publish date	15.11.2013
Date modified	15.11.2013

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
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 77 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
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
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 160 and 239
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 160 and 239 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
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.

2.3 Mobile OS issues

ID_3_1 Android

ID_3_1_1 Avoiding conflict between two joyn clients on the same device (Android only)

Type	Requirement
Related spec [1] clause	N/A
Related TC [2] ID	ID_RCS_1_4_x
Publish date	13.07.2012
Date modified	15.11.2013

Description

Note this recommendation applies to joyn clients (embedded or OTT) and that any joyn value-add service propositions which involve complementing the joyn proposition with additional services or joyn services using alternative platforms are not required to follow the procedures described in this section.

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 OTT 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 which is 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.

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 Avoiding to use the standard port with Android 4.0.3 and 4.0.4

Type	Recommendation
Related spec [1] clause	N/A
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	2.9.3
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 2.9.3.1 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	2.1
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	2.7.3
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	3.3.6
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
Related TC [2] ID	N/A
Publish date	15.11.2013
Date modified	15.11.2013

Description

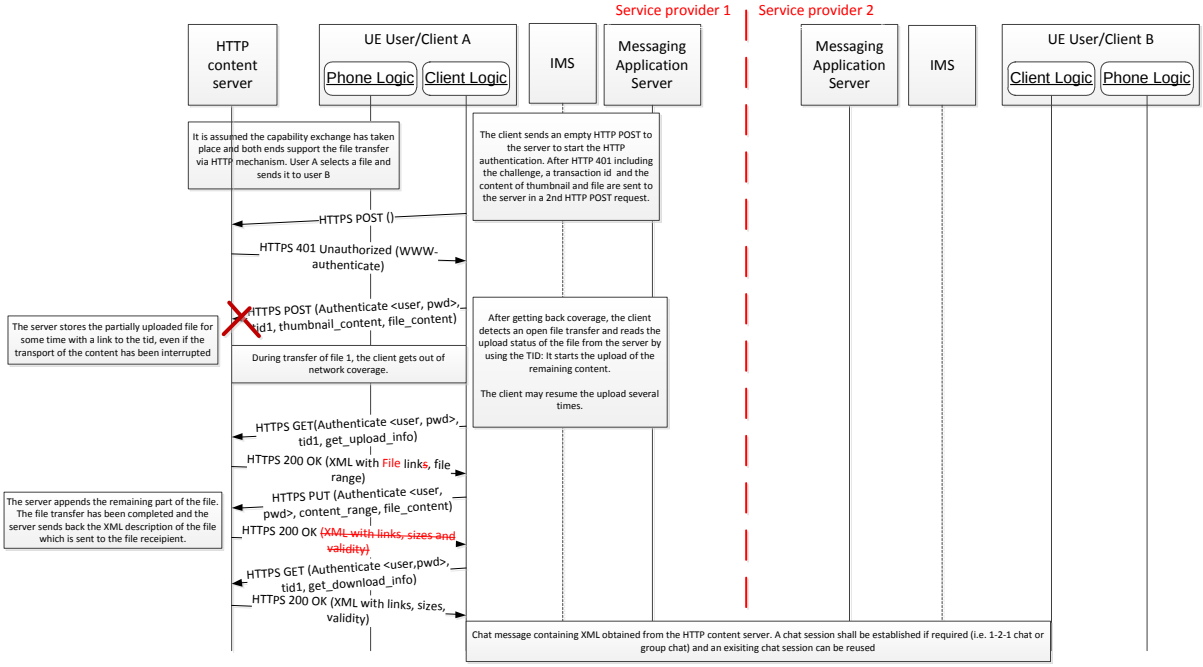
In order to provide more clarity around the procedures regarding the FT via HTTP upload resume procedure described in PRD GSMA RCS 5.1 version 2 section 3.5.4.8.1.1.1, the following clarifications shall be taken into account:

- 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, 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	Recommendation
Related spec [1] clause	N/A
Related TC [2] ID	N/A
Publish date	15.11.2013
Date modified	15.11.2013

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
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
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	Recommendation
Related spec [1] clause	3.4.4.1.7
Related TC [2] ID	ID_RCS_7_4_1x
Publish date	15.11.2013
Date modified	15.11.2013

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
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
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	Recommendation
Related spec [1] clause	3.4.4.1.5
Related TC [2] ID	ID_RCS_7_7_1
Publish date	15.11.2013
Date modified	15.11.2013

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
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
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].

2.5 MSRP issues

ID_5_1 MSRP passive role

Type	Clarification
Related spec [1] clause	2.13.1.3.2
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
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.

2.6 RTP/RTCP issues

ID_6_1 Use of the VideoShare profiles

Type	Recommendation
Related spec [1] clause	2.7.3
Related TC [2] ID	RCS_ID_6_1_3
Publish date	04.07.2013
Date modified	17.12.2013

Description

The originator of the Video Share session can indicate support for both Baseline (BP) and Constraint Baseline (CBP) profiles 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	Recommendation
Related spec [1] clause	2.7.3
Related TC [2] ID	RCS_ID_6_1_3
Publish date	22.08.2013
Date modified	22.08.2013

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	2.7.3
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	2.7.3
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 if during establishment of the Video Share session the Terminating party doesn't 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).

2.7 End User Confirmation Request (EUCR) issues

ID_7_1 Terms and Conditions

Type	Recommendation
Related spec [1] clause	2.14
Related TC [2] ID	ID_RCS_10_x_x
Publish date	04.07.2013
Date modified	04.07.2013

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 2.14 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).

Document Management

Document History

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
0.1	26.09.2013	First draft version with initial guidelines transferred from RCS Implementation Guidelines	RCS IOT MNO	Konstantin Savin / GSMA
0.2	05.11.2013	Second draft version updated with latest CR (ID_2_4 – ID_2_10, ID_3_1_1, ID_4_5 – ID_4_11) approved by IOT MNO Group within META3 timeframe	RCS IOT MNO	Konstantin Savin / GSMA
1.0	15.11.2013	Additional clarifications added on Max Message Size (ID_2_11), added note into clarification ID_4_7, new recommendation ID_4_12 on forwarding group chat message to legacy clients and new clarification on FTviaHTTP bodies (ID_4_13). First version approved by RCS IOT MNO Group	RCS IOT MNO	Konstantin Savin / GSMA
1.1	17.12.2013	Additional note to ID_6_1 on usage of the level per H.264 profile, new recommendation ID_1_3 on HTTP Content server URL prefixes format, new clarification ID_2_12 on version checking after restart have been incorporated into the document. All changes have been approved by RCS IOT MNO Group.	RCS IOT MNO	Konstantin Savin / GSMA
1.2	07.03.2014	New clarification ID_1_4 on sender FTvHTTP upload retries in error cases, new clarification ID_2_13 on client behaviour when receiving of the 403 response to HTTP provisioning request, new clarification ID_2_14 on the use of max_adhoc_group_size parameter in HTTP requests, new recommendation ID_2_15 on ACS behaviour when user enters incorrect MSISDN, new clarification ID_4_14 on client de-registration cases, new clarification ID_5_1 on receiving of an empty MSRP while taking passive role and new recommendation ID_5_2 on IMDN.Message-ID parameter length have been incorporated into the document. All changes	RCS IOT MNO	Konstantin Savin / GSMA

		have been approved by RCS IOT MNO Group.		

Other Information

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