FFT Doc 16.002 v1.0 (April 2016)

French Federation of Telecommunications
Standards Committee
IP Interconnection Working Group
Architecture Sub-group

IP interconnection
Interface specification
for RCS interconnection

Part 1: Endorsement of GSMA IR.90 for Joyn Blackbird
Part 2: Additional topics

French Federation of Telecoms

Internet

http://www.fftelecom.org

SYNOPSIS

1. Context

1.1. Purpose

The purpose of this document is to define the SIP/SDP interconnection interface for the national interconnection between two French Third Party Operators (TPO) for RCS services.
The scope of services supported is Joyn BlackBird.

1.2. Standards

See "Interface specification for RCS interconnection - Endorsement of GSMA IR 90" document for the endorsement to GSMA IR.90 standard for Joyn BlackBird.

1.3. References

[RFC3261]	IETF RFC 3261 "Session Initiation Protocol (SIP)"
[RFC3262]	IETF RFC 3262 "Reliability of Provisional Responses in the Session Initiation Protocol (SIP)"
[RFC3264]	IETF RFC 3264 "An Offer/Answer Model with the Session Description Protocol (SDP)"
[RFC3311]	IETF RFC 3311 "The Session Initiation Protocol (SIP) UPDATE method"
[RFC3312]	IETF RFC 3312 "Integration of Resource Management and Session Initiation Protocol (SIP)"
[RFC3323]	IETF RFC 3323 "A Privacy Mechanism for the Session Initiation Protocol (SIP)"
[RFC3325]	IETF RFC 3325 "Private Extensions to the Session Initiation Protocol (SIP) for Network Asserted Identity within Trusted Networks".
[RFC3326]	IETF RFC 3326 "The Reason Header Field for the Session Initiation Protocol (SIP)"
[RFC3407]	IETF RFC 3407 "Session Description Protocol (SDP) Simple Capability Declaration"
[RFC3556]	IETF RFC 3556 "Session Description Protocol (SDP) Bandwidth Modifiers for RTP Control Protocol (RTCP) Bandwidth"
[RFC3840]	IETF RFC 3840 "Indicating User Agent Capabilities in the Session Initiation Protocol (SIP)"
[RFC3862]	IETF RFC 3862 "Common Presence and Instant Messaging (CPIM): Message Format"
[RFC3966]	IETF RFC 3966 "The tel URI for Telephone Numbers"
[RFC4028]	IETF RFC 4028 "Session Timers in the Session Initiation Protocol (SIP)"
[RFC4320]	"Actions Addressing Identified Issues with the Session Initiation Protocol's (SIP) Non-INVITE Transaction"
[RFC4566]	IETF RFC 4566 "Session Description Protocol (SDP)"
[RFC4488]	IETF RFC 4488 "Suppression of Session Initiation Protocol (SIP) REFER Method Implicit Subscription"
[RFC4575]	IETF RFC 4575 "A Session Initiation Protocol (SIP) Event Package for Conference State"
[RFC4975]	IETF RFC 4975 "The Message Session Relay Protocol (MSRP)"
[RFC5366]	IETF RFC 5366 "Conference Establishment Using Request-Contained Lists in the Session Initiation Protocol (SIP)"
[RFC5368]	IETF RFC 5368 "Referring to Multiple Resources in the Session Initiation Protocol (SIP)"
[RFC5438]	IETF RFC 5438 "Instant Message Disposition Notification (IMDN)"
[RFC5547]	IETF RFC 5547 "A Session Description Protocol (SDP) Offer/Answer Mechanism to Enable File Transfer"
[RFC5923]	IETF RFC 5923 "Connection Reuse in the Session Initiation Protocol (SIP)"
[RFC6135]	IETF RFC 6135 "The Alternative Connection Model for the Message Session Relay Protocol (MSRP)"
[RFC6714]	IETF RFC 6714 "Connection Establishment for Media Anchoring (CEMA) for the Message Session Relay Protocol (MSRP)"
[MSRP sessmatch]	IETF Simple MSRP sessmatch draft version 10 (http://tools.ietf.org/html/draft-ietf-simple-msrp-sessmatch-10)
[RCS5.1 UNI]	GSMA "Rich Communication Suite 5.1 Advanced Communications Services and Client Specification" V4.0 (28/11/2013)
[OMA IM]	OMA "Instant Messaging using SIMPLE" (ref: OMA-TS-SIMPLE_IM-V2_0-20130809-D) (09/08/2013)
[JOYN BLACKBIRD]	GSMA "joyn Blackbird Product Definition Document" V4.0 (06/10/2014)

[Architecture_FFT]	FFT, "Architecture d'interconnexion RCS/Joyn, Principes et recommandations", FFT, Doc. 16.001, V1.0 (April 2016)
[Profile_FFT_RCS_End]	FFT "Interface specification for RCS interconnection – Part 1: Endorsement of GSMA IR.90 for Joyn Blackbird" (ongoing publication)

1.4. Glossary

FQDN	Fully Qualified Domain Name
MIME	Multipurpose Internet Mail Extensions
NNI	Network To Network Interface
RCS	Rich Communication Suite
SIP	Session Initiation Protocol
SDP	Session Description Protocol
TCP	Transport Control Protocol
TPO	Third Party Operator
UDP	User Datagram Protocol
URI	Uniform Resource Identifier

2. SIP interconnection equipment behavior

The interconnection equipment should act as a SIP B2BUA for SIP routing information (as indicated in 3GPP TS 24.229 §5.10.1) for security reasons (Topology Hidding).

When it acts as a SIP B2BUA (recommended), the interconnection equipment shall emit only one Via header, its own address in the Contact header, no Record-Route header, except for Group Chat. In this latter use case it shall be transparent to the Contact header field and insert a Record-Route header: see §4.3.1.

When it acts as a SIP proxy, it typically emits several Via and Record-Route headers, corresponding to the encountered nodes in the path, and an address in the Contact header corresponding to another node than interconnection equipment itself.

The compatibility of the operator to one of these both modes is ensured by the respect of the SIP procedures concerning the headers mentioned above.

3.   SIP Signalling messages

3.1.   Definitions

<u>When defined within the current specification</u>, only the SIP signalling elements (e.g. methods, option tags, message bodies, identity formats…) defined and authorized (mandatory or optional) as described within the current specification can be exchanged over the interconnection interface.

3.2.   Transport protocol

According to [RFC 3261] 3 modes are possible: TCP or UDP with IP fragmentation or UDP with switch to TCP for messages larger than 1300 bytes.

When TCP is used, the TCP connection shall be reused, according to [RFC5923] (Connection Reuse in the SIP).

3.3.   SIP methods and headers

3.3.1.   SIP methods

Table 1 contains the SIP methods required to support the capabilities and services identified in section §1.1.1.

Mandatory methods
INVITE
ACK
BYE
CANCEL
OPTIONS
MESSAGE
REFER
SUBSCRIBE
NOTIFY

Table 1: Mandatory SIP methods

Optionnaly, re-INVITE and or UPDATE methods may be used if the optional keep-alive mechanism for active SIP sessions as defined in [RFC4028] is used for Video and Image share services.
Otherwise, these methods shall not be used (neither for keep-alive mechanism for other services than Video and Image share nor for other purposes than keep-alive).

Optional methods (for keep-alive purpose for video and Image share)
Re-INVITE
UPDATE

Table 2: Optional SIP methods (for keep-alive purpose for Video and Image share services)

No other method than the ones listed in Table 1 and 2 is supported.

Table 3 lists the required SIP methods to support per RCS feature/service.

RCS feature/service		Required SIP methods to support
Capability discovery and update	Based on OPTIONS	OPTIONS
Content sharing (during a voice call)	Image share	INVITE ACK CANCEL

		BYE
	Video share	INVITE
		ACK
		CANCEL
		BYE
Chat (based on OMA SIMPLE IM)	1-to-1 chat	INVITE
		ACK
		CANCEL
		BYE
		MESSAGE
	Group chat	INVITE
		ACK
		CANCEL
		BYE
		REFER
		SUBSCRIBE
		NOTIFY
File transfer (standalone)	Over HTTP	INVITE
		ACK
		CANCEL
		BYE
		MESSAGE
	Over MSRP	INVITE
		ACK
		CANCEL
		BYE

Table 3: List of required SIP methods to support per feature/service

3.4. Maximum SIP elements size

Each network operator is responsible to check that the maximum size of SIP message or header or body it applies does not prevent a RCS service to be delivered.

A particular attention is given to Contact headers length that must respect a maximum number of digits. **This maximum shall be defined and exchanged between the two interconnected operators.**

See Annex B of "Interface specification for RCS interconnection - Endorsement of GSMA IR 90" for defined values.

Larger messages are rejected with a 513 "Message Too Large" response.

3.5. SIP Message bodies

The supported SIP bodies are:
- **application/sdp** (for SDP body, as defined in [RFC4566], with additionally [RFC5547] for File Transfer and Image Share and [RFC4975] for MRSP based services).
- **message/cpim** (for CPIM body, as defined in [RFC3862] and [RFC5438] for IM and IMDN) for Chat.
- **application/resource-lists+xml** (for MIME resource-list body, as defined in [RFC5366]) for Group Chat.
- **application/conference-info+xml** (for the list of participants, as defined in [RFC4575]) for Group Chat.

Message	Supported bodies
INVITE	application/sdp
	message/cpim
	application/resource-lists+xml

MESSAGE	message/cpim
NOTIFY	application/conference-info+xml
REFER	application/resource-lists+xml
200 OK (OPTIONS)	application/sdp
200 OK (INVITE)	application/sdp

Table 4: List of supported SIP bodies per message

When more than one body is present in the same message, the body is a multipart MIME.
It is required that the Content-Type header for multipart entities complies with the syntax defined in the [RFC2046] §5.1.1. Especially the use of the "boundary" parameter is required. In reception both formats of the "boundary" parameter, with and without quotes, shall be supported.

When the body is simple, the SIP message shall contain at least Content-Type, optionally Content-Disposition and optionally Content-Length (depending on transport protocol used, mandatory for stream-oriented, optional otherwise).

When the body is multipart, the SIP message shall contain:
− At least the following <u>SIP</u> headers for the whole body:
    o Content-Type (set to "multipart/mixed; boundary=<boundary-name>"),
    o optionally Content-Length (depending on the used transport protocol: mandatory for stream-oriented transport protocol, optional otherwise)
    o and optionally MIME-Version.
− The following <u>MIME</u> headers before each part of the multipart body:
    o Content-Type
    o and optionally Content-Disposition (e.g. Content-Disposition: "recipient-list" for MIME resource-list body).
No other MIME header is expected; in particular Content-Length MIME header shall not be present.

<u>Note:</u> at short term, it has been observed that some joyn client may send partial Content-Length MIME headers in INVITE requests containing multipart SDP and message/cpim bodies before each body itself.
If received, they must be ignored in reception. Only the Content-Length SIP header for the whole message body shall be taken into account when received.

3.6. Supported option tags of SIP extensions

The supported option tags of SIP extensions are:
− "timer" option-tag if the optional keep-alive mechanism for active SIP sessions as defined in the [RFC4028] is used for Video and Image share services.
− "norefersub" and "multiple-refer" option-tags which may be present in REFER transaction for adding participant(s) in a Group Chat, according to rules and procedures of [RFC4488] and [RFC5368] (cf [OMA IM] §7.1.1.7).

4. Identities considerations

4.1. Identities formats and address parameters

The identities formats supported for the Request-URI, From, To, P-Asserted-Identity, Referred-By and Refer-To headers if present are described in the following table.

The address formats supported for the Route, Record-Route, Via, and Contact headers if present are also described in the following table.

SIP URI format shall comply with [RFC3261]/19.1 and TEL URI with [RFC3966].

Global number and local number formats shall comply with [RFC3966].

Supported formats at NNI (NOTE 1)	
From	1. SIP URI like globalnumber@domainname with or without user=phone 2. Tel URI in global number format
To	1. SIP URI like globalnumber@domainname with or without user=phone 2. Tel URI in global number format 3. SIP URI in local number format @domainname with phone-context set to home-local-domain, with or without user=phone 4. Tel URI in local number format @domainname with phone-context set to home-local-domain 5. SIP URI as received in Contact header in INVITE transaction for the Group Chat establishment (towards Controling Function AS)
P-Asserted-Identity **(NOTE 2, 3, 4)**)	1. SIP URI like globalnumber@domainname with or without user=phone 2. Tel URI in global number format
Request-URI	1. SIP URI like globalnumber@domainname with or without user=phone 2. SIP URI as received in Contact header in INVITE transaction for the Group Chat establishment (towards Controling Function AS)
Referred-By	1. Tel URI in global number format 2. SIP URI like globalnumber@domainname with or without user=phone
Refer-To	1. Tel URI in global number format 2. Tel URI in local number format @domainname with phone-context set to home-local-domain (cf. §4.3.2)
Via	IP address / port at least for topmost value
Route (**NOTE 5**)	SIP URI (using an IP address)
Contact	SIP URI When the SIP URI in the Contact header identifies the interconnection equipment and may be used for routing purposes, it shall contain an IP address. When it corresponds to the Controlling Fonction for Group Chat (see §4.3.1), the SIP URI in Contact header may use a FQDN.

Supported formats at NNI (NOTE 1)	
Record-Route (**NOTE 6**)	SIP URI (using an IP address at least for topmost value)

NOTE 1: When several formats are listed (e.g. 1. 2. 3…), this means that:
- all formats must be supported in the receiving direction.
- at least one format of the list must be supported in the sending direction.

NOTE 2: According to [RFC3325], "There may be one or two P-Asserted-Identity values. If there is one value, it MUST be a sip, sips, or tel URI. If there are two values, one value MUST be a sip or sips URI and the other MUST be a tel URI."

NOTE 3: The name-addr format (i.e. with brackets <>) is recommended to be used when URI parameters are present.

NOTE 4: P-Asserted-Id may contain "rcse-standfw" in the user part of the SIP URI (in the INVITE request that sets-up the session to be used for fowarding the delivered and displayed notifications received when delivering stored messages – see scenarios in [RCS 5.1 UNI] B.1.4 and B.1.5).

NOTE 5: Sent in the in-dialog requests if a Record-Route has been previously received.

NOTE 6: When the interconnection equipment does not set its own address in the Contact header, it shall emit a Record-Route addressing itself in the requests/responses establishing a dialog in order to allow the correct routing of the in-dialog requests (see §4.3.1).

Table 5: Supported format identities

Moreover, the following principles shall be taken into consideration when dealing with phone numbers:
- In global-number format, the "+" is mandatory in front of the number as described in [RFC3966]
- The telephone number must contain only digits and must represent a national mobile number (national number means a number extracted from the national numbering plan, independantly of its format).

RCS services delivery can not be guaranteed if the recommended formats in this section are not respected.

4.2. Eligible destinations

The RCS service relies on two types of destinations at the NNI interface for requests establishing a dialog or standalone requests:
- Requests to an end-user represented by his phone number,
- Requests to an AS represented by an alphanumeric SIP URI (in the current version of the service, the only cases are the requests sent to a Controlling Function AS, for the Group Chat scenario).

For requests to an end-user represented by his phone number:
Each MNO shall send to the other one only requests to phone numbers currently managed by the latter. In particular, the originating operator is responsible to apply the number portability query when appropriate. There is no additional requirement to check that the addressed phone number is a joyn user within the remote network operator.
As long as the network operators do not use a shared database containing all the joyn users, incoming requests to any national mobile number that is not associated to a joyn user should be rejected by the terminating network.

For requests to an AS represented by an alphanumeric SIP URI:
The domain name used by each operator for addressing its AS shall be declared to the other operator. It may be the same as or different from the one used for addressing end users. See 4.3.2.

4.3. Group chat specificities

4.3.1. Reuse of the Contact address outside the initial dialog

The Contact address of the Controling Function AS for Group Chat, qualified by "isfocus" feature tag, shall be reusable in the Request-URI of a request issued:

- Outside the initial dialog in which this Contact address has been created (e.g. SUBSCRIBE and REFER requests),
- Once the initial dialog is closed (e.g. INVITE for Rejoin and Restart scenarii).

For that purpose, the standardized solution described in section 5.10.5 of 3GPP TS 24.229 shall be supported. That is:

The interconnection equipment shall transparently forward a received Contact header containing the "isfocus" media feature tag. When transparently forwarding a received Contact header field of a dialog-forming request or response, the interconnection equipment shall include its own URI in a Record-Route header field in order to ensure that it is included on the route of subsequent requests.

4.3.2. Management of home domain names

Each network operator shall be able to manage all metropolitain home-local-domains of interconnected networks, i.e. shall be able to convert a national mobile number known by its home-local-domain into a global E.164 number.

See Annex B of "Interface specification for RCS interconnection - Endorsement of GSMA IR 90" for defined home-local-domains values.

Reminder: If the target number is a non-international format telephone number, the phone-context value is set as defined in [3GPP TS 24.229] for home local numbers (for example *tel:0634578901;phone-context=<home-domain-name>*, cf [RCS5.1 UNI] §2.5.3.1).

4.3.3. REJOIN

A point of attention is raised concerning REJOIN mechanisms over NNI. a REJOIN should only occur over NNI for the following scenarii:

- A participant being part of an idle Groupchat wants to send a message to that specific Groupchat. Before sending the message, the Groupchat must be restarted by the participating function
- A participant being part of an idle Groupchat wants to invite a new member to that specific GroupChat. Before sending the REFER , the Groupchat must be restarted by the participating function
- Depending on the implementation, a participant who recovers his connection while he lost it being part of an active Groupchat, can REJOIN this specific Groupchat. If the Groupchat is idle at that moment, the participating function may restart the Groupchat.

4.4. Identities requirements

At the signalling interface, the "P-Asserted-Identity" header must be present in the initial and standalone requests.

- For requests issued from an end user, it shall contain the telephone number corresponding to that end user, provided (or verified) by the network operator serving that end user and expressed in a valid global-number format.
- For an INVITE request intended to setup a session for the forwarding of delivered and displayed notifications that result from the delivery of stored messages, it shall contain a SIP URI with "rcse-standfw" as user part.
- For an INVITE request that result from a REFER request, it shall contain the identity (phone number in global format) of the end user issuing the REFER request derived from the P-Asserted-Identity of that REFER request.

When present in an INVITE request, the Referred-By header shall contain the asserted identity of the end user that initiates the action the INVITE request results from (e.g. the identity of the user that initiates or restarts a Group Chat, the identity of the user that requests the addition of a participant within an ongoing Group Chat, or the identity of the user that issues the notifications that causes an INVITE request with "rcse-standfw" in the P-Asserted-Identity).

4.5. Procedures for multidevice handling

Though multidevice is not part of Blackbird, each Blackbird client shall support the procedures described in section 2.4.2 of [RCS5.1 UNI] in order to enable the introduction of multidevice configurations later on. Among the two technical solutions described in section 2.4.2 of [RCS5.1 UNI] (GRUU or sip.instance), only the one based on the sip.instance feature tag is supported over the NNI interface. GRUU procedures are not supported.

If present, sip.automata feature tag, defined in [RFC3840], shall be transparently transmitted.

5.   Media session management

SDP offer/answer exchange shall be performed according to [RFC3261], [RFC3264] and [RFC4566].

SDP information is only supported in the body of INVITE, re-INVITE (cf Note), 200 OK (INVITE), 200 OK (re-INVITE) (cf Note) and 200 OK (OPTIONS) messages.

Note: applicable only when the optional keep-alive mechanism for active SIP sessions as defined in [RFC4028] is used for Image and Video share services.

At minimum, the SDP parameters used in [RFC3264] shall be supported.

For handling MSRP sessions on the NNI interface:

−   [RFC6135] (The Alternative Connection Model for the Message Session Relay Protocol (MSRP)) shall be supported.
    As a result, the direction of the establishment of the TCP connection shall follow the rules of this RFC, meaning that the TCP connection shall be established from the originating network towards the terminating network.
    The procedures to populate the a=setup attribute value shall be compliant with this RFC. In particular, the terminating network shall include the a=setup attribute set to "passive" in the SDP answer, so that the originating network will establish the TCP connection.

−   IETF Simple MSRP sessmatch draft version 10 (http://tools.ietf.org/html/draft-ietf-simple-msrp-sessmatch-10) shall be supported if the interconnection equipment in MSRP media plane on the NNI interface is not B2BUA (NB: solution used in RCS specifications, the solution based on [RFC6714] (CEMA for MSRP) is not applicable for RCS). In this case, there is no topology hiding at MSRP level. The useful information to be used from "from-path" and "to-path" MSRP headers for the matching is the "session-id". See §2.8.2 "MSRP session matching" from [RCS5.1 UNI].

Not supported SDP parameters shall be passed transparently.

5.1. SIP session establishment

5.1.1.   Initial INVITE message

This section assumes offer/answer rules solely based on [RFC3261] and [RFC3264]. Additional offer/answer rules defined in [RFC3262] and [RFC3311] are not supported.

Initial INVITE messages shall contain an SDP offer. The SDP answer shall be present in the 200 OK response.

Initial INVITE messages with an SDP offer shall not be coded with the address of connection (c= line) set to 0.0.0.0.

For MSRP session set up, the initial INVITE messages shall contain an "a=accept- types" and an "a=accept-wrapped-types" SDP attributes as media attribute for the MSRP media line.
The "a=accept- types" shall be set to "message/cpim" for Chat sessions (1-to-1 and Group Chat) and for 1-to-1 chat it shall also include "application/imiscomposing+xml".
The "a=accept-wrapped-types" shall be set according to the allowed services. For example for Chat sessions (1-to-1 and Group Chat) it shall be set to "text/plain" and "message/imdn+xml" content-types. For Group Chat it shall also include "application/imiscomposing+xml" content-type. For File Transfer using HTTP it shall also include "application/vnd.gsma.rcs-ft-http+xml".

5.1.2.   Codec negotiation rules

In a media stream "m=" line, codecs shall be listed in order of preference for SDP negotiation, the first codec format listed being the preferred one.

If an SDP answer is received indicating support of more than one codec among those proposed in the SDP offer, only the first one shall be considered.

If there are no media formats in common in the SDP offer received in an initial INVITE, it shall be rejected by a 488 "Not acceptable here" response.

5.2. Terminating a session

The procedures used to terminate a session are described in [RFC3261], with the following precision:

– When the calling party side wishes to terminate the session during the early-dialog phase it is recommended to use the CANCEL method instead of the BYE method.
If present in BYE or CANCEL request, the Reason header shall be transparently transmitted.
When terminating an early-dialog by a CANCEL because of no answer from the other interconnected network, the CANCEL must be sent after the INVITE transaction timeout timer has expired (timer B following [RFC3261]). See Annex B of "Interface specification for RCS interconnection - Endorsement of GSMA IR 90" for defined values.

- When a party wishes to terminate an established session/dialog, it is recommended for this party to only send a BYE and not to close the TCP session. When the other party receives the BYE, it will close the TCP session and answer 200 OK to the BYE (cf [OMA IM] §7.1.1.12).
This recommendation avoids crossing BYE requests from both ends which can lead to undesired side effects.

5.3. RTP/RTCP packet source

In a session, the same IP address and port number shall be used to send and receive RTP packets (symmetric IP address and port number).

Note: The port number for sending/receiving RTCP packets MUST be equal to "the port number negotiated for RTP" + 1.

5.4. Codecs

5.4.1. Video share service

Please refer to [Architecture_FFT] §4.2.7.

---

6. Session and link management

6.1. Keep alive

6.1.1. Keep alive for active SIP sessions

For Image and Video share services, a keep alive mechanism can be used between 2 terminals to check that communications are still active by using the mechanism defined in [RFC4028].
No additional keep alive mechanism is used.

6.1.2. Keep alive for interconnection signalling links

No keep alive mechanism is used.

6.2. MSRP media inactivity management

6.2.1. General

Each network operator shall not perform MSRP media inactivity procedures if that could lead to release the session before the service logic decides it, i.e. network equipement in media plane shall not have management timers with inferior values to service ones.
See Annex B of "Interface specification for RCS interconnection - Endorsement of IR 90" for defined values.

6.2.2. Group chat case

As required by [RCS5.1 UNI] §3.4.4.1.3.3, the Participating Function (PF) chat inactivity timers must be greater than the Controlling Function (CF) ones in order to avoid confusion between inactivity release and voluntary release (i.e. PF transmits the voluntary departure and CF decides for inactivity). A voluntary departure is definitive whereas a user can rejoin a Group Chat after inactivity period.
See Annex B of "Interface specification for RCS interconnection - Endorsement of GSMA IR 90" for defined values.

6.3. Congestion

On reception of a 503 "Service Unavailable" response, the mechanisms defined in [RFC3261] section 21.5.4 apply.

6.4. Groupchat contexts persistence and Controlling Function

Groupchat contexts (list of participants, contributionID, Session Identity …) can be stored at Controlling Function (CF) level. It will allow the network to restart a Groupchat by only receiving a REJOIN request from a device and avoid this device to restart a Groupchat with potentially a not up-to-date list of participants.
These contexts need to be flushed regularly. This flush need to be performed following a timer here called "Tcf". When Tcf is reached, the next REJOIN request will make the device restart the Groupchat on its own network's CF. Therefore, it is important to synchronise this timer "Tcf" between all interconnected networks in order to have a better Grouchat repartition hosted between the Controlling Function servers.

See Annex B of "Interface specification for RCS interconnection - Endorsement of GSMA IR 90" for defined values.

7. Document management

Document History

History of the present document		
0.1	28/07/2015	First draft presented to the FFT working Group
0.2	23/10/2015	2nd draft for clarifications
1.0	07/04/2016	No comments from the consultation phase. Approved public version.