RCS Interworking Guidelines
Version 14.0
13 October 2017

This is a Non-binding Permanent Reference Document of the GSMA

Security Classification: Non-confidential

Access to and distribution of this document is restricted to the persons permitted by the security classification. This document is confidential to the Association and is subject to copyright protection. This document is to be used only for the purposes for which it has been supplied and information contained in it must not be disclosed or in any other way made available, in whole or in part, to persons other than those permitted under the security classification without the prior written approval of the Association.

Copyright Notice

Disclaimer

The GSM Association ("Association") makes no representation, warranty or undertaking (express or implied) with respect to and does not accept any responsibility for, and hereby disclaims liability for the accuracy or completeness or timeliness of the information contained in this document. The information contained in this document may be subject to change without prior notice.

Antitrust Notice

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

Table of Contents

1 Introduction

1.1 Overview

This document illustrates the inter-Service Provider aspects of RCS (Rich Communication Suite). The aim is to minimize any interoperability issues when deploying RCS services between Service Providers by making sure guidelines for deployment options are documented. This is necessary for example due to the number of different possible implementation alternatives existing in the corresponding specifications. The intention is not to reinvent the wheel by creating new specifications, but instead to reuse those already existing by making sure Network-to-Network Interface (NNI) specific details of RCS are well documented.

The most relevant RCS document is the GSMA “Rich Communication Suite 7.0 Advanced Communications Services and Client Specification” [RCS7.0] which details the service features that define an RCS Release and illustrates the technical details of different RCS services. In addition, there are a number of endorsement documents, such as GSMA “Rich Communication Suite 7.0 Endorsement of CPM 2.2 Conversation Functions” [RCS-CPM-CONVFUNC-ENDORS] describing which sections of a particular specification are supported by RCS.

For further information about RCS, see http://www.gsma.com/network2020/rcs/

User-to-Network Interface (UNI) specific issues are out of scope, since they do not directly impact NNI. Whatever UNI transport is used for accessing the home network RCS services (for example, 2G, 3G, 4G, Global Access Network (GAN) or ADSL) is transparent from the NNI point of view.

In general, the following RCS services are relevant for this document:

- Capability exchange based on Open Mobile Alliance (OMA) Session Initiation Protocol for Instant Messaging and Presence Leveraging Extensions (SIMPLE) Presence and Session Initiation Protocol (SIP) OPTIONS
- Chat
- Video Share based on GSMA [IR.74]
- Geo-location sharing
- Voice call based on [IR.92] and [IR.51]
- Video call based on [IR.94] and [IR.51]
- Enriched Calling based on [RCC.20]

General GSMA interworking guidelines are fully applicable to RCS, so for example the guidance given in [IR.34], [IR.65], [NG.105] and [IR.77] related to issues such as addressing, routing, Quality of Service (QoS) and security need to be taken into account. They are not listed in detail within this document. See http://www.gsma.com/newsroom/technical-documents/ for these recommendations.

It should be noted that in general within context of GSMA the term “interworking” means the same as “interconnection”. Thus, for example “IM interworking” does not imply conversion between different messaging technologies, but interconnection of IM between Service Providers.

Annex A illustrates the mapping between NNI and UNI parameters, including recommended handling of the parameters per RCS service.

Roaming

For devices that are configured to use the IP Multimedia Subsystem (IMS) Access Point Name (APN), the IMS voice roaming architecture as specified in [IR.65] is applicable for all RCS services.

For devices that are configured to use the Home Operator Services (HOS) APN, the home-routed roaming architecture as specified in [IR.88] and [IR.33] is applicable for all RCS services using the HOS APN in the Home Public Mobile Network (HPMN) to connect to the IMS.

Inter-Service Provider aspects associated with these RCS services are defined in later sections of this document.

Legacy

"Legacy" services including Circuit Switched (CS) voice, CS video, Short Message Service (SMS) and Multimedia Messaging Service (MMS) are expected to work as they do today, therefore it is not necessary for additional guidelines in the RCS context.

Note: It is also possible to run CS based services over Packet Switched (PS) based inter-Service Provider network, using for example MSC-S/SIP-I and Signalling Transport (SIGTRAN) technologies. This, however, is transparent to RCS and is therefore out of scope for this particular document. See the corresponding GSMA Networks Group documentation (such as [IR.83]) for further details.

Abbreviations

Term	Description
APN	Access Point Name
AS	Application Server
B2BUA	Back-to-Back User Agent
BG	Border Gateway
CPM	Converged IP Messaging
CS	Circuit Switched
IARI	IMS Application Reference Identifier
IBCF	Interconnection Border Control Function
ICSI	IMS Communication Service Identifier
IM	Instant Messaging
IMS	IP Multimedia Subsystem
IPX	IP eXchange
IWF	InterWorking Function
LBS	Location Based Services
LTE	Long Term Evolution

Term	Description
MaaP	Messaging as a Platform
MSRP	Message Session Relay Protocol
NNI	Network-to-Network Interface
NVAS	Network Value Added Services
P2P	Peer-to-Peer
PS	Packet Switched
RCS	Rich Communication Suite
RTP	Real-time Transport Protocol
SIMPLE	Session Initiation Protocol for Instant Messaging and Presence Leveraging Extensions
SIP	Session Initiation Protocol
SPI	Social Presence Information
TrGW	Transition Gateway
URI	Uniform Resource Identifier
XCAP	XML Configuration Access Protocol
XDM	XML Document Management
XML	eXtensible Markup Language

1.5 References

Ref	Doc Number	Title
[1]	[24.229]	3GPP TS 24.229, 3rd Generation Partnership IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP) http://www.3gpp.org
[2]	[29.165]	3GPP TS 29.165, 3rd Generation Partnership Project Inter-IMS Network to Network Interface http://www.3gpp.org
[3]	[AA.80]	GSMA PRD AA.80 – “Agreement for IP Packet eXchange Service Agreement” http://www.gsma.com
[4]	[IR.33]	GSMA PRD 33 – “GPRS Roaming Guidelines” http://www.gsma.com
[5]	[IR.34]	GSMA PRD 34 – “Guidelines for IPX Provider networks (Previously Inter-Service Provider IP Backbone Guidelines)” http://www.gsma.com
[6]	[IR.51]	GSMA PRD IR.51 – “IMS Profile for Voice, Video and SMS over Wi-Fi” http://www.gsma.com/
[7]	[IR.65]	GSMA PRD IR.65 - “IMS Roaming and Interworking Guidelines” http://www.gsma.com

Ref	Doc Number	Title
[8]	[IR.67]	GSMA PRD IR.67 – "DNS/ENUM Guidelines for Service Providers & GRX/IPX Providers" http://www.gsma.com/
[9]	[IR.74]	GSMA PRD IR.74 - "Video Share Interoperability Specification" http://www.gsma.com/
[10]	[IR.77]	GSMA PRD IR.77 – "Inter-Operator IP Backbone Security Requirements For Service Providers and Inter-operator IP backbone Providers" http://www.gsma.com/
[11]	[IR.83]	GSMA PRD IR.83 – " SIP-I Interworking Description" http://www.gsma.com/
[12]	[IR.88]	GSMA PRD IR.88 - "LTE and EPC Roaming Guidelines" http://www.gsma.com/
[13]	[IR.92]	GSMA PRD IR.92 - "IMS Profile for Voice and SMS" http://www.gsma.com/
[14]	[IR.94]	GSMA PRD IR.94 - "IMS Profile for Conversational Video Service" http://www.gsma.com/
[15]	[CPM1.0-AD]	OMA Converged IP Messaging Architecture http://www.openmobilealliance.org
[16]	[RCC.20]	GSMA PRD RCC.20 "Enriched Calling Technical Specification", http://www.gsma.com/
[17]	[RCS7.0]	GSMA PRD RCC.07 "Rich Communication Suite 7.0 Advanced Communications Services and Client Specification" http://www.gsma.com/
[18]	[RCS-CPM-CONVFUNC-ENDORS]	GSMA PRD RCC.11 "Rich Communication Suite 7.0 Endorsement of OMA CPM 2.2 Conversation Functions", http://www.gsma.com/
[19]	[NG.105]	GSMA PRD NG.105 – "ENUM Guidelines for Service Providers and IPX Providers"

2

Overall IMS NNI Architecture

The IMS NNI architecture is an important part of RCS NNI since RCS heavily utilizes IMS core system as specified by 3rd Generation Partnership Project (3GPP) to perform a number of key functions such as handling of SIP signalling, authentication, authorization, charging and routing support.

It should be noted that both main alternatives for IMS NNI, either using Mw/Gi/SGi interfaces, or using Ici/Izi interfaces are possible in RCS NNI. In other words, individual Service Providers can select the most optimal solution suitable. These two options are fully

interoperable, therefore a Service Provider using Mw/Gi/SGi can interwork with a Service Provider using Ici/Izi without any modifications needed.

For further details of IMS NNI architecture, see Section 3 “Interworking Guidelines” in [IR.65], which illustrates the general service interoperability between IMS networks. For inter-Service Provider guidelines applicable for IMS based services including RCS, see Section 5 “Service Related Guidelines” in [IR.65].

Detailed inter-Service Provider guidelines associated with RCS services are indicated in later Sections of this document.

IP Interconnection

3 Overview

3.1

There is a clear need for an IP based inter-Service Provider connection in RCS, simply because RCS is largely an IP based service. Meaning, existing CS/ Time-Division Multiplexing (TDM) based networks used for transporting voice between the Service Providers are not enough for the needs of RCS since they cannot be used for transporting SIP signalling or MSRP media.

IPX (IP eXchange) as defined in [IR.34] is an evolved version of GSMA GRX (GPRS Roaming eXchange) private inter-Service Provider IP backbone which has been commercially used since 2000 for all PS roaming traffic between GSMA Service Providers. IPX has been selected by GSMA as the preferred mechanism for the general IP roaming and interconnection, including also RCS. Therefore this document also concentrates on the model where IPX is utilized. This is in line with the existing IMS interworking recommendation given in the GSMA PRD [IR.65].

IPX is seen as the most optimal solution for providing the necessary global reach with low and predictable delay in a secure environment, that is something that is impossible to reach for example by internet based RCS NNI.

For the avoidance of doubt, this does not exclude usage of other alternatives, such as bilateral leased line, for RCS interworking purposes when seen fit by the participating Service Providers.

Further details on IPX, including the usage of different connectivity options and IPX Proxy, can be found in [IR.34] and [AA.80].

3.2

Application and transport layer protocols utilized by RCS services as documented in the [RCS7.0] Table “RCS protocols” of Section 2.8 “RCS Protocols” are valid also for NNI.

IPX

IPX is a global, private, IP network which supports end-to-end quality of service and the principle of cascading interconnect payments. IPX is completely separated from the public Internet. The IPX architecture consists of different IPX Providers connecting together via an IPX peering point for traffic exchange. Both signalling (such as SIP) and media (such as Real-time Transport Protocol (RTP) is transported within the IPX network. In IPX all parties

are bound by the end-to-end SLA. IPX can be used to transport any IP based service between Service Providers, both in roaming and interworking scenarios.

Figure 1 shows a high-level point of view of IPX network connecting three Service Providers with two IPX providers.

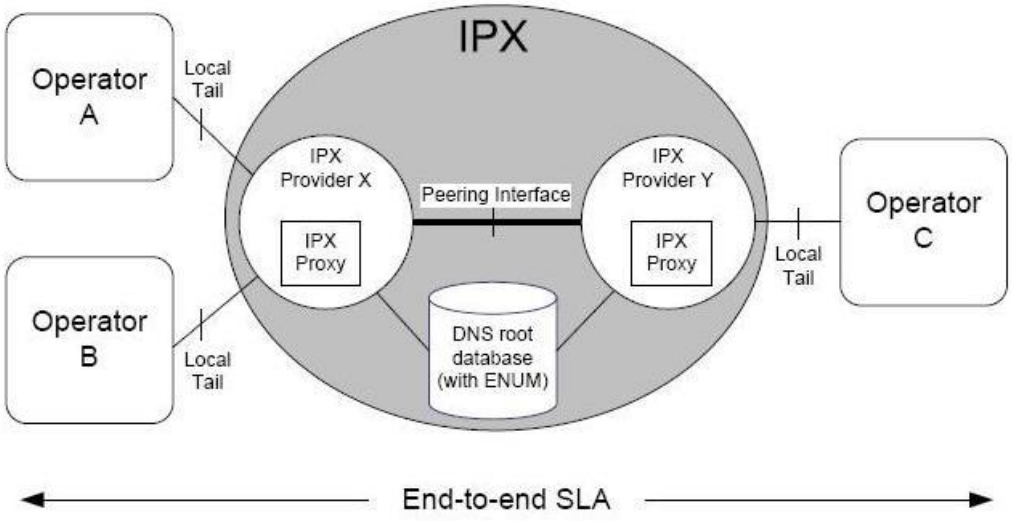

Figure 1: High-Level View of IPX (from IR.34)

IPX has three connectivity options:

- Transport-Only Connectivity Option

  A bilateral agreement between two Service Providers using the IPX transport layer with guaranteed QoS end-to-end. This model is not service aware

- Bilateral Service Transit Connectivity Option

  A bilateral agreement between two Service Providers using the IPX Proxy functions and the IPX transport layer with guaranteed QoS end-to-end. This model provides the opportunity to include service-based interconnect charging in addition to the transport charging of the transport-only model

- Multilateral Service Hub Connectivity Option

  A model providing multilateral interconnect with guaranteed end-to-end QoS and including service-based interconnect charging. Hubbing/multilateral connectivity is where traffic is routed from one Service Provider to many destinations or interworking partners via a single agreement with the IPX Provider. The hub functionality is provided by IPX Proxies

It should be noted that an IPX Proxy is not necessarily needed for RCS interworking as an IPX using the Transport-Only Option can handle the basic transportation of RCS traffic from one Service Provider to another.

In practice IPX offers the support of the necessary carrier-grade QoS features, security and global reach for any IP based service used between different Service Providers, including RCS. RCS uses the IMS NNI without change since, from the IMS core system point of view IPX is just an IP network. There is no need for modifications of either 3GPP IMS specifications or IMS node implementations due to inclusion of IPX.

Services

Capability Discovery

4

4.1.1 SIP OPTIONS Based

4.1

The present Section focuses on the interworking between two networks supporting the capability and new user discovery mechanism based on SIP OPTIONS as described in [RCS7.0] Section 2.6 “Capability and new user discovery mechanisms”. As a general principle, the capability discovery based on SIP OPTIONS interworking between two IMS networks (IMS-NNI) shall follow [IR.65].

In addition to general guidelines, the SIP OPTIONS NNI shall comply to the rule that the only feature tags which are allowed in either the contact or the accept-contact-header are those described in the [RCS7.0] Section 2.6 “Capability and new user discovery mechanisms” in addition to any service or capability tags which have been registered against the relevant standardization or regulation bodies (for example OMA, GSMA).

Finally, and as a general principle, those capability tags associated to specific RCS services where, no interworking agreement exists between the service providers shall not be included on the NNI interface. For example, two Service Providers who support [IR.74] based Video Share, but do not have an interworking agreement covering that service. If that capability is then allowed to cross the NNI, the users get the impression that the service can be used between them even though that will likely not be possible. For the particular case of RCS IP Video Call, this may also result in the addition of the +g.gsma.rcs.ipvideocallonly tag defined in [RCS7.0] if based on the interworking agreements RCS IP Video Call is supported on the NNI, but RCS IP Voice Call is not.

4.1.2 Presence Based

The present section focuses on the interworking between two networks supporting the capability and new user discovery mechanism based on Presence as described in [RCS7.0] Section 2.6, “Capability and new user discovery mechanisms.” As a general principle the capability discovery based on presence interworking between two IMS networks (IMS NNI) shall follow [IR.65].

The presence based capability discovery mechanism should follow the same general presence service NNI considerations as defined in Section 5 of this document. To support capability exchange, XDM interworking is not required.

In addition to these guidelines, the Presence NNI shall comply to the rule that the only service descriptions allowed in the presence document are those described in [RCS7.0] Section 2.6 “Capability and new user discovery mechanisms”, and Table “Complete SIP OPTIONS tag and Presence Service ID usage for RCS” in addition to any service

description which has been registered against the relevant standardization or regulation bodies (for example OMA, GSMA).

Finally, and as a general principle, those service descriptions associated to specific RCS services where no interworking agreement exists between the Service Providers shall not be included in the NNI service descriptions. For example, two Service Providers who support [IR.74] based Video Share, but have no interworking agreement covering that service. If that capability is then allowed to cross the NNI, the users get the impression that the service can be used between them even though that will likely not be possible.

4.1.3 Interworking between Capability Discovery

Network Interworking for Capability Discovery is only required between Service Providers that do not support SIP OPTIONS exchange and those Service Providers that use SIP OPTIONS as the discovery mechanism or that have disabled Capability Discovery at the UNI.

In cases where such an Interworking Function (IWF) is necessary, the IWF architecture is negotiated and agreed between interconnecting operators. The architecture must ensure that all messages that require interworking treatment are routed to the appropriate IWF.

An IWF may be required to perform one or both of the following functions:

- Respond to SIP OPTIONS RCS capability exchange requests based on information obtained from a Presence Server ([RCS7.0] Figure “Capability interworking via network: Options request”).
- Respond to SIP SUBSCRIBE requests based on information obtained using SIP OPTIONS requests ([RCS7.0] Figure “Capability interworking via network: Presence request”).

A properly deployed and functioning IWF should have no impact at the NNI level.

Specifically:

The SIP OPTIONS exchange at the NNI must conform to the SIP OPTIONS based specifications as defined in the Section 4.1.1.

The Presence interface at the NNI must conform to the Presence specifications as defined in the Section 4.1.2.

4.1.3.1 Interworking: Incoming SIP OPTIONS

See [RCS7.0] Figure “Capability interworking via network: Options request“: When the IWF receives a SIP OPTIONS capabilities request that requires interworking, the IWF shall form and send an anonymous fetch SIP SUBSCRIBE addressed to the targeted presentity and send it to the network for routing to the appropriate Presence Server.

Since a SIP OPTIONS is targeted for one UE/presentity, the anonymous fetch SIP SUBSCRIBE is always a single/individual SIP SUBSCRIBE.

If the IWF receives a SIP NOTIFY in response to the SIP SUBSCRIBE, and the SIP NOTIFY contains a presence document, the IWF shall check the received presence doc for service

descriptions that correspond to RCS services as defined [RCS7.0] specification Table "Complete SIP OPTIONS tag and Presence Service ID usage for RCS". Default IWF policy means that all RCS service descriptions which are present and "OPEN" in the presence document will cause the IWF to form a response to the SIP OPTIONS with the corresponding Service Tag.

In the event the presence document does not define any open RCS services the IWF should respond to the SIP OPTIONS with a 480 Temporarily Unavailable response.

In the event the targeted User is not provisioned in the IMS network, the SIP SUBSCRIBE generated by the IWF should return a 404 Not Found response. In this case, the IWF should respond to the SIP OPTIONS with a 404 Not Found response.

In all other response cases, including timeout and error cases, the IWF should respond to the SIP OPTIONS request with the appropriate response selected from those defined in [RCS7.0] Section 2.6.1.1 "Capability discovery process through SIP OPTIONS message."

4.1.3.2 Interworking: Incoming SIP SUBSCRIBE

See [RCS7.0] Figure "Capability interworking via network: Presence request": When the IWF receives an individual SIP SUBSCRIBE the IWF shall treat the SIP SUBSCRIBE as anonymous fetch:

- Send a SIP OPTIONS request to the targeted entity. The service tags defined in the SIP OPTIONS request are a function of the policy defined at the IWF for the relevant domain. A SIP SUBSCRIBE request does not contain service capabilities information and thus does not provide the IWF with information to populate service tags in the SIP OPTIONS request. There must be at least one RCS service tag defined in the SIP OPTIONS query to prevent the receiving RCS user from assuming the originator is not an RCS capable subscriber. Two approaches can be used to populate the service tags in the SIP OPTIONS query:
    - Using static mapping rules: The SIP OPTIONS request is populated with one or more service tags based on a Service Provider policy defined at the IWF. For example, the capability discovery via presence service tag could be provided in all SIP OPTIONS requests.
    - Through discovery: The SIP OPTIONS request is populated with one or more service tags based on IWF service discovery. For example, subsequent to receiving a SIP SUBSCRIBE request, the IWF issues a SIP SUBSCRIBE request targeted to the originator of the initial SUBSCRIBE. The IWF uses the RCS service description information provided in the resulting NOTIFY to form the SIP OPTIONS request using the corresponding RCS Service Tags as defined in the [RCS7.0] Table "Complete SIP OPTIONS tag and Presence Service ID usage for RCS"
- Respond to the SIP SUBSCRIBE request. The response the IWF provides to the SIP SUBSCRIBE depends on the response received to the IWF generated SIP OPTIONS request.
    - If the IWF receives 200 OK response for a SIP OPTIONS request with RCS service tags, the IWF shall then respond to the original SUBSCRIBE

message with a 200 OK. The IWF will compose a presence document that will define a service description that corresponds to each RCS services service tag defined in the SIP OPTIONS response based on [RCS7.0] Table “Complete SIP OPTIONS tag and Presence Service ID usage for RCS”. The resulting presence document is sent to the SIP SUBSCRIBE originator in a NOTIFY message. Default IWF policy is that all RCS service tags present in the SIP OPTIONS response will cause the IWF to define a corresponding “OPEN” service description in the presence document.

- In the event there is a 200 OK response to the SIP OPTIONS request, but it contains no RCS service tags for which a mapping is defined, the IWF should respond to the SIP SUBSCRIBE request with a 480 Temporarily Unavailable response.
- In the event the targeted presentities not provisioned in the IMS network, the SIP OPTIONS request generated by the IWF should elicit a 404 Not Found response. In this case, the IWF should respond to the SIP SUBSCRIBE request with a 404 Not Found response.

For all other responses to IWF generated SIP OPTIONS requests, including timeout and error cases, the IWF should respond to the SIP SUBSCRIBE request with the most appropriate error response.

4.1.3.3 IWF Policy Considerations

Multiple aspects of IWF functionality will be impacted by or controlled by policies defined in each Service Provider network as well as policies defined at the IWF itself.

- IWF policies: It is possible for the Service Providers to jointly or singly define policies that are enforced at the IWF. Examples of such policies include:
  - Domain level policies: Policies to define unique service mapping and filtering polices based on domain or some other criteria. This includes service mapping details such as rules on handling or mapping open/closed services as well as consideration of additional service details that are defined in service descriptions.
  - Service level Policies: Policies to filter selected proprietary or other services from exposure across the IWF and thus the NNI across all domains and users.

4.2 Messaging & File Transfer

Standalone messaging, Chat/Group Chat and File Transfer may use one or more of the SIP header fields defined by OMA CPM, which need special handling over NNI.

NOTE: File Transfer using MSRP as defined in OMA CPM is used only for Geolocation Push during a Call.

The following Table 1 contains the list of SIP header fields that are endorsed by RCS from OMA CPM, and which shall be passed over IMS NNI unaltered, whenever they are present in a SIP request (for example SIP MESSAGE, or SIP INVITE).

Item	Header field	Ref. Specification	Usage	Description
1	Conversation-ID	RCS (endorsed from OMA CPM V2.1)	Mandatory	Identifies a conversation, which can include standalone message(s) and chat session(s).
2	Contribution-ID	RCS(endorsed from OMA CPM V2.1)	Mandatory	Identifies a specific messaging request, such as a standalone message, a chat session or a disposition notification.
3	InReplyTo-Contribution-ID	RCS(endorsed from OMA CPM V2.1)	Optional	Identifies a CPM request to which the current request replies to (for example standalone message(s), or chat session(s). Header field is mandatory in replies.
4	Session-Replaces	RCS (endorsed from OMA CPM V2.1)	Optional	It carries the value of the CPM Contribution-ID of the 1-to-1 session being replaced with the current group session. It is mandatory in SIP INVITE sent to the original participant in 1-1 session being extended.
5	Message-Expires	RCS (endorsed from OMA CPM V2.1)	Optional	It carries the expiry time associated with the Large Message Mode CPM Standalone Message set by the user for content validity.

Table 1: RCS specific SIP header fields

Any mapping applicable over NNI between these SIP header fields in the various inter-operability combinations between messaging realizations is detailed in the following sub-sections.

4.2.1 OMA CPM NNI

4.2.1.1 OMA CPM to OMA CPM NNI

OMA CPM (Converged IP Messaging) may be used for both Chat (see [RCS7.0] Sections 3.2.3 “1-to-1 Chat” and 3.2.4 “Group Chat”) and Standalone Messaging (see [RCS7.0] Section 3.2.2 “Standalone Messaging”).

The RCS feature set is reduced compared to the full set of features offered by the OMA CPM specifications. For example predefined groups are not supported in RCS. For further information see [RCS-CPM-CONVFUNC-ENDORS].

The CPM NNI follows [IR.65] and consists of MSRP requests and responses carried over the CPM-CF and CPM-PF2 interfaces (as defined in [CPM1.0-AD]) between Messaging Servers, and consists of IP-1 between IMS core systems (SIP) (IP-1 being the same interface as used by XDM & Presence, that is 3GPP Mw interface).

The Message Store related requests are local to the Service Provider’s network and therefore require no NNI support.

As per the OMA CPM specifications, the RCS NNI uses the model where both originating and terminating Service Providers are always using a Messaging Server, both for the signalling and media paths. That is CPM traffic uses server-to-server connection over NNI.

4.2.1.2 OMA CPM to Legacy

As described in Section 3.2.2.5 “Interworking with Legacy Messaging Services” of [RCS7.0], if a CPM Standalone Message is sent to a non-IMS user, the originating network will interwork the message to SMS or MMS depending on the message characteristics. If the destination user is in another network the originating network delivers the interworked message to that network using the applicable legacy messaging NNI. The same behaviour applies in case a CPM Standalone Message is sent to a user in a network with which there is no interworking agreement for CPM Standalone Messaging. In that case the SIP INVITE request might be rejected at the NNI with one of the following error responses:

- 488 Not Acceptable Here;
- 606 Not Acceptable.

In case the terminating user is an IMS user not supporting CPM Standalone Messaging and there is an interworking agreement for CPM based Standalone Messaging with the terminating network, the message can be interworked to SMS or MMS in the terminating network. In this case the NNI will be according to Section 4.2.1.

4.2.1.3 File Transfer via HTTP

The [RCS7.0] specification describes the transfer of files by:

- Uploading the file to a server in the originating network using a HTTPS POST procedure
- Sending the link to the file and, when applicable, the thumbnail correspondent to the file together with some additional data (validity and size) using a [RCS7.0]messaging service (standalone messaging, one to one chat or group chat) to the receiver. Note that the delivery notifications also rely on the delivery and display notifications associated to the messaging service used (standalone messaging, one to one chat or group chat).
- Once the receiver gets the information mentioned in the previous bullet, downloading the content using a HTTPS GET procedure.

From the NNI point of view:

The same considerations made for standalone messaging, one to one chat and group chat shall apply to the delivery of the information that enables the receiver to fetch the file and the delivery notifications. It shall be noted that all MSRP end-points shall support the new content type (application/vnd.gsma.rcs-ft-http+xml) defined in [RCS7.0] to carry the information associated to a FT via HTTP procedure (links and additional data).

The fetch procedure (HTTPS GET) is, by default, left out of the scope of the RCS NNI. To ensure that the files are accessible independently of the recipient’s coverage (3GPP and non-3GPP access), the FT via HTTP store and forward server in the originating network shall be reachable via the Internet. A Service Provider may consider adding additional manipulation on the messaging server and including a HTTP proxy to secure that:

- All the transactions associated to the file transfer via HTTP procedures go through a controlled infrastructure on the terminating Service Provider and, optionally,
- The download of the file/thumbnail data to happen through a dedicated link between the sender FT via HTTP store and forward server and the mentioned HTTP proxy on the terminating service provider based on a bilateral agreement between both originating and terminating service providers.

4.2.2 MSRP Chunk Size Handling

When MSRP is used as a media transport for RCS services, such as Standalone Messaging, Large Message Mode or Chat, MSRP messages can be sent in chunks.

The Max_MSRP_Chunk_Size shall be specified in the interworking agreement.

If the MSRP Chunk size is not negotiable at the protocol level, then to reduce the risk of MSRP message rejection or MSRP session disconnection by the MSRP receiver side, a global Max MSRP Chunk Size is set to 500 Kbytes. All Service Providers shall support the MSRP chunk size up to 500 Kbytes. That is, the sender shall send chunks no greater than 500 Kbytes and receiver shall be able to handle chunks up to at least 500 Kbytes.

If the OMA CPM MSRP chunk negotiation procedures are used (see [RCS-CPM-CONVFUNC-ENDORS]), the Max MSRP Chunk Size may be exceeded and the chunk size values shall be subject to the negotiation.

4.3 Content Sharing

4.3.1 Video Share

- The NNI architecture of Video Share, as well as NNI of the Video Share signalling and media shall follow Section 2 of this document.
- The NNI of Video Share service during voice call shall follow Section 3.3.1.1 “Video Share” and subsequent Sections of [RCS7.0]

4.3.2 Enriched Calling Session Service

The NNI architecture for the signalling and the MSRP media of the Enriched Calling Session Service shall follow Section 2 of this document. The Enriched Calling Session Service is defined in [RCC.20]. The data is carried within the session via MSRP, or via SIP MESSAGE request for disposition notifications.

The NNI architecture for pictures and audio messages exchanged by the sender uploading a file to a server and the recipient downloading it, is out of scope of the RCS NNI as described in Section 4.2.1 of this document.

4.4 IP Voice and Video Call

4.4.1 IP Voice Call

General technical guidelines on how IP voice call interworking between two IMS networks (IMS NNI) is handled for the RCS services is found in [IR.65].

Note: IP voice call communication between a device in one Service Provider's network and a device in another Service Provider's network shall not have any impact on the IMS NNI, independently of which access network is being used.

4.4.2 IP Video Call

General technical guidelines on how IP video call interworking between two IMS networks (IMS-NNI) is handled for the RCS services shall follow [IR.65]. The RCS IP call feature tags defined in [RCS7.0] shall be removed before the signalling is carried over NNI

Note: IP video call communication between device in one Service Provider's network and device in another Service Provider's network shall not have any impact on the IMS NNI, independently of which access network is being used.

4.5 Geolocation

4.5.1 Location Push

Location Push service is based on the CPM MSRP File Transfer service when used during a voice call and based on the RCS Chat service otherwise. See Section 3.2.6 "Geolocation Push services" in [RCS7.0] for Geolocation Push service description.

4.6 Services related to Messaging as a Platform (MaaP)

4.6.1 Chatbot Communication

Chatbot communication between subscribers and Chatbot Platforms is based on Capability Discovery service described in Section 4.1 and on the Messaging and File Transfer services described in Section 4.2, and thus uses the NNI as described for those services. The business relationship between a Chatbot Platform and a service provider that allows communication with Chatbots hosted by a Chatbot Platform is out of scope of this document.

4.6.2 Communication using Plug-ins

Chat communication between subscribers is based on Capability Discovery service described in Section 4.1 and on the Messaging and File Transfer services described in Section 4.2, and thus uses the NNI as described for those services.

5 Identification of Services

5.1 Overview

Identification of services is an important aspect of interworking. For example; possible intermediate IPX nodes (such as IPX Proxy), and also terminating networks as regards securing interworking agreements and potential termination fees, etc. While charging and the aspects agreement are out of scope for this document (and for NG in general), there's still the need to provide a technical description of this functionality which then could be utilized commercially.

According to [24.229], charging and accounting is expected to be based upon the contents of the P-Asserted-Service header and the actual media related contents of the SIP request and not the Accept-Contact header field contents or the contact reached.

Note: During a transition period towards RCS compliance [RCS7.0], not all RCS services make use of the standardized P-Asserted-Service value. When they do, the value is listed along with the rest of the information that may be used to identify a service. Furthermore, some RCS services share the same value for P-Asserted-Service.

Capability Query

- SIP

5.2

- OPTIONS containing in the Accept-Contact and Contact header fields at least one of the following feature tags and values that could possibly occur combined
  - +g.3gpp.iari-ref="urn%3Aurn-7%3A3gpp-application.ims.iari.rcse.im"
  - +g.3gpp.iari-ref="urn%3Aurn-7%3A3gpp-application.ims.iari.rcse.ft"
  - +g.3gpp.cs-voice
  - +g.3gpp.icsi-ref="urn%3Aurn-7%3A3gpp-service.ims.icsi.mmtel"; video
  - +g.3gpp.iari-ref="urn%3Aurn-7%3A3gpp-application.ims.iari.rcs.geopush"
  - +g.3gpp.icsi-ref="urn%3Aurn-7%3A3gpp-service.ims.icsi.gsma.rcs.extension"
  - +g.3gpp.icsi-ref="urn%3Aurn-7%3A3gpp-service.ims.icsi.gsma.callcomposer"
  - +g.3gpp.icsi-ref=”urn%3Aurn-7%3A3gpp-service.ims.icsi.gsma.callunanswered"
  - +g.3gpp.icsi-ref=”urn%3Aurn-7%3A3gpp-service.ims.icsi.gsma.sharedmap"
  - +g.3gpp.icsi-ref=”urn%3Aurn-7%3A3gpp-service. ims.icsi.gsma.sharedsketch"

- anonymous SUBSCRIBE/NOTIFY with event = "presence"

5.3

Standalone Messaging

- SIP:
  - MESSAGE (in case of Pager Mode CPM Standalone Messages)
    - P-Asserted-Service: urn:urn-7:3gpp-service.ims.icsi.oma.cpm.msg or urn:urn-7:3gpp-service.ims.icsi.oma.cpm.msg.group and
    - not carrying content of the type “message/imdn+xml”; or
  - INVITE (in case of Large Message Mode CPM Standalone Messages)
    - P-Asserted-Service: urn:urn-7:3gpp-service.ims.icsi.oma.cpm.largemsg or urn:urn-7:3gpp-service.ims.icsi.oma.cpm.largemsg.group

5.4

- MSRP in the session established using SIP INVITE

One-To-One Chat

- SIP
  - INVITE

- P-Asserted-Service: urn:urn-7:3gpp-service.ims.icsi.oma.cpm.session and
- username part of the URI in P-Asserted-Identity header field different from “rcse-standfw”

- MSRP in the session established using SIP INVITE

Group Chat

- SIP

5.5

- INVITE, SUBSCRIBE and REFER (in case of chat sessions)
  - P-Asserted-Service: urn:urn-7:3gpp-service.ims.icsi.oma.cpm.session.group

- MSRP in the session established using SIP INVITE

Disposition Notifications

5.6

- SIP
  - MESSAGE (used for Standalone Messaging notifications)
    - P-Asserted-Service: urn:urn-7:3gpp-service.ims.icsi.oma.cpm.msg or urn:urn-7:3gpp-service.ims.icsi.oma.cpm.msg.group or urn:urn-7:3gpp-service.ims.icsi.oma.cpm.largemsg or urn:urn-7:3gpp-service.ims.icsi.oma.cpm.largemsg.group and
    - carrying content of the type message/imdn+xml in a CPIM body; or
  - MESSAGE (used for Chat disposition notifications)
    - P-Asserted-Service: urn:urn-7:3gpp-service.ims.icsi.oma.cpm.session or urn:urn-7:3gpp-service.ims.icsi.oma.cpm.session.group and
    - carrying content of the type message/imdn+xml in a CPIM body; or
  - MESSAGE (used for Enriched Calling Service Session notifications with P-Asserted-Service header field)
    - P-Asserted-Service: urn:urn-7:3gpp-service.ims.icsi.gsma.callcomposer and
    - carrying content of the type message/imdn+xml in a CPIM body; or
  - INVITE (used for Chat disposition notifications)
    - P-Asserted-Service: urn:urn-7:3gpp-service.ims.icsi.oma.cpm.session and
    - with “rcse-standfw” as user part of the URI in the P-Asserted-Identity header field; or
- MSRP in the session established using SIP INVITE or, for Chat disposition notifications, MSRP within the session established for the Chat itself.

5.6.1 HTTP File Transfer

A Chat Message with *application/vnd.gsma.rcs-ft-http+xml* as the CPIM content-type property is sent in an MSRP session (identified as in sections 5.4 and 5.5).

Video Share

- SIP

5.7

- SIP INVITE (based on Video Share with P-Asserted-Service header field)
    - P-Asserted-Service: urn:urn-7:3gpp-service.ims.icsi.gsma.videoshare
- RTP in session established using SIP INVITE

Enriched Calling Session

5.8

- SIP INVITE
    - P-Asserted-Service: urn:urn-7:3gpp-service.ims.icsi.gsma.callcomposer, or
    - P-Asserted-Service: urn:urn-7:3gpp-service.ims.icsi.gsma.callunanswered, or
    - P-Asserted-Service: urn:urn-7:3gpp-service.ims.icsi.gsma.sharedmap, or
    - P-Asserted-Service: urn:urn-7:3gpp-service.ims.icsi.gsma.sharedsketch
- MSRP in session established using SIP INVITE

5.9

IP Voice Call

- SIP INVITE
    - P-Asserted-Service: urn:urn-7:3gpp-service.ims.icsi.mmtel
    - Accept-Contact and Contact header fields containing the feature tag +g.3gpp.icsi-ref="urn%3Aurn-7%3A3gpp-service.ims.icsi.mmtel” and
    - only audio media in SDP in 200 OK response
- RTP in session established using SIP INVITE

5.10

IP Video Call

- SIP INVITE
    - P-Asserted-Service: urn:urn-7:3gpp-service.ims.icsi.mmtel
    - Accept-Contact and Contact header fields containing the feature tag +g.3gpp.icsi-ref="urn%3Aurn-7%3A3gpp-service.ims.icsi.mmtel”
    - Accept-Contact and Contact header fields containing the “video” capability indication and
    - audio and video media in SDP in 200 OK response

NOTE: If the call may not be converted into an IP Voice Call, the Accept-Contact and Contact header fields will carry also the +g.gsma.rcs.ipvideocallonly feature tag;

- Separate RTP streams for audio and video in session established using SIP INVITE

Geo-location PUSH

- SIP INVITE (for transfer during a voice call)

5.11

- Accept-Contact and Contact header fields containing the feature tag +g.3gpp.iari-ref="urn%3Aurn-7%3A3gpp-application.ims.iari.rcs.geopush"
- MSRP in the session established using SIP INVITE and
- Request URI is set to a user's address (i.e. not to a Group Chat session identity) and
- Without "isfocus" parameter in the Contact Header field.
- A Chat Message with *application/vnd.gsma.rcspushlocation+xml* as the CPIM content-type property. This Chat Message is sent in an MSRP session (identified as in Sections 5.5 and 5.6).

Message Revoke Requests and Responses

5.12

- SIP
  - MESSAGE
    - P-Asserted-Service: urn:urn-7:3gpp-service.ims.icsi.oma.cpm.session
    - Accept-Contact header field containing feature tag +g.3gpp.icsi-ref="urn%3Aurn-7%3A3gpp-service.ims.icsi.oma.cpm.session" and
    - Accept-Contact header field containing feature tag +g.gsma.rcs.msgrevoke; or

5.13 Traffic related to Messaging as a Platform (MaaP)

5.13.1 Chatbot sessions

- SIP
  - INVITE
    - Accept-Contact header field containing feature tag +g.3gpp.iari-ref="urn%3Aurn-7%3A3gpp-application.ims.iari.rcs.chatbot".

5.13.2 Chat Message traffic differentiation for MaaP Communication

Chat Messages related to plugins or Chat Messages carrying advertisements or other chatbot specific traffic is differentiated from regular Chat Messages exchanged with a chatbot as follows as per section 3.6.7.2 in [RCS7.0]:

- MSRP
  - A Chat Message that is not one of the traffic types to be identified does not have the CPIM header <any namespace>.Traffic-Type; or
  - A Chat Message related to a plugin has the CPIM header <any namespace>.Traffic-Type set to value "plugin"; or
  - A Chat Message related to an advertisement has the CPIM header <any namespace>.Traffic-Type set to value "advertisement"; or

- A Chat Message related to a payment has the CPIM header <any namespace>.Traffic-Type set to value"payment"; or
- A Chat Message related to premium content has the CPIM header <any namespace>.Traffic-Type set to value "premium"; or
- A Chat Message related to a subscription has the CPIM header <any namespace>.Traffic-Type set to value "subscription".

DNS & ENUM

For Domain Name System (DNS) usage in RCS interworking, see general IMS related guidelines in [IR.67] Section 4.5 “IP Multimedia core network Subsystem (IMS)”. ENUM guidelines as illustrated in [NG.105] are applicable also for the purpose of RCS, including the Mobile Number Portability (MNP) issues described in Annex C “Solving Number Portability in ENUM”.

6

Annex A Configuration Parameters with NNI Impact

NNI parameter	UNI parameter	Recommended NNI handling
Capability Discovery		
Preferred Capability Discovery Mechanism	CAPABILITY DISCOVERY MECHANISM	Indicates the preferred capability discovery mechanism to be used on the NNI.
Messaging & File Transfer		
Chat enabled	CHAT AUTH	This should be covered in the interworking agreements. If a Service Provider disables Chat service for all users, then the Chat service traffic should not be allowed to cross the NNI based on the service identification (see Section 5).
Group Chat enabled	GROUP CHAT AUTH	This should be covered in the interworking agreements. If a Service Provider disables Group Chat service for all users, then the Group Chat service traffic should not be allowed to cross the NNI based on the service identification (see Section 5).
Standalone message enabled	STANDALONE MGS AUTH	This should be covered in the interworking agreements. If a Service Provider disables Standalone Message service for all users, the Standalone Message service should not be allowed to cross the NNI based on the service identification (see Section 5).
Max size of message [bytes]	MAX SIZE IM	As described in [RCS7.0] and Section 4.1, this parameter is part of the capability exchange and any differences between interconnected Service Providers will therefore be honoured at the protocol level.
Max size of large message [bytes]	MAX SIZE STANDALONE	As described in [RCS7.0] and Sections 4.1, this parameter is part of the capability exchange and any differences between interconnected Service Providers will therefore be honoured at the protocol level.
Max number of participants in group chat session	MAX_AD-HOC_GROUP_SIZE	Any differences in the value between interconnected Service Providers will be honoured at the protocol level since the final decision is with the Controlling Messaging Server. Such differences might lead to inconsistencies in the user experience and possible failed attempts though. It is therefore recommended that Service Providers with lots of NNI traffic between themselves (e.g., those within the same country) use similar values.

1-to-1 IM session inactivity timer [seconds]	IM SESSION TIMER	This parameter indicates how long a Service Provider will keep a 1-to-1 Chat session in which there is no traffic active. As the tearing down of the session can be initiated independently from either side, any differences between interconnected Service Providers will be honoured at the protocol level. Since differences will lead to inconsistencies in the user experience, it is recommended that Service Providers with a lot of NNI traffic between themselves (for example, those within the same country) use similar values.
Group IM session inactivity timer [seconds]	Not available	This parameter indicates how long a Service Provider will keep a hosted Group Chat session in which there is no traffic active. As the tearing down of the session is always initiated from the Controlling Function, any differences between interconnected Service Providers will therefore be honoured at the protocol level. Since differences will lead to inconsistencies in the user experience, it is recommended that Service Providers with lots of NNI traffic between themselves (e.g. those within the same country) use similar values.
One-to-One Chat maximum Session duration [seconds]	Not available	An operator may limit the maximum duration of a 1-to-1 Chat sessions. If that is the case, this would affect the user experience of users in interconnected networks that support the Chat service and expected traffic patterns on the NNI.
One-to-One Chat maximum number of messages	Not available	An operator may limit the maximum number of messages exchanged in a 1-to-1 Chat session. If that is the case, this would affect the user experience of users in interconnected networks that support the Chat service and expected traffic patterns on the NNI.
Group Chat maximum Session duration [seconds]	Not available	An operator may limit the maximum duration of a Group Chat session. If that is the case, this would affect the user experience of users in interconnected networks that support the Chat service and expected traffic patterns on the NNI.
Group Chat maximum number of messages	Not available	An operator may limit the maximum number of messages exchanged in a Group Chat session. If that is the case, this would affect the user experience of users in interconnected networks that support the Chat service and expected traffic patterns on the NNI.
FT maximum file size [Kbytes]	FT MAX SIZE	As described in [RCS7.0] and Section 4.1, this parameter is part of the capability exchange and any differences between interconnected Service Providers will therefore be honoured at the protocol level. Since differences will lead to inconsistencies in the user experience and possible failed attempts, it is recommended that Service Providers with lot of NNI traffic between themselves (e.g., those within the same country) use similar values.

Auto-accept of group chat	IM SESSION AUTO ACCEPT GROUP CHAT	Any differences in the value between interconnected Service Providers will be honoured at the protocol level since a final decision is with the invited clients. Such differences might lead to inconsistencies in the user experience though. It is therefore recommended that Service Providers with lot of NNI traffic between themselves (e.g., those within the same country) use similar values.
Interworking with SMS/MMS	IM CAP NON RCS	If this functionality is enabled, a user is able to invite non-RCS contacts to a chat session requiring the behaviour described in Section 4.3. Therefore the interworking agreements should cover this parameter
Message Revocation Supported	CHAT REVOKE TIMER	This parameter indicates if the revocation of messages is supported. Revocation requests may be initiated by the originating Messaging Server or the originating client (if configured). If revocation is not supported by the terminating network revocation requests should not be sent across the NNI.
File Transfer HTTP retention period	Not Available	Indicates for how long a file that was sent using File Transfer via HTTP will be indicated as available for download in the File Transfer via HTTP XML bodies that are sent by the Service Provider over the NNI. Any differences in the value between interconnected Service Providers will be honoured at the protocol level since a final decision is with the invited clients. Such differences might lead to inconsistencies in the user experience though. It is therefore recommended that Service Providers with lots of NNI traffic between themselves (for example, those within the same country) use similar values.
Auto Accept of File Transfer	FT AUT ACCEPT	Any differences in the value between interconnected Service Providers will be honoured at the protocol level since a final decision is with the invited clients. Such differences might lead to inconsistencies in the user experience though. It is therefore recommended that Service Providers with lot of NNI traffic between themselves (for example, those within the same country) use similar values.
Max MSRP chunk size	Not available	The maximum MSRP chunk size supported for MSRP media transport. This will not only avoid the potential MSRP message rejection across networks but also affect the dimensioning of an NNI. The upper limit for this parameter is 500KB. To minimize the rechunking over NNI, the Service Providers with a lot of NNI traffic may consider using the same value.
Content Sharing		
VS maximum duration [seconds]	VS MAX DURATION	Maximum connection time of a Video Share in seconds. After expiration of this time limit, the receiving Service Provider can force to disconnect the session.

VS Bandwidth	Not Available	The maximum bandwidth allowed for a video share session in the operator's network. This will affect the dimensioning of an NNI.
Geolocation		
Max length of geo-location text	GEOLOCATION TEXT MAX LENGTH	This parameter influences the size of the file transfer that crosses NNI (both for PUSH and PULL based on File Transfer) and should be negotiated between the interconnect Service Providers.

Table 2: Configuration Parameters with NNI Impact per RCS Service

Annex B Interworking Form

The Interworking Form for IMS based services, especially for RCS:


RCS IW Form.xlsx

Annex C Document Management

C.1 Document History

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
0.1	12/02/09	Very first early draft	RCS Programme	Tero Jalkanen / TeliaSonera
0.2	20/02/09	Minor update	RCS Programme	Tero Jalkanen / TeliaSonera
0.3	17/03/09	Major update	RCS Programme	Tero Jalkanen / TeliaSonera
0.4	31/03/09	Version for Kista workshop	RCS Programme	Tero Jalkanen / TeliaSonera
0.5	15/04/09	Update based on Kista workshop feedback	RCS Programme	Tero Jalkanen / TeliaSonera
0.6	04/06/09	Major update for RCS Berg meeting	RCS Programme	Tero Jalkanen / TeliaSonera
0.7	19/06/09	Update based on RCS#5 discussions	RCS Programme	Tero Jalkanen / TeliaSonera
0.8	01/07/09	Update based on PWP#40 discussions	RCS Programme	Tero Jalkanen / TeliaSonera
0.9	20/07/09	Updated based on email approval comments	RCS Programme	Tero Jalkanen / TeliaSonera
0.91	19/08/09	Final version for DAG	RCS Programme	Tero Jalkanen / TeliaSonera
1.0	01/10/09	Final approved version for public distribution	RCS Programme	Tero Jalkanen / TeliaSonera
2.0	21/07/10	Incorporated Major CR 001 (IR.65 related updates)	RCS Programme	Tero Jalkanen / TeliaSonera
2.1	21/10/10	Incorporated Minor CR 002 (RCS R3 related updates)	RCS Programme	Tero Jalkanen / TeliaSonera
3.0	30/07/12	Incorporated Major CR 003 (RCS 5.0 related update)	RCS Programme	Tero Jalkanen / TeliaSonera
4.0	15/02/13	Incorporated Major CR 1001 (RCS 5.1 related update)	RCS Programme	Tero Jalkanen / TeliaSonera
5.0	25/04/13	Incorporated Major CR 1002 (Interworking form for RCS 5.1)	RCS Programme	Tero Jalkanen / TeliaSonera
6.0	06/08/13	Incorporated Major CR 1003 (RCS 5.1 v2.0 Update)	RCS Programme	Tero Jalkanen / TeliaSonera
7.0	23/10/13	Incorporated Major CR 1004 (Maintenance Update for RCS 5.1 v3.0)	RCS Programme	Tero Jalkanen / TeliaSonera
8.0	12/02/14	Incorporated Major CR 1005 (Maintenance Update for RCS 5.1 v4.0)	RCS Programme	Tero Jalkanen / TeliaSonera

9.0	14/07/14	Incorporated Major CR 1006 (Alignment with RCS 5.2)	RCS Programme	Tero Jalkanen / TeliaSonera
10.0	25/09/2014	Incorporated Major CR1007 (Updates for Service Identification)	IREG	Tero Jalkanen / TeliaSonera
11.0	28/02/2015	Incorporated Major CR1008 (Alignment with RCS 5.3)	NG	Tero Jalkanen / TeliaSonera
12.0	01/04/2015	Incorporated Major CR1009 (Further alignment with RCC.07)	NG	Tero Jalkanen / TeliaSonera
13.0	06/05/2016	Incorporated Major CR1010 (Alignment with RCS 6.0)	NG	Tero Jalkanen / Telia Company
14.0	13/10/2017	Incorporated Minor CR 1011 (ENUM Reference Correction) & Major CR 1012 (Universal Profile 2.0 Update)	NG	Tero Jalkanen / Telia Company

Other Information

Type	Description
Document Owner	NG
Editor / Company	Tero Jalkanen / Telia Company

It is our intention to provide a quality product for your use. If you find any errors or omissions, please contact us with your comments. You may notify us at prd@gsma.com

Your comments or suggestions & questions are always welcome.