Rich Communication Suite

Release 2

Management Objects

1.1

February 25, 2010

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

Security Classification – NON-CONFIDENTIAL GSMA Material		

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 Scope

The service definition of Rich Communication Suite (RCS) does not require end users to manually configure any settings in order to use RCS services. This document defines which parameters are to be configured by a Device Management (DM) server, or initialized using any mechanisms indicated in [DMBOOT] onto an RCS2 terminal as well as how they are configured.

The scope of this document is RCS Release 2.

1.2 References

[FUNCDESC]	RCS Release 2 Functional Description
[TECHREAL]	RCS Release 2 Technical Realization
[IMENDORSE]	RCS Release 2 Endorsement of OMA SIP/SIMPLE IM 1.0
[24.173ENDORSE]	RCS Endorsement of 3GPP TS 24.173 MMTel
[26.114ENDORSE]	RCS Endorsement of 3GPP TS 26.114 MMTel Media Handling
[SIMPLEIM]	Instant Messaging using SIMPLE, 1.0, http://www.openmobilealliance.org/
[OMADSDM]	OMA-TS-DS_MO-V1_0-20090212-C http://www.openmobilealliance.org
[PRESENCE]	Presence SIMPLE Specification, 1.1, http://www.openmobilealliance.org
[PRESENCEIG]	Implementation Guidelines for OMA Presence SIMPLE v1.1 Presence, http://www.openmobilealliance.org
[PRESENCEMO]	OMA Management Object for Presence SIMPLE 1.1, http://www.openmobilealliance.org
[XDM1.1_Core]	XML Document Management (XDM) Specification 1.1, XML Document Management (XDM) Specification
[XDMIG]	Implementation Guidelines for OMA XDM v1.1 Presence, http://www.openmobilealliance.org
[XDMMO]	OMA Management Object for XML Document Management 1.1, http://www.openmobilealliance.org
[OMADDF]	OMA Device Management. Device Description Framework 1.2 http://www.openmobilealliance.org
[DMBOOT]	OMA Device Management Bootstrap V1.2 http://www.openmobilealliance.org
[33.978]	3GPP TS 33.978 Security aspects of early IP Multimedia Subsystem (IMS), http://www.3gpp.org
[24.167]	3GPP TS 24.167 IMS 3GPP IMS Management Object (MO), http://www.3gpp.org
[24.229]	3GPP TS 24.229 IMS Call Control based on SIP and SDP, http://www.3gpp.org

2 MANAGEMENT OBJECT PARAMETERS

2.1 General

Unless otherwise specified (that is, unless a RCS client configuration parameter is explicitly mentioned as subject of possible user modification), the RCS related parameters described in this document are locked from end-user modification. They may be set at initial start-up of the RCS client or modified (while the client is running) via network OMA procedures initiated by the Device Management Server of the RCS operator

This section describes the parameters needed to configure an RCS client for the initiation of RCS service and for a continuous provisioning by RCS service provider.

- When suitable Managed Objects (MO) exist in related SDO documentation (OMA documentation or 3GPP documentation), RCS client configuration parameters correspond to the endorsement of such MO, for example, Device Management Object in [XDMMO], [PRESENCEMO], [24.167] and [IMENDORSE] respectively.
- When RCS specific parameters are required (no suitable parameter has been defined by OMA) such parameters are described in a dedicated section of this document and defined as extensions of the relevant OMA MO

In the following sections,
- "M" stands for "Support Mandatory in an RCS terminal"
- "N.A." stands for "Not Applicable for RCS"

2.2 Presence related configuration

2.2.1 RCS endorsement of OMA Presence Client provisioning parameters

OMA Presence Client provisioning parameters are defined in [PRESENCEMO]. Table 1lists the OMA Presence parameters applicable to RCS.

Parameter Name	Description	Support in RCS
CLIENT-OBJ-DATA-LIMIT	maximum size of the MIME object in SIP PUBLISH request	M
CONTENT-SERVER-URI	HTTP URI of the content server to be used for content indirection	N. A.
SOURCE-THROTTLE-PUBLISH	minimum time interval (in seconds) between two consecutive publications	M
MAX-NUMBER-OF-SUBSCRIPTIONS-IN-PRESENCE-LIST	Limits the number of back-end subscriptions allowed for a presence list. This parameter applies to the "rcs" list (as described in section 4.4.2 in [TECHREAL])	M
SERVICE-URI-TEMPLATE	syntax of the service URI	M, with value "<xui>;pres-list=<id>" according to section 5.5.1

		in [PRESENCEIG

Table 1 RCS Endorsed OMA Presence Parameters

2.2.2 Specific RCS Client provisioning parameters linked with Presence

Following RCS specific parameters shall be possible to configure on the UE

- Parameters associated with the Hyper-Availability attribute (as described in section 2.1.3.1 in [FUNCDESC] and section 4.2.2 in [TECHREAL])
  - "HyperAvailability Period" (as described in section 2.1.3.1 in [FUNCDESC] and section 4.2.2 in [TECHREAL])
- Parameters associated with the Favorite Link attribute (as described in section 2.1.3.2 in [FUNCDESC])
  - Automatic / manual mode for the favorite link.
    - In the case automatic mode is activated, there is additional parameter "list of pre-defined Favorite link URIs" to be configured

  Favourite link attribute parameter SHALL NOT BE LOCKED
- Parameters associated with the Presence (Portrait) Icon attribute (as described in section 4.8.1 in [TECHREAL])
  - Icon maximum size in bytes (maximum 200Kb)
- Parameters associated with the Note attribute (as described in section 4.2.2 in [TECHREAL])
  - Maximal length of presence tagline at Presentity side. The reason to have at Presentity side a configurable attribute on the RCS client to control the maximum size of the Note is to make the end user aware of what the limit is (when typing the content of the Note/free text) and thus to avoid that enforcement of this limit at Network / watcher side would lead to truncating the note. This value should have a lower value than the one defined at watcher side in the OMA Presence Implementation guideline [PRESENCEIG].
- Parameters associated with the Operator restriction on the publication and display of service capabilities (as described in section 2.1.7 in [FUNCDESC] and section 4.9 in [TECHREAL])
  - Control on the retrieval of service capabilities via an anonymous presence fetch: When the retrieval is set to "Not Allowed", the RCS rule for anonymous fetch of Presence Information is set by the UE to provide an empty document (at least telling the fetching terminal that the contact address supports Presence). Thus, in this case, only "buddies" of a user can get the "capabilities" information (together with the Presence Social Information) on this user.
  - Use of the anonymous fetch operation by the device ("Allowed" or "Not Allowed").
  - Display of the ability of user's contacts to share Social Presence Information ("Allowed" or "Not Allowed").
  - Default expiry time of PUBLISH (as described in section 4.6 and 4.7 in [TECHREAL])

2.3 XDM related configuration

2.3.1 RCS endorsement of OMA XDM Client provisioning parameters

OMA XDM Client provisioning parameters are defined in [XDMMO]. Table 2 lists the OMA XDM parameters applicable to RCS.

Parameter Name	Description	RCS usage
XCAP Root URI	The root of all XCAP resources (which points to the Aggregation Proxy address). This is used when accessing via XCAP.	M
XCAP Authentication user name	HTTP digest “username”, for accessing an XDMS using the XCAP protocol	O(3)
XCAP Authentication Secret	HTTP digest password	O(3)
XCAP Authentication type	Authentication method for XDMS over XCAP. Possible values: Early IMS (1), (2) or Digest	M

Table 2 RCS Endorsed OMA XDM Parameters

Notes:

1. The Early IMS value is a specific RCS value that is not defined in OMA
2. Support of Early IMS authentication for XCAP according to of section 6.3 of [33.978] and sections 6.3 and 6.4 in [XDM1.1_Core], by in the HTTP GET request to the Aggregation Proxy supplying the "X-3GPP-Intended-Identity" header to indicate the user identity.
3. In case of Early IMS, the XCAP Authentication user name and password is not needed.

2.3.2 Specific RCS Client provisioning parameters linked with XDM

Following RCS specific parameters shall be possible to configure on the UE

- Parameters associated with the “rcs_revokedcontacts” list (as described in section 2.1.4.6 in [FUNCDESC] and section 4.4.4 in [TECHREAL])
    - Duration that a contact should remain in this list

2.4 IM related configuration

2.4.1 RCS endorsement of OMA IM Client provisioning parameters

Note: OMA IM Client provisioning parameters are defined in [SIMPLEIM]. This Table 3 only lists which of those IM application parameters are applicable.

Parameter Name	Description	RCS usage
PRES-SRV-CAP	flag used for the IM Server to indicate the Presence publish capability of a Presence information element of the IM Server on behalf of the IM Client	N.A. Set to the OMA value indicating that the capability is not supported in the network
MAX_AD-	Maximum number of	M

HOC_GROUP_SIZE	Participants allowed for an Ad-hoc IM Group Session	
CONF-FCTY-URI	SIP URI used for setting up an Ad-hoc IM Group or 1-1 IM Session	M [(1), (2)]
EXPLODER-URI	SIP URI used for sending SIP MESSAGE, for example, Sending SIP MESSAGE to an Ad hoc Group	N.A.[(1)]
CONV-HIST-FUNC-URI	SIP URI for IM user's conversation history storage	N.A.[(1)]
DEFERRED-MSG-FUNC-URI / MSG-STORE-URI	SIP-URI used for IM User's message-store account for deferred messaging	N.A.[(1)]
DELETE-URI	SIP URI used when message(s) are to be deleted	N.A.[(1)]

Table 3 RCS Endorsed OMA IM Parameters

Notes:

1. For RCS these are populated with the sip URI= "sip:foo@bar" which is assumed to be a dummy value
2. Presence of a dummy URI ("sip:foo@bar") in the CONF-FCTY-URI parameter implies that the RCS Group Chat service is to be disabled in the client.

2.4.2 Specific RCS Client provisioning parameters linked with IM

Following RCS specific parameters shall be possible to configure on the UE

- Parameters associated with the Chat service (as described in section 2.4.2 in [FUNCDESC] and section 8.2 in [TECHREAL])
  - Enable/Disable the Chat service
  - Enabling sending of message via legacy messaging when chat invite fails
  - Automatic or manual accept of a incoming 1-to-1 IM session request (default value = auto-accept,)
  - Maximum size of the content sent within a 1-to-1 chat session
  - Maximum size of the content sent in a group chat session
  - Timer for termination of inactive (idle) chat session (recommended value 30 minutes, no timeout shall also be possible)

2.5 File transfer related configuration

2.5.1 Specific RCS Client provisioning parameters linked with File transfer

Following RCS specific parameters shall be possible to configure on the UE

- Parameters associated with the File transfer service (as described in section 2.3 in [FUNCDESC] and section 7 in [TECHREAL])
  - Maximum file size allowed for a File Transfer

2.6 IMS Core /SIP related configuration

2.6.1 General

Settings for SIP and IMS Core related parameters.

2.6.2 RCS endorsement of 3GPP IMS Management Object (MO)

Basic IMS/SIP Client parameters are defined in 3GPP TS “IMS 3GPP IMS Management Object (MO)” [24.167]. They do not direct depend on RCS, but correct settings of these parameters are essential for RCS operation. They are populated by the operator according to the deployment conditions of the IMS Core network providing access to RCS services.

2.6.3 Specific RCS Client provisioning parameters linked with SIP/IMS

This section lists additional SIP and IMS Core level parameters that are applicable for an RCS client.

Parameter Name	Description	RCS usage
IMS Mode Authentication Type	Specifies the type of authentication support for SIP. Note: In “IETF” Digest authentication is assumed. Accepted values are: • Early IMS • IMS AKA • SIP DIGEST (without TLS)	M
Realm	Realm to use for authentication (Digest mode only)	O M if Digest mode used
Realm User Name	Realm username to use for authentication (Digest mode only)	O M if Digest mode used
Realm User Password	Realm user password to use for authentication (Digest mode only)	O M if Digest mode used
TEL or SIP URI – international	Specifies whether telephone numbers in international format shall in outgoing SIP requests be sent as TEL URIs [RFC3966] or as SIP URIs with “user”-parameter set to “phone” [RFC3261] Reference: [TECHREAL] section 3.1.3	M
TEL or SIP URI - for non international format	Specifies whether telephone numbers in non international format shall in outgoing SIP requests be sent as TEL URIs [RFC3966] or as SIP URIs with “user”-parameter set to “phone” [RFC3261] Reference: [TECHREAL] section 3.1.3	M
Register Q-value	Q-value in Contact	M

	parameter in SIP Register Required in a multi-terminal deployment to control forking of incoming SIP requests	Recommended value: 0.5

Table 4 RCS recommendation for SIP/IMS Parameters

2.7 Configuration related with Address book Back-up/Restore

2.7.1 General

For the proper operation of the Address Book back-up/restore feature, the parameters described in [OMADSDM] need to be supported by a RCS terminal.

2.7.2 RCS endorsement of OMA DS Management Object

Editor's Note: FFS

2.8 Configuration related with broadband secondary device introduction (RCS2)

2.8.1 General

With the Introduction of the broadband secondary device in RCS2, there are 2 new features in a broadband RCS2 device:

- Control of service delivery
- MMTEL client

Control of service delivery: in a Broadband RCS2 device, as specified in [TECHREAL], this User control facility is itself controlled by the operator that may defined the set of services subject to this function
Specific RCS parameters must be define to ensure this control

MMTEL client: For RCS 2, there are no explicit requirements for parameters that should be controlled by the operator. Nevertheless, if some vendors/operators want to introduce such control, it is advise to take account the MTIS (Media Telephony Service for IMS) parameters defined in [26.114] chapter 15

2.8.2 Specific RCS Configuration parameters for Control of service delivery

- Voice Calls: Network authorization for user controlling delivery
- Chat Network authorization for user controlling delivery
- Sending SMS Network authorization for user controlling delivery
- File Transfer Network authorization for user controlling delivery
- Video Sharing Network authorization for user controlling delivery
- Image Sharing Network authorization for user controlling delivery

2.8.3 RCS endorsement of MTIS parameters (optional)

Following parameters, under the "speech" node can be endorsed

Parameter Name	Description	RCS usage
Priority	Priority of the codec	O
Codec type	Only "AMR" and "AMR-WB" are defined in MTIS, it could be extended to support	O

	additional codec	
Bandwidth	The bandwidth (in Kbit/s) that must be negotiated by the device in SDP answer/response paradigm when using the codec	O
Mode Set	Used if the operator wants to limit the number of AMR or AMR-WB mode to be used by the device	O

3 TECHNICAL SUPPORT FOR THE CONFIGURATION OF DATA ON A RCS TERMINAL

3.1 General

OMA DM v1.2 is used to configure the objects listed in this document.

3.2 Parameters specific to RCS

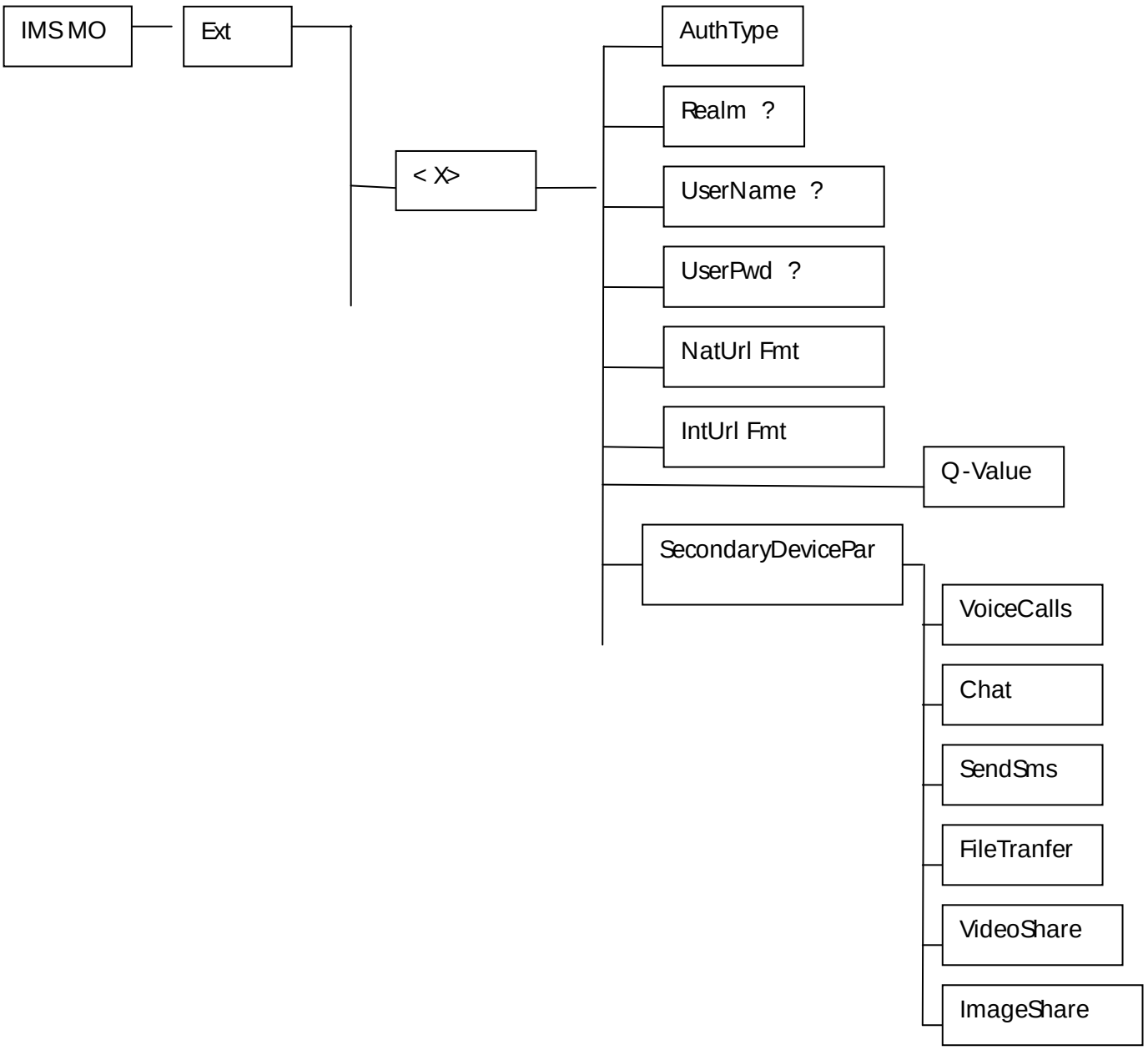
For parameters specific to RCS (for which there exist no OMA DM object), the extension capability of existing OMA DM objects is used as follows:

- Specific RCS Client provisioning parameters linked with Presence and defined in section 2.2.2 correspond to extension (EXT) of [PRESENCEMO].
- Specific RCS Client provisioning parameters linked with XDM and defined in section 2.3.2 correspond to extension (EXT) of [XDMMO].
- Specific RCS Client provisioning parameters linked with IM and with File transfer and defined in section 2.4.2and section 2.5.1 correspond to extension (EXT) of [SIMPLEIM].
- Specific RCS Client provisioning parameters linked with IMS Core / sip and defined in section 2.6.3 correspond to extension (EXT) of the 3GPP IMS MO [24.167].

Editor's Note: Those extensions correspond to the "RCS" vendor name.

4. RCS MANAGEMENT SUB TREES

4.1 IMS MO sub tree



Node: /<X>

Under this interior node are placed the RCS parameters related to the IMS UA enabler

Status	Occurrence	Format	Min. Access Types
Required	One	node	Get

- Values: N/A

Type property of the Node is: urn:gsma:mo:rcs:2.0:IMS-ext

Node: /<X>/AuthType

Leaf node that describe the type of IMS authentication for the user

Status	Occurrence	Format	Min. Access Types
Required	One	chr	Get

- Values: ‘EarlyIMS’, ‘AKA’, ‘Digest’

Node: /<X>/Realm

In case the IMS mode for authentication is ‘digest’, this leaf node exists and contains the realm URL affected to the user

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	chr	Get

- Values: <Realm URL>

Example: ‘authenticatorY.operatorX.com’

Node: /<X>/UserName

In case the IMS mode for authentication is ‘Digest’, this leaf node exists and contains the realm User name affected to the user for IMS authorization/registration

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	chr	Get

- Values: <use name affected to user for IMS authentication/registration purpose>

Example: ‘Alice’

Node: /<X>/UserPwd

In case the IMS mode for authentication is ‘Digest’, this leaf node exists and contains the User name affected to the user for IMS authorization/registration

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	chr	Get

- Values: <password affected to user for IMS authentication/registration purpose>

Example: ‘secretxyz’

Node: /<X>/NatUrlFmt

This leaf node indicates which format (SIP URL or Tel URL) is to be used in case the callee numbering is dialled in national format

Status	Occurrence	Format	Min. Access Types
Required	One	chr	Get

- Values: 0, 1

0: Tel URL format is to be used (example: 0234578901; phone-context=<home-domain-name>)
1: SIP URL format is to be used (example: 0234578901@operator.com; user=phone)

/<X>/IntUrlFmt

This leaf node indicates which format (SIP URL or Tel URL) is to be used in case the callee numbering is dialled in international format

Status	Occurrence	Format	Min. Access Types
Required	One	chr	Get

- Values: 0, 1

0: Tel URL format is to be used (example: +1234578901)
1: SIP URL format is to be used (example: +1234578901@operator.com; user=phone)

/<X>/QValue

This leaf node indicates the Q-value to be put in the Contact header of the Register method. This is useful in case of multi-device for forking algorithm.

Status	Occurrence	Format	Min. Access Types
Required	One	chr	Get

- Values: ‘0.1’, ‘0.2’, ‘0.3’, ‘0.4’, ‘0.5’, ‘0.6’, ‘0.7’, ‘0.8’, ‘0.9’, ‘1.0’

/<X>/SecondaryDevicePar

Presence of this interior node indicates that the RCS2 device is a secondary device. This node is not instantiated in case of primary device
Under this node are instantiated the parameters necessary to control the ability for the user to restrict RCS services on the secondary device. Notion of primary and secondary device is defined in [TECHREAL]

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	node	Get

/<X>/SecondaryDevicePar/VoiceCalls

This leaf node is instantiated in case the device is a RCS2 secondary device. It allows the operator to authorize or not the device user to control the voice call delivery on this secondary device. Notion of primary and secondary device are defined in [TECHREAL].

Status	Occurrence	Format	Min. Access Types
Required	One	chr	Get

- Values: 0, 1
  0- Indicates authorization
  1- Indicates non authorization

/<X>/SecondaryDevicePar/Chat

This leaf node is instantiated in case the device is a RCS2 secondary device. It allows the operator to authorize or not the device user to control the voice call delivery on this secondary device. Notion of primary and secondary device is defined in [TECHREAL].

Status	Occurrence	Format	Min. Access Types
Required	One	chr	Get

- Values: 0, 1
  0- Indicates authorization
  1- Indicates non authorization

/<X>/SecondaryDevicePar/SendSms

This leaf node is instantiated in case the device is a RCS2 secondary device. It allows the operator to authorize or not the device user to enable/disable the restricted SMS service (only possibility to send an SMS on a secondary device) on this secondary device. Notion of primary and secondary device is defined in [TECHREAL].

Status	Occurrence	Format	Min. Access Types
Required	One	chr	Get

- Values: 0, 1
  0- Indicates authorization
  1- Indicates non authorization

/<X>/SecondaryDevicePar/FileTransfer

This leaf node is instantiated in case the device is a RCS2 secondary device. It allows the operator to authorize or not the device user to control the incoming File Transfer reception on this secondary device. Notion of primary and secondary device is defined in [TECHREAL].

Status	Occurrence	Format	Min. Access Types
Required	One	chr	Get

- Values: 0, 1
  0- Indicates authorization
  1- Indicates non authorization

/<X>/SecondaryDevicePar/VideoShare

This leaf node is instantiated in case the device is a RCS2 secondary device. It allows the operator to authorize or not the device user to control the incoming VideoShare session reception on this secondary device. Notion of primary and secondary device is defined in [TECHREAL].

Status	Occurrence	Format	Min. Access Types
Required	One	chr	Get

- Values: 0, 1
  0- Indicates authorization
  1- Indicates non authorization

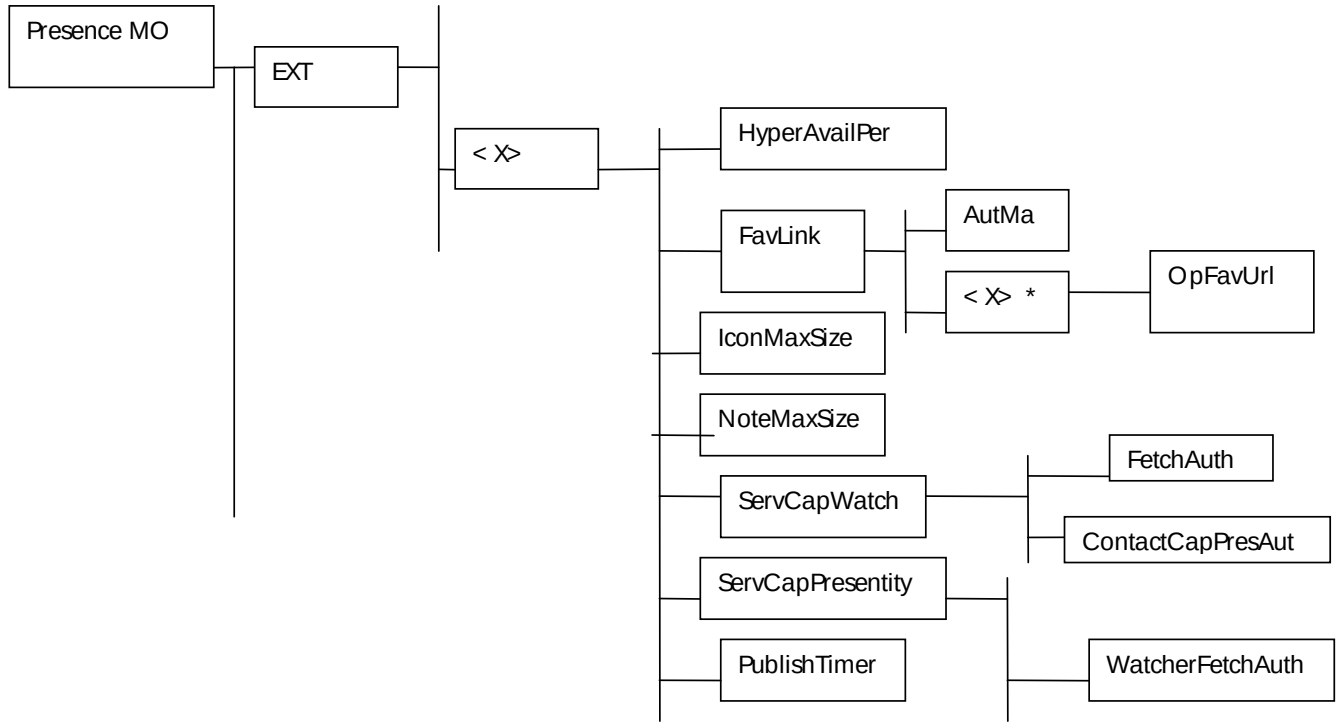
/<X>/SecondaryDevicePar/ImageShare

This leaf node is instantiated in case the device is a RCS2 secondary device. It allows the operator to authorize or not the device user to control the incoming ImageShare session reception on this secondary device. Notion of primary and secondary device is defined in [TECHREAL].

Status	Occurrence	Format	Min. Access Types
Required	One	chr	Get

- Values: 0, 1
  0- Indicates authorization
  1- Indicates non authorization

4.2 Presence MO sub tree



Node: /<X>

Under this interior node are placed the RCS parameters related to the Presence UA enabler

Status	Occurrence	Format	Min. Access Types
Required	One	node	Get

Type property of the Node is: urn:gsma:mo:rcs:2.0:Presence-ext

Node: /<X>/HyperAvailPer

This leaf node contains the value of the duration of the HyperAvailability state

Status	Occurrence	Format	Min. Access Types
Required	One	int	Get

- Values: <The value of the timer that defines the duration of the user HyperAvailability>

Node: /<X>/FavLink

Interior node under which parameters related to the operator provided Favorite Link(s)

- Occurrence: One
- Format: node
- Access Types: Get

Status	Occurrence	Format	Min. Access Types
Required	One	node	Get

Node: /<X>/FavLink/AutMa

Leaf node that determines the operator policy for Favorite Link instantiation in the local presence document of the presentity

Status	Occurrence	Format	Min. Access Types
Required	One	chr	Get

- Values: ‘Auto’, ‘Man’, ‘Auto+Man’

Node:/<X>/FavLink/<X>

A Place holder interior node where to place 0 or more OpFavUrl leaf nodes

Status	Occurrence	Format	Min. Access Types
Required	ZeroOrMore	node	Get

Node: /<X>/FavLink/<X>/OpFavUrl

Leaf node that represent a Favorite URL configured by the operator

Status	Occurrence	Format	Min. Access Types
Required	One	chr	Get

- Values: <The URL of the favourite link>

Node: /<X>/IconMaxSize

Leaf node that represent the maximum authorized size for an icon

Status	Occurrence	Format	Min. Access Types
Required	One	int	Get

- Values: <Icon maximum data size in bytes>

This maximum must be inferior to 200 Kb

Node: /<X>/NoteMaxSize

Leaf node that represent the maximum authorized size for a note

Status	Occurrence	Format	Min. Access Types
Required	One	int	Get

- Value: <Note maximum length in characters >

This value should have a lower value than the one defined at watcher side in the OMA Presence Implementation guideline [PRESENCEIG]

Node: /<X>/ServCapWatch

Interior node that represent operator setting of parameters linked with watcher behaviour of the device.

Status	Occurrence	Format	Min. Access Types
Required	One	node	Get

Node: /<X>/ServCapWatch/FetchAut

Leaf node that represent the authorization for the presence UA to automatically fetch (anonymous subscribe) service presence information of user contacts declared in the local address book

Status	Occurrence	Format	Min. Access Types
Required	One	chr	Get

- Values: 0, 1
  0- Indicates that this automatic fetch is not authorized
  1- Indicates that this automatic fetch is authorized

Node: /<X>/ServCapWatch/ContactCapPresAut

Leaf node that indicates if the device is authorized to display to the user the ability of the user contacts declared in the local address book to share Social Presence Information

Status	Occurrence	Format	Min. Access Types
Required	One	chr	Get

- Values: 0, 1
  0- Indicates that rendering is not authorized
  1- Indicates that rendering is authorized

Node: /<X>/ServCapPresentity

Interior node that represent operator setting of parameters linked with presentity behaviour of the device

Status	Occurrence	Format	Min. Access Types
Required	One	node	Get

Node: /<X>/ServCapPresentity/WatcherFetchAut

Leaf node that indicates if watchers are authorized to “anonymous” fetch service capabilities of the user

Status	Occurrence	Format	Min. Access Types
Required	One	chr	Get

- Values: 0, 1

0- Indicates that watchers are authorized to fetch user service capabilities
1- Indicates that watchers are not authorized to fetch user service capabilities

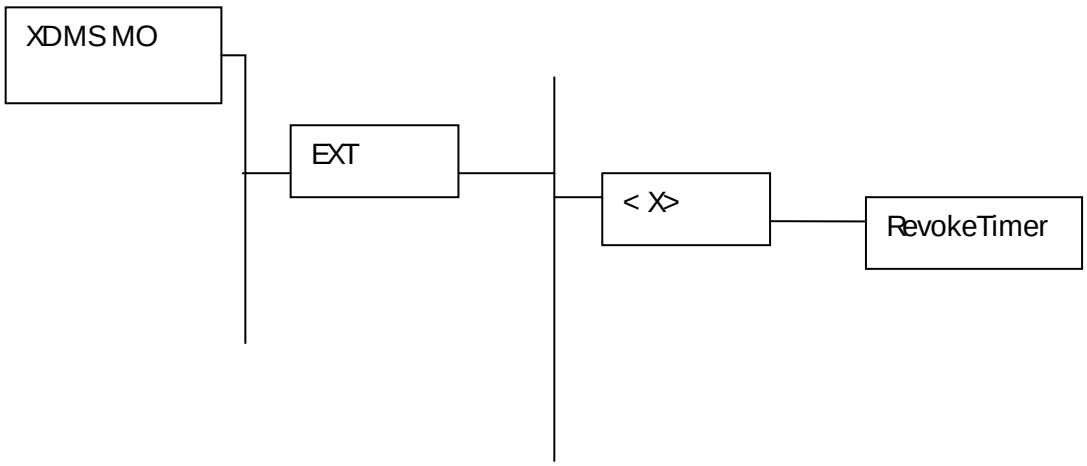
Note: In case they are not authorized, the device must set RCS rules accordingly (to provide an empty document to watchers)
Node: /<X>/PublishTimer

Leaf node that indicates the timer value for the Presence Publish refreshment

Status	Occurrence	Format	Min. Access Types
Required	One	int	Get

- Values: < Timer value in seconds>

4.3 XDMS MO sub tree



Node: /<X>

Interior node where XDM related parameters are stored

Status	Occurrence	Format	Min. Access Types
Required	One	node	Get

Type property of the Node is: urn:gsma:mo:rcs:2.0:xdm-ext

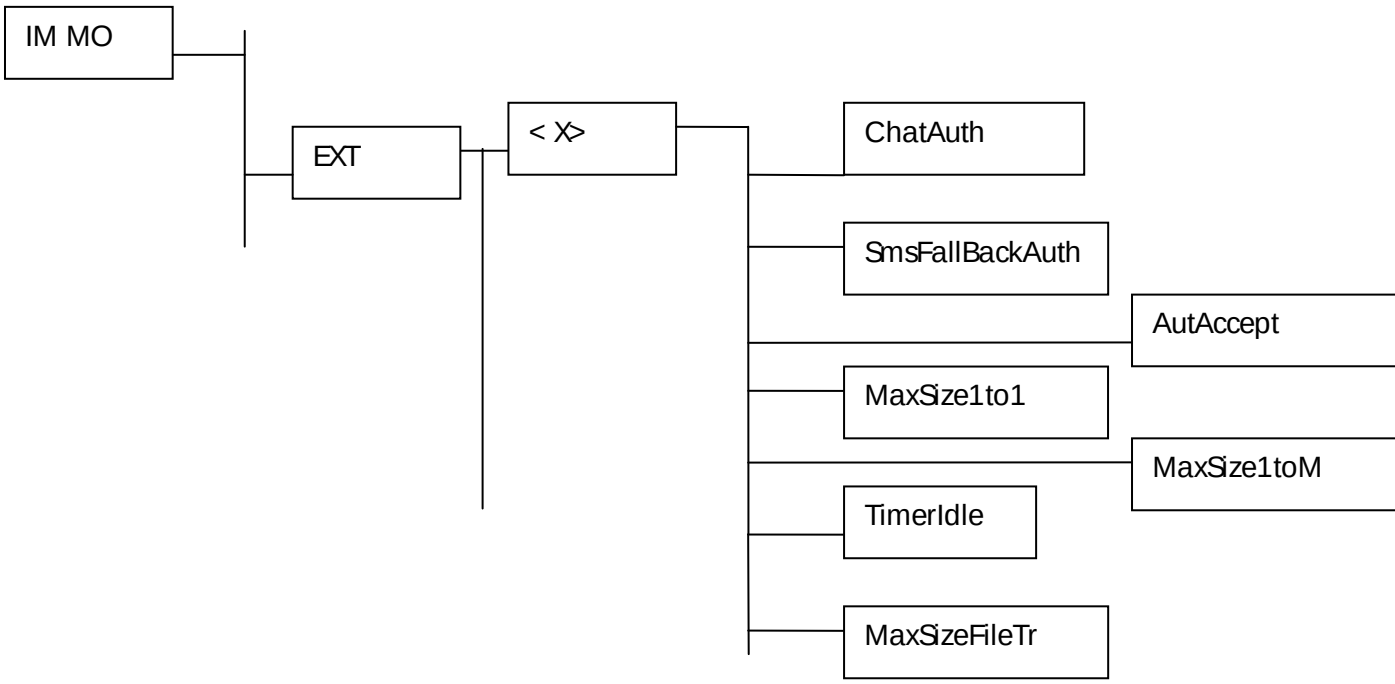
Node: /<X>/RevokeTimer

Leaf node that indicates the duration a contact should remain in the RCS revocation list

Status	Occurrence	Format	Min. Access Types
Required	One	int	Get

- Values: < Timer value in seconds>

4.4 IM MO sub tree



Node: /<X>

Interior node where IM related parameters are stored

Status	Occurrence	Format	Min. Access Types
Required	One	node	Get

Type property of the Node is: urn:gsma:mo:rcs:2.0:im-ext

Node: /<X>/ChatAuth

Leaf node that represent the authorization for user to use Chat service

Status	Occurrence	Format	Min. Access Types
Required	One	chr	Get

- Values: 0, 1
  0- Indicates that Chat service is disabled
  1- Indicates that Chat service is enabled

Node: /<X>/SmsFallbackAuth

Leaf node that represent the authorization for the device to propose automatically a SMS fallback in case of chat initiation failure

Status	Occurrence	Format	Min. Access Types
Required	One	chr	Get

- Values: 0, 1
  0- Indicates authorization is ok
  1- Indicates authorization is non ok

Node: /<X>/AutAccept

Leaf node that represent the automatic/manual chat session answer mode

Status	Occurrence	Format	Min. Access Types
Required	One	chr	Get

- Values: 0, 1
  0- Indicates manual answer mode
  1- Indicates automatic answer mode (default value)

Node: /<X>/MaxSize1To1

Leaf node that represent the maximum authorized size of a content chat message in a 1 To 1 chat session

Status	Occurrence	Format	Min. Access Types
Required	One	int	Get

- Value: <content maximum size in bytes>

Node: /<X>/MaxSize1ToM

Leaf node that represent the maximum authorized size of a chat content message in a 1 To M chat session

Status	*Occurrence*	*Format*	*Min. Access Types*
Required	*One*	*int*	*Get*

- Value: <content maximum size in bytes>

Node: /<X>/TimerIdle

Leaf node that represent the timeout for a chat session in idle mode (when there is no chat user activity)

Status	Occurrence	Format	Min. Access Types
Required	One	int	Get

- Value: <Timer value in seconds>

Node: /<X>/MaxSizeFileTr

Leaf node that represent the maximum authorized size of a file that can be transfers using the RCS File Transfer service

Status	Occurrence	Format	Min. Access Types
Required	One	int	Get

- Value: <content maximum size in bytes

DOCUMENT MANAGEMENT

Document History

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
0.1	02.07.2009	Baseline document created from the RCS1 document and adding broadband RCS2 access related parameters		Alain Bultinck/ ALU
0.2	10.13.2009	Incorporation of the approved CR 2009-RCS2-BF0002-ed02 that introduces the RCS2 formal data model		Alain Bultinck/ ALU
0.3	11.26.2009	Incorporation of the approved CR RCS2 BF0006 ed3. This CR introduces the new object notation form and provides editorial corrections		Alain Bultinck/ALU
0.4	12.02.2009	Incorporation of the approved CR RCS2-BF0012R1 that concerns with group chat restriction parameter		Alain Bultinck/ALU
1.0	11.12.2009	Update 0.4 (Approved at Plenary 3/12/09) with front pages for DAG approval. No review comments received during consistency review See SPEC DOC RCS SPEC R2_017 in https://infocentre.gsm.org/cgi-bin/docindex.cgi?33477 Alignment version numbering with other R2 specs	RCS Programme	Dirk Raeymaekers/ NSN
1.1	25.02.2010	Approved by DAG/EMC, removal DAG review sheet	RCS Programme	Dirk Raeymaekers /NSN

Other Information

Type	Description
Document Owner	Alain Bultinck
Editor / Company	Alcatel-Lucent