Rich Communication Suite Release 3 Managed Objects

V2.0

16 March 2011

*This is a **Non-Binding** Permanent Reference Document of the GSM Association.*

Security Classification – NON-CONFIDENTIAL GSMA Material

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 RCS terminal as well as how they are configured.

The scope of this document is RCS Release 3.

1.2 References

[FUNCDESC]	RCS Release Functional Description
[TECHREAL]	RCS Release Technical Realization
[IMENDORSE]	RCS Release 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
[MMSMO]	OMA Management Object for MMS, Candidate Version 1.3 – 28 Jan 2008 http://www.openmobilealliance.org
[CONNMO]	Standardized Connectivity Management Objects for use with OMA Device Management, Approved Version 1.0 – 07 Nov 2008 http://www.openmobilealliance.org
[CONNMOHTTP]	Standardized Connectivity Management Objects HTTP Proxy Parameters for use with OMA Device Management, Approved Version 1.0 – 24 Oct 2008 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
[24.341]	TS 24.341: Support of SMS over IP networks; Stage 3, v8.1.0 http://www.3gpp.org

[IR.84]	PRD IR.84 Video Share Phase 2 Interoperability Specification 1.1 http://www.gsmworld.com/
[SUPL]	Secure User Plane Location, Approved Version 1.0 – 15 Jun 2007 http://www.openmobilealliance.org/
[SUPLMO]	OMA Management Object for SUPL. Approved Version 1.0 15 Jun 2007 http://www.openmobilealliance.org/

2 Management Object Parameters

2.1 General

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

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

- When suitable Managed Objects (MO) exist in related standards documentation (OMA documentation or 3GPP documentation), RCS client configuration parameters correspond to the endorsement of such MO, e.g. 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 1 lists 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 User Equipment (UE).

- Parameters associated with the availability Status feature (as described in section 2.1.3.1 in [FUNCDESC] and section 4.2.2 in [TECHREAL])
  - Use of Availability status feature by the device (“Allowed” or “Not Allowed”) (as described in section 2.1.3.1 in [FUNCDESC] and section 4.2.2 in [TECHREAL])

- Parameters associated with the Favourite Link attribute (as described in section 2.1.3.2 in [FUNCDESC])
  - Automatic / manual mode for the Favourite Link.
  - In the case automatic mode is activated, there is additional parameter “list of pre-defined Favourite 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])

Parameter associated with the label associated with the Favourite Link [TECHREAL]

- Control of the length of the label (in terms of number of characters)

Parameters associated with location attribute (as described in section 6.2 in [TECHREAL])

- Control of the length of the descriptive text (length in terms of number of characters)
- Control of the maximum validity lifetime of location item
- Control of the minimum duration between consecutive location updates

Parameters associated with watcher fetch operation control introduced in [TECHREAL] in order:

- To configure per contact the minimum time between 2 fetch operations for the same contact
- To configure the maximum amount of fetch operations during a certain time for all contacts

Parameters associated with the watcher nickname function introduced in [TECHREAL]

- Control of the nickname length the user is allowed to define (length in terms of number of characters)

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

The 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-HOC_GROUP_SIZE	Maximum number of Participants allowed for an Ad-hoc IM Group Session	M
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 e.g. 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, it 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 directly 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	O M if Digest mode

	only)	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 parameter in SIP Register Required in a multi-terminal deployment to control forking of incoming SIP requests	M 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 backup/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

This is for future study.

2.8 Configuration related with Broadband secondary device

2.8.1 General

With the Introduction of the Broadband secondary device in RCS, there are features in a Broadband RCS device that needs configuration:

- Control of service delivery
- MMTEL
- SMS originating over IP
- MMS

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

MMTEL: For RCS, 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

SMS over IP: As specified in [TECHREAL], when sending a short message from the RCS Broadband Access Client, the address of the operator's SMS-C needs to be supplied in the SIP request containing the short message. See [24.341] chapter 5.3.1.

MMS: As specified in [TECHREAL], before sending a Multimedia Message from the RCS Client, and also when retrieving the Multimedia Message, the addresses of the operator's HTTP proxy and MMS centre (MMSC) needs to be configured.

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 additional codec	O
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

2.8.4 RCS endorsement of OMA MMS parameters

MMS Client provisioning parameters are defined in OMA Management Object for MMS [MMSMO]. RCS Broadband Access Clients may use this object for provision of the required parameters for accessing the MMS service.

Specifically, the URL to the MMS Centre (MMS Proxy-Relay server) shall be provided.

2.8.5 RCS endorsement of OMA Connectivity Management Objects parameters

Short Message Service Centre (SMS-C) Address: a PSI in form of a TEL URI or SIP URI The NAP object defined in [CONNMO] may be used for this purpose.

Specifically the address type field and the address field shall be provided (with SMSC address information)

HTTP proxy Client provisioning parameters are defined by the “proxy” object in [CONNMO] and further specified in [CONNMOHTTP]. RCS Broadband Access Clients may use this object for provision of the required parameters for accessing the HTTP proxy.

Specifically, the proxy type, proxy address and the authorization type and credentials (username & password) shall be provided.

2.9 Configuration related with [IR.84] introduction

VideoShare Phase 2 involves the introduction of a video share content server in the network. The address of this server must be configured in the device.
For that purpose, specific RCS nodes are introduced under the RCS IMS MO

2.10 Configuration related with Secure User Plane Location (SUPL) introduction

RCS3 introduces SUPL [SUPL] for providing localization social presence information.

SUPL Client provisioning parameters are defined in OMA Management Object for SUPL [SUPLMO]. RCS may use this object for provision of the required parameters for accessing the H-SLP (Home SUPL Location Platform).

Specifically, the Addr and AddrType the H-SLP shall be provided.

2.11 Content sharing related configuration

2.11.1 Specific RCS Client provisioning parameters linked with Content Sharing

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

- Parameters associated with the Content Sharing service
- Maximum authorized size of the content that can be sent within an Image Share session. This parameter enables the operator of the inviting user’s RCS client to control the maximum size of the content that the inviting user’s RCS client is authorized to send in an Image Share session
- Maximum authorized duration time of a Video Share session. This parameter enables the operator of the inviting user’s RCS client to control the maximum duration time of a Video Share session that the inviting user’s RCS client is authorized to handle.

- Note: These parameters are placed in the IMS MO sub-tree.

3 Technical Support for the Configuration of Data on a RCS Terminal

3.1 General

OMA DM v1.2 shall be used by RCS mobile terminal in order to handle configuration of the objects listed in this document.

3.2 Parameters specific to RCS

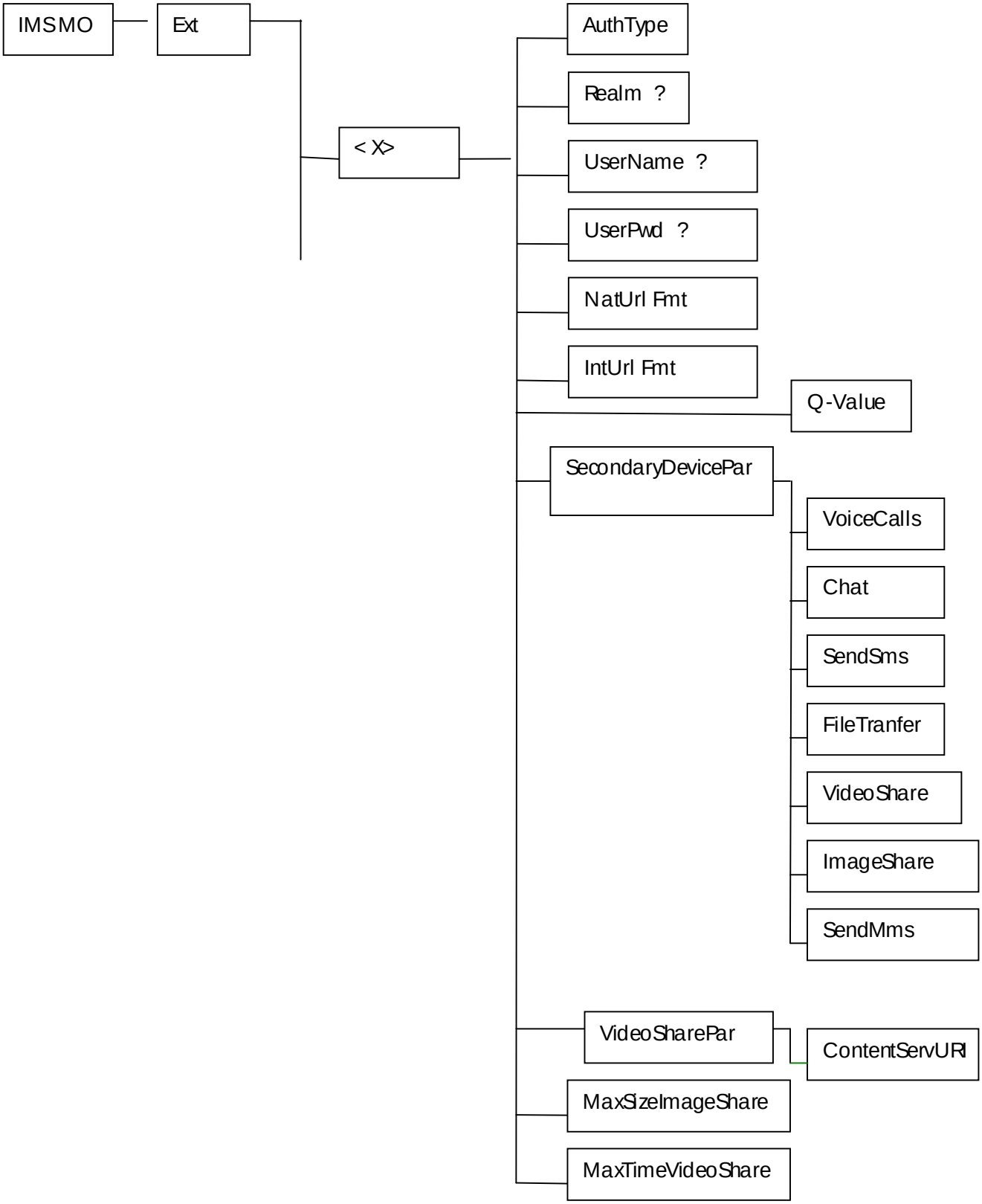
For parameters specific to RCS (for which there exist no OMA DM objects), the extension capability of existing OMA DM objects is used as follows:

- 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 2.4.2 and 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 nodes 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:3.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 the format (SIP URL or Tel URL) 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)

Node: /<X>/IntUrlFmt
This leaf node indicates the format (SIP URL or Tel URL) 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)

Node: /<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’

Node: /<X>/SecondaryDevicePar
Presence of this interior node indicates that the RCS 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

Node: /<X>/SecondaryDevicePar/VoiceCalls
This leaf node is instantiated in case the device is a RCS 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

Node: /<X>/SecondaryDevicePar/Chat
This leaf node is instantiated in case the device is a RCS secondary device. It allows the operator to authorize or not the device user to control the incoming chat session acceptation 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

Node: /<X>/SecondaryDevicePar/SendSms
This leaf node is instantiated in case the device is a RCS 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

Node: /<X>/SecondaryDevicePar/FileTransfer
This leaf node is instantiated in case the device is a RCS 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

Node: /<X>/SecondaryDevicePar/VideoShare
This leaf node is instantiated in case the device is a RCS 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].
Note: For a RCS2 device, this parameter applies to RCS VideoShare phase 1 service. For RCS3 and upper releases of RCS this applies to RCS VideoShare phase 1 and VideoShare phase 2 services.

Status	Occurrence	Format	Min. Access Types
Required	One	chr	Get

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

Node: /<X>/SecondaryDevicePar/ImageShare
This leaf node is instantiated in case the device is a RCS 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

Node: /<X>/SecondaryDevicePar/SendMms
This leaf node is instantiated in case the device is a RCS3 (or upper version) secondary device. It allows the operator to authorize or not the device user to enable/disable the restricted MMS service (only possibility to send an MMS 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

Node: /<X>/VideoSharePar
Optional Interior node that must be populated in a RCS device (from RCS3 and upper versions) if the network offers the related [IR.84] VideoShare phase 2 features with a video content server in the network.

Status	Occurrence	Format	Min. Access Types
Required	One	node	Get

Node: /<X>/VideoSharePar/ContentServURI
Leaf node where is stored the address of the network content server root file

Status	Occurrence	Format	Min. Access Types
Required	One	chr	Get

Values: <The URL of content server root file>

Node: /<X>/MaxSizeImageShare

Leaf node that represent the maximum authorized size of the content that can be sent in an Image Share session

Status	Occurrence	Format	Min. Access Types
Required	One	Int	Get

- Value: <content maximum size in bytes>. Value equals to 0 means no limitation.

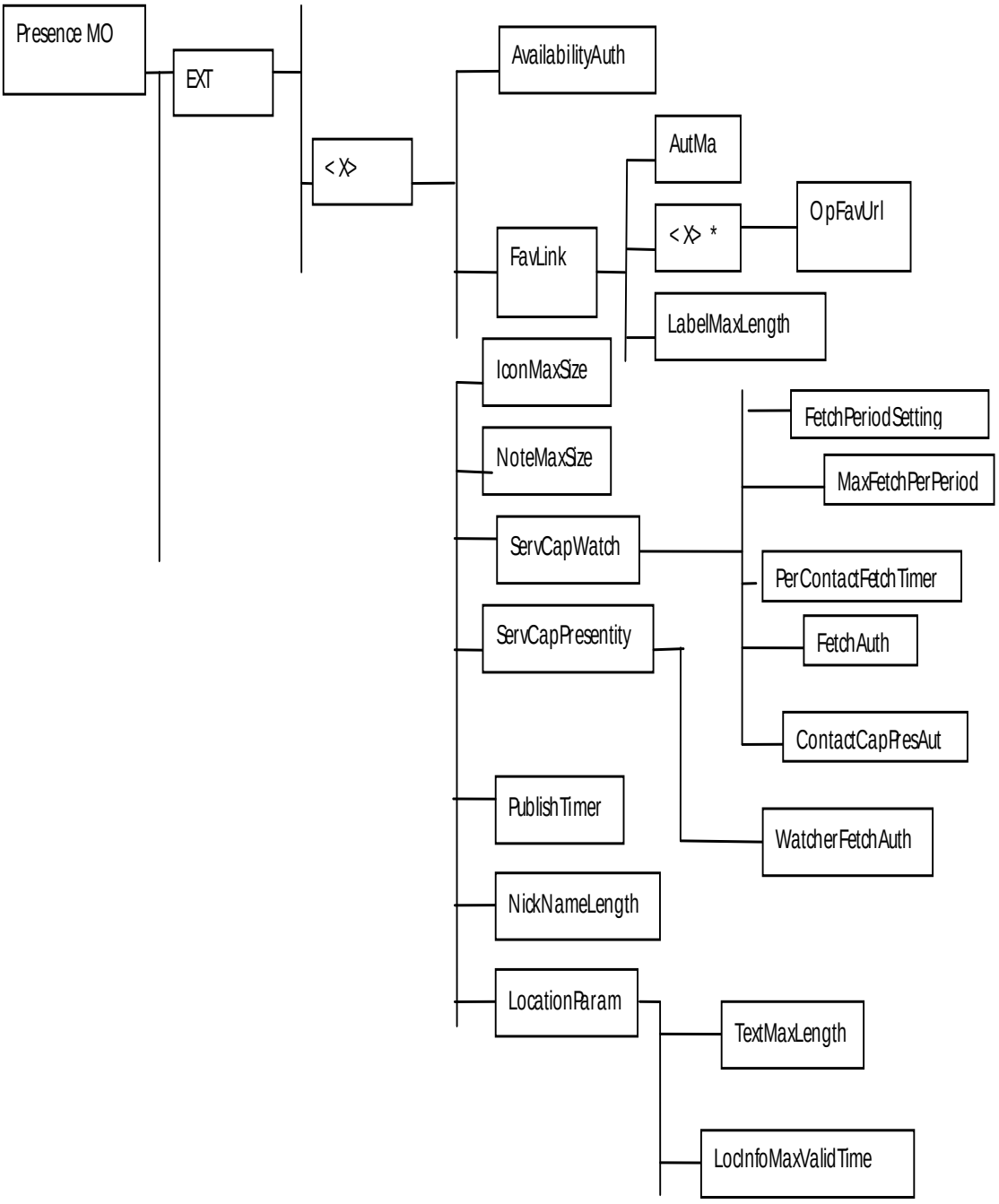
Node: /<X>/MaxTimeVideoShare

Leaf node that represent the maximum authorized duration time for a Video Share session

Status	Occurrence	Format	Min. Access Types
Required	One	Int	Get

- Value: <Timer value in seconds>. Value equals to 0 means no limitation.

4.2 Presence MO sub tree



Node: /<X>
Under this interior nodes 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:3.Presence-ext

Node: /<X>/AvailabilityAuth

Leaf node that represent the authorization for the Presence UA to use Availability status feature

Status	Occurrence	Format	Min. Access Types
Required	One	chr	Get

- Values: 0, 1
  0- Indicates that the use of Availability status is not authorized
  1- Indicates that the use of Availability status is authorized

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/LabelMaxLength
A leaf node that represents the maximum size authorized for the label associated with the favourite link

Status	Occurrence	Format	Min. Access Types
Required	One	int	Get

Value: an integer that must be less or equal to 200
A watcher must be able to display up to 200 characters for this attribute

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>/ServCapWatch/FetchPeriodSetting
Leaf node that indicates, in seconds, the period duration for the calculation of the number of Fetch operation authorized during this period.

Status	Occurrence	Format	Min. Access Types
Required	One	int	Get

Value: integer that represents a time value in seconds

Node: /<X>/ServCapWatch/MaxFetchPerPeriod
Leaf node that indicates the maximum Fetch operations that are authorized globally for the User Agent during each Period (Period parameter defined in the previous /ServCapWatch/FetchPeriodSetting node).

Status	Occurrence	Format	Min. Access Types
Required	One	int	Get

Value: integer that represents the total amount of Fetch operations per each period, independently of the number of contacts that have to be fetched

Node: /<X>/ServCapWatch/PerContactFetchTimer
Leaf node that indicates the maximum time that must separate 2 consecutive Fetch operations for one particular contact.

Status	Occurrence	Format	Min. Access Types
Required	One	int	Get

Value: integer that represent, in seconds, this interval period.
Note: If there is a conflict between this setting and the setting of the node: /<X>/ServCapWatch/MaxFetchPerHour, the MaxFetchPerHour node take the priority (The value setting in the /<X>/ServCapWatch/PerContactFetchTimer will not be representative)

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>

Node: /<X>/NickNameLength
Leaf node that represents the maximum number of characters allowed for the user chosen nickname.

Status	Occurrence	Format	Min. Access Types
Required	One	int	Get

Value: must be less or equal to 200.
Note: A RCS client must be able to handle of up to 200 characters

Node: /<X>/LocationParam
Interior node where Location related parameters are stored

Status	Occurrence	Format	Min. Access Types
Required	One	node	Get

Node: /<X>/LocationParam/TextMaxLength
Leaf node that represents the maximum numbers of characters authorized for the textual attribute of the Location information

Status	Occurrence	Format	Min. Access Types
Required	One	int	Get

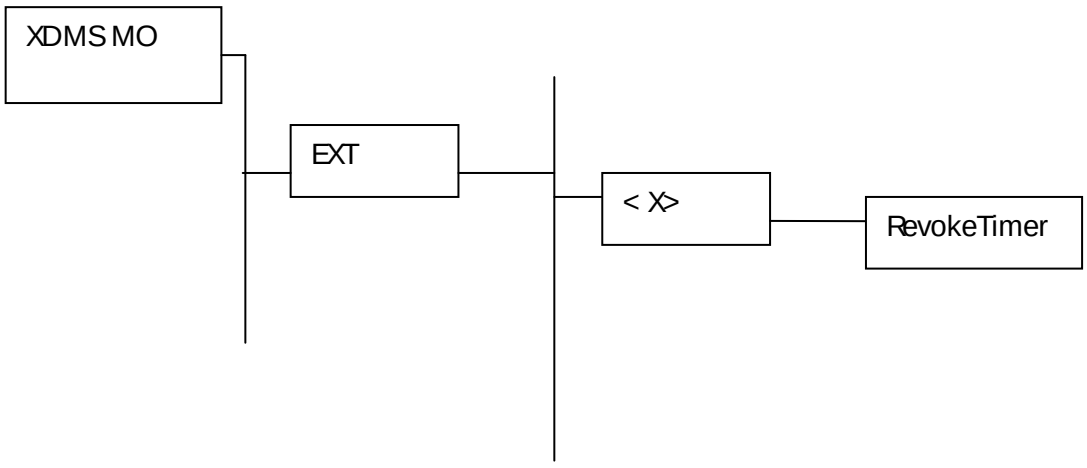
Value: must be less or equal to 200.
Note: A watcher must be able to render of up to 200 characters

Node: /<X>/LocationParam/LocInfoMaxValidTime
Leaf node that represents the maximum validity duration time for a location item.
This parameter must be taken account by the device presence UA when setting the “until” attribute of the presence items place-type, time-offset and the usage-rule/retention-expiry item value

Status	Occurrence	Format	Min. Access Types
Required	One	int	Get

Value: duration 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

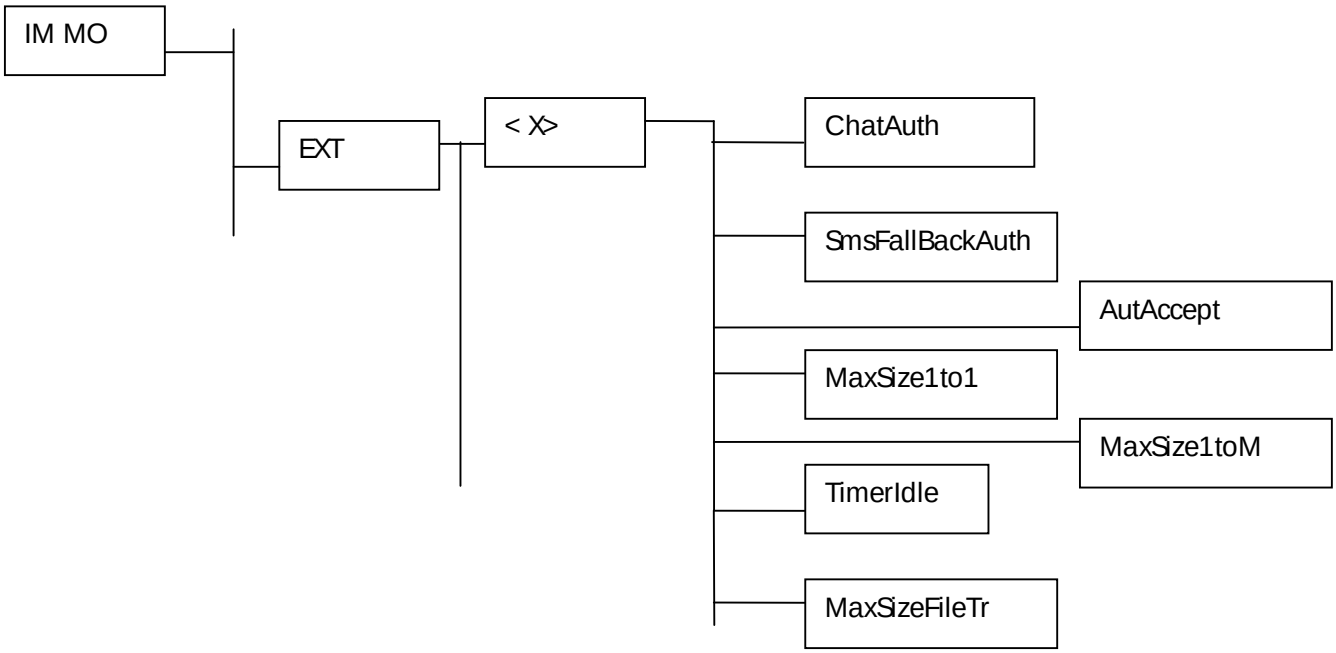
Type property of the Node is: urn:gsma:mo:rcs:3.xdm-ext

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:3.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	23 February 2010	Baseline document created from the RCS2 document	RCS Programme	Alain Bultinck/ ALU
0.2	15 March 2010	Baseline for Tel Aviv TG	RCS Programme	Alain Bultinck/ ALU
0.3	06 May 2010	Incorporation of the MO-RCS3-BF0002-Miscellaneous-comments-icorp	RCS Programme	Alain Bultinck/ ALU
0.4	24 June 2010	Update 0.3 (Approved at Plenary 17/6/10) with front pages for DAG approval.	RCS Programme	Dirk Raeymaekers /NSN
0.5	19 July 2010	For approval	EMC	Mark Hogan GSMA
1.0	Aug 2010	Approved by DAG/EMC	RCS Programme	Dirk Raeymaekers/ NSN
1.1	01 December 2010	Incorporation of the approved CRs RCS3-TR-BF0102R01 RCS3-TR-BF0103R02 RCS3-TR-BF216R01	RCS Programme	Alain Bultinck/ALU
2.0	16 March 2011	Change requests for approval by DAG & EMC	EMC	Alain Bultinck/ALU

Other Information

Type	Description
Document Owner	RCS Project
Editor / Company	Alain Bultinck