RCS-e - Advanced Communications: Services and Client Specification

Version 1.2-preview

05 August 2011

RCE GEN 001

This is a draft preview of the Version 1.2 of the "RCS-e - Advanced Communications: Services and Client Specification"

Security Classification – NON CONFIDENTIAL GSMA MATERIAL

Copyright Notice

Antitrust Notice

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

I. Index of contents

II. Index of figures

III. Index of tables

IV. Document change log

Version	Date	Comments
1.0	12/02/2011	Version ready for release to GSMA
1.1-final draft-1	11/03/2011	Version ready for release to GSMA. This is a draft version published for general review. Please note the final 1.1 version will not contain major functionality additions or changes of the existing one compared to this draft.
1.1-final draft-2	23/03/2011	Version ready for release to GSMA incorporating the comments received on the previous draft. This version is again published for general review. Please note the final 1.1 version will not contain major functionality additions or changes of the existing one compared to this draft.
1.1	06/04/2011	Version ready for release to GSMA
1.2-preview-draft1	05/08/2011	Version ready for release to GSMA incorporating those changes required for initial commercializations.

Table 1. Document change log

V. Scope and summary of changes respect to the previous version

The present version of the specification, 1.2, supersedes the previous version 1.1 which is now considered as deprecated. Consequently, all the commercial RCS-e deployments happening from August 2011 onwards should follow this version of the specification until a new version, superseding the present one, is published.

The main motivation behind publish this version is, based on the feedback provided by vendors and the experience acquired during the initial IOTs, to both:

- Correct the errors present in the version 1.1 of the specification, and,
- Elaborate in those areas where the specification did not provide enough information to those working on providing a RCS-e version 1.1 compliant implementation, potentially leading to interoperability issues.

As a reference, the main deltas between the RCS-e specification versions 1.1 and 1.2 are listed in the following table:

Section	Title	Change description
V.	Scope and summary of changes respect to the previous version	Table introduced to explain the main differences compared to version 1.1 issued April 08, 2011
2.1	First time registration and client configuration provisioning	- IP:port and FQDN:port removed from configuration parameters SIP proxy and XDM server -Configuration Parameter 'IM SESSION START' introduced to control the '200 OK' feedback message
2.2.2.1.2	Autoconfiguration mechanisms	Requirements added for the configuration mechanism via OMA DM: • Multiple management authorities • Active operator DM account selected by SIM card change • Setting protection by ACL • Need to define management object for operator • Setting status after successful configuration Detailing the alternative configuration mechanism via http/https: • Hot swap use case added for http/https request

		• Initial http request and follow up switch to https by using a cookie • List of https request GET parameters • Configuration URL to be accessed via http • Response details incl. changed settings for disabling further autoconfiguration boot queries • Optional user messages delivered within autoconfiguration incl. message parameter definition and use case review Table of possible response scenarios and security considerations added
2.3.1.1	SIP OPTIONS message extension to support capability discovery	Case of several IARI tags included in an option request defined
2.8	RCS-e protocols	Reference to the list of preferred options for the transport and security for the signalling and media protocols, which is included in the configuration parameters (Annex A section A.2.7)
2.9.2.1	Device incoming SIP request / From/P-Asserted-Identity	Further rule exception for P-asserted-identity added
2.9.3.3	Device outgoing SIP request / User alias	Further clarifications of the use of alias information
2.12.2	LTE capability discovery using the RCS-e	mmtel tag reused
3.2.2.1	Delta between RCS-e and RCS Release 2 on the IM functionality / Functional level	Differences between RCS-e and RCS Release 2 on functional level are described: • Store notifications (delivered and displayed) in IM server • Clarification for delivering notifications outside a session • Multimedia messages out of scope in RCS-e due to store and forward complexity; transference of files to take place in a separate session Clarification on chat rejection mechanism
3.2.2.2	Delta between RCS-e and RCS Release 2 on the IM functionality/ Technical/Protocol level	Differences between RCS-e and RCS Release 2 on technical/protocol level are described: • Clarification for identification of stored messages

		• Delivery notification field used to confirm successful display of message • No need for RCS-e clients to request MSRP reports Additional requirement for sender to set display-name in the SIP From and CPIM From header
3.2.2.3	Delta between RCS-e and RCS Release 2 on the IM functionality/ Delivery notifications	Differences between RCS-e and RCS Release 2 on delivery notifications topic are described: • Clarification about store and forward of delivery notifications in case the recipient is not available Description of use case the message is marked as spam
3.2.2.4	Delta between RCS-e and RCS Release 2 on the IM functionality / Display notifications	Differences between RCS-e and RCS Release 2 on display notifications topic are described: • Clarification of display notifications delivery within or outside of a MSRP session Clarification about store and forward of displayed notifications in case the recipient is not available
3.2.4.1	Initiating a chat	Further failure conditions included
3.2.4.2	Answering a chat	Detailed description of handling the new configuration parameter IM START SESSION
3.2.4.6	’Is Composing’ notification	Clarification about ’Is Composing’ notification in relation to CPIM header
3.2.4.9	Chat abnormal interruption	Further clarification included in case message was not sent
3.2.4.10	Re-Opening a chat	Clarification of sending outstanding displayed notifications
3.2.4.15 to 3.2.4.19	New chapters: Spam/Blacklist filter, Emoticons, chat message size limitations, race conditions, store & forward notification handling	New chapters contain information about: • Details on SPAM transaction handling • Handling of emoticons • Recommendation for chat message size limit • Handling of simultaneous invites • Handling of late invites (previous one has already been accepted)

		Handling of multiple notifications in short time periods Clarifications on the fact spam filter applies to both IM and file transfer
3.2.5.1	Clarifications on groupal chat experience	Added remarks on UX requirements regarding participants list
3.2.5.4	New chapter: Chat message size limitations	Recommendation for chat message size limit
3.3.18	New chapter: Call divert/forwarding	Clarification about restrictions in case a user has call divert/forwarding activated
A.1.3	Management objects parameter additions / IM related configuration	IM SESSION START configuration parameter added
A.2.4	IM MO sub tree addition	“imSessionStart” parameter added to IM sub tree
A.2.7	Other RCS-e configuration sub tree	Further configuration parameters defining the transport protocol used to carry signalling and media data for different access types are included to sub tree Other MO under ‘transportProto’ node
A.3.1	OMA-CP configuration XML structure	Configuration structure updated
A.4	New chapter: Autoconfiguration XML sample	XML example file included
Annex B	IM Store and forward diagrams	Call flows updated
Annex C	RCS-e IM/Chat and multidevice	Call flows updated

Table 2. Document change log

VI. Definitions and terms

Type	Description
2G	Second generation of Global System for Mobile Communications (GSM)
AS	Application server
AVC	Advanced video codec
CS	Circuit switched
DHCP	Dynamic Host Configuration Protocol
DTM	Dual transfer mode
FQDN	Fully Qualified Domain Name
GIBA	GPRS-IMS-Bundled Authentication
GSMA	GSM Association
HD	high-definition voice
HTTP	Hyper-Text Transfer Protocol
HTTPS	HTTP Secure
IM	Instant messaging. The term *chat* is also applied in this document to the same concept.
IM-AS	IM application server
IMDN	Instant Message Disposition Notification
IMEI	International Mobile Station Equipment Identity
IMS	IP Multimedia System
IMSI	International Mobile Subscriber Identity
IMS AKA	IMS Authentication and Key Agreement
IP	Internet Protocol
LTE	Long term evolution
MNO	Mobile network operator
MSISDN	Mobile Subscriber Integrated Services Digital Network Number
MSRP	Message Session Relay Protocol
NAT	Network Address Translation
OEM	Original Equipment Manufacturer
OFDM	Orthogonal frequency division multiplex
OMA-CP	OMA Client Provisioning
OMA-DM	OMA Device Management
PCO	Protocol Configuration Options
P-CSCF	Proxy-Call Session Control Function
PDP	Packet Data Protocol
PS	Packet switched
RADIUS	Remote Authentication Dial In User Service
RCS	Rich Communication Suite
RTP	Real-Time Transport Protocol
SDP	Session Description Protocol
SIP	Session Initiation Protocol
SMS	Short message service

SSO	Single sign on (type of IMS authentication)
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
URI	Uniform Resource Identifier
UX	User Experience
VoLTE	Voice over LTE
Wi-Fi	Synonym for WLAN, Wireless Local Area Network
XCAP	XML Configuration Access Protocol
XDM	XML Document Management
XDMS	XML Document Management Server
XML	Extensible Markup Language

Table 3. Abbreviations and acronyms

VII. Document cross-references

Ref	Name	Document reference
1	[3GPP TS 24.167]	3GPP TS 24.167 version 10.2.0 (2011-03), 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; 3GPP IMS Management Object (MO)
2	[3GPP TS 24.229]	3GPP TS 24.229 version 10.3.0 (2011-03), 3rd Generation Partnership IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP)
3	[IETF-DRAFT-SIPCORE-KEEP12]	IETF SIP Core keep IETF draft version 12
4	[IETF-DRAFT-SIMPLE-MSRP-SESSMATCH10]	IETF Simple MSRP seesmatch draft version 10
5	[PRD-IR.92]	GSMA PRD IR.92 - “IMS Profile for Voice and SMS” 1.0 18 March 2010
6	[RCS1-FUN-DESC]	Rich Communication Suite Release 1 Functional Description Version 2.0 14 February 2011
7	[RCS1-TEC-REAL]	Rich Communication Suite Release 1 Technical Realization Version 2.0 14 February 2011
8	[RCS2-FUN-DESC]	Rich Communication Suite Release 2 Functional Description Version 2.0 14 February 2011
9	[RCS2-MO]	Rich Communication Suite Release 2 Management Objects Version 2.0 14 February 2011
10	[RCS2-TEC-REAL]	Rich Communication Suite Release 2 Technical Realization 2.0 14 February 2011
11	[RCS2-SD]	Rich Communication Suite Release 2 Endorsement of OMA Service Defintion Version 2.0 14 February 2011
12	[RCS2-OMA-SIMPLE-ENDORS]	Rich Communication Suite Release 2 Endorsement of OMA SIP/SIMPLE IM 1.0 Version 2.0 14 February 2011
13	[RCS4- TEC-REAL]	Rich Communication Suite Release 4 Technical Realization 1.0 14 February 2011
14	[RCS4-IR92-ENDORS]	GSMA RCS Release 4 Endorsement of [PDR-IR92] 14 February 2011
15	[RFC3261]	SIP (Session Initiation Protocol) IETF RFC
16	[RFC3711]	The Secure Real-time Transport Protocol (SRTP) IETF RFC

17	[RFC3966]	The TEL-URI for Telephone Numbers IETF RFC
18	[RFC4028]	The Session Timers in the Session Initiation Protocol (SIP) IETF RFC
19	[RFC4122]	The Universally Unique IDentifier (UUID) URN Namespace IETF RFC
20	[RFC4961]	Symmetric RTP / RTP Control Protocol (RTCP) IETF RFC
21	[RFC5438]	Instant Message Disposition Notification (IMDN) IETF RFC
22	[RFC5626]	Managing Client-Initiated Connections in the Session Initiation Protocol (SIP) IETF RFC
23	[RFC5627]	Using Globally Routable User Agent URIs (GRUUs) in the Session Initiation Protocol (SIP) IETF RFC
24	[RFC6135]	Alternative Connection Model for the Message Session Relay Protocol (MSRP) IETF RFC

Table 4. Normative reference

1. Introduction

The purpose of this document is to provide the detailed specifications that shall complement the current RCS Release 2 specification in order to set the initial reference implementation of the RCS-e services.

This initial implementation has been named RCS-e Advanced Communications as it focuses on the communications service aspects of the GSMA RCS Release 2 specification. Building on established interoperability principles within the mobile operator ecosystem, this specification provides further optimisation of the RCS Release 2 specification in order to accelerate time to market and simplify the customer proposition, Figure 1. This renewed focus is based on results from customer trials to date and a better understanding of where operators can further enhance their data network offering to deliver more value to customers and complement established 3rd party services.

The current document does not detail the *"social information via presence"*[1] functionality described in the RCS Release 2 specification. However, an operator can decide to launch RCS-e service including both the RCS social presence information defined in RCS Release 2 specification in addition to the advanced communications services defined in the present document. Both parts shall co-exist within a device implementation if requested by an operator.

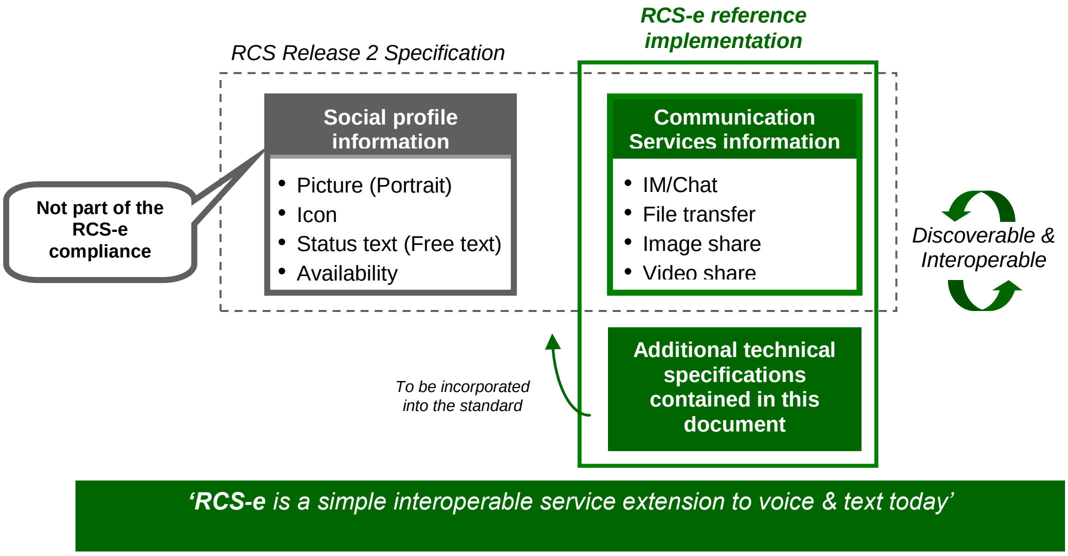

RCS-e reference implementation
RCS Release 2 Specification
Social profile information
• Picture (Portrait)
• Icon
• Status text (Free text)
• Availability
Not part of the RCS-e compliance
Communication Services information
• IM/Chat
• File transfer
• Image share
• Video share
Discoverable & Interoperable
To be incorporated into the standard
Additional technical specifications contained in this document
'RCS-e is a simple interoperable service extension to voice & text today'

Figure 1. RCS-e positioning

As a headline, RCS-e provides a *'simple interoperable extension to voice and text today.'* The services are designed to run over data and can stand alone (e.g. I share a picture from the media gallery) or used in combination with voice (e.g. see-what-I-see video).

[1] By this term we are referring to the set of functionalities defined in the RCS Release 1 and 2 specifications and presented in [RCS1-FUN-DESC] in sections from 2.1.2 to 2.1.6.

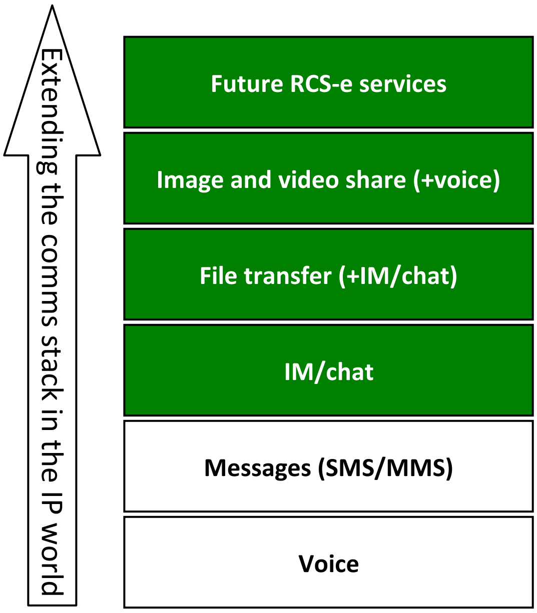


Figure 2. RCS-e Industry Proposition – *'extending the communications stack'*

1.1 *RCS-e Principles*

The fundamental mechanism that enables RCS-e is service or capability discovery. For example, when a user, User A, scrolls through his/her Address Book and selects a RCS-e contact, the client performs an instant service capability check, being able to display the services which are available to communicate.

This mechanism is implemented using SIP OPTIONS. SIP OPTIONS is a peer-to-peer request routed by the network that will generate one of 2 types of response:

1) The contact is registered for service and the contact's service capabilities, *at this point in time*, are received and logged by User A, or,

2) The contact is either not registered (they are provisioned but not registered) or Not Found (they are not provisioned for service).

This discovery mechanism is important in that it allows User A to determine what services are available before they are called and allows operators to roll-out new agreed services to their own schedule. RCS-e therefore provides an adaptive framework for new service deployment.

RCS-e implementation allows operators to also use SIP OPTIONS as the preferred mechanism to initially discover (and/or periodically check) the service capabilities of all the contacts of his/her address book when he/she first registers for service.

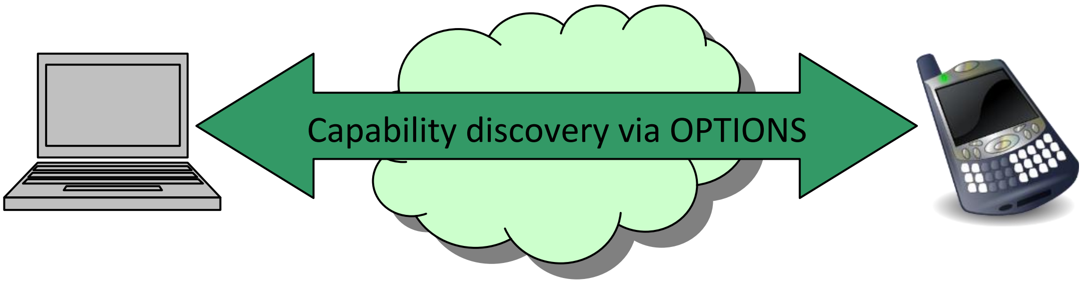


Figure 3. RCS-e capability discovery

1.2 *OEM Integration*

This specification is independent from any specific device operating system and is not intended to prescribe the supplier user experience. However, where appropriate key service logic is illustrated through wireframes to aid the reader. It is fully expected that each handset supplier will map the basic service principles defined in this document within their own products and drive innovative and differentiated experiences.

1.3 *Conformance*

The minimum conformance to the RCS-e specification can be achieved by a terminal providing the necessary functionality to support both the capability and new user discovery based on SIP OPTIONS message (covered in detail in sections 2.3.1 and 2.4.1 respectively) plus the IM/chat functionality (covered in detail in section 3.2).

The rest of services covered in the present specification are optional, ensuring that RCS-e can target low end devices and, therefore, boost the market penetration curve.

The terminal conformance to RCS-e specification can be summarized in the following terms[2]:

- All the necessary procedures to provision and register with the core network elements (e.g. IMS, RCS AS, etc.) **SHALL**[2] be supported
- Capability/service and new user discovery via SIP OPTIONS and ANONYMOUS fetch mechanism (covered in detail in sections 2.3.1, 2.3.2 and 2.4.1) **SHALL**[2] be supported
- IM/chat functionality (covered in detail in section 3.2) **SHALL**[2] be supported
- File transfer, image share and video share functionality (covered in detail in sections 3.3 and 3.4) **MAY**[2] be supported.
    - The motivation behind making these services optional is to facilitate the penetration of RCS-e services in all the handset tiers and, ultimately, a RCS-e handset **SHALL**[2] try to support all the feasible RCS-e services taking into account the relevant hardware and software limitations.

  Please note that in any case a MNO implementing RCS-e **SHALL**[2] provide the RCS file transfer, image share and video share functionality at network level.

[2] Please note the terms SHALL and MAY contained in the conformance summary are used as described in IETF RFC2119 (http://www.apps.ietf.org/rfc/rfc2119.html)

Please also note that although outside the conformance and consistently with section 1.1, a RCS-e terminal **MAY**[2] also be supplemented with the *"social information via presence"*[3] features as defined in the GSMA RCS Release 2 specifications.

1.4 *Scope and future evolution*

This document establishes the core principles and services framework of RCS-e through the initial, RCS Release 2 defined, set of functionality. However, the framework is designed to be extensible and support new services going forward.

New services and features will include, but are not limited to:

- RCS Home Services (fixed line, PC and mobile)
- Additional capabilities and services (e.g. HD voice, advanced geolocation services, etc.)
- Enhanced network address book services

It is intended to ensure backward compatibility when introducing new/extended services.

Finally, it should be noted that the aim of the present document is to only specify functionality which can be validated in standard IMS/RCS Release 2 pre-production and production environments without any need for major customisation or changes apart from those MNOs may introduce to optimise or differentiate their networks.

[3] By this term we are referring to the set of functionalities defined in the RCS Release 1 and 2 specifications and presented in the RCS Release 1 Functional Realization document (version 1.1) in sections from 2.1.2 to 2.1.6.

2. Registration and capabilities discovery process

2.1 *First time registration and client configuration provisioning*

The RCS-e registration process can only take place once the client is configured and the user (uniquely identified by the relevant IMS identity [TEL-URI or SIP-URI]) is correctly provisioned to access the RCS-e services.

In order to give the end user the impression that the new services are working out of the box and to minimise the operational impact on mobile network operators, both processes are performed automatically.

A mobile network implementing RCS-e should be able to detect when a user attaches to the network with a RCS-e capable handset for the first time. This event triggers two processes:

- Service provisioning: The relevant configuration is performed in the network to make the RCS-e services available to the user (e.g. provisioning an account on the IMS core and relevant application servers).
- Client configuration: The network pushes the client configuration using one of the mechanisms described in section 2.2.2.1.2. The configuration document comprises a set of configuration parameters, some required to operate and others to configure the client behaviour.

The minimum set of client settings is presented in the following tables: The first table covers the parameters referring to the IMS registration while the second focuses in RCS-e specific parameters. Please note all the parameters described the configuration can be only modified by the MNO (via MNO customization settings or one of the procedures described in section 2.2.2.1.2) and it is not accessible to the terminal user:

Configuration parameter	Comments	RCS-e usage
SIP proxy	P-CSCF address	Mandatory Parameter
XDM server	XDMS address	Mandatory parameter (It is mandatory and becomes relevant only if USE PRESENCE is set to 1)
TEL-URI	User’s TEL-URI	Optional parameter

SIP-URI	User's SIP-URI	Mandatory parameter[4]
SIP USER/PASSWORD	For alternative digest authentication to SSO/GIBA	Mandatory parameter

Table 5. Summary of IMS registration related configuration parameters

Note 1:

Configuration parameters	Comments	RCS-e usage
IM CONFERENCE FACTORY URI	This is the parameter containing the URI for the IM server. The parameter is optional and if not configured, means that the MNO is not deploying an IM server. Consequently features requiring IM server (i.e. 1-to-many chat) will not be available for those customers.	Optional Parameter
IM CAP ALWAYS ON	This parameter configures the client to support store and forward when presenting the IM capability status for all the contacts. If set to **1**, the IM capability for all RCS-e contacts will be always reported as available. Otherwise (**0)**, the capability will be reported based on the algorithm presented in section 2.7. For example, this can be used in MNOs that are implementing the store and forward functionality for IM	Optional parameter (It is mandatory if IM CONFERENCE FACTORY URI is set)

[4] When using GIBA, the temporary public identity used for IMS registration is built according to the procedure defined in 3GPP TS 24.229 (it does not rely on the SIP-URI and TEL-URI configuration parameters). Only one of the SIP-URI or TEL-URI configuration parameter must be configured. The configured parameter is used to select the URI which must be used by the RCS-e client during non-REGISTER transactions. If both TEL-URI and SIP-URI are defined, the TEL-URI should be used.
When using Digest, a SIP-URI must be configured. This URI is used for REGISTER and non-REGISTER transactions.

IM WARN SF	In case, IM CAP ALWAYS ON is set to enabled (use of store and forward), a new parameter is used called IM WARN SF for UI purpose only. If IM WARN SF parameter is set to (1) then, when chatting with contacts which are offline (Store and Forward), the UI must warn the user of the circumstance (e.g. message on the screen). Otherwise (0), there won't be any difference at UX level between chatting with an online or offline (Store and Forward) user.	Optional parameter (It is mandatory if IM CONFERENCE FACTORY URI is set and IM CAP ALWAYS ON is set to 1)
IM SESSION START	This parameter defines the point in a chat when the receiver sends the 200 OK back to the sender so the MSRP session can be established:0 (RCS-e default): The 200 OK is sent when the receiver consumes the notification opening the chat window. 1 (RCS default): The 200 OK is sent when the receiver starts to type a message back in the chat window. 2: The 200 OK is sent when the receiver sends a message (i.e.the message will not generate an invite but instead will be buffered in the client until the MSRP session is established.	Mandatory parameter
POLLING PERIOD	This is frequency in seconds to run a periodic capabilities update for all the contacts in the phone address book whose capabilities are not available (e.g. non-RCS-e users) or are expired (see CAPABILITY INFO EXPIRY parameter. Please note that if set to 0, this periodic update is no longer performed.	Mandatory parameter
CAPABILITY INFO EXPIRY	When using the OPTIONS discovery mechanism and with the aim of minimizing the traffic, a timestamp will be kept together with the capability information fetched using options. When performing a whole addressbook capability discovery (i.e. polling), an OPTIONS exchange takes place only if the time since the last capability update took place is greater than this expiration parameter	Optional parameter (It is mandatory if POLLING PERIOD is set to a value greater than 0)
USE PRESENCE	This parameter allows enabling or disabling the presence related features on the device. If set to 0, presence is disabled, if set to 1, presence is enabled and the parameters related to presence defined in [RCS2_MO] apply.	Mandatory Parameter

PRESENCE DISCOVERY	This parameter allows enabling or disabling the usage of capabilities discovery via presence. If set to 0, the usage of discovery via presence is disabled. If set to 1, the usage of discovery via presence is enabled. This parameter will consequently influence the inclusion of the associated tag to presence discovery in OPTIONS exchanges.	Optional parameter (It is mandatory and becomes relevant only if USE PRESENCE is set to 1)
PRESENCE PROFILE	This parameter allows enabling or disabling the usage of the *social information via presence*. If set to 0, the usage of the *social information via presence* feature is disabled. If set to 1, the *social information via presence* feature is enabled. This parameter will consequently influence the inclusion of the associated tag to *social information via presence* in OPTIONS exchanges.	Optional parameter (It is mandatory and becomes relevant only if USE PRESENCE is set to 1)
ENABLE RCS-E SWITCH	As described in section 2.10, the user shall be able configure to allow or disallow RCS-e and/or internet traffic in the handset settings. If this parameter is set to 1, the setting is shown permanently. Otherwise it may (MNO decision) be only shown during roaming.	Mandatory Parameter
RCS-E ONLY APN	This is the reference/identifier to the APN configuration which should be used to provide PS connectivity ONLY to RCS-e as described in section 2.10.	Mandatory Parameter
FT WARN SIZE	This is a file transfer size threshold in KB to warn the user that a file may end up in significant charges. Please note that if set to 0, the user will not be warned.	Mandatory Parameter
FT MAX SIZE	This is a file transfer size limit in KB. If a file is bigger than FT MAX SIZE, the transfer will be automatically cancelled. Please note that if set to 0, this limit will not apply.	Mandatory Parameter
END USER CONF REQ ID	This is identity used for sending the end user confirmation request.	Optional Parameter

Table 6. Summary of RCS-e client configuration parameters

Please note the detailed information on the extended managed objects for RCS-e is covered in *ANNEX A: Extensions to the data model*.

After configuration, the client is ready to register with the network for the first time. Once this registration is completed, the user is able to access the RCS-e services. These configuration options could also be updated afterwards by the MNO by pushing new configuration document using OMA DM.

Finally, please note that with the aim of reducing the complexity, the P-CSCF address used by the RCS-e client is selected from the list in the IMS Management Object. The other auto-configuration mechanisms (e.g. based on DHCP; based on the PCO info received during PDP context activation) are left out of the scope of this specification. An MNO may request an OEM to implement such functionality as a customization, however, the validation of this functionality will remain outside of the RCS-e compliance.

2.1.1 RCS-e client configuration storage

The RCS-e and, to extend, the IMS configuration should be stored securely in the handset and should not be accessible to the user unless express requirement of a particular MNO.

It should be noted that a precondition to provide access to the RCS-e functionality should be that all the mandatory parameters described in section 2.1 (Table 6) must be correctly configured. In the case any of the parameters is not configured or configured with an unexpected value, the RCS-e functionality should be disabled and in any case presented or accessible to the user (i.e. the phone behaves as it would be a non-RCS-e enabled phone). In this state, the RCS-e functionality can be only restored by completing the first-time registration procedure (see section 2.2.2.1; the first-time registration includes the RCS-e client configuration using one of the procedures described in section 2.2.2.1.2).

If a RCS-e configured device is reset, the RCS-e client should securely back up the configuration in the device together with the associated IMSI prior to the reset. Please note that this also applies in the event of swapping SIM cards. The configuration associated to the old SIM should also be securely backed up before triggering a first time registration.

The motivation behind the RCS-e configuration backup is to facilitate the scenario where following a reset or after a SIM swap, the original SIM card is re-introduced in the device. Instead triggering a first time registration, the RCS-e configuration is restored.

In those terminals where the processes mentioned in the previous paragraphs (reset, SIM card swap), the terminal also deletes the contacts (e.g. for example a particular MNO is enforcing this sort of policy where a SIM swap causes the deletion of the contacts), the associated RCS-e information (i.e. cached capabilities per contact and RCS-e contact list) should be also removed. Please note that in this case, the RCS-e information associated to contacts is not backed up.

2.2 *Registration process*

The RCS-e registration process uses the standard IMS registration procedure. The client sends a SIP REGISTER message to the network using the configuration parameters (SIP proxy as presented in Table 5). If supported, the network shall authenticate the message using single sign-on (SSO/GIBA) authentication.

When SSO/GIBA authentication fails (e.g. the MNO equipment does not support it or it is not supported over Wi-Fi), then digest authentication will be performed. This authentication mechanism is based on a challenge which the network sends to the client and which needs to be responded using the configured username/password pair (see Table 5 for reference).

Please note that in the flow diagrams contained in this document which involve a registration, we have assumed that:

- SSO/GIBA authentication takes place first
- If it fails (e.g. MNO network equipment does not support it) digest authentication is then tried

As part of the registration process, the network provides a validity period for the registration (SIP expire time). If the client is to remain registered after the registration validity period expires, it must register again.

Finally note that a precondition to register is that all the mandatory parameters presented in Table 5 and Table 6 should be correctly configured. In addition to this and if RCS-e is the only IMS based functionality available on the phone (i.e. no other IMS services like VoIP are incorporated), the precondition is extended to also have all the mandatory parameters presented in Table 6 correctly configured.

2.2.1 Additional message authentication

Depending on the network configuration, other SIP messages (apart from SIP REGISTER) may also require authentication. There are several authentication mechanisms that can be considered:

- SSO/GIBA authentication (transparent to the terminal as it is handled by the MNO core network)
- IMS AKA authentication
- Digest (user/password authentication)

For simplicity the present specification does only require terminals to implement digest authentication (required for some Wi-Fi scenarios) and SSO/GIBA (due to the lower impact on the terminal/client side). An MNO may request to add additional authentication mechanisms as a customization, however this functionality is outside the scope of this specification and, consequently, the associated verification is outside the RCS-e conformance.

It should be noted that in the following sections diagrams and with the aim of increasing the readability, we have assumed that SSO/GIBA authentication is successful when accessing through the PS network and, as mentioned before, digest authentication is used when accessing over a non-PS network (i.e. Wi-Fi scenarios).

In addition to the SIP messages, XCAP exchanges between the client and the XDMS server may also require authentication. For simplicity, mobile operator networks may use the same user credentials and authentication mechanism for both XCAP and SIP messages.

2.2.2 Registration process and scenarios

2.2.2.1 First-time registration

The assumptions in this case are that user A has been already provisioned to access the RCS-e services (e.g. the tariff includes the service) however he/she has never used a RCS-e enabled phone before.

Prior to the registration, it is necessary to provision the user on the network (known as auto provisioning) and to configure the client with the right settings. Once the auto provisioning and client configuration has completed, the first time registration procedure takes place. Once the client is provisioned, the first step is register and to find the subset among the existing contacts (if any) who are also RCS-e users.

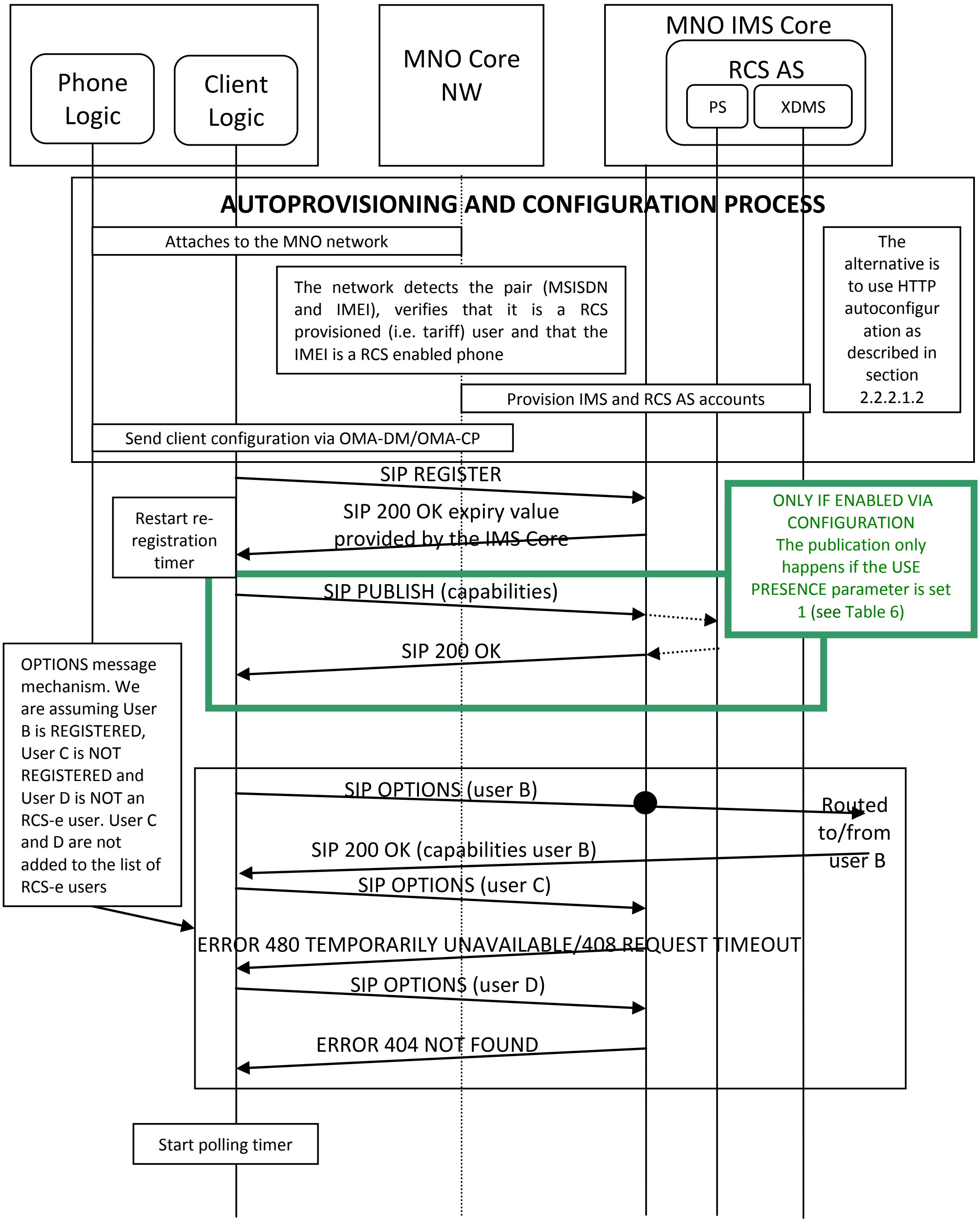

Phone Logic
Client Logic
MNO Core NW
MNO IMS Core
RCS AS
PS
XDMS
AUTOPROVISIONING AND CONFIGURATION PROCESS
Attaches to the MNO network
The network detects the pair (MSISDN and IMEI), verifies that it is a RCS provisioned (i.e. tariff) user and that the IMEI is a RCS enabled phone
Provision IMS and RCS AS accounts
The alternative is to use HTTP autoconfiguration as described in section 2.2.2.1.2
Send client configuration via OMA-DM/OMA-CP
SIP REGISTER
SIP 200 OK expiry value provided by the IMS Core
Restart re-registration timer
ONLY IF ENABLED VIA CONFIGURATION The publication only happens if the USE PRESENCE parameter is set 1 (see Table 6)
SIP PUBLISH (capabilities)
SIP 200 OK
OPTIONS message mechanism. We are assuming User B is REGISTERED, User C is NOT REGISTERED and User D is NOT an RCS-e user. User C and D are not added to the list of RCS-e users
SIP OPTIONS (user B)
Routed to/from user B
SIP 200 OK (capabilities user B)
SIP OPTIONS (user C)
ERROR 480 TEMPORARILY UNAVAILABLE/408 REQUEST TIMEOUT
SIP OPTIONS (user D)
ERROR 404 NOT FOUND
Start polling timer

Figure 4. First time registration sequence diagram

Note that if the terminal is configured to handle presence related functionality (USE PRESENCE set 1 as presented in Table 6), this process will be used to identify those contacts supporting the “social information via presence” and the capability discovery via presence functionalities. Additionally, and provided the capability discovery via presence functionality is enabled (see PRESENCE DISCOVERY parameters in Table 6), the terminal should also update the XDMS list of RCS-e contacts supporting this functionality as presented in Figure 16.

In the previous diagram we have referenced service provisioning and configuration.
When the handset is powered on, the network may be able to identify that the user/handset pair shall use RCS-e services and, as a consequence, trigger the relevant handset configuration. The triggering process is network specific and outside the scope of this specification.

An alternative to this automated mechanism could be a manually triggered configuration (e.g. requested by an operator in a store).

2.2.2.1.1 Additional first time configuration scenarios

In addition to the scenario described in the previous section (first time the user registers with the IMS network), there are several additional scenarios where same sequence applies:

- When the customer changes to another RCS-e enabled device: In this case, the sequence is identical with the only difference that the IMS provisioning (i.e. provision IMS and RCS AS accounts) is not required as it was performed before.
- When the customer changes the SIM card: In this case, the sequence is identical to the one described in the previous section.
- Configurations update implying changes in the user's IMS identity (i.e. TEL-URI and/or SIP-URI).
- A configuration update implying changes in the capability discovery mechanism: As presented later in the document, switching the capability discovery mechanism parameter automatically triggers the same process described in Annex A (section A.2) as a complement to the RCS Release 2 managed objects.

2.2.2.1.2 Autoconfiguration mechanisms

This specification contemplates three alternative mechanisms in order to perform the autoconfiguration of the RCS-e functionality in terminals:

- OMA-DM[5]: This is the same mechanism proposed for RCS and based on the managed object configuration proposed in Annex A, section A.2. All RCS-e capable handsets (incl. open-market devices) shall support following requirements for OMA-DM:
    - Multiple management authorities where operator DM accounts are persistent, not editable and not visible by the user (e.g. SW updates don't delete/overwrite DM accounts) and accessible by the respective active operator DM account only (protected by OMA DM ACL mechanism).
    - Active operator DM account needs to be selected and activated on SIM card change.
    - The settings are protected against non-operator authorities (by OMA DM ACL mechanism).
    - Each operator should have its own RCS-e management sub-tree and the DM account does have access to the device settings (e.g. for the purpose of access settings configuration if needed).

[5] Consistently with RCS Release 2 specifications, the OMA-DM version which shall be implemented for RCS-e device configuration is OMA-DM version 1.2.

  - Active operator RCS-e management sub-tree needs to be visible, selected and activated on SIM card change.
  - Settings are active/updated and used on RCS-e client after successful configuration.
- OMA-CP [6] : This is an alternative mechanism (considering OMA-DM as the preferred standard mechanism for RCS-e) based on the OMA-CP specific configuration proposed in Annex A, sections A.2 and A.3

Although the previous mechanisms are preferred, the RCS-e specification proposes an alternative optional mechanism which can be requested by a MNO (i.e. during customization) with the following main goals:

- Enabling a configuration procedure transparent to the user (OMA-CP drawback)
- Reducing autodetection mechanism complexity on network infrastructure

The new mechanism is based on a HTTP (HTTPS) request made by the handset to a configuration server to get the configuration data:

- Every time the handset boots (or when the SIM is swapped without rebooting the terminal [hot swap]), there is an initial HTTP request to the RCS-e configuration server to get the current configuration settings version
- In case the versions do not match, the server will include a configuration XML with all the settings. This configuration XML will be identical to the one used in OMA-CP (contents are covered in detail in Annex A, sections A.2 and A.3).
- If it is necessary to force a reconfiguration (e.g. SIM card swap), the handset will reset the version value to 0 (the server configuration shall always have a value bigger than 0).
- If the MNO has to disable the RCS-e functionality from a handset/client, the response will be an empty XML setting the version to 0.
- The detailed on the exchanges (e.g. format employed for the requests) are covered below:

This alternative configuration mechanism works on the following pre-assumptions:

- As a security measure and to make sure the network can implement the necessary procedures to resolve the user's MSISDN (i.e. RADIUS requests, header enrichment, etc.), the configuration can only take place if connected using an MNO PS[7] data network and, therefore, the handset should have the necessary APN configuration to perform the connection.

- Because some of those mechanisms presented in the previous paragraph require an initial HTTP request, the proposal is first to perform an HTTP request:

[6] The OMA-CP version which shall be implemented for RCS-e device configuration is OMA-CP version 1.1.

[7] Please note that if a device does not have a PS connection, the autoconfiguration can also happen over WiFi. The decision to implement this mechanism is up to the discrection of each MNO.

- The handset/client performs a HTTP request to the RCS-e autoconfiguration server qualified domain name. In this initial request the relevant GET parameters (e.g. version) should not be included.
- As a result of this request, the autoconfiguration server returns an HTTP OK response. Then the client will then perform a second request, this time HTTPS (same URL, only the protocol change). Note that the RCS-e configuration server should be able to correlate both http and https requests on the server side. In order to achieve this, the server will setup a cookie in the response to the initial HTTP request (Set-Cookie header) and it will expect to receive that cookie in the subsequent HTTPS request (Cookie header).

- From the UX point of view, the customer is not aware of the configuration process (i.e. background process with no pop-ups or notifications shown on the screen).

It should also be noted that this mechanism also contributes to reduce the complexity of the auto-detection mechanism because the handset will proactively request an update of the configuration settings every time the handset is rebooted.

<u>RCS-e Initial configuration request:</u>

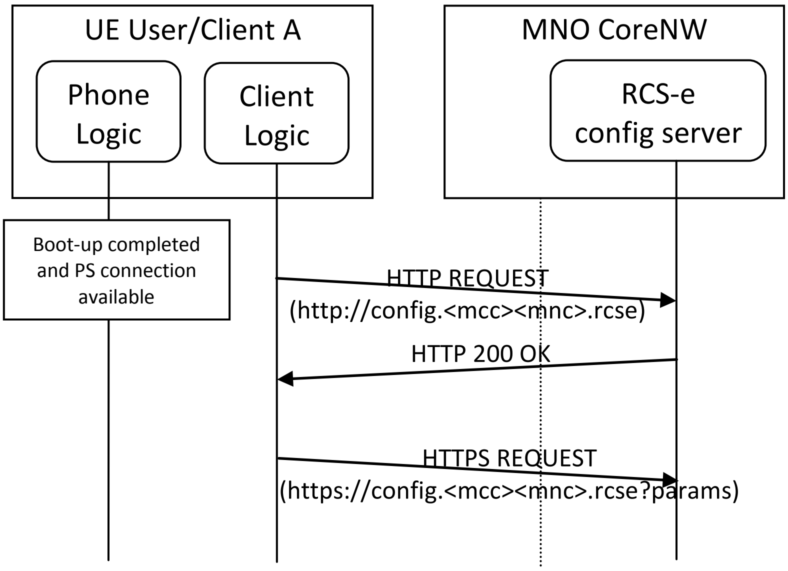

UE User/Client A
Phone Logic
Client Logic
MNO CoreNW
RCS-e config server
Boot-up completed and PS connection available
HTTP REQUEST
(http://config.<mcc><mnc>.rcse)
HTTP 200 OK
HTTPS REQUEST
(https://config.<mcc><mnc>.rcse?params)

Figure 5. RCS-e alternative configuration: Initial request

- Parameters: The following information is passed as GET parameters:

Parameter	Description	Mandatory	Format
vers	This is either -1, 0 or a positive integer. 0 indicates that the configuration must be updated (e.g. configuration is damaged, non-existent or follows a SIM change). A positive value indicates the version of the static parameters (those which are not subscriber dependent) so the server can evaluate whether	Y	Int (-1, 0 or a positive integer)
IMSI	If available, the subscriber's IMSI should be sent as a parameter	N (if the OS platform allows it, it shall be included)	String (15 digits)
client_vendor	String that identifies the vendor providing the RCS-e solution.	Y	String (4)
client_version	String that identifies the RCS-e solution version.	Y	String (10 max)
terminal_vendor	String that identifies the terminal OEM.	Y	String (4)
terminal_model	String that identifies the terminal model.	Y	String (10 max)
terminal_sw_version	String that identifies the terminal software version..	Y	String (10 max)
IMEI	If available, the subscriber's IMEI should be sent as a parameter. The idea is that for those MNOs supporting a comprehensive handset database, the terminal_X parameters can be then ignored and the IMEI used instead, of course, if available to the RCS-e	N (if the OS platform allows it, it shall be included)	String (15 digits)

Table 7. RCS-e alternative configuration: HTTPS request GET parameters

Please note that the client and terminal vendor, model and version parameters format and values should be agreed with the relevant MNO prior to any handset or client commercialization or update.

- The configuration server URL will follow the RCS-e specification version 1.1 standard:
    - http://config.<mcc><mnc>.rcse (e.g. http://config.21401.rcse)
- The application then will check MCC and MNC in the IMSI and complete the prior name depending on the MNO.
- Please note this URL is only routable from the PS domain so the autoconfiguration can only happen via PS.

In case a handset is employed in an MNO that does not support RCS-e, this domain will not be resolved, so the application will take it as a client not valid scenario.

RCS-e configuration server response:

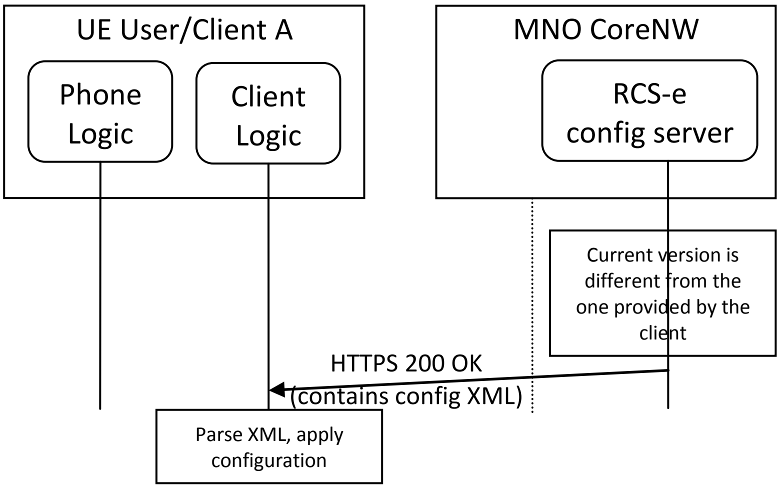


Figure 6. RCS-e alternative configuration: Server response

- The server first validates the client and terminal parameters and then checks if the version provided by the client matches the latest version of the configuration available on the server.
  - The response will always contain two parameters:
    - The configuration version
    - The validity of the configuration in seconds
  - If the version matches (i.e. no new configuration settings required), the configuration XML will be empty except for the version and the validity parameters:
    - The version parameter will be set to the same value sent in the request
    - The validity parameter will be reset to the server configured value

```
<?xml version="1.0"?>
      <wap-provisioningdoc version="1.1">
            <characteristic type="VERS">
                  <parm name=”version” value=”X”/>
                  <parm name=”validity” value=”X”/>
            </characteristic>
      </wap-provisioningdoc>
```

Table 8. RCS-e alternative configuration empty XML (no configuration changes required)

- If the MNO would like to disable the RCS-e functionality from a handset/client, the response will be a XML containing only the version set to 0:

```
<?xml version="1.0"?>
      <wap-provisioningdoc version="1.1”>
            <characteristic type="VERS">
                  <parm name=”version” value=”0”/>
                  <parm name=”validity” value=”0”/>
            </characteristic>
      </wap-provisioningdoc>
```

Table 9. RCS-e alternative configuration empty XML (reset RCS-e client)

- Please note that even RCS-e is disabled on the phone, the phone should still perform the autoconfiguration query every time the phone is booted up.
    - If the MNO would like to disable the RCS-e functionality from a handset/client including the autoconfiguration query performed at boot, the response will be a XML containing only the version and the validity set to -1:
        - Note that if the SIM is swapped or the terminal resetted, the terminal should again query for configuration settings on every boot.

```
<?xml version="1.0"?>
      <wap-provisioningdoc version="1.1”>
            <characteristic type="VERS">
                  <parm name=”version” value=”-1”/>
                  <parm name=”validity” value=”-1”/>
            </characteristic>
      </wap-provisioningdoc>
```

Table 10. RCS-e alternative configuration empty XML (reset RCS-e client and stop autoconfiguration query)

- If the case the server has an updated configuration, the response will contain a configuration XML (i.e. content-type text/xml) configuration that the client needs to parse and apply:
    - The XML format is identical to the one use for OMA-CP configuration (see Annex A, sections A.2 and A.3) with a new parameter addition to include the version, the validity and the message section. A sample of the complete autoconfiguration XML is provided for reference in section A.4.

Any other response different from the ones described in this section (i.e. an HTTP error) should trigger the handset/client to try to get the configuration settings the next time the handset boots (or the client is started) and in the particular case of a 403 error, the handset/client implementation shall also remove the current configuration (as a validity=version 0 response is received).

User messages delivered within autoconfiguration

As an optional addition (i.e. the new tag may not be present), the XML can be used to convey a user message associated to the result of an autoconfiguration server response. The additional XML section is displayed below:

```
<?xml version="1.0"?>
      <wap-provisioningdoc version="1.1”>
            …
            <characteristic type="MSG">
                  <param name=”title” value=”Example”/>
                  <param name=”message” value=”Hello world”/>
                  <param name=”Accept_btn” value=”1”/>
                  <param name=”Reject_btn” value=”0”/>
            </characteristic>
            …
      </wap-provisioningdoc>
```

Table 11. RCS-e alternative configuration: User notification/message sample

The meaning of the different parameters is the following:

- **Title:** The window title where the message is displayed.
- **Message:** This is the message which has to be displayed to the user. Please note the message may contain references to HTTP addresses (websites) that need to be highlighted an converted into links by the terminal/client.
- **Accept_btn:** This indicates whether the “Accept” button is shown underneath the message box. The action associated to the Accept button on the terminal/client side is always to clear the message box.
- **Reject_btn:** This indicates whether the “Decline” button is shown underneath the message box. The action associated to the Reject button on the terminal/client side is always to disable the RCS-e switch setting in the handset.

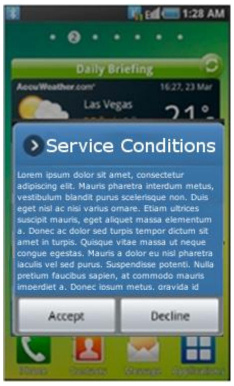
The MSG characteristic is optional and will be only present in two kind of responses:

- The one containing the full configuration settings.
- The one disabling the RCS-e configuration on the phone (version and validity set to 0).

The handset should display the message and the relevant/configured buttons in the following scenarios:

- After receiving the full configuration settings, only if:
    - No working configuration was available before
    - Following a terminal reset
    - Following a SIM swap no working configuration was available (backup) for that SIM
- After receiving the disabling RCS-e configuration response.

Finally, it should be noted that the RCS-e handset/client needs to send the language locale settings to the server as the language the message is served depends on this parameter. In order to do so, the client should use the HTTP Accept-Language header in all the requests and set the value consistently with the handset locale.



Service Conditions

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Mauris pharetra interdum metus, vestibulum blandit purus scelerisque non. Duis eget nisl ac nisi varius ornare. Etiam ultrices suscipit mauris, eget aliquet massa elementum a. Donec ac dolor sed turpis tempor dictum sit amet in turpis. Quisque vitae massa ut neque congue egestas. Mauris a dolor eu nisl pharetra iaculis vel sed purus. Suspendisse potenti. Nulla pretium faucibus sapien, at commodo mauris imperdiet a. Donec ipsum metus, gravida id

Figure 7. Autoconfiguration server notification example

<u>Use cases review:</u>

Although it has been already introduced, in this chapter we try to compile the different use cases so we have a clear picture of what will be the device behaviour on each scenario.

1 **First detection**: is the first time a client is using an RCS-e device. If the process goes well the device will receive the proper configuration XML. One of the parameters sent is the validity period. If the device has no problem in the registration process, it won´t ask the server again until the validity has expired. As it has been mentioned, this process could require some retries until the provisioning in IMS is performed.
Please note that for those RCS-e embedded implementations, the handset RCS-e related UX should remain disabled (i.e. vanilla behaviour) until a valid configuration is received.

2 **Version checking: no changes.** If the validity has expired, or the client has been asked to retry again the device will send a request in order to check if the configuration it has is the proper one. If the version it has is the last one, the client will receive a XML containing only the same version with the validity reset to the value specified in the server. That means that the configuration the handset/client currently has is correct and, consequently, the validity is renewed.

3 **Version checking: new version available.** If a new version of some of the fixed parameters (i.e. registration IP) or if the client has asked for a reconfiguration through Customer Care, the user will receive a new configuration XML the next time it asks for a new version

4 **Validation process is not OK.** If either the RCS-e handset/client or customer are not (longer) allowed to access the RCS-e service, the device will receive an XML with the version and validity set to 0. **Consequently, the handset/client must remove the existing configuration and remove the RCS-e specific UX (i.e. vanilla behaviour).**

5 **SIM change:** If the SIM changes, the previous configuration should be backed up and the handset/client should behave as not configuration is available (i.e. first-time configuration) and, therefore, make a request for new configuration. Please note that the exception that if there was already a configuration backup associated

to the new SIM available on the handset/client, the validity should be checked and, if still valid, it should be used instead making a new request.

6 **User with different RCSe devices.** If the client is using different RCS-e devices, the same configuration will be valid for all. The described process will ensure the device he/she is currently using has the last version.

7 **User asks Customer Care to disable the RCS-e service.** In this case the user will be unprovisioned on IMS network, and the following times the application asks for a reconfiguration it will always receive an XML with version and validity set to 0. The process will be that way until the time the user requests Customer Care to be re-provisioned. **Consequently, the handset/client must remove the existing configuration and remove the RCS-e specific UX (i.e. vanilla behaviour).**

Please notice that all the scenarios described fit with one of the following behaviours of the application on the device:

- The first time the RCS-e handset/client implementation, if does not have the proper configuration (version 0 or it is not able to complete registration process), will send a request every time a boot sequence is completed (or when the client is restarted).
- If it has received the proper configuration it won´t ask for a new version unless:
    - the validity period has expired, or,
    - it is not able to complete IMS registration
- If the response of the server is 503 Retry-After, it will retry the request after the time specified in the “Retry-After” header.
- If any other error occurs (e.g. not able to resolve the URL or getting an error from the autoconfiguration server) the application will retry the next time it reboots:
    - In the particular case of a 403, the existing configuration should be removed from the handset implementation/client.
    - In other error case scenarios (e.g. a 500 Internal Error is issued by the autoconfiguration server or the autoconfiguration server is not reachable), if there is valid configuration, the terminal/client should keep using it even expired.
    - The following notes apply to both 403 and other errors:
        - Please note that to cover that scenarios where a handset migrates to a network without RCS-e support, the number of unsuccessful consecutive retries is set to 20.
        - If the error persists, the RCS-e behaviour is disabled (both general RCS-e behaviour if valid configuration still available and the autoconfiguration sequence at boot).
        - Again, if the SIM is swapped or the terminal resetted, the terminal should again query for configuration settings on every boot.

Finally and to complete all the possible responses scenarios (including error cases), please find the possible responses in the following table:

Response	Use case	Client behaviour	Reject option/action
200 OK	Initial HTTP request response	The client sends the HTTPS request including the cookie	No
503 Retry after	The server is processing the request/provision.	Retry after the time specified in the "Retry-After" header	No
200 OK + XML with full configuration	New configuration sent to the terminal	Process configuration, try to register and if successful, not try reconfiguration until the validity period is expired	Only if no working configuration before
200 OK + XML with version and validity period only	No update needed	Retry only after validity period	No
200 OK + XML with version and validity period only and both set to 0	Customer or device are not valid or the customer has been unprovisioned from RCS-e	Retry only after validity period If a configuration was available, it should be removed from the client.	Always
200 OK + XML with version and validity period only and both set to -1	Customer or device are not valid or the customer has been unprovisioned from RCS-e	The client should no longer retry autoconfiguration until SIM is changed or a factory reset performed. If a configuration was available, it should be removed from the client.	Always
500 Internal Server error (or any other HTTP error except 403)	Internal error during configuration/provision	Retry on next reboot (validity is ignored), next time the client starts	N/A
403 Forbidden	Invalid request (e.g. missing parameters, wrong format)	The configuration is removed in the handset and version is set to 0. Retry on next reboot, next time the client starts (ignoring validity)	N/A
The autoconfiguration server is not reachable	Autoconfiguration server missing or down	Retry on next reboot (validity is ignored), next time the client starts	N/A

Table 12. Summary of RCS-e autoconfiguration responses and scenarios

Security considerations:

The current design relies on the fact that it is not possible to perform a man-in-the-middle attack where a 3rd party can impersonate the configuration server because we are connecting over PS.

To secure interoperability between MNOs and to reduce the complexity on the handset/client implementation, the usage of public root certificates issued by a recognized CA is encouraged (such as those used by standard webservers which are widely recognized by browsers and web-runtime implementations both in PCs and handsets).

2.2.2.2 Registration

User A is provisioned for service and the first/time registration has already taken place. The user was not registered is now trying to perform a registration using PS, and therefore assuming that SSO/GIBA authentication is available:

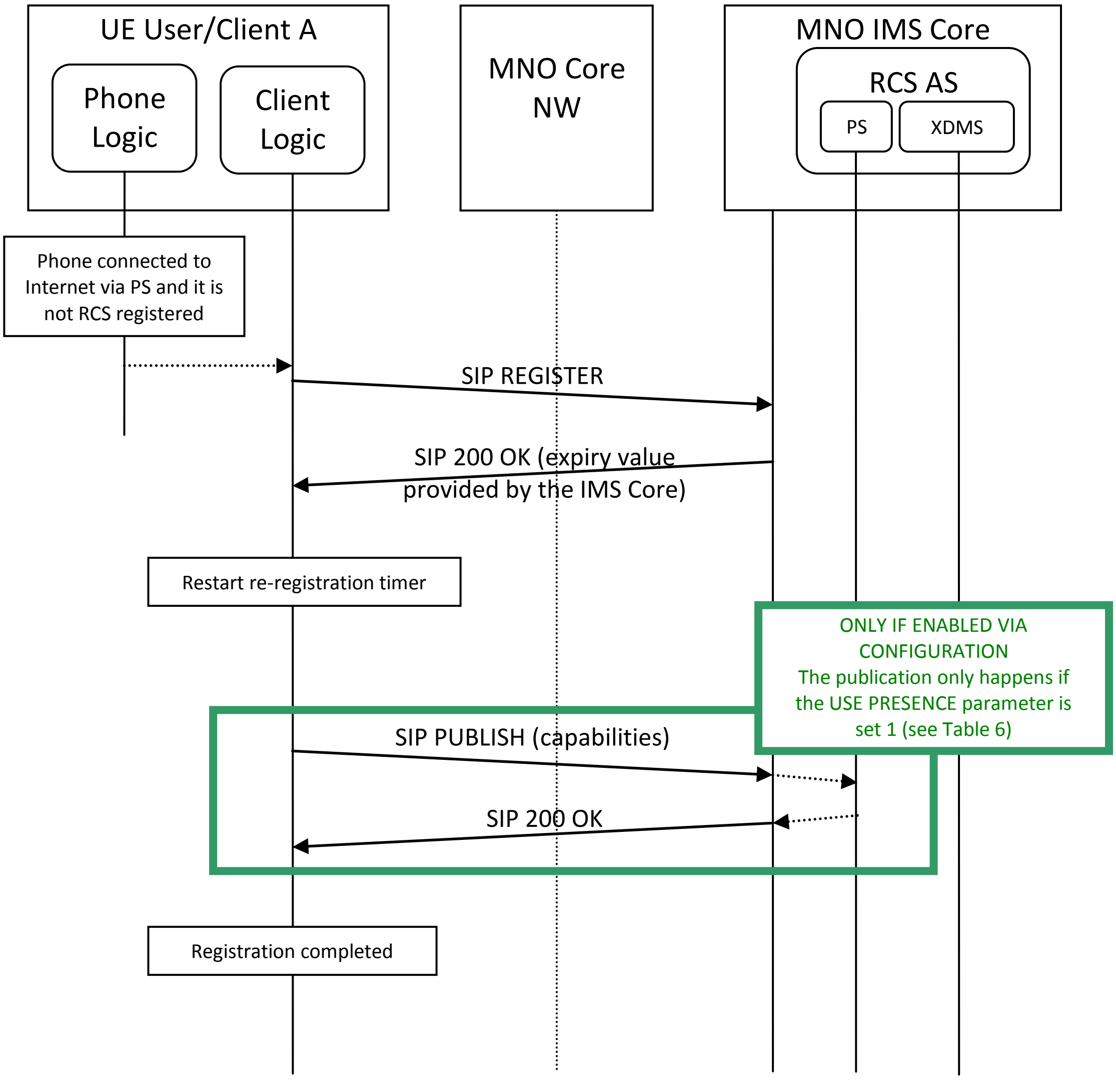

UE User/Client A
Phone Logic
Client Logic
MNO Core NW
MNO IMS Core
RCS AS
PS
XDMS
Phone connected to Internet via PS and it is not RCS registered
SIP REGISTER
SIP 200 OK (expiry value provided by the IMS Core)
Restart re-registration timer
ONLY IF ENABLED VIA CONFIGURATION
The publication only happens if the USE PRESENCE parameter is set 1 (see Table 6)
SIP PUBLISH (capabilities)
SIP 200 OK
Registration completed

Figure 8. Registration from offline over PS (assuming SSO/GIBA)

If the initial authentication (SSO/GIBA) fails (i.e. the MNO equipment does not support it or the user is trying to register via Wi-Fi), the client must then retry using digest authentication (USER + PASSWORD).

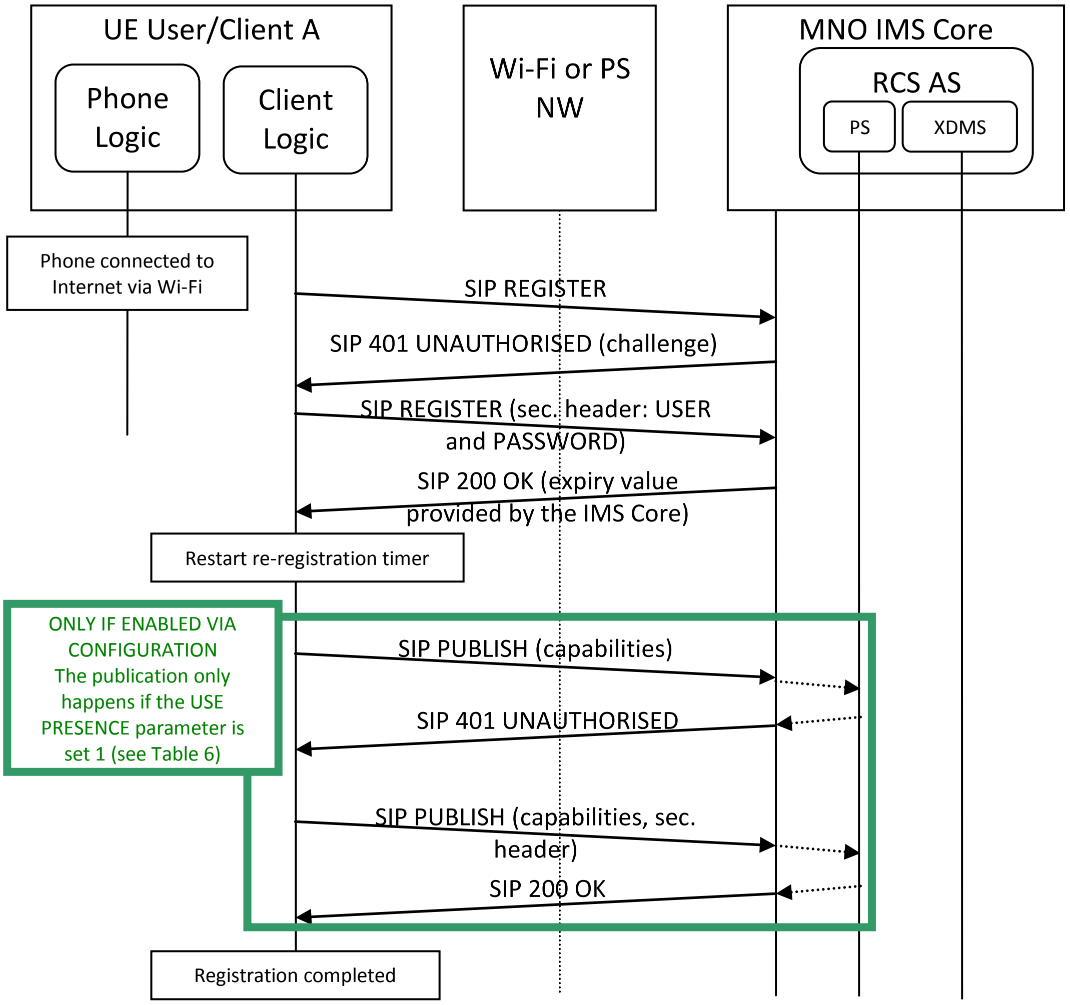

UE User/Client A
Phone Logic
Client Logic
Wi-Fi or PS NW
MNO IMS Core
RCS AS
PS
XDMS
Phone connected to Internet via Wi-Fi
SIP REGISTER
SIP 401 UNAUTHORISED (challenge)
SIP REGISTER (sec. header: USER and PASSWORD)
SIP 200 OK (expiry value provided by the IMS Core)
Restart re-registration timer
ONLY IF ENABLED VIA CONFIGURATION The publication only happens if the USE PRESENCE parameter is set 1 (see Table 6)
SIP PUBLISH (capabilities)
SIP 401 UNAUTHORISED
SIP PUBLISH (capabilities, sec. header)
SIP 200 OK
Registration completed

Figure 9. Registration from offline over Wi-Fi or PS networks without SSO/GIBA authentication support

Please note that in the same scenarios and provided the terminal is configured to handle presence related functionality (USE PRESENCE set 1 as presented in Table 6), it should be noted that:

- The publication shall follow the procedures defined in [RCS1-TEC-REAL][8] and [RCS2-TEC-REAL] [9] (e.g. use of the defined Service-descriptions and the PublishTimer expiry timer) .
- XCAP exchanges shall anyway support XCAP exchanges according to the procedure defined in [RCS1-TEC-REAL] and [RCS2-TEC-REAL] and authentication parameters defined in [RCS2-TEC-REAL]). In addition to this, the XDMS exchanges may also use the same security mechanism based on digest authentication using the same parameters as for SIP messages:

[8] Rich Communication Suite Release 1 Technical Realization 2.0, 14 February 2011
[9] Rich Communication Suite Release 2 Technical Realization 2.0, 14 February 2011

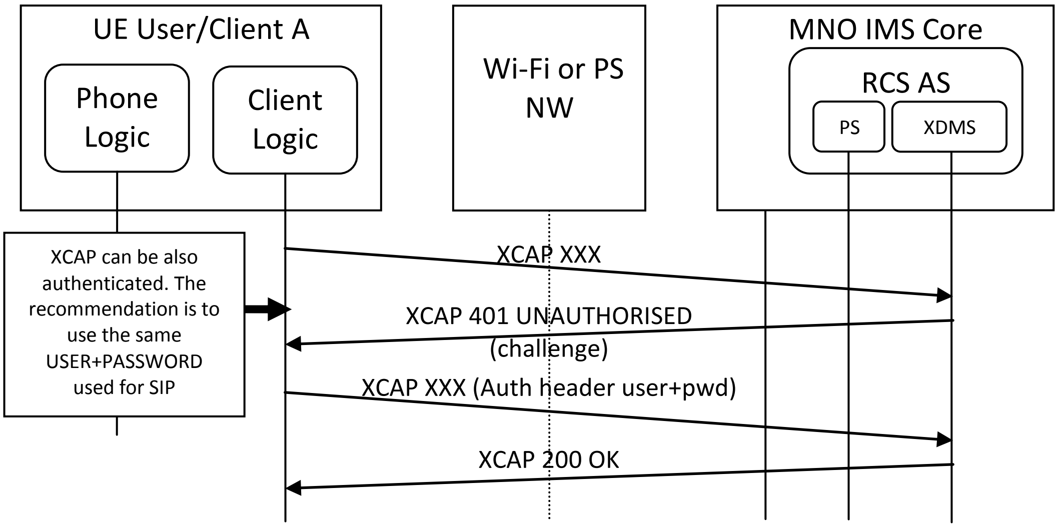

UE User/Client A
Phone Logic
Client Logic
Wi-Fi or PS NW
MNO IMS Core
RCS AS
PS
XDMS
XCAP can be also authenticated. The recommendation is to use the same USER+PASSWORD used for SIP
XCAP XXX
XCAP 401 UNAUTHORISED (challenge)
XCAP XXX (Auth header user+pwd)
XCAP 200 OK

Figure 10. XCAP exchanges when using digest authentication

2.2.2.3 Re-registration

User A is already registered, however registration expires (timer since last registration reaches the expiry value provided by the network). In this case, the client needs to re-register following the flow presented below. Please note for simplicity, in the following diagram we have assumed that SSO/GIBA authentication is available.

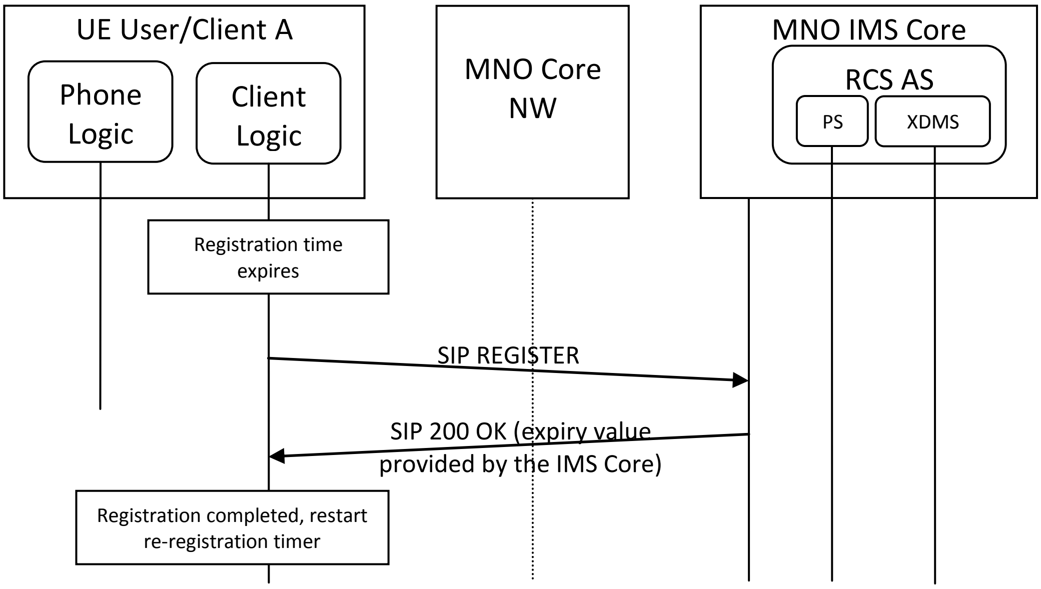

UE User/Client A
Phone Logic
Client Logic
MNO Core NW
MNO IMS Core
RCS AS
PS
XDMS
Registration time expires
SIP REGISTER
SIP 200 OK (expiry value provided by the IMS Core)
Registration completed, restart re-registration timer

Figure 11. Re-registration

2.2.2.4 Deregistration

User A is registered however based on the phone logic, the connexion to the service is no longer possible. Among the possible reasons, we have listed the most relevant:

- powering down, battery low,…

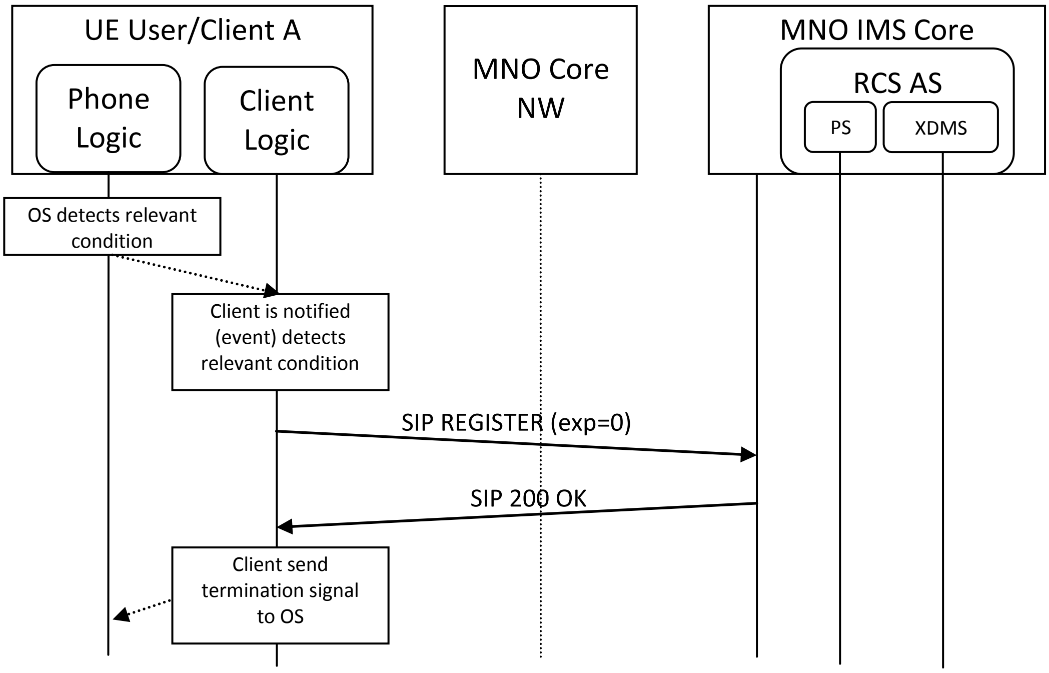

UE User/Client A
Phone Logic
Client Logic
MNO Core NW
MNO IMS Core
RCS AS
PS
XDMS
OS detects relevant condition
Client is notified (event) detects relevant condition
SIP REGISTER (exp=0)
SIP 200 OK
Client send termination signal to OS

Figure 12. Deregistration

2.2.2.5 Registration status and available capabilities

In case the registration process is not successful or following a deregistration, the user should not be able to access any RCS-e service and all RCS-e contacts services/capabilities shall be reported to the user as not available independently of any setting (e.g. the IM CAP ALWAYS ON setting presented in Table 6 is ignored).

2.2.2.6 Registration frequency optimization

RCS-e client shall not send more register request than what is needed to maintain the registration state in the network. When the IP connectivity is lost and restored with the same IP address, the RCS-e client shall:

- only send a register refresh upon retrieval of IP connectivity if the duration for sending a register-refresh since the last register has been exceeded,
- only send an initial register upon retrieval of IP connectivity if the registration has expired, and,
- not send de-register request upon imminent loss of IP connectivity.

2.3 *Capability discovery*

The capability or service discovery mechanism is key to RCS-e. The capability discovery is a process which enables a user to understand the subset RCS-e services which are available to access and/or communicate with other contacts at certain point of time.

2.3.1 Capability discovery process through OPTIONS message

The primary and mandatory method for capability discovery is based on the SIP OPTIONS message, a peer-to-peer message exchanged between clients.

When a SIP OPTIONS message is sent from User A to User B, User A will receive one of 3 types of response:

1) User B is Registered and the response from User B's client will comprise CAPABILITY STATUS – the set of services currently available (using tags as described in section 2.3.1.1).
    - Note the response must contain, at least, the RCS-e IM tag *(+g.3gpp.iari-ref="urn%3Aurn-7%3A3gpp-application.ims.iari.rcse.im"*). If it is not contained there, the response will be equivalent to the case presented below in bullet 3.
2) If User B is currently not registered (e.g. phone is off), then the network will respond with one of the following message error: 480 TEMPORARILY UNAVAILABLE (graceful deregistration took place) or 408 REQUEST TIMEOUT.
3) If User B is not provisioned for RCS-e the network will respond with a message error: 404 NOT FOUND[10].

Note that from a user experience perspective response 2) [11] and 3) are the same and no RCS-e services will be shown to User A as available to communicate with User B.

The SIP OPTIONS message shall be sent in the following scenarios:

- post first time registration to obtain the registration state and default set of capabilities for each contact in the phone address book (note one SIP OPTIONS is sent per IMS identity [i.e. TEL-URI/MSISDN or SIP-URI] stored in the address book)[12],
- when a new contact is added to the phone address book,
- periodically (frequency determined by the POLLING PERIOD parameter as presented in section 2.1 Table 6) to all the contacts in the phone address book whose capabilities are not available (e.g. non-RCS-e users) or are expired (see CAPABILITY INFO EXPIRY parameter in section 2.1 Table 6 for reference),

[10] Please note that the response provided may depend on the network configuration. A better approach for the terminal is to parse the response and if it is not either a 200 OK containing the capabilities as feature tags, a 480 TEMPORARILY UNAVAILABLE or a 408 REQUEST TIMEOUT, the target user should be considered as non-RCS. For simplicity, the present document assumes in the following sections that the response provided by the MNO core network is always 404 NOT FOUND, however, the previous statement should be taken into account.

[11] Please note that in this case if IM CAP ALWAYS ON (see Table 6) is enabled, the IM/chat should still be reported to the user as available even the other end is not registered.

[12] Please note a contact may have several MSISDNs or associated SIP-URIs. The client will use ALL the user's MSISDNs/SIP-URIs to send SIP OPTIONS messages. If it is discovered that more than one of the associated TEL-URIs/SIP-URIs are IMS provisioned, each will be treated as a separate RCS-e user. For example, if displaying the list of RCS-e contacts, two or more entries for a user will be shown ("John Smith mobile" and "John Smith home"), so the user can choose.

- when a contact's primary MSISDN is modified or a new MSISDN is added (where users have several subscriptions and each subscription is potentially associated with a RCS-e account),
- when checking the available RCS-e services/capabilities to communicate with another user (e.g. from the address book and call-log),
- after the establishment voice call to obtain the real-time capabilities for the call or IM session provided this has not been performed before (see previous bullet),
- during a voice call, file transfer or IM session when the relevant available capabilities change, and,
- when there is a communications event (text, email, call or IM) with another user in the address book.

Please note that in some cases it is not required because the options exchange just happened shortly before the communication takes place (e.g. to send the SMS, the user went to the addressbook, selected a user [options exchange takes place] and chooses to send a SMS).

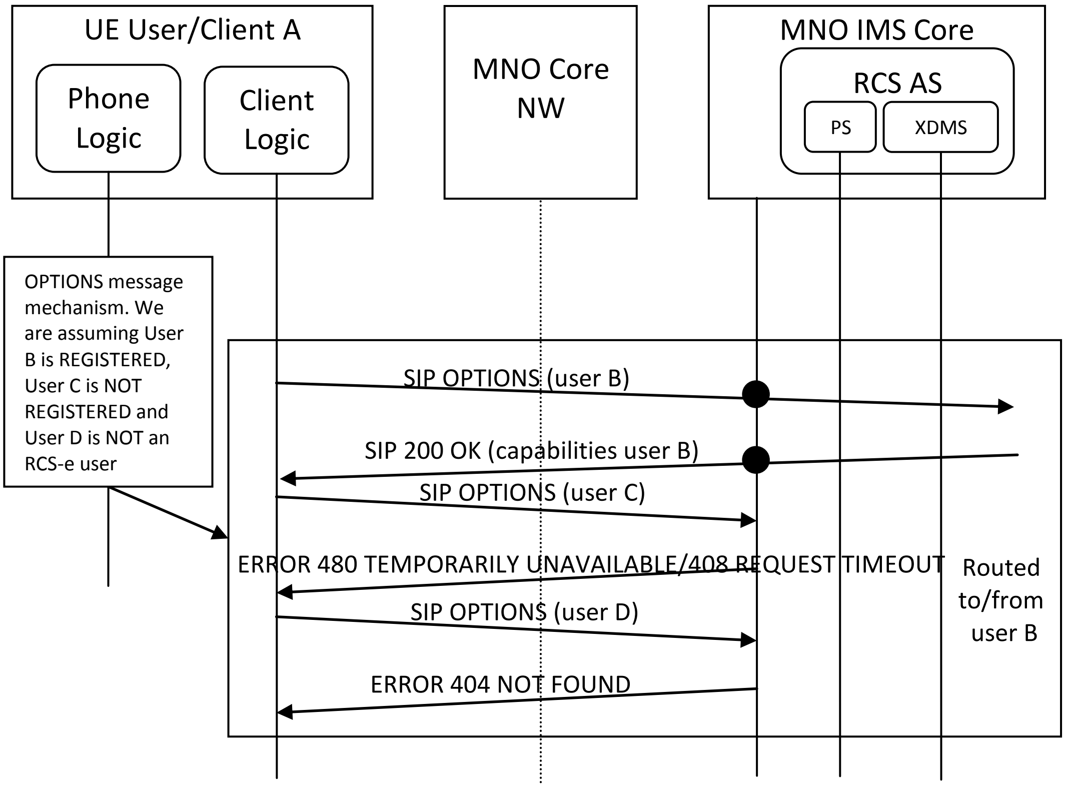

UE User/Client A
Phone Logic
Client Logic
MNO Core NW
MNO IMS Core
RCS AS
PS
XDMS
OPTIONS message mechanism. We are assuming User B is REGISTERED, User C is NOT REGISTERED and User D is NOT an RCS-e user
SIP OPTIONS (user B)
SIP 200 OK (capabilities user B)
SIP OPTIONS (user C)
ERROR 480 TEMPORARILY UNAVAILABLE/408 REQUEST TIMEOUT
SIP OPTIONS (user D)
ERROR 404 NOT FOUND
Routed to/from user B

Figure 13. Capabilities discovery via SIP OPTIONS message

2.3.1.1 SIP OPTIONS message extension to support capability discovery

The RCS (Release 1 and 2) specifications only provide a mechanism to exchange the capability status (based in SIP OPTIONS exchange) regarding to image and video share services during a call. This mechanism is based in the use of tags contained transported in the *Accept-contact* and *Contact* headers for the SIP OPTIONS and its responses:

- The tags corresponding to the set of functionalities supported by the requesting terminal at the time this request is made are carried in both the Contact and Accept-contact headers of the SIP OPTIONS message.
- The tags corresponding to the subset of the functionalities that are supported by the receiver are included in the Contact header of the 200 OK response.

Consequently with the RCS Release 2 specification, the following tags can be employed to identify image and video share service capabilities:

RCS-e service	Tag
Image share	+g.3gpp.iari-ref="urn%3Aurn-7%3A3gpp-application.ims.iari.gsma-is"
Video share	+g.3gpp.cs-voice

Table 13. Standard RCS Release 2 SIP OPTIONS tags

In order to support the full service discovery functionality consistently presented in this document, it is necessary to extend the tag mechanism by performing the following changes:

- There is one unique tag (*+g.oma.sip-im*) traditionally assigned to two services (IM and file transfer). Nevertheless and in order to both uniquely identify RCS-e clients and provide per service capability granularity the following changes are introduced:
    - *+g.3gpp.iari-ref="urn%3Aurn-7%3A3gpp-application.ims.iari.rcse.im"* tag is used ONLY to identify the RCS-e IM service[13], and,
    - *+g.3gpp.iari-ref="urn%3Aurn-7%3A3gpp-application.ims.iari.rcse.ft"* tag is defined to uniquely identify file transfer service

RCS-e service	Tag
IM/Chat	+g.3gpp.iari-ref="urn%3Aurn-7%3A3gpp-application.ims.iari.rcse.im"
File transfer	+g.3gpp.iari-ref="urn%3Aurn-7%3A3gpp-application.ims.iari.rcse.ft"

Table 14. Additional tags to cover the remaining RCS-e services

- For those clients supplementing the RCS-e functionality with the *"social information via presence"*[14] functionality (i.e. the PRESENCE PROFILE parameter is set to 1; see Table 6), a new tag is defined to represent such features:

[13] Although the RCS-e IM service is based and endorses the OMA-IM definition, it comes with some customizations and additional functionalities which make the potential interaction with standard OMA-IM clients non-ideal from the UX point of view. Consequently, a new tag has been defined to signal that differences and distinguish the RCS-e IM service for non-RCS-e clients supporting the standard OMA-IM functionality.

[14] By this term we are referring to the set of functionalities defined in the RCS Release 1 and Release 2 standards and presented in [RCS1-TEC-REAL] in sections from 2.1.2 to 2.1.6.

  - The *+g.3gpp.iari-ref="urn%3Aurn-7%3A3gpp-application.ims.iari.rcse.sp"* tag identifies the contacts supporting the *"social information via presence"* features.

- For those clients willing to implement a discovery mechanism based on presence (i.e. the PRESENCE DISCOVERY parameter is set to 1; see Table 6), independently on whether the *"social information via presence"* functionality is supported or not, a new tag is defined:
  - The *+g.3gpp.iari-ref="urn%3Aurn-7%3A3gpp-application.ims.iari.rcse.dp"* tag identifies the contacts supporting capability discovery via presence.

RCS-e service	Tag
IM/Chat	+g.3gpp.iari-ref="urn%3Aurn-7%3A3gpp-application.ims.iari.rcse.im"
File transfer	+g.3gpp.iari-ref="urn%3Aurn-7%3A3gpp-application.ims.iari.rcse.ft"
Image share	+g.3gpp.iari-ref="urn%3Aurn-7%3A3gpp-application.ims.iari.gsma-is"
Video share	+g.3gpp.cs-voice
Social presence information	+g.3gpp.iari-ref="urn%3Aurn-7%3A3gpp-application.ims.iari.rcse.sp"
Capability discovery via presence	+g.3gpp.iari-ref="urn%3Aurn-7%3A3gpp-application.ims.iari.rcse.dp"

Table 15. Complete SIP OPTIONS tag proposal for RCS-e

Please note that the new tags defined in this section should be ONLY employed for SIP OPTIONS exchanges and that the standard tags should be used to identify the services in the rest of relevant SIP transactions (i.e. *+g.oma.sip-im for chat/IM*). Note also that the *+g.oma.sip-im* feature tag may also be listed during this OPTIONS exchange.

Finally, it should be taken into account that when several IARI tags are included in an option request, and consistently with [RCS4- TEC-REAL] section 3.2, IARI tags shall be concatenated using commas as described in the example below:

```
+g.3gpp.iari-ref="urn%3Aurn-7%3A3gpp-application.ims.iari.rcse.im,urn%3Aurn-7%3A3gpp-application.ims.iari.rcse.ft"
```

Table 16. IARI tag concatenation format example

2.3.1.2 Future extensions to the mechanism

In addition to the mentioned additions and to allow a MNO (or group of MNOs) to deploy additional services which can also benefit from the RCS-e discovery mechanism, an additional tag format is defined:

- *+g.3gpp.iari-ref=*"*urn%3Aurn-7%3A3gpp-application.ims.iari.rcse.<operatorID>.<service name>*"[15]
- Valid examples are:
  - +g.3gpp.iari-ref="urn%3Aurn-7%3A3gpp-application.ims.iari.*rcse.*OR.serviceA"
  - +g.3gpp.iari-ref="urn%3Aurn-7%3A3gpp-application.ims.iari.*rcse.*TEL.serviceB"
  - +g.3gpp.iari-ref="urn%3Aurn-7%3A3gpp-application.ims.iari.*rcse.*TI.serviceC"
  - +g.3gpp.iari-ref="urn%3Aurn-7%3A3gpp-application.ims.iari.*rcse.*DT.serviceD"
  - +g.3gpp.iari-ref="urn%3Aurn-7%3A3gpp-application.ims.iari.*rcse.*VF.serviceE"

Please note the *operatorID* and the *serviceName* are up to each MNO choice. The only requirement for a MNO following this approach is to include these tags in the relevant interoperability agreements with other MNOs to avoid any interoperability issues.

RCS-e service	Tag
Operator specific service	+g.3gpp.iari-ref="urn%3Aurn-7%3A3gpp-application.ims.iari.*rcse.*<operatorID>.<service name>"

Table 17. SIP OPTIONS tag proposal for future lines of work

Please also note a set of LTE specific tags have been defined as part of the RCS-e specification and are covered in detail in section 2.12.2.

2.3.1.3 SIP OPTIONS exchange optimisations

As presented in section 2.3.1, there are several scenarios where the SIP OPTIONS message has to be used to update the capabilities. Depending on the circumstances and use cases, there could be occasions where the OPTIONS message exchange may happen relatively often (i.e. very frequent GPRS bearer changes).

To avoid the overhead and increase the efficiency, the client may implement a mechanism to those situations where the OPTIONS message exchange happens too often. Examples of how this mechanism can be achieved are listed below:

- Introduce a degree of hysteresis (i.e. a capabilities update is sent/requested only when the circumstances which led to the change remain stable for a certain period of time).
- Implement a validity timer (i.e. if the latest capabilities we have were fetched less than X seconds ago, they are still considered as valid).

Please note this spec does not specify the specific mechanisms which should be implemented leaving space to OEMs and third parties to drive innovative and differentiated solutions, which differentiates their products from competitors.

2.3.1.4 UI integration optimisations

In addition to the optimizations to minimize the traffic generated by the SIP OPTIONS exchanges when possible, there are two additional optimizations related with the discovery mechanism integration on the UI that should be taken into account:

- The round trip time for a SIP OPTIONS exchange (send and receive response) is expected to range values under 1 second. Taking this into account, the UI has to be optimized to minimize the impact of this exchange delay.
- When sending the SIP OPTIONS messages to several users (e.g. first time registration or when polling), it is recommended to employ a non-aggressive strategy and allowing time between each exchange to:
    - Minimize potential network impact
    - Avoid any impact on the user experience (e.g. slower UI, blockings, etc.)

Please note that again in this case this spec does not specify the specific mechanisms which should be implemented leaving space to OEMs and third parties to drive innovative and differentiated solutions, which differentiates their products from competitors.

2.3.1.5 SIP OPTIONS and multidevice support

Ultimately, the choice of supporting multidevice is up to each individual MNO. The considerations contained in this section will only apply to those operators willing to include RCS-e multidevice support in their networks.

In a multidevice scenario, when the user is registered on the IMS CORE with different devices using the same IMS identity (i.e. TEL-URI or SIP-URI), the OPTIONS exchange will return incomplete information:

- The capabilities contained in the OPTIONS message refer only to the originating device (i.e. the originating user may be logged in with the same TEL-URI in several devices).
- The IMS Core, depending on the configuration, either sends the OPTIONS message to the first registry in the IMS CORE or forks the OPTIONS to all the registered devices. In any case, only the first response is passed back to the requester, discarding the others. In other words, the capabilities returned in the OPTIONS response will be the ones from only one of the devices of the user.

The preferred implementation for handling the OPTIONS in a multidevice environment is left up MNO discretion with the only requirement that it should not have impact on the terminal side (i.e. no changes on the client side). A possible solution for extending the OPTIONS mechanism to a multidevice scenario is to include a custom Application Server implementing the following logic:

- A trigger will be setup in the IMS CORE to send all the OPTIONS from an RCS-e user to the AS.

- The AS will fork the OPTIONS request to all the user registered devices and will aggregate all the capabilities returned into one OPTIONS response message in case the forking is not already implemented by the IMS core network.
- Once the responses from the different multidevices are received, the AS will aggregate all the capabilities from the replies and sent them back to the caller.
- Even not all the replies have been received in less than a configurable amount of time (note the recommendation is to set the value to optimise the UX on the terminal) the AS will return the aggregated information received so far.

In order to implement this feature, an application server should be able to uniquely identify each user device to perform the forking of the OPTIONS message and to intercept and process the responses. The mechanism to have these individual identities (GRUU) is covered in section 2.14.

While multidevice support is an item left to each MNO to decide whether it is supported or not, the RCS-e capability discovery mechanism based on the SIP OPTIONS message is a mandatory requirement and the behaviour will be the one specified before to ensure seamless interworking between MNOs.

2.3.2 Capability discovery via presence[16]

In addition to the SIP OPTIONS mechanism defined in section 2.3.1, the MNO deploying a presence server may provide the capability discovery mechanism via presence as defined in section 4 of [RCS1-TEC-REAL] and section 6 of [RCS2-TEC-REAL].

This mechanism can be used by a client whose PRESENCE DISCOVERY parameter has been set to 1, and only with contacts who have been identified as RCS-e capable as per the procedure defined in section 2.4.1, and who have indicated the support of discovery via presence (i.e. the *+g.3gpp.iari-ref="urn%3Aurn-7%3A3gpp-application.ims.iari.rcse.dp"* tag was included either in the OPTIONS message or response).

- Please note the contact will be also added to an XDM list of contacts supporting this feature so it is possible to optimize future capability polling as described in section 2.3.2.1.

Effectively, the RCS-e client needs to have the necessary functionality to distinguish between contacts who support the presence capability discovery and those who do not (e.g. storing it as a property in the addressbook).

As a reference, the capability discovery mechanism via presence (based on capabilities publication and anonymous fetch) is presented below:

- Each client supporting the capability discovery via presence will publish its capabilities on the presence server (SIP PUBLISH) when registering

[16] It is assumed that the operator implementing this mechanism has a policy where the RCS service capabilities can be fetched via anonymous subscribe. Otherwise, this mechanism cannot be implemented.

- When querying, the client polls each one or more contacts (list) capability status using the SIP ANONYMOUS SUBSCRIBE requests with an expiry time of 0 and processing the NOTIFY responses.
- The NOTIFY response contains the capabilities as described in the RCS Release 2 data model[17].

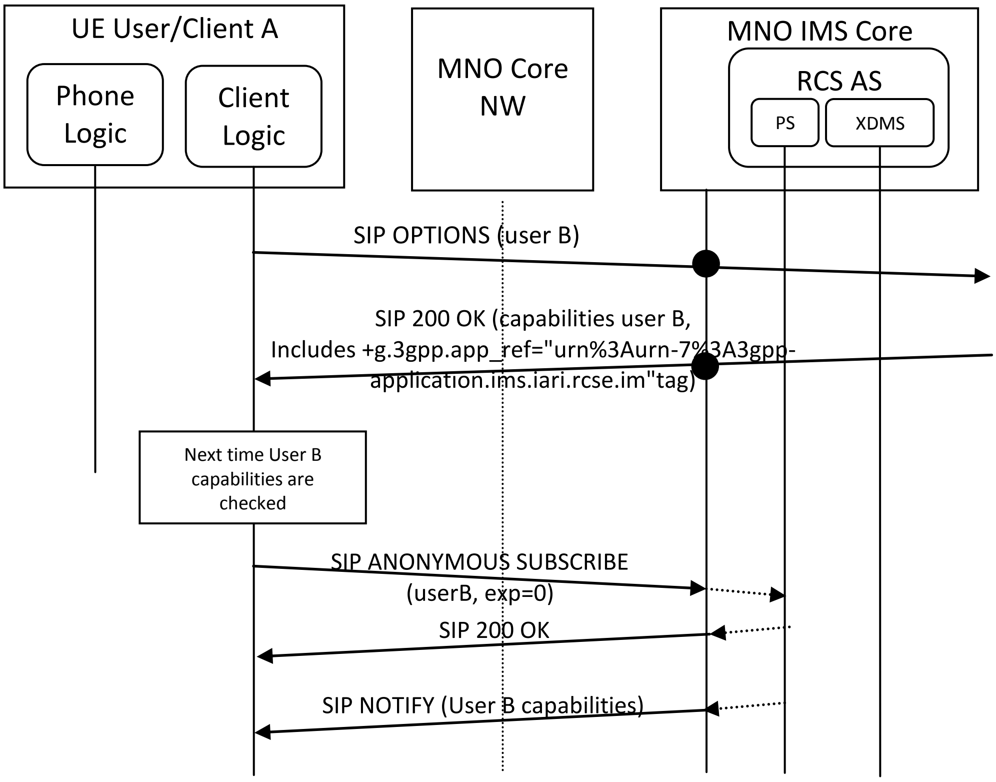

UE User/Client A
Phone Logic
Client Logic
MNO Core NW
MNO IMS Core
RCS AS
PS
XDMS
SIP OPTIONS (user B)
SIP 200 OK (capabilities user B, Includes +g.3gpp.app_ref="urn%3Aurn-7%3A3gpp-application.ims.iari.rcse.im"tag)
Next time User B capabilities are checked
SIP ANONYMOUS SUBSCRIBE (userB, exp=0)
SIP 200 OK
SIP NOTIFY (User B capabilities)

Figure 14. Capabilities discovery via PRESENCE

2.3.2.1 Enhancing ANONYMOUS SUBSCRIBE mechanism with XDMS lists

The standard mechanism can be enhanced by using a XDMS list of all the contacts supporting the presence based capability discovery mechanism in the Address Book and subscribing once to the list instead of one SUBSCRIBE per contact. This will return an aggregated NOTIFY message instead of several message making the mechanism more efficient, particularly in those scenarios where the whole contact list status/capabilities must be queried.

In this particular scenario, it is relatively likely that the terminal address book may already contain several contacts, therefore, generating a XDMS list at this time and use it to query, reduces the amount of messages exchanged with the presence server.

For the scope of this document it is considered that the XDMS list mechanism enhancement is implemented and used.

[17] [RCS2-TEC-REAL], Section 4.2

2.4 *New user discovery mechanism*

With the main aim of optimising the UX and minimising the unnecessary traffic generated by an RCS-e client, a list containing the subset of RCS-e contacts should be generated and maintained by the client. This list should include both registered and not registered contacts; in contrast, it does not include not provisioned contacts.

In addition to this, the first view of the address book shall clearly identify the RCS-e capable contacts thanks to the list, with a visual RCS-e flag.

In order to keep this list updated, when a new contact is added to the phonebook it is necessary to evaluate whether is an RCS-e contact using the standard capability discovery based on SIP OPTIONS.

Finally note that a new contact may come from different sources and, therefore, the mechanism described in the following sections applies to all the scenarios presented below:

- Added manually by the user
- Synchronized via 3rd party servers or PC
- Received via Bluetooth or handling a VCARD file received, for example via e-mail

…

2.4.1 Discovery via OPTIONS message

The SIP OPTIONS message can be employed not only to determine the capabilities but also to identify whether a contact is or not an RCS-e user, independently whether he/she is registered at the time the query is performed.

When a SIP OPTIONS message is sent from User A to User B, User A will receive one of 6 types of response:

1) User B is Registered and the response from User B’s client will comprise CAPABILITY STATUS – the set of services currently available (based on tags as described in section 2.3.1.1). Therefore, if this response is received and at least the RCS-e IM service tag (*+g.3gpp.iari-ref="urn%3Aurn-7%3A3gpp-application.ims.iari.rcse.im"*) is included, the user is identified as a RCS-e user.
2) If User B is currently not registered (e.g. phone is off, out of coverage or roaming with data services disabled), then the network will respond with one of the following error messages: 480 TEMPORARILY UNAVAILABLE (graceful deregistration took place) or 408 REQUEST TIMEOUT. From the user discovery point of view, this response is ignored:
    - If user B was previously identified as an RCS-e user (i.e. options message or a complete 200 OK response with the capabilities was received from him/her before), it will remain like that.
    - Otherwise, the user will remain as a non-RCS-e user

3) If User B is not provisioned for RCS-e the network will respond with a message error: 404 NOT FOUND[18]. Therefore, if this message is received, the user is identified as a non-RCS-e user.
4) In addition to this, if a SIP OPTIONS is received and at least the RCS-e IM service tag (*+g.3gpp.iari-ref="urn%3Aurn-7%3A3gpp-application.ims.iari.rcse.im"*) is included, the sender is identified as an RCS-e user. In this particular case, when user B receives the OPTIONS message with capabilities from user A, user B identifies user A as an RCS-e user.
5) If User B was identified as a RCS-e user and the response to the OPTIONS message indicates that User B is no longer a RCS-e user (no longer provisioned as described in the previous bullet point 3 or the RCS-e IM tag [*+g.3gpp.iari-ref="urn%3Aurn-7%3A3gpp-application.ims.iari.rcse.im"*] is no longer included), user B should be identified as a non-RCS-e user and, consequently, removed from the list of RCS-e which is maintained in the handset or device.
6) Please note there is a possibility a RCS-e user who is not within the addressbook contacts may send OPTIONS messages or responses (e.g. when receiving a call or making a call using a MSISDN not included in the contacts). In this case the capabilities shall be stored temporarily in the terminal for one of the following purposes:
    - Use the value during a subsequent IM/chat, file transfer or call (image/video share), and,
    - To add the information to the new contact (both the fact that it is a RCS-e user and the cached capabilities) in case the user decides to add a new addressbook entry following a communication.

To illustrate the behaviour, the following example is provided. User A is registered and decides to add or modify a new contact which results in a new IMS identity for the contact (e.g. new MSISDN which implies a new TEL-URI). As a consequence, the client needs to verify whether the contact is an RCS-e user and, therefore, add it to the list the terminal maintains.

[18] Please note that the response provided may depend on the network configuration. A better approach for the terminal is to parse the response and if it is not either a 200 OK containing the capabilities as feature tags, a 480 TEMPORARILY UNAVAILABLE or a 408 REQUEST TIMEOUT, the target user should be considered as non-RCS. For simplicity, the present document assumes in the following sections that the response provided by the MNO core network is always 404 NOT FOUND, however, the previous statement should be taken into account.

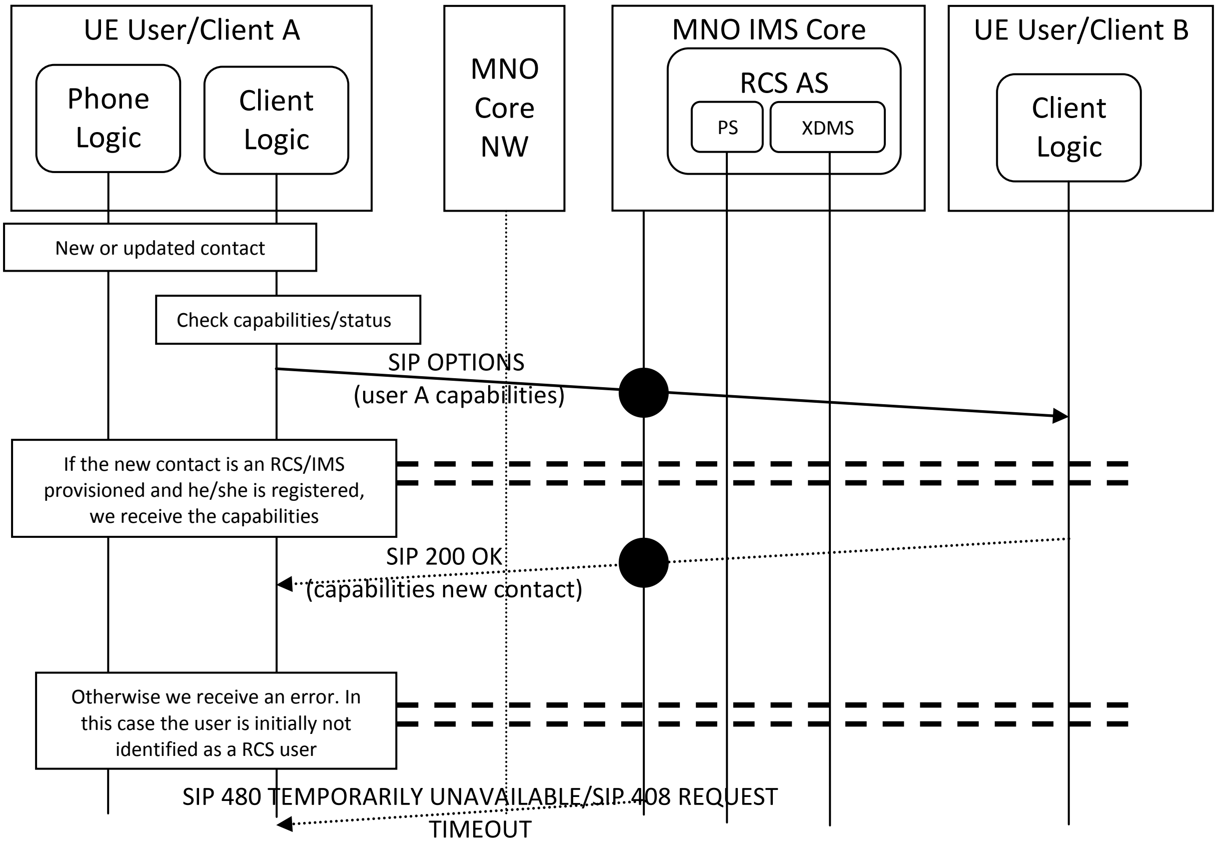

UE User/Client A
Phone Logic
Client Logic
MNO Core NW
MNO IMS Core
RCS AS
PS
XDMS
UE User/Client B
Client Logic
New or updated contact
Check capabilities/status
SIP OPTIONS (user A capabilities)
If the new contact is an RCS/IMS provisioned and he/she is registered, we receive the capabilities
SIP 200 OK (capabilities new contact)
Otherwise we receive an error. In this case the user is initially not identified as a RCS user
SIP 480 TEMPORARILY UNAVAILABLE/SIP 408 REQUEST TIMEOUT

Figure 15. Adding/Editing a contact

As part of the capabilities, this process will identify those contacts supporting the “social information via presence” and the "capability discovery via presence" functionalities. Please note that:

- if the PRESENCE DISCOVERY is set to 1 (see Table 6), the client should also update the XDM list of RCS contacts supporting this functionality with the newly identified contacts supporting the capability discovery via presence functionality.

- if the PRESENCE PROFILE is set to 1 (see Table 6), the client may use the procedures related to the exchange of "social information via presence" defined in [RCS1-TEC-REAL] with the newly identified contacts supporting the "social information via presence" functionality.

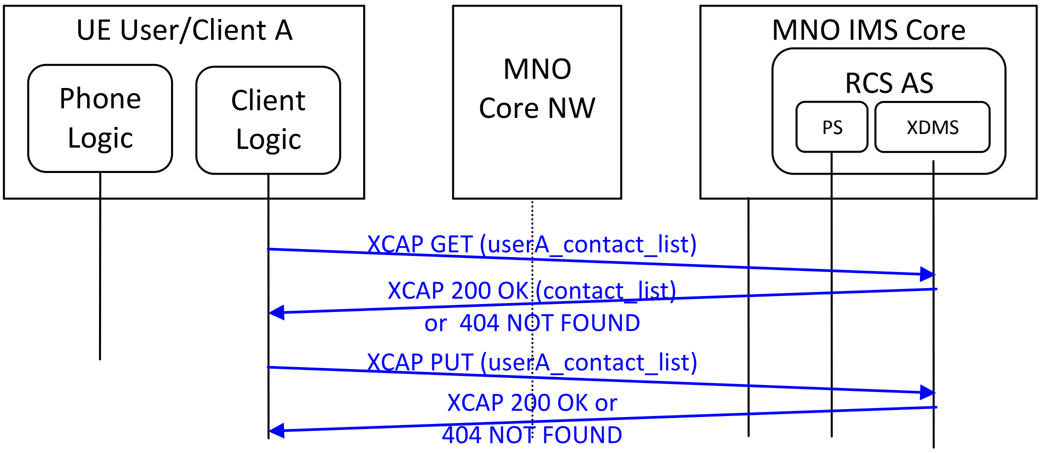


Figure 16. Updating the XDMS list of contacts supporting "social information via presence" functionality

Additionally, it should be noted that if User A is NOT registered at the time the new contact(s) are added, the terminal should keep the necessary information in the phone so the next time the RCS-e client completes the registration process described in Figure 15 and, if applicable, Figure 16.

2.5 *Capability polling mechanism*

In order to enhance the discovery of new users and, ultimately, keep the list of RCS-e contacts up to date, the present specification proposes a mechanism, capability polling, consisting in polling the status/capabilities of all the contacts contained in the addressbook whose capabilities are not available (e.g. non-RCS-e users) or are expired (see CAPABILITY INFO EXPIRY parameter in section 2.1 Table 6 for reference),

It should be noted that the capability polling mechanism is optional and will be only performed if the right configuration is in place (i.e. if the POLLING_PERIOD parameter presented in Table 6 is set to 0, this polling mechanism will not take place).

Assuming the POLLING_PERIOD is configured to be greater than 0 and after the polling timer expires, the client will perform the following mechanism to update the list of RCS-e contacts and update their capabilities.

Please note it should be taken into account that when using OPTIONS, the capability polling is only performed on:

- those contacts without capability information (non-RCS-e users and RCS-e users with unknown capabilities), and,
- the rest of RCS-e contacts, provided the associated capability information is older that the CAPABILITY_INFO_EXPIRY parameter (see Table 6 for further reference)[19].

[19] Please note this is a traffic optimization to reduce the amount of SIP OPTIONS messages generated by capability polling

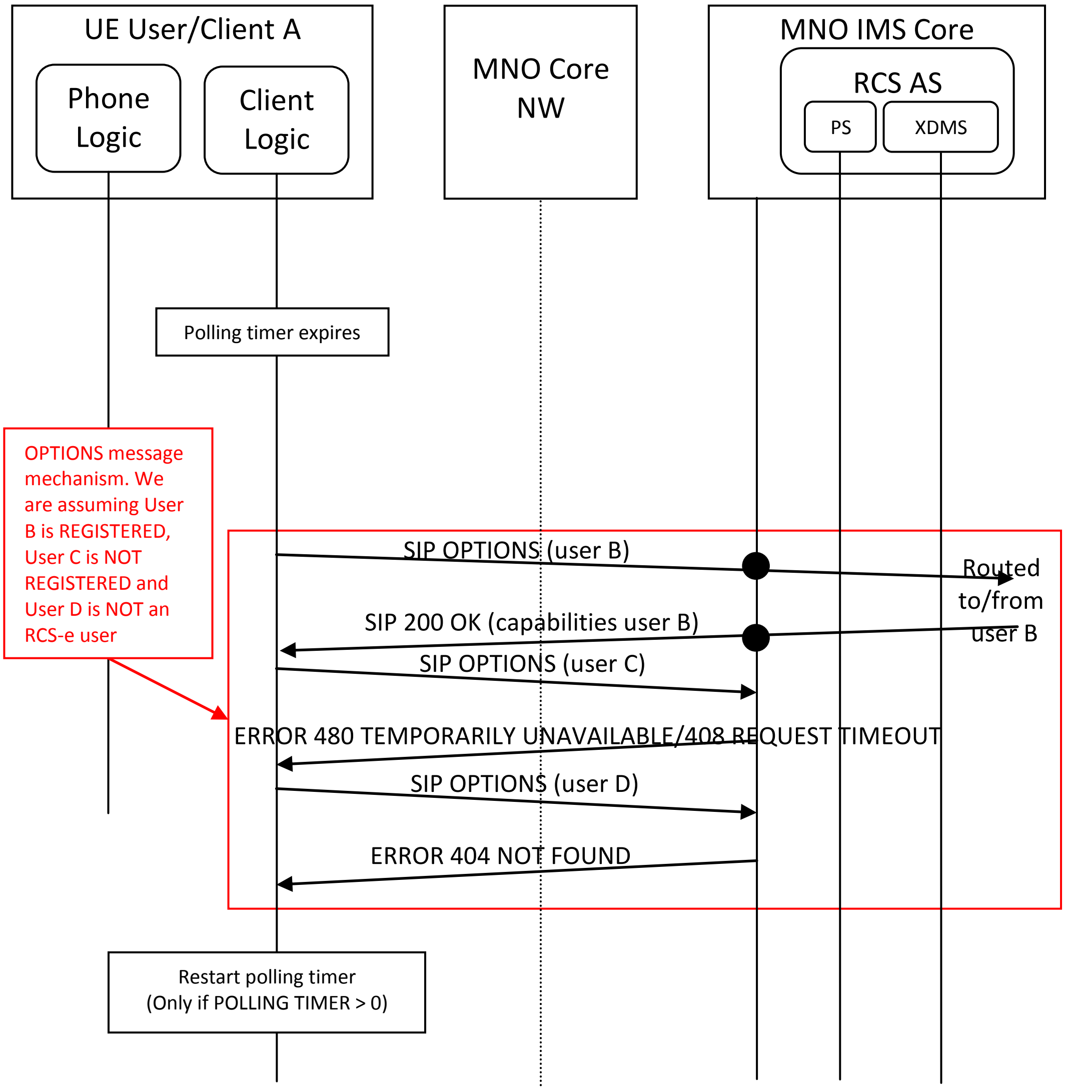

UE User/Client A
Phone Logic
Client Logic
MNO Core NW
MNO IMS Core
RCS AS
PS
XDMS
Polling timer expires
OPTIONS message mechanism. We are assuming User B is REGISTERED, User C is NOT REGISTERED and User D is NOT an RCS-e user
SIP OPTIONS (user B)
Routed to/from user B
SIP 200 OK (capabilities user B)
SIP OPTIONS (user C)
ERROR 480 TEMPORARILY UNAVAILABLE/408 REQUEST TIMEOUT
SIP OPTIONS (user D)
ERROR 404 NOT FOUND
Restart polling timer
(Only if POLLING TIMER > 0)

Figure 17. Capabilities polling via OPTIONS message

We previously mentioned that for clients/terminals configured with PRESENCE DISCOVERY set to 1 (see Table 6) , an XDM list may be maintained containing those contacts supporting the capability discovery via presence. This list can be used to employ the anonymous fetch (ANONYMOUS SUBSCRIBE) mechanism instead of OPTIONS.

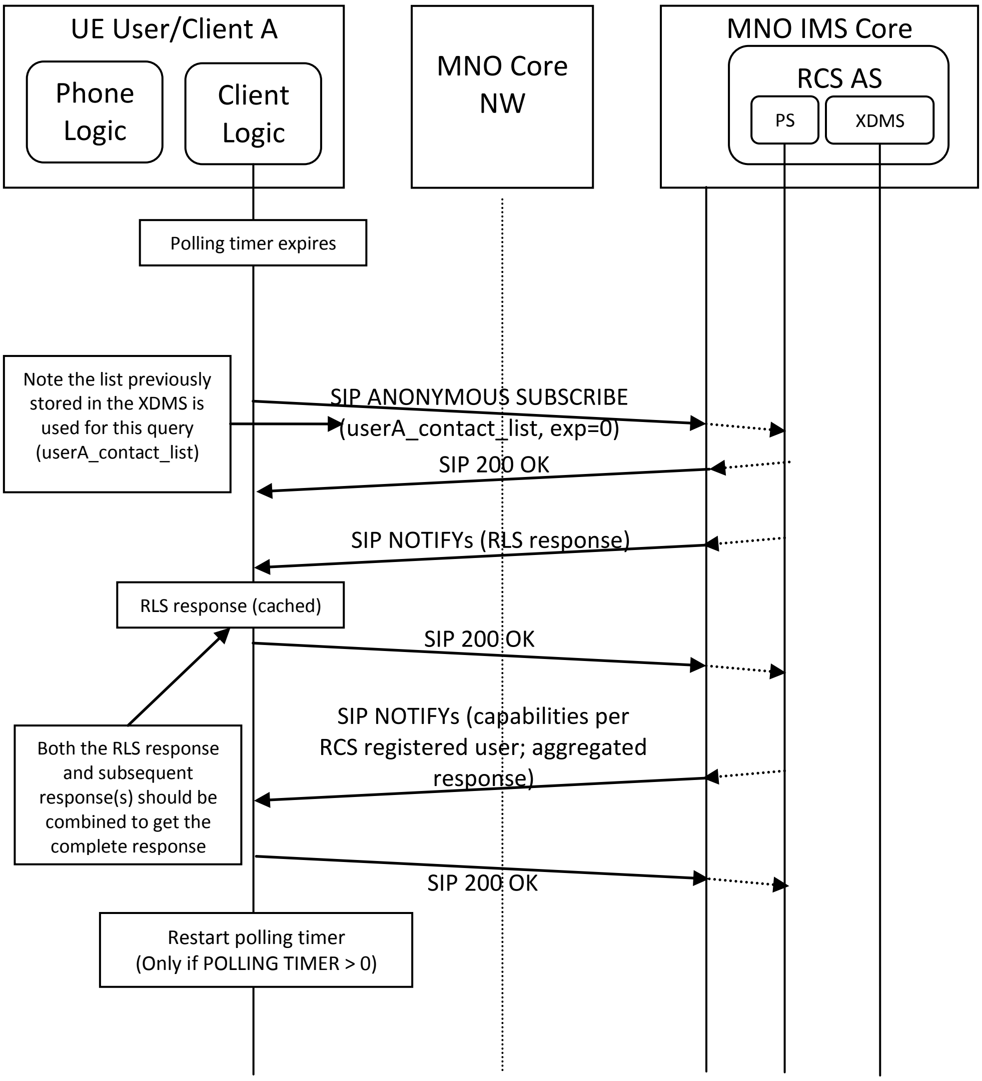

UE User/Client A
Phone Logic
Client Logic
MNO Core NW
MNO IMS Core
RCS AS
PS
XDMS
Polling timer expires
Note the list previously stored in the XDMS is used for this query (userA_contact_list)
SIP ANONYMOUS SUBSCRIBE (userA_contact_list, exp=0)
SIP 200 OK
SIP NOTIFYs (RLS response)
RLS response (cached)
SIP 200 OK
SIP NOTIFYs (capabilities per RCS registered user; aggregated response)
Both the RLS response and subsequent response(s) should be combined to get the complete response
SIP 200 OK
Restart polling timer (Only if POLLING TIMER > 0)

Figure 18. Capabilities polling via anonymous fetch

Please note that an RCS-e client should support both individual and aggregated NOTIFY responses[20].

[20] Depending on the network configuration, only the first notification (RLS) may be the only one received will be received by the RCS-e client with a subscription with Expiry Header value set to 0. The dialog in this IMS core is suppressed so the second notification will not be received by the RCS-e client. So if the first notification is partial and if we don't receive the second notification, we potentially lost capabilities contacts information.
This problematic requires further study and will be addressed in future versions of the specification.

Finally, and as a summary of the capability and new user discovery mechanism composition the following diagram is provided.

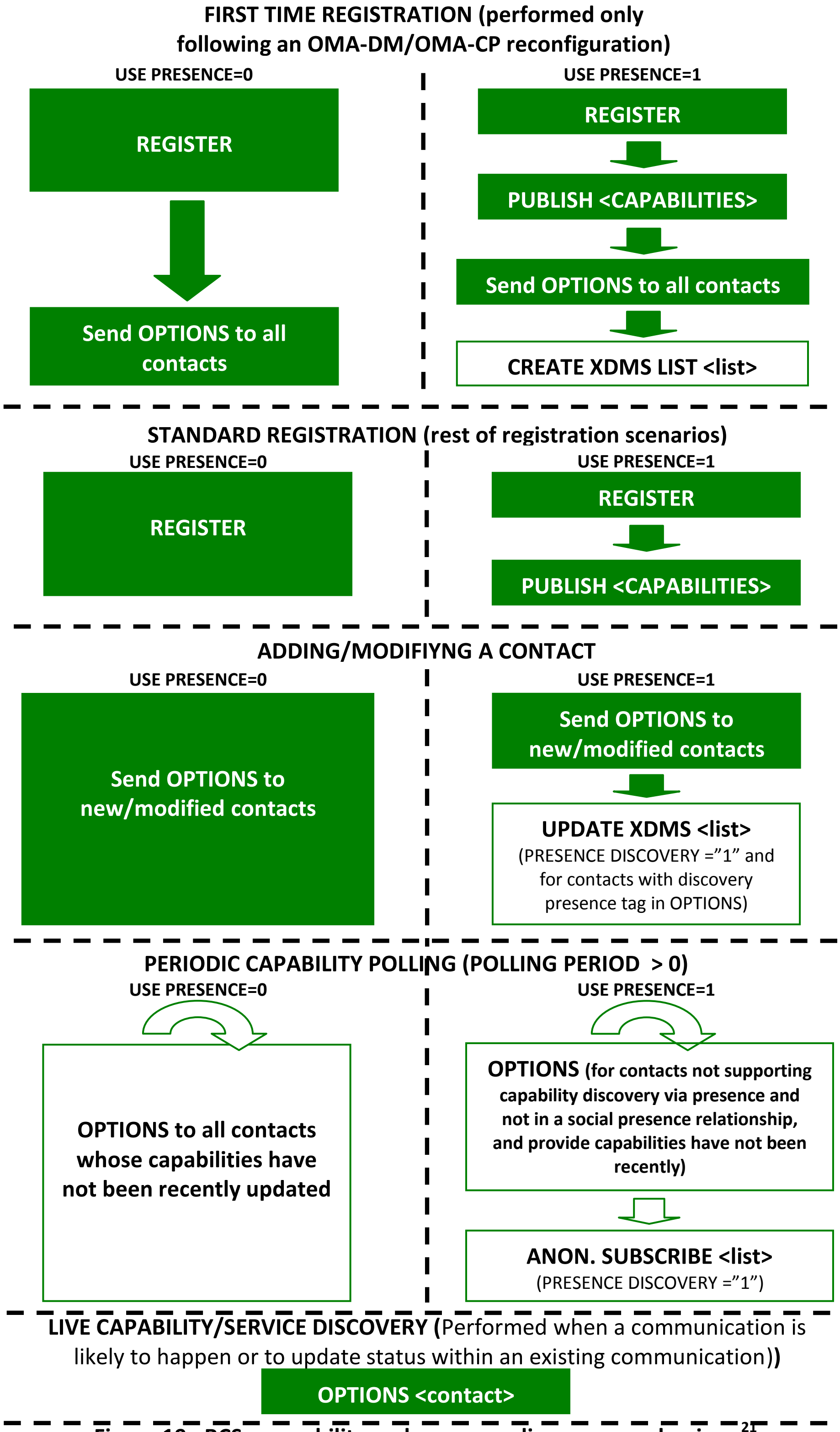

FIRST TIME REGISTRATION (performed only following an OMA-DM/OMA-CP reconfiguration)
USE PRESENCE=0
REGISTER
Send OPTIONS to all contacts
USE PRESENCE=1
REGISTER
PUBLISH <CAPABILITIES>
Send OPTIONS to all contacts
CREATE XDMS LIST <list>
STANDARD REGISTRATION (rest of registration scenarios)
USE PRESENCE=0
REGISTER
USE PRESENCE=1
REGISTER
PUBLISH <CAPABILITIES>
ADDING/MODIFIYNG A CONTACT
USE PRESENCE=0
Send OPTIONS to new/modified contacts
USE PRESENCE=1
Send OPTIONS to new/modified contacts
UPDATE XDMS <list> (PRESENCE DISCOVERY ="1" and for contacts with discovery presence tag in OPTIONS)
PERIODIC CAPABILITY POLLING (POLLING PERIOD > 0)
USE PRESENCE=0
OPTIONS to all contacts whose capabilities have not been recently updated
USE PRESENCE=1
OPTIONS (for contacts not supporting capability discovery via presence and not in a social presence relationship, and provide capabilities have not been recently)
ANON. SUBSCRIBE <list> (PRESENCE DISCOVERY ="1")
LIVE CAPABILITY/SERVICE DISCOVERY (Performed when a communication is likely to happen or to update status within an existing communication))
OPTIONS <contact>

Figure 19. RCS-e capability and new user discovery mechanisms[21]

[21] The green boxes represent mandatory procedures, meanwhile the clear boxes represent optional procedures.

2.6 *Management of supplementary RCS functionality*

As presented in the introduction, a RCS-e deployment (terminal and network) can be supplemented with the *"social information via presence"*[22] functionality (i.e. presence invitation and social information sharing features) included in RCS Release 2 specifications, however, this does not form part of the RCS-e compliance. For those clients implementing this set of functionalities, the following procedure is proposed to ensure interoperability[23]:

- Prior to be able to send an invitation to a contact (e.g. from the addressbook), the terminal will use the OPTIONS mechanism to determine if the other end also supports this set of features (i.e. both ends include the *+g.3gpp.iari-ref="urn%3Aurn-7%3A3gpp-application.ims.iari.rcse.sp"* tag in the relevant headers).
- If both clients support the *"social information via presence"* functionality, then the user is presented with the possibility of inviting the contact to share the social presence information. If not, the terminal should not present this possibility to the user for that contact.

The management of contacts supporting the "*social information via presence"* shall follow the procedures defined in [RCS2-TEC-REAL] and [RCS1-TEC-REAL]. As such, the contacts with whom the user has established a social presence relationship shall be added to the "rcs" list defined in section 4.4.2 of [RCS1-TEC-REAL]. As capabilities are already provided via presence for the members of the "rcs" list, they should be excluded from the XDM list defined in section 2.4.1

2.7 *RCS-e and capabilities*

The RCS-e capabilities represent the list of services that a RCS-e user/client can access at certain point of time. The capabilities depend on four factors:

- User MNO provisioning status: An operator may choose to limit service to customers depending on payment status (i.e. chat and file share, but not video)

- The terminal HW: A terminal with limited HW (i.e. no capability to process video) may not be able to access all the RCS-e

[22] Please note that by the term "social profile information", we are referring to all the related features present in RCS Release 2 which allow a user to create a social profile information, invite users to share, declare hyperability state and receive updates based on RCS presence functionality. Please note this functionality is covered in the RCS Release 1 specs, Functional Description v2.0 ([RCS1-FUN-DESC]), sections 2.1.2, 2.1.3 and 2.14.

[23] Please note that the present specification allows the deployment of RCS communication services without the need for a presence server and the associated XDM servers, therefore, the present specification provide the necessary guidance to secure interoperability.

- The terminal status: Even if a terminal HW supports all the services, it could be that the device status introduces a limitation (e.g. receiving files is not possible when the file storage is full)

- Connectivity status: Certain services may require certain level of network QoS. For example, streaming video over a 2G GPRS does not provide the adequate user experience.

As a summary, please find the table below:

SERVICE	TERMINAL and STATUS REQUIREMENTS	DATA BEARER				
		2G	EDGE	3G	HSPA	Wi-Fi
chat	None	Y	Y	Y	Y	Y
file transfer (FT)	Minimum threshold of free space to store files	MNO choice	MNO choice	Y	Y	Y
Image share	Minimum threshold of free space to store files. The terminal should be on an active call[24] with the user the image is willing to be shared with. Not available in multiparty calls.	MNO choice	MNO choice	Y	Y	Y
Video share (separate en/decoding)	Support video profile (encoding /decoding). The terminal should be on an active call[25] with the user the video is willing to be shared with. It is not available in multiparty calls.	N	N	One way only	Y[26]	Y[26]

[24] In this context, the term active call is used to indicate that a voice call is taking place with the user the image is shared with and that this call is not on-hold, waiting or forwarded/diverted.

[25] In this context, the term active call is used to indicate that a voice call is taking place with the user the video is shared with and that this call is not on-hold, waiting or forwarded/diverted.

[26] In this case both ends may share video simultaneously meaning that there is a possibility to have a bi-directional flow of video (see the other party's video while I am also sharing video with him/her). The meaning is that if a user is already sharing video with the other end, the other user may decide to also share video simultaneously, not that the two-ways video share can start simultaneously.

Table 18. RCS-e services HW and data bearer requirements

When referring to bidirectional video share, we mean that once user A is sharing video with user B and provide the right coverage conditions are in place, user B could also start to share video with A simultaneously. In this case each video share session is independent and should be handled separately.

Please note in the table before and for all the services it is assumed that:

- The phone is working adequately. In the event the terminal detects an issue that prevent one or more services from operating, the relevant capabilities should be reported as not available.
- There is enough battery: Some phones may prevent using some or all the services when the battery level achieves certain level. In this situation, basic and emergency functionality should be prioritised.
- The phone is registered and is able to access IMS/RCS-e core network and relevant servers.

For clarification purposes and in addition to the previous ones, the following assumptions are made for the image and video share cases:

- Both the sharing and receiving end are in a call (CS) between them
- The call is not a multiparty call
- The call is not on hold
- The call is not waiting
- A call forward or divert is not in place

In other words, the relevant image and video share tags described in section 2.3.1.1 SHALL be included only if:

1. the OPTIONS exchange happens when the user is on an active call, and,
2. the destination (sending OPTIONS) or the requester (receiving an OPTIONS message which has to be replied with a response) is the other end of the active call.

As a consequence of the information presented above, a RCS-e client which is registered will at least support chat. Note that while capability exchange is reciprocal, User A and User B's capabilities may be different and services shall be made available accordingly (e.g. A may support video encode and B may support decode, but both need to be under 3G or better data coverage for the service to work).

In addition to the information presented above, we should take into account that some terminals do not support 2G DTM (dual-transfer mode). For that devices and provide they are using a 2G data coverage (meaning that no services are available during the call), the PS connection will automatically drop once they engage on a CS call.

2.7.1 Capability Extensions

The default set of RCS-e capabilities is described in section 2.3.1.1 (one per tag described in Table 15), however, given the extensibility of the service framework further capabilities may be added (i.e. following the proposal given in Table 17 or agreeing more common services and the associated tags in future versions of the specification).

2.7.2 IM store and forward

As presented in Table 6 (IM CAP ALWAYS ON), there is the possibility to configure the client to assume that the MNO will be providing the IM store and forward functionality, which basically consist on storing the messages which are sent to users who are offline (i.e. no data connectivity or phone off) at the time the chat message is sent.

If this parameter is enabled, there is an impact from the IM capability which is presented to the user.

As a consequence, we have 4 different types of contacts for IM capability:

ID	Targeted contact is RCS-e IM capable ?	Provider MNO supports Store& Forward ?	Targeted contact is connected to the network ?	Impact on starting IM
1	NO	N/A	No relevant	IM never possible with that contact
2	YES	NO	NO	Not possible to start an IM at that time
3	YES	YES	NO	Possible to send an IM that will be delivered later by the Store and Forward server as soon as the Contact is connected
4	YES	No relevant	YES	IM is possible and messages are immediately delivered

Table 19. Store and forward possible scenarios

The store and forward functionality and behaviour on the client is controlled by a couple of configuration parameters (see Table 6 for further reference):

- IM CAP ALWAYS ON:
  - When an operator implements store and forward, all its RCS-e customers will have the IM CAP ALWAYS ON is set to enabled. This means that all RCS-e contacts (currently registered or not) are presented with the IM service as available (3 and 4 according to Table 19).
  - When store and forward is not implemented by the MNO, all its RCS-e customers will have the IM CAP ALWAYS ON configuration parameter is set to disabled (2 and 4 according to Table 19).

  As a summary: IM CAP ALWAYS ON is enabled when store and forward is used, otherwise it is disabled

- Additionally and assuming IM CAP ALWAYS ON is enabled, there is an second parameter, IM WARN SF, which can be used to control the UX behaviour:
    - If IM WARN SF parameter is enabled: In scenarios 3 and 4, the user shall be aware that messages delivered to unregistered users will be only delivered once the other party is back online (e.g. switches the phone on or gets back in coverage).
    - If IM WARN SF parameter is disabled, there shall not be any visible difference between scenarios 3 and 4 from the UX point of view. In other words, the user shall not be aware on whether the messages are being stored or directly delivered to the other party.

2.7.3 Video interoperability

As presented in section 2.7, the video share service availability is mainly dependent on the network coverage. This is based on the assumption that both ends (source and destination) share the ability of handling a common video format and specific profile.

In order to guarantee the interoperability of all RCS-e during the video share scenario, all RCS-e devices supporting the video share service shall, at least, support the following video format:

- Video format: H.264/MPEG-4 Part 10 // AVC (Advanced Video Coding)
    - H.264 Profile: Baseline Profile (BP)
    - H.264 Level: 1b

Please note that it is recommended to support additional video formats providing different levels of quality and to use them in an adaptive fashion depending both on the terminal status and the network conditions/coverage.

In case a RCS-e terminal supports several profiles, the final choice should be based in the outcome of the SDP media negotiation where both ends (sender and receiver) will present the supported video formats at that particular point in time (i.e. taking each device and network/connectivity status).

2.8 *RCS-e protocols*

The following table summarises the list of protocols employed by RCS-e clients. It must be noted that the choice will not impact MNO interoperability:

Protocol name	Description	Transport layer	Secure transport layer/protocol
Session initiation protocol (SIP)	Client-IMS core signalling protocol	UDP/IP or TCP/IP	SIP over TLS or IP Sec
Media Session Relay Protocol (MSRP)	chat messages, media (pictures) and file exchange protocol	TCP/IP	MSRP over TLS or IPSec

Real-time protocol (RTP)	Media (video) exchange	UDP/IP	Secure RTP (SRTP)[27] or IPSec

Table 20. RCS-e recommended protocols

It is recommended that RCS-e clients support both SIP/UDP and SIP/TCP as the choice of the SIP transport protocols used to transport the signalling data belongs to each MNO.

Regarding the impact of NAT traversal in the different protocols involved in RCS-e, the following considerations shall be taken into account:

- Regarding SIP protocol:
  - CRLF keep-alive [IETF-DRAFT-SIPCORE-KEEP][28] support is MANDATORY when SIP/TCP or SIP/TLS is used by the RCS-e client.
  - STUN keep-alive [IETF-DRAFT-SIPCORE-KEEP] support is RECOMMENDED when SIP/UDP is used by the RCS-e client as it allows network capacity optimization.
  - RCS-e client using SIP/UDP and not supporting sipcore-keep:
    - SHALL support symmetric signalling (i.e. IP/port used to send SIP messages is the same as the one used to receive SIP messages).
    - SHALL perform TCP switchover for large SIP messages.

- MSRP sessions, the RCS-e client SHALL support:
  - [RFC6135][29]
  - [IETF-DRAFT-SIMPLE-MSRP-SESSMATCH][30]

- Regarding NAT traversal of RTP sessions, the RCS-e client should implement the mechanism described in section 2.8.1.

The support of TLS based or IP Sec based protocols to secure the signalling and media exchanges is RECOMMENDED particularly for those scenarios where the data has to be carried over a network outside the MNO domain (i.e. Wi-Fi access). At the time this spec is published, this functionality is left as optional and how interoperability between RCS-e client and MNO can be achieved is left for further studies.

Finally, please note that to secure interoperability of devices across different MNO networks (i.e. when porting devices across networks or using open market devices/clients), the list of preferred options for the transport and security for the signalling (SIP) and media (RTP and MSRP) protocols is included in the configuration parameters (see Annex A, section A.2.7). Consequently, a MNO will provide this information as part of the configuration (first-time or re-configuration scenarios as described in section 2.2.2.1).

[27] Secure RTP as per IETF RFC 3711 [RCF 3711] available at http://www.ietf.org/rfc/rfc3711.txt

[28] Sipcore keep functionality is described in the following IETF draft: http://tools.ietf.org/html/draft-ietf-sipcore-keep-12

[29] The Alternative Connection Model for the Message Session Relay Protocol (MSRP) IETF RFC is available at http://tools.ietf.org/html//rfc6135.

[30] Simple MSRP seesmatch as described in the following IETF draft: http://tools.ietf.org/html/draft-ietf-simple-msrp-sessmatch-10

2.8.1 RTP and NAT traversal

As presented in the previous section, a RCS-e client has to implement several mechanisms to avoid the negative impact of NAT traversal, which can both occur when connecting over:

- PS: Mainly due to the scarce of IPv4 public addresses and proxying performed at APN level, or,
- Wi-Fi: In this case due to the fact the network topology between the access point and the Internet may vary between deployments.

In order to combat the negative effects of NAT traversal on the RTP protocol, the RCS-e client should implement the following mechanisms:

- SHALL support a keep-alive mechanism in order to open and maintain the NAT binding alive regardless of whether the media stream is currently inactive, send-only, receive-only or send-receive. Possible standard keep-alive mechanisms are STUN keepalive (as per 3GPP TS 24.229) or empty (no payload) RTP packet with a payload type of 20 (as per 3GPP TS 24.229).
- SHALL use symmetric media (i.e. use the same port number for sending and receiving packets) as defined in [RFC4961][31] mechanism which is summarized below:
  - When an invitation for video share is received and accepted, the 200 OK response contains a SDP body containing all the necessary fields (including the destination port) for the sender to send the RTP packets.
  - Immediately after sending the 200 OK response, the receiver will send a keep-alive packet back to the sender to secure the media path:
    - The source port shall be identical to the one included in the m field of the SDP payload inside the 200 OK response.
    - The destination port shall be identical to the one included in the m field of the SDP payload inside the SIP INVITE message.
  - The sender should allow enough time for the media path to be secured.

[31] The symmetric RTP / RTP Control Protocol (RTCP) IETF RFC is available at http://tools.ietf.org/html//rfc4961.

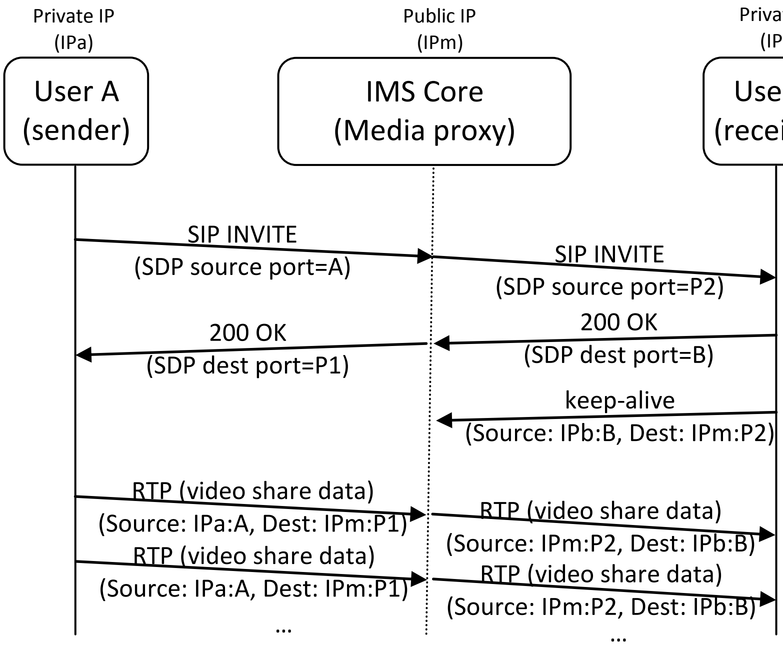


Figure 20. RTP symmetric media path establishment

- SHALL use RTCP.

Please note that for readability purposes, the procedures described in this section have not been included in the diagrams covering video share functionality in section 3.3.

2.9 *Addressing and identities*

2.9.1 Overview

Telephone numbers in the legacy address book must be usable (regardless of whether RCS-e contacts have been enriched or not) for the identification of contacts of incoming and outgoing SIP requests.

Also, RCS-e users, especially in Enterprise segments, may be assigned a non MSISDN based identity. The RCS-e client would be provisioned with the appropriate SIP URI parameter as seen in Table 6, leaving the TEL-URI parameter empty.

Consequently, a RCS-e enabled terminal address book should also be able to store IMS URIs as part of a contact details.

2.9.2 Device Incoming SIP Request

2.9.2.1 From/P-Asserted-Identity

For device incoming SIP requests, the address(es) of the contact are, depending on the type of request, provided as a URI in the body of a request or contained in the P-Asserted-Identity and/or the From headers. If P-Asserted-Identity is present, the From header will be ignored. The only exceptions to this rule are when the P-Asserted-Identity matches the one defined for the store and forward notifications, the one used for incoming group chat invitations or the one used for delivering stored messages, in which the Referred-by header should be used to retrieve the originating user instead.

The receiving client will try to extract the contact's phone number out of the following types of URI's:

- TEL URI's (for example tel:+1234578901, or tel:2345678901;phone-context=<phonecontextvalue>)
- SIP URI's with a "user=phone" parameter, the contact's phone number will be provided in the user part (i.e. sip:+1234578901@operator.com;user=phone or sip:1234578901;phone-context=<phonecontextvalue>@operator.com;user=phone)

Once the MSISDN is extracted it will be matched against the phone number of the contacts stored in the Address Book. If the received URI is a SIP URI but does not contain the "user=phone" parameter, the incoming identity should be checked against the IMS URI address of the contacts in the address book instead.

In case more than one P-Asserted-Identity is received in the message, all identities shall be processed until a matched contact is found.

2.9.3 Device Outgoing SIP Request

2.9.3.1 Identification of the target contact

If the target contact contains an IMS URI the value shall be used by the RCS-e client when generating the outgoing request even if an MSISDN is also present for the contact. This applies to the SIP Request-URI and the "To" header (as defined in [3 GPP TS 24.229]) for 1-1 communication, as well as to the URIs used in the recipient list included in outgoing SIP requests for group chat.

In case no IMS URI is present the RCS-e client shall use the telephone number (in local format for example 0234578901 or global format +1234578901) set in the address book or a dial string entered by the user.

In case of international-format telephone number, the device should support TEL-URI (for example tel:+12345678901) as defined in [RFC 3966][32] and SIP-URI (for example sip:+12345678901@domain;user=phone) with the user parameter set to "phone" as defined in [RFC 3261][33]. This should be configurable on the device according to the Service Provider's requirements or constraints related to national regulatory framework of SIP-SIP interconnection (MNO will provide this choice during customization). If none of the above constraints apply, the use of TEL-URI is recommended since the domain name of the SIP-URI is not significant.

In case of non-international format telephone number, the RCS-e client should support TEL-URI and SIP-URI (the user parameter should be set to "phone") with a phone-context

[32] The Tel URI for telephone numbers IETF RFC is available at http://tools.ietf.org/html//rfc3966.

[33] The SIP: Session Initiation Protocol IETF RFC is available at http://tools.ietf.org/html//rfc3261.

value set as defined in [TS 24.229] [34] for home local numbers (for example tel:0234578901;phone-context=<home-domain-name>). Like the international number case, whether a TEL-URI or a SIP URI is used should be configurable on the device according to the Service Provider's requirements or constraints related to national regulatory framework of SIP-SIP interconnection. If none of the above constraints apply, the use of TEL-URI is recommended.

2.9.3.2 Self-Identification to the network and the addressed contact:

For generating an outgoing request the SIP URI or TEL URI the RCS-e client shall set the From header and the P-Preferred-Identity header with the SIP or TEL URI which has been provisioned. If both SIP-URI and TEL-URI are configured, TEL-URI should be used.

2.9.3.3 User alias

The user shall be able to specify an alias or name to be used for RCS-e services. This information will be sent when establishing a communication to another user so he can get more information than just the MSISDN in case the originating user is not in the receiver Address Book. This case will probably very common in a one to many group chat.

This alias information will be set in the From header of the SIP request and also in the CPIM From header. On the receiving side, if there is no alias in the From header of the SIP request, then the alias in the CPIM From header should be used.

When receiving a request, the RCS-e client device shall follow the rules explained in section 2.9.2.1 and extract the MSISDN or SIP URI. In order to avoid spam and identity manipulation, the receiver shall check the identity of the calling user against the Address Book. If the user is not in the Address Book, the alias information must be used then to provide more information about the calling user but clearly displaying in the UI that the identity is unchecked and it could be false. Otherwise the name of the contact in the address book shall be used instead.

2.10 *Data traffic and roaming considerations*

Until a global roaming agreement on IP based services is agreed and implemented by MNOs, the RCS-e IP traffic in roaming is going to be considered as standard data traffic and will not be distinguishable by the device or the visiting network from other Internet data traffic.

In addition to this, many of the majority of handset platforms only support one APN active at the time. To overcome these difficulties and allow the final user to have greater control of the behaviour of the handset regarding data traffic, RCS-e handsets will come configured with two different APNs:

- Internet APN with RCS-e traffic enabled
- RCS e-only APN with no Internet access

[34] 3GPP TS 24.229 version 10.3.0 (Mar-11): IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3

The user shall be able configure to allow or disallow RCS-e and/or internet traffic in the handset settings when roaming according to the following alternatives:

Data traffic switch	RCS-e switch	APN to use	Comments
Enabled	Disabled	Internet APN	RCS-e client shall not register on the IMS network. When not roaming, this is optional and it is up to the MNO to show this option
Enabled	Enabled	Internet APN	Standard configuration
Disabled	Enabled	RCS-e only APN	RCS-e only configuration
Disabled	Disabled	none	No data configuration

Table 21. APN configuration proposal for data traffic and roaming

Note the RCS-e only APN is configured via the RCS-E ONLY APN parameter presented in section 2 Table 6.

This approach can be used not only for roaming but to protect the user from unexpected charges. Therefore, an MNO can decide to display this setting permanently (covering home network scenarios). The behaviour of whether to show the setting permanently is driven by the configuration parameter ENABLE RCS-E SWITCH (see Table 6). If enabled, the setting is permanent. If disabled, the setting is only proposed during roaming.

Finally note that the default configuration (e.g. both Internet and RCS-e enabled) shall be a configuration option available to MNOs during device customization.

2.10.1 Data connection notifications

Taking into account both the regulatory frameworks applying to some markets, it could be necessary to notify the user when a PS connection is going to be initiated. From the data connection notification point of view, there are three possible configurations:

Setting	Terminal behaviour
never connect	• connection disabled • no pop-up
always ask	• pop-up*: requesting confirmation to go online and informing about possible data charges • user has the following options: reject, confirm to connect ones or to switch to 'always connect' and connect • when user confirms the connection is enabled *Alternatively, a shortcut to the device data settings, together with a warning that data charges might apply, is presented where the user may enable the connection.
always connect	• connection enabled • no pop-up

Table 22. Data connection notification options

Consistently with the configuration switches presented in the previous section (RCS-e on/off, data on/off), an RCS-e handset shall be able to apply the data connection notification options (described in Table 22) individually to each of the following connections:

- Internet home: Standard data connection occurring within the MNO provider home network.
- Internet roaming: Standard data connection when roaming.
- RCS-e home: Data connection required for RCS-e occurring within the MNO provider home network.
- RCS-e roaming: Data connection required for RCS-e when roaming

As for the data connection switches presented in section 2.10, it is up to each MNO to decide during customization on whether:

a) Define the default settings (e.g. always connect for all home connections and always ask for roaming ones)

b) Define whether the data connection notification settings are shown as part of the handset configuration settings (i.e. the user is able to change the notification behaviour) instead.

2.11 *Privacy considerations*

At the moment this version of the specification is published, the work to put together a set of guidelines to address the user privacy issues associated to RCS-e is not yet completed. We are including this section to signal the intention of including the outcome of that work in future revisions of this specification.

As a first step and to allow commercialization in those countries with strict privacy regulations, the mechanisms presented in section 2.10 may be also used for privacy purposes, particularly, when the RCS-e switch is made permanently accessible to the user (i.e. not only for roaming cases) via device (ENABLE RCS-E SWITCH configuration parameter set to 1; see Table 6 for further reference).

2.12 *RCS-e and LTE*

The aim of the present section is to give an overview of the possibilities to complement and integrate LTE and RCS-e.

Please note that at the time this specification is published, the work to integrate LTE and RCS-e is not completed, therefore, this section only contains references to those areas where the work has been completed leaving for future versions of the specification the remaining elements for a complete integration.

2.12.1 LTE and Voice over LTE

LTE (Long Term Evolution) is a radio access network based on OFDM (Orthogonal Frequency Division Multiplexing) for the air interface. LTE has been developed in 3GPP (from Release 8 onwards). The key objective of the LTE is to enhance performance and efficiency (e.g. improving downlink/uplink bit rates [Mbps], improving downlink/uplink cell spectrum efficiency (bps/Hz/cell), reducing air interface latency [ms],...).

Voice over LTE (VoLTE) ([PDR-IR.92]) addresses the support for PS based voice, voice supplementary services and SMS. VoLTE is complementary to RCS in terms of services, since dealing with voice services.

Finally it should be noted that it is intended for RCS-e to comply to [RCS4-IR92-ENDORS][35].

2.12.2 LTE capability discovery using the RCS-e

A couple of OPTIONS capability tags (see sections 2.3.1.1 and 2.3.1.2 for further reference on OPTIONS tags) have been introduced in RCS-e to improve the LTE bearer and voice capabilities:

Tag	Usage
+g.3gpp.icsi-ref="urn%3Aurn-7%3A3gpp-service.ims.icsi.mmtel"	As VoLTE is a variant of quality guaranteed VoIP, the mmtel tag is reused to indicate that a VoLTE capable handset is under LTE coverage[36]

Table 23. SIP OPTIONS tag proposal for LTE

These tags are available for future use and may be used for general or service specific optimizations always in conjunction and aligned with the relevant LTE specifications.

2.12.3 LTE and Video share functionality

Video share used over high bandwidth connections such as LTE allows high bitrate bearers, thus allowing better user experience e.g. when using a large screen.

An RCS-e device shall support H.264 video codec with level 1.3 in order to provide 384/768 kbps video over an LTE bearer or over similar high bitrate bearer. Please note that this is an addition to the mandatory format H.264 profile baseline with level 1b

Assumption for use of high bitrate bearer is that connectivity and video parts of both terminals support it and have LTE or other high bitrate broadband access; otherwise the video bitrate will be reduced to the level 1b (as presented in section 2.7.3) in order to assure compatibility.

2.13 *End User Confirmation Requests*

There are several scenarios where the MNO requires an End User approval for some specific purpose, like for example accepting the Terms and Conditions for a Service. Up to

[35] RCS Release 4 Endorsement of GSMA IR.92 GSMA “IMS Profile for Voice and SMS” version 1.0 ([PRD-IR.92]). Both documents are available at www.gsmworld.com

[36] Consistently with the definition present in section 5.1.1.2.1 of 3GPP TS 24.229

now there was not a standard mechanism that allows the MNO to directly ask the End User in this kind of situations.

The RCS-e specification provides a framework that will allow the MNO to inform the End User about a certain situation by opening a dialog in the handset terminal presenting all the available information and ask the user to confirm or decline the proposed request.

The end user confirmation request is implemented using an SIP MESSAGE[37] method containing a XML payload of type application/end-user-confirmation-request+xml that will be sent by the MNO serving the End User to his RCS-e handset/client.

Upon the reception of the SIP MESSAGE, the end user terminal will check the P-Asserted-Identity of the incoming message and match it against the configured URI for the service as defined in Table 6 and extract the request information from the XML payload body. A dialog or notification will be displayed to the End User (UX dependant) showing the confirmation request and related information.

The End User confirmation response will be encapsulated in an XML body with a payload of type application/end-user-confirmation-response+xml and returned either in the SIP MESSAGE response back to the MNO or in a new SIP MESSAGE
The information contained in the end user confirmation request is the following

- **id:** Unique identifier of the request.
- **type:** Determines the behaviour of the receiving handset. It can take one of the following two values:
    - *volatile*, the answer shall be returned inside the 200 OK response. If the SIP INFO message times out without end user input, the request will be discarded.
    - *persistent*, the answer shall be returned inside of a new SIP MESSAGE request. The confirmation request does not time out.
- **pin:** Determines whether a pin is requested to the end user. It can take one of the following two values: *true* or *false*. If the attribute is not present it shall be considered as *false.* This pin request can be used to add a higher degree of confirmation and can be used to allow certain operations like parental control for example.
- **Subject:** text to be displayed as notification or dialog title
- **Text:** text to be displayed as body of the dialog.

Several Subject or Text nodes can be present in the xml body to be able to support multiple languages. In case more of one element is presented a language (*lang)* attribute must be present with the two letter language code according to the ISO 639-1. RCS-e

[37] Please take into account that according to RFC 3428, the size of MESSAGE requests outside of a media session MUST NOT exceed 1300 bytes, unless the UAC has positive knowledge that the message will not raverse a congestion-unsafe link at any hop, or that the message size is at least 200 bytes less than the lowest MTU value found en route to the UAS. Larger payloads may be sent as part of a media session, or using some type of content-indirection. Therefore, this should be taken into account when considering the length of the messages.

clients shall check the language attribute and display the text data of the element that matches the current language used by the user. In case that there is no language matching the user one, the first node of Subject and Text shall be used.

If the type of the confirmation request is *persistent* the MNO can send an optional acknowledgement message of the transaction back to the user with a welcome message, an error message or further instructions. This acknowledgement message will be encapsulated in an XML body with a payload of type application/end-user-confirmation-ack+xml and returned in the 200 OK body of the confirmation SIP MESSAGE.

The following table specifies the xsd schema of the xml payload for the end user confirmation request:

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
elementFormDefault="qualified">
  <xs:element name="EndUserConfirmationRequest">
    <xs:complexType>
      <xs:sequence>
        <xs:element ref="Subject" maxOccurs="unbounded"/>
        <xs:element ref="Text" maxOccurs="unbounded"/>
      </xs:sequence>
      <xs:attribute name="id" use="required"/>
      <xs:attribute name="type" use="required"/>
      <xs:attribute name="pin"/>
    </xs:complexType>
  </xs:element>
  <xs:element name="Subject">
    <xs:complexType>
      <xs:attribute name="lang"/>
    </xs:complexType>
  </xs:element>
  <xs:element name="Text">
    <xs:complexType>
      <xs:attribute name="lang"/>
    </xs:complexType>
  </xs:element>
</xs:schema>
```

Table 24. End User Confirmation Request XSD

The information contained in the end user confirmation response is the following

- **id:** Unique identifier of the request.
- **value:** with the end user confirmation. It can take one of the following two values *accept* or *decline*.

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
elementFormDefault="qualified">
  <xs:element name="EndUserConfirmationResponse">
    <xs:complexType>
      <xs:attribute name="id" use="required"/>
      <xs:attribute name="value" use="required"/>
      <xs:attribute name="pin" use="optional"/>
    </xs:complexType>
  </xs:element>
</xs:schema>
```

Table 25. End User Confirmation Response XSD

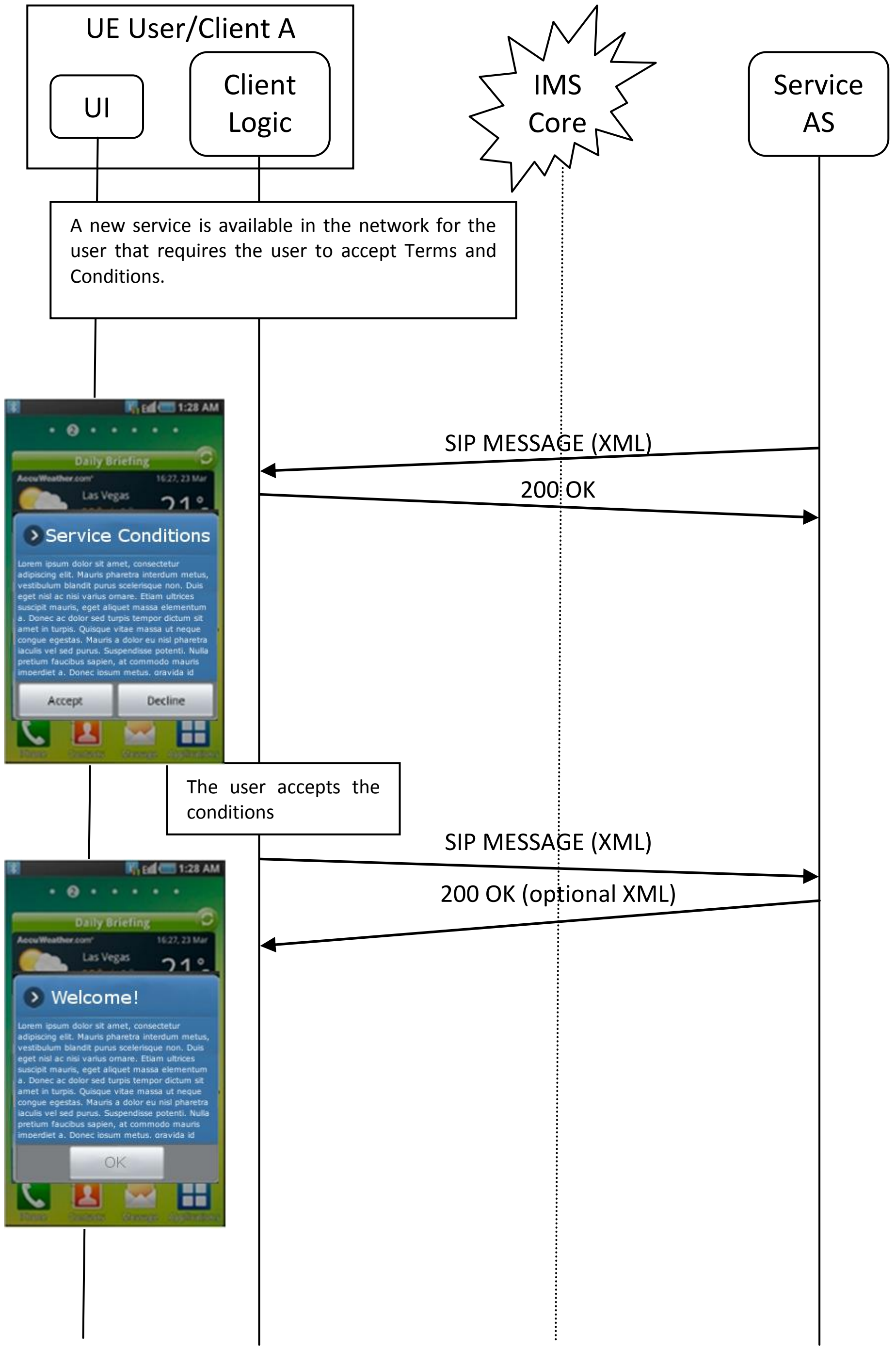
The information contained in the end user acknowledge response is the following

- **id:** Unique identifier of the request.
- **status:** with the end user confirmation. It can take one of the following two values *ok* or *error*.
- **subject:** text to be displayed as notification or dialog title
- **text:** text to be displayed as body of the dialog.

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema                    xmlns:xs="http://www.w3.org/2001/XMLSchema"
elementFormDefault="qualified">
  <xs:element name="EndUserConfirmationAck">
    <xs:complexType>
      <xs:sequence>
        <xs:element ref="Subject" maxOccurs="unbounded"/>
        <xs:element ref="Text" maxOccurs="unbounded"/>
      </xs:sequence>
      <xs:attribute name="id" use="required"/>
      <xs:attribute name="status" use="required"/>
    </xs:complexType>
  </xs:element>
  <xs:element name="Subject">
    <xs:complexType>
      <xs:attribute name="lang"/>
    </xs:complexType>
  </xs:element>
  <xs:element name="Text">
    <xs:complexType>
      <xs:attribute name="lang"/>
    </xs:complexType>
  </xs:element>
</xs:schema>
```

Table 26. End User Confirmation Acknowledgement XSD

2.13.1 Example UC1: Accepting terms and conditions



A new service is available in the network for the user that requires the user to accept Terms and Conditions.

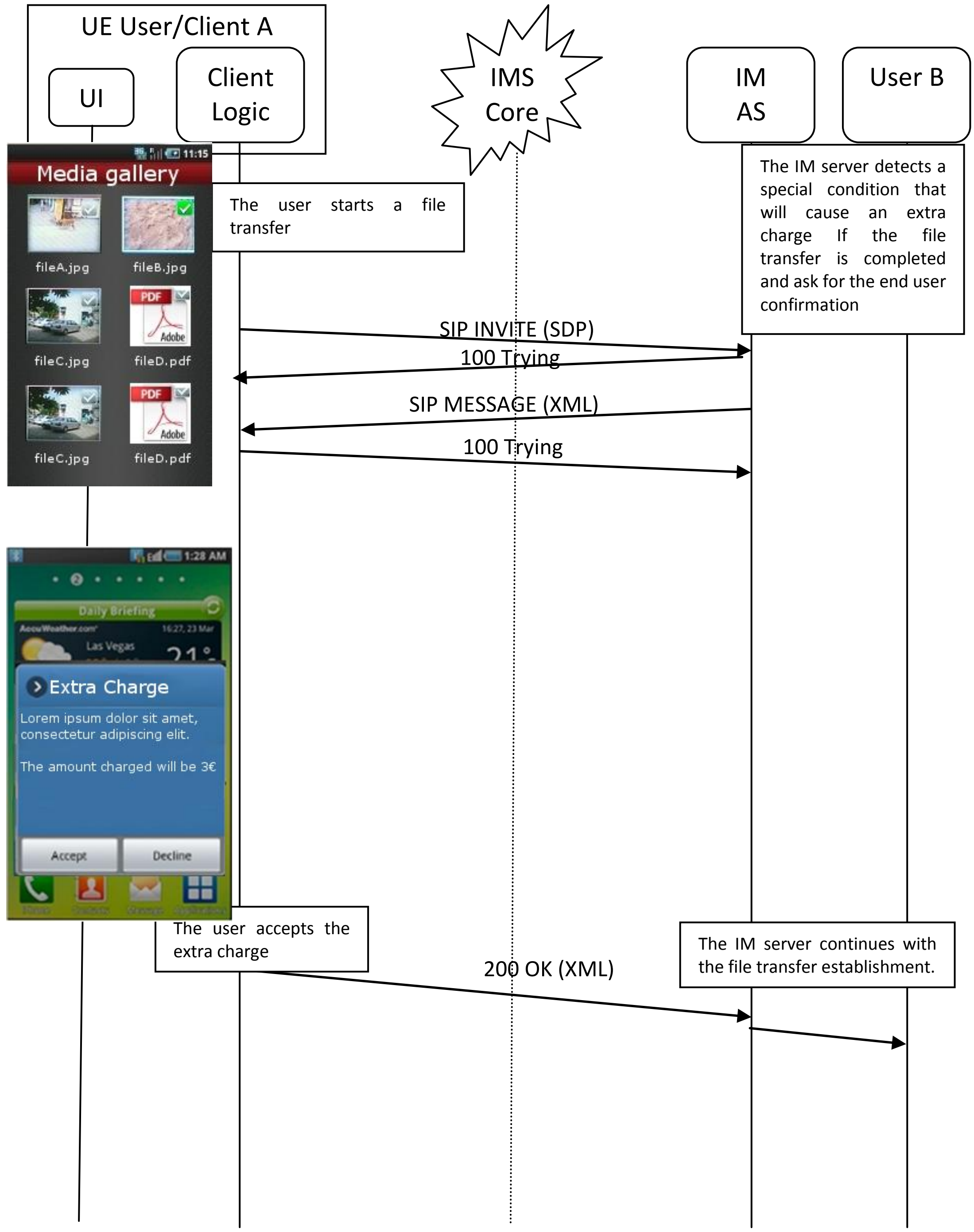
Lorem ipsum dolor sit amet, consectetur adipiscing elit. Mauris pharetra interdum metus, vestibulum blandit purus scelerisque non. Duis eget nisl ac nisi varius ornare. Etiam ultrices suscipit mauris, eget aliquet massa elementum a. Donec ac dolor sed turpis tempor dictum sit amet in turpis. Quisque vitae massa ut neque congue egestas. Mauris a dolor eu nisl pharetra iaculis vel sed purus. Suspendisse potenti. Nulla pretium faucibus sapien, at commodo mauris imperdiet a. Donec ipsum metus, gravida id

The user accepts the conditions

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Mauris pharetra interdum metus, vestibulum blandit purus scelerisque non. Duis eget nisl ac nisi varius ornare. Etiam ultrices suscipit mauris, eget aliquet massa elementum a. Donec ac dolor sed turpis tempor dictum sit amet in turpis. Quisque vitae massa ut neque congue egestas. Mauris a dolor eu nisl pharetra iaculis vel sed purus. Suspendisse potenti. Nulla pretium faucibus sapien, at commodo mauris imperdiet a. Donec ipsum metus, gravida id

Figure 21. Terms and Condition UC example

2.13.2 Example UC2: Accepting Extra Charges



The user starts a file transfer

The IM server detects a special condition that will cause an extra charge If the file transfer is completed and ask for the end user confirmation

Extra Charge

Lorem ipsum dolor sit amet, consectetur adipiscing elit.

The amount charged will be 3€

The user accepts the extra charge

The IM server continues with the file transfer establishment.

Figure 22. Extra Charge UC example

2.14 *GRUU and multidevice support*

RCS-e clients and terminals SHALL support GRUU as specified in [RFC5627][38]. When the user agent generates a REGISTER request (initial or refresh), it SHALL include the Supported header field in the request. The value of that header field SHALL include "gruu" as one of the option tags. This alerts the registrar for the domain that the UA supports the GRUU mechanism.

In each contact included in the REGISTER request, the client SHALL include a "*sip.instance*" tag, whose value is the instance ID that identifies the user agent instance being registered. To avoid potential privacy issues, IMEI SHALL NOT be used as the device-id value of *sip.instance*; instead this device-id value must be an UUID (generated by the handset as specified in [RFC4122][39]) and must not be modified over time If the REGISTER response is a 2xx, each Contact header field may contain a "pub-gruu" conveying the public GRUU for the user agent instance. Please note that the GRUU support is not mandatory for the network operators so user agents shall be ready to not receive any GRUU from the registrar.

If a user agent obtains GRUUs from the registrar, it shall use the public GRUU as a URI parameter for the user agent in non-REGISTER requests and responses that it emits, for example, an INVITE request and 200 OK response.

If a user agent does not obtain a GRUU from the registrar, it shall include the *sip.instance* feature tag in the Contact header with the same device-id value in any non-REGISTER request and responses that it emits. Please note that the destination UA should follow the standard procedure for tags and move them from the contact to accept-contact header when issuing responses or signalling (i.e. message notifications associated to an IM/chat invitation) associated to the initial request.

Please note that for simplification and because long-term standard [RFC5627][38] approach is preferred, the diagrams contained in ANNEX C show the behaviour in a network supporting *pub-gruu* generation. The diagrams for a network supporting the *sip.instance* tag only, would be equivalent but changing the relevant mechanism to carry the device ID (*sip.instance* instead *pub-gruu*).

[38] The Obtaining and Using Globally Routable User Agent URIs (GRUUs) in the Session Initiation Protocol (SIP) IETF RFC is available at http://tools.ietf.org/html//rfc5627. Please note this spec also refers and incorporate parts of IETF RFC 5626 http://tools.ietf.org/html//rfc5626.

[39] The Universally Unique IDentifier (UUID) URN Namespace IETF RFC is available at http://tools.ietf.org/html//rfc4122.

3. RCS-e sequence and UX diagrams

The user must be able to access RCS-e services from the following terminal UI entry points:

- Address book and call-log: The user should be able to access the IM/chat and file transfer services. Note the file transfer is combined with chat on the receiver to create a communication context (i.e. the receiver wants to clarify why the sender is sharing that file). The chat session won't start until the receiver sends the first message, so it is possible to accept the file without chatting.
  In addition to this, the first view of the address book shall clearly identify the RCS-e capable contacts with a RCS-e flag.

- Chat application: The user should be able to access chat directly from the application list. In this case the user can access either one-to-one or, optionally, multi-chat (selecting/inviting more than one user). The user can also access to the chat history and continue a previous chat.

- File browser, media gallery and camera application: The user can access file transfer service. Note the file transfer is combined with chat at UX layer on the receiver to create a communication context (e.g. the receiver wants to clarify why the sender is sharing that file). Although once the incoming file is accepted the transfer is presented on a chat window on the receiver side, the chat session won't start until the receiver sends the first message.

- Chat window: It is possible to aggregate a new contact(s) to an existing chat session. In addition to this, file transfer is also available in one-to-one chat. Although from the protocol point of view, it is necessary to handle a new SIP invitation and MSRP transfer (i.e. file transfer occurs in a separate MSRP context, not in the one used for chat), from the UX point of view, the communication context is already established so it is not necessary to implement any additional actions.

- Call screen: Video and image transfer (live video, stored video or picture). Please note the communication context is already established so it is not necessary to implement any additional actions.

Finally, it should be noted that a precondition to provide access to the RCS-e functionality should be that all the mandatory parameters described in section 2.1 (Table 6) must be correctly configured. In the case any of the parameters is not configured or configured with an unexpected value, the RCS-e functionality should be disabled and in any case presented or accessible to the user (i.e. the phone behaves as it would be a non-RCS-e enabled phone and all RCS-e specific UX elements are no longer presented to the user).

3.1 *Access to RCS-e services through address book or call-log interaction*

The address book (and to extend the call-log window as an alternative for users who have been recently phoned) is the centrepiece to access all services.

From the address book/call-log the user has access to the following services:

- The user can identify which services are available for each contact. When a contact is selected, the service capability is updated via SIP OPTIONS to provide the current, real-time, status for the contact.
- If available, the user can start a chat
- If available, the user can start a file transfer

3.1.1 General assumptions

In the following sections we will be showing the relevant chat message flows and reference user experience (UX). Please note that the following assumptions have been made:

- For simplicity, the internal mobile network interactions are omitted in the diagrams showed in the following sections.

3.1.2 Capabilities update process

The capabilities update process is described in the following diagram. In this case the contact (user B) is a RCS-e contact which is registered. Please note the capabilities are only updated on 1-to-1 chats. In multichat sessions, there are no other services available and the ultimately responsibility to maintain and report the status of the session is the IM application server.

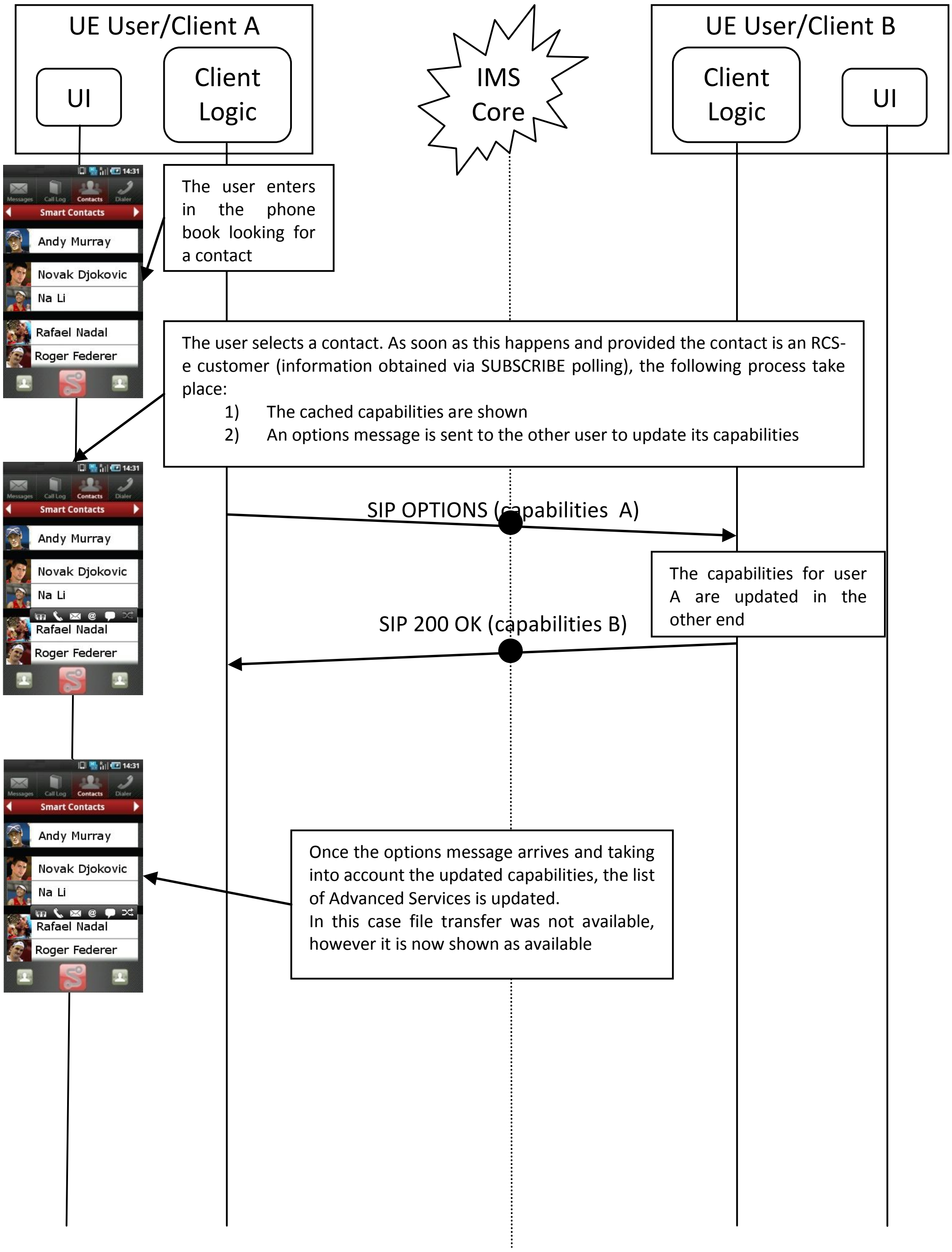
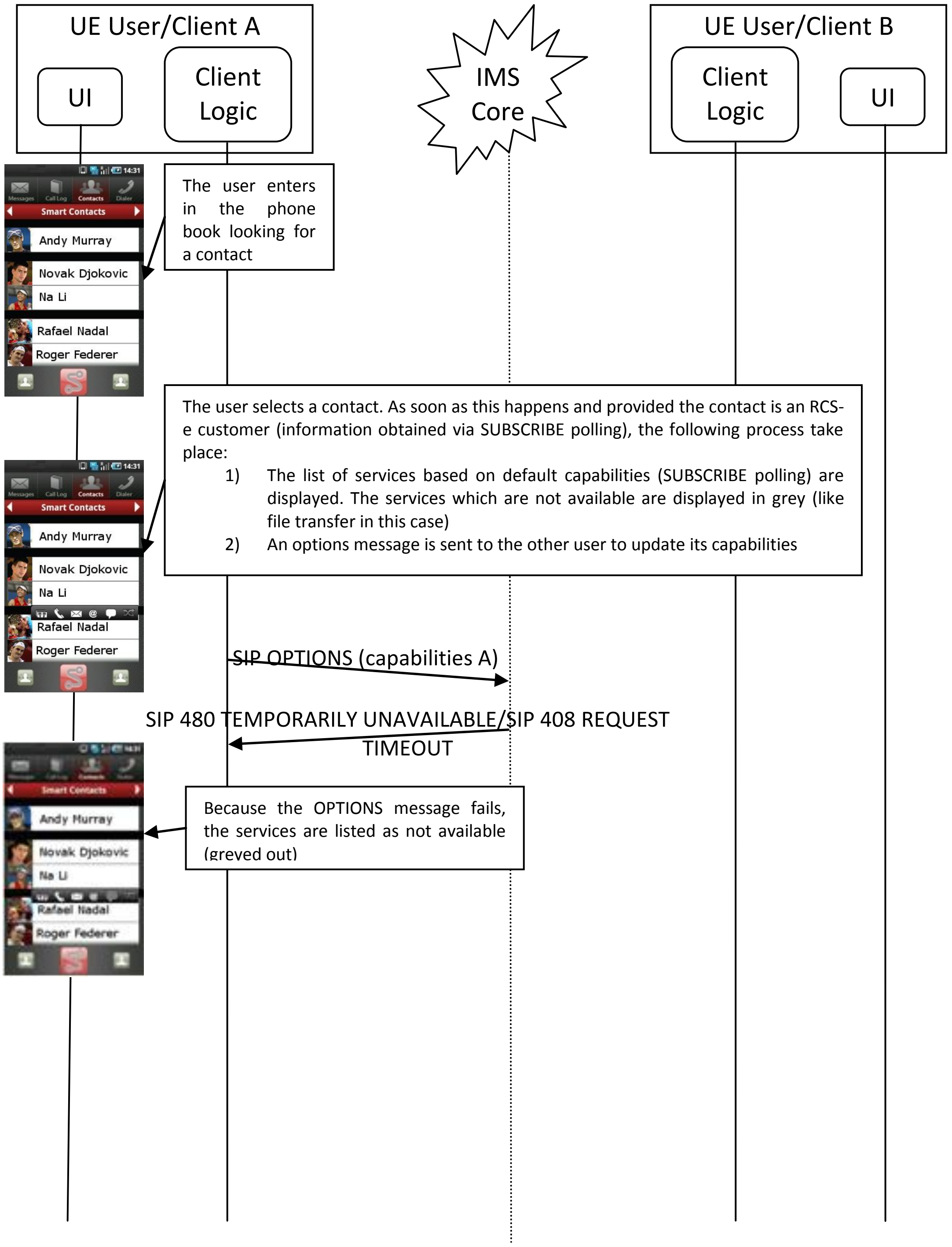

UE User/Client A
UI
Client Logic
IMS Core
UE User/Client B
Client Logic
UI
Smart Contacts
Andy Murray
Novak Djokovic
Na Li
Rafael Nadal
Roger Federer
The user enters in the phone book looking for a contact
The user selects a contact. As soon as this happens and provided the contact is an RCS-e customer (information obtained via SUBSCRIBE polling), the following process take place:
1) The cached capabilities are shown
2) An options message is sent to the other user to update its capabilities
SIP OPTIONS (capabilities A)
The capabilities for user A are updated in the other end
SIP 200 OK (capabilities B)
Once the options message arrives and taking into account the updated capabilities, the list of Advanced Services is updated.
In this case file transfer was not available, however it is now shown as available

Figure 23. Address book: Capabilities update

If User B is either not a RCS-e user or it is not registered, the network provides a response to the OPTIONS message (404 NOT FOUND, 480 TEMPORARILY UNAVAILABLE/408 REQUEST TIMEOUT respectively; please refer to section 2.3.1 for further reference). In this case, the User A's client assumes that no services are available to communicate with User B[40].



The user enters in the phone book looking for a contact

The user selects a contact. As soon as this happens and provided the contact is an RCS-e customer (information obtained via SUBSCRIBE polling), the following process take place:

1) The list of services based on default capabilities (SUBSCRIBE polling) are displayed. The services which are not available are displayed in grey (like file transfer in this case)
2) An options message is sent to the other user to update its capabilities

Because the OPTIONS message fails, the services are listed as not available (greyed out)

Figure 24. Address book: Capabilities update (II)

[40] It should be noted that in this case if IM CAP ALWAYS ON (see Table 3) is enabled, the IM/chat should still be reported to the user as available even the other end is not registered.

3.2 *IM/chat service*

The IM service enables users to exchange messages between one or more users instantaneously. Chat is a baseline service available to any registered user.

3.2.1 General assumptions

RCS-e IM (Chat) is a baseline service, available to any registered user, using [RCS2-OMA-SIMPLE-ENDORS][41] as a specification basis. As new optional features are introduced (e.g. store and forward, "displayed" notification), some adjustments, clarifications or modifications need to be brought to [RCS2-OMA-SIMPLE-ENDORS][41]. The delta between RCS Release 2 IM and RCS-e IM are highlighted in section 3.2.2.

3.2.2 Delta between RCS-e and RCS Release 2 on the IM functionality

3.2.2.1 Functional Level

The following optional new features are introduced in RCS-e:

- store and forward

The deployment of this feature is at the MNO's discretion. This feature requires an IM server to store messages and notifications (delivered and displayed) when the destination user is not online and send it to the user when he goes online again (i.e. store and forward).

- "displayed" message disposition

This new disposition allows the sender of a message to be notified when this message has been displayed on a device of the receiving user.

Note that this notification cannot certify that the recipient has actually read the message, it can only indicate that the message has been displayed on the recipient's terminal UI.

- delivery of notifications (delivery and displayed) outside a session

It should be possible to deliver notifications independently on whether the MSRP session associated to a chat has been established or not. When delivery these notifications outside a MSRP session, SIP MESSAGE should be used instead as described later in this section.

- Local Black List

The terminal/Client shall support a locally stored IM Black List. Basic guidance is provided in section 3.2.4.1.

- Conversation history

The terminal/Client shall support a locally stored conversation. The implementation details are not yet covered in this version of the specification.

[41] RCS Release 2 - Endorsement of OMA SIP/SIMPLE IM 1.0 - v2.0 available at www.gsmworld.com

- User Alias

A user defined name can be sent when establishing a communication with another user.

Please note that as a consequence of adding the mentioned new features, some of the exisiting ones had to be limited:

- Small multimedia messages within a chat

To reduce the complexity associated to the store and forward feature, the multimedia messages feature is out of scope in RCS-e. The transference of files while a chat is taking place shall be performed on a separate session (this is a protocol level, from user experience perspective, the user should be able to transfer file while in chat), irrespectively of the file type or nature.

- Chat rejection

Unlike in RCS Release 2 and due to the new chat acceptance mechanism based on user activity, there is no concept of rejection at UX level. At the technical/Protocol Level, the 603 DECLINE is not used in RCS-e, instead the terminating side ignores the invitation and just waits for the request to expire.

3.2.2.2 Technical/Protocol Level

Compared to RCS Release 2, in order to support store and forward and message disposition, RCS-e adds:

- Support of [RFC5438][42]

  RCS-e relies on the support of Instant Message Disposition Notification (IMDN) as defined in [RFC5438][42] to request and forward dispositions of all the exchanged messages.

- Device identification using the mechanisms described in section 2.14.
- Message identification for all messages (including those conveyed in the SIP INVITE and notifications delivered via SIP MESSAGE)
- Auto-acceptance of store and forward IM Server PUSH of stored notifications

  Only the device which has sent the relevant message shall accept the notification.

- store and forward IM Server PUSH of stored messages
- Message delivery and displayed notifications

The introduction of these concepts brings modification in the following requests compared with RCS Release 2:

- SIP INVITE

[42] The Instant Message Disposition Notification (IMDN) IETF RFC is available at http://tools.ietf.org/html//rfc5438.

  - When an IM session is initiated by a Client, the SIP INVITE, still has to convey the message in the "subject" Header. In addition in RCS-e, the message has to be replicated in a CPIM/IMDN[43][44] wrapper including the DateTime; Message-ID and Disposition-Notification header fields. The deviceID shall be carried using the mechanisms described in section 2.14.
- The client is able to identify that a IM-AS is pushing stored messages because the invite originated from the IM-AS is for a 1-2-1 chat and contains a Referred-by header (consistently with the explanation provided in section 2.9.1). Using this mechanism the handset/client implementation is able to differentiate a session for delivering differed messages and only send notifications back. If the user replies with a new message, then a separate session shall be established after all the deferred messages have been delivered (please refer to NOTE 5 in Annex B section B.12).
  - When an IM-AS is delivering stored notifications with the aim of signalling the client that the session has to be auto-accepted, the p-asserted-id header is set to a known value (*rcse-standfw@<domain>*).
  - GRUU (GRUU public identities, *pub-gruu*, as presented in section 2.14) will be used to support the Auto-acceptance of PUSH of stored notifications. Only the client whose device identifier matches the *pub-gruu* value is allowed to accept the session. This new request shall also use the well-known URI identifier in the P-Asserted-Identity (*rcse-standfw@<domain>*)[45].

- SIP MESSAGE

RCS-e relies on SIP MESSAGE requests to carry notifications (delivery and display) of messages sent prior the establishment of a media session. Again, the SIP MESSAGE shall carry a CPIM/IMDN[44] wrapper including the DateTime; Message-ID, Disposition-Notification header fields. In addition to this, it should also contain the delivery notification field to confirm the reception or the displayed notification to confirm the message was displayed by the other end. The deviceID shall also be transported following the mechanisms described in section 2.14. The Accept-Contact header of the SIP MESSAGE used for IMDN shall carry the *+g.oma.sip-im* feature tag[46].

The use of SIP MESSAGE for Pager Mode messages is still not supported (consistently with RCS Release 2).

- MSRP SEND

[43] It should be noted that a SIP INVITE carrying a CPIM/IMDN will indeed have a multipart body because a SDP configuration is still required.

[44] The CPIM/IMDN wrapper should be UTF-8 encoded to avoid any potential internationalization issues.

[45] Consequently, the *rcse-standfw@<domain>* value becomes reserved and cannot be used by any identity.

[46] This ensures that initial filter criteria already in place in GSMA RCS R1/R2/R3 environments will route these SIP MESSAGEs to the OMA SIMPLE IM server.

In RCS-e, all messages (IM) are conveyed in CPIM/IMDN[44] wrappers, which is strictly forbidden in RCS Release 2.

When applicable, these MSRP SEND requests with CPIM/IMDN[44] wrappers are used by the sender to request IMDN 'delivered' and 'displayed' notifications and by the receiver to provide the IMDN same notifications.

Because delivery reports are requested via CPIM/IMDN in RCS-e, RCS-e devices should not request successful MSRP REPORTs, in other words, the Success-Report flag should either not be included at all (since the default value is 'no'), or be set to 'no'.

Finally, in order to support the use of aliases, the limitation added in [RCS_IMENDORSE][41] for the use of display-name are removed in RCS-e. As well, an additional requirement is added which is that the sender should set the display-name in both the SIP From header and in the CPIM From header of outgoing requests.

3.2.2.3 Delivery notifications

There are two possible scenarios that should be considered:

1. Delivery notifications associated to messages that have been delivered before a MSRP session has been established

In this case, the mechanism which the receiver's client shall use is to send the notification using SIP MESSAGE. More in details, the CPIM/IMDN[44] wrapper should carry the same msg-ID contained in the original message plus an 'delivered' notification as described in [RFC5438] [42] section 7.2.1.1.

2. Delivery notifications associated to messages that have been delivered after a MSRP session has been established

In this case, the MSRP SEND message carrying a CPIM/IMDN[44] wrapper with a 'delivered' notification as described in [RFC5438][42] section 7.2.1.1 and presented before in this section. Again the original message CPIM/IMDN[44] msg-id shall be carried to identify the message this notification is associated to.

The sender client side shall support both scenarios, process the delivery notification and display this information to the user. The recommendation is to show this information only within the IM window without a need for a pop-up or information message when the user is outside the IM application.

When the recipient of a 'delivery' notification is not available and in those case where an IM-AS is available (either sender side or receiver), the IM-AS should be able to store and forward this notification independently on whether they are delivered within a MSRP session or outside via SIP MESSAGE.

Please note that in multidevice scenarios, when a session is set up and delivery notifications start to arrive for stored messages, the IM server needs to ensure that they are not forwarded to the current device in the IM session if that participant is not the right one.

3.2.2.4 Display notifications

There are two possible scenarios that should be considered:

1. Delivery of displayed notifications when a MSRP context is in place:

   In this case, display notifications are carried using the MSRP SEND message, with a CPIM/IMDN[44] wrapper carrying a 'displayed' notification as described in [RFC5438][42] (section 7.2.1.2). Again the original message CPIM/IMDN[44] msg-id shall be carried to identify the message this notification is associated to.

2. Delivery of displayed notifications when a MSRP context is not established:

   In this case, the mechanism which the receiver's client shall use is to send the notification using SIP MESSAGE. More in details, the CPIM/IMDN[44] wrapper should carry the same msg-ID contained in the original message plus an 'displayed' notification as described in [RFC5438] [42] section 7.2.1.1.

The sender client side shall support both scenarios, process the displayed notification and display this information to the user. As for the delivery notifications, the recommendation is to show this information only within the IM window without a need for a pop-up or information message when the user is outside the IM application.

It should be noted that the displayed notification is optional meaning the user (receiver) shall have access to a configuration parameter to enable or disable this notification via UI (i.e. a user can disable sending back displayed notifications to the sender).

When the recipient of a 'displayed' notification is not available and in those case where an IM-AS is available (either sender side or receiver), the IM-AS should be able to store and forward this notification independently on whether they are delivered within a MSRP session or outside via SIP MESSAGE.

Please note that in multidevice scenarios, when a session is set up and delivery notifications start to arrive for stored messages, the IM server needs to ensure that they are not forwarded to the current device in the IM session if that participant is not the right one.

3.2.3 Client assumptions

In the following sections we will be showing the relevant chat message flows and reference user experience (UX). Please note that the following assumptions have been made:

- For simplicity, the internal mobile network interactions are omitted in the diagrams showed in the following sections.
- Each MNO MAY deploy an IM Server (NB IM server is optional in RCS-e specifications), to handle all messages from its customers.

- Prior to the chat, the user accessed its address book or IM/chat application to start the communication. As described before, while these actions are performed an OPTIONS message is sent to double-check the available capabilities. In the following diagrams we are assuming that this exchange (OPTIONS and response) have already taken place, and therefore, both ends are aware of the capabilities and, consequently, the available RCS-e services. If that is not the case, the OPTIONS message should be sent at the same time the chat is being setup.

- All the IM service exchanges presented in this document follow the RCS Release 2 GSMA specification [RCS2-OMA-SIMPLE-ENDORS][41] regarding client terminals with the following differences:
  - Procedures have been introduced to inform the sender about the delivery status of an IM sent before the session is established (i.e. IM in the Subject header of a SIP INVITE). These procedures are derived from Instant Message Disposition Notification (IMDN for short) [RFC5438] [42] and adapted to the context of session-mode instant messaging.
  - The terminal UI must be implemented in a way that the user can clearly distinguish if the message has been sent (but not yet received), received, or displayed. In addition, the time the message was originally sent shall be also presented.
  - Procedures, based on the IMDN disposition 'displayed' have been introduced at the sender side to request 'displayed' notifications and at the receiver side to provide 'displayed' notifications.
  - A Store and Forward functionality can be used in IM Server. The procedures followed by the Store and Forward functionality of an IM Server are covered in ANNEX B.
  - Procedures for Multi-device support with Store and Forward mode have been introduced in order to ensure consistent delivery of deferred delivered/displayed notifications to the intended device.

MNO support of the store and forward functionality is optional in RCS-e. To allow a MNO to provide store and forward functionality to its customers even in cases where the IM session is established toward an MNO that doesn't support store and forward, the messages may be stored in the sender’s IM server.

From the UX experience point of view, there are three possible entry points to this service:

- Address book/Call-log: chat can be initiated to any RCS-e contact with IM capability as described in 3.2.2.1.

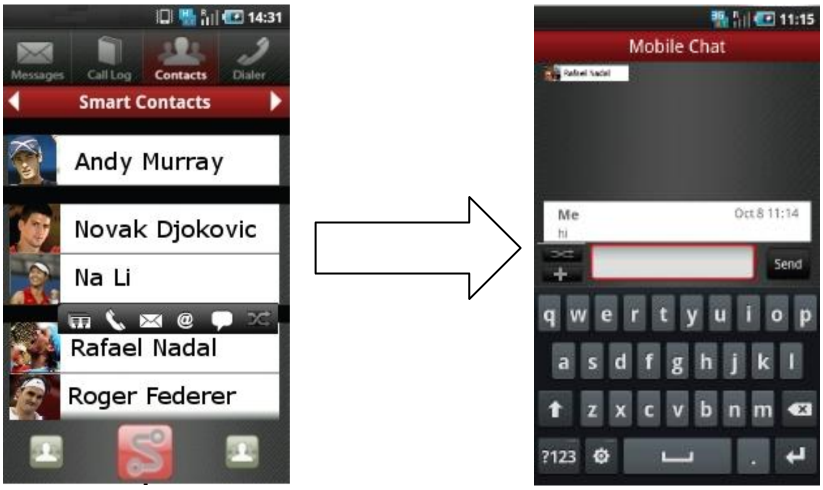


Figure 25. Reference UX for accessing chat from address book/call-log

- IM/Chat application: There should be a dedicated IM/chat application entry point in the phone menu – task oriented initiation. This application will provide access to the chat history and gives the possibility to start a new chat.

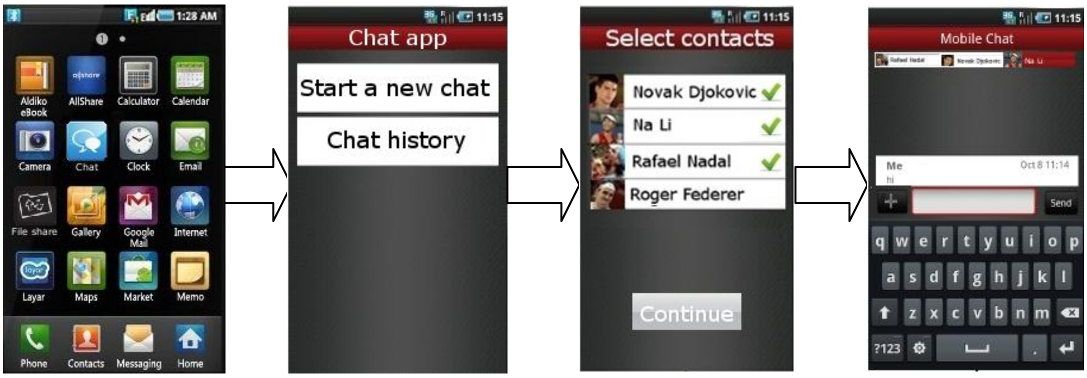
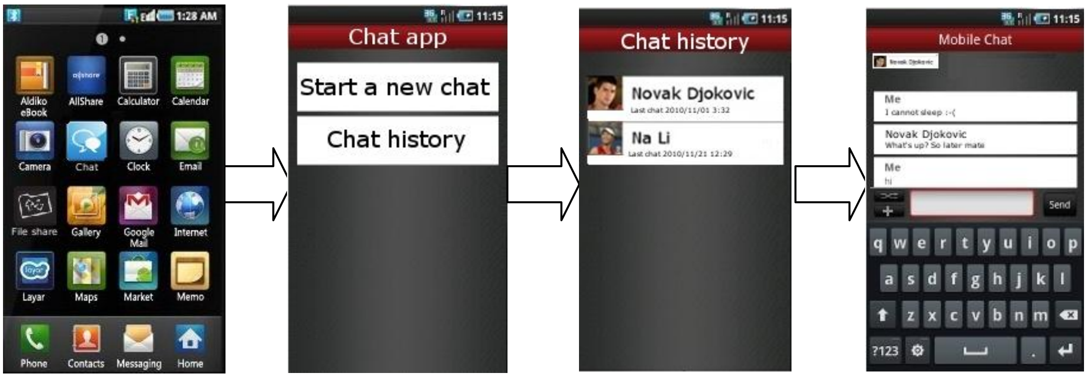


Figure 26. Reference UX for starting a chat from the IM/chat application

Once the IM/chat application is opened, the user will be presented with the complete list of RCS-e contacts with IM capability. Contacts which are currently not registered will be shown or not depending on the IM store and forward policy chosen by the MNO.

In addition to the *"start a new chat"* functionality, the IM/chat application allows the user to browse the chat history, both one-to-one and one-to many sessions:



Me
I cannot sleep :-(

Novak Djokovic
What's up? So later mate

Me
hi

Figure 27. Reference UX for starting chat from the IM/chat application history

File transfer (receiver): When transferring a file and with the aim of establishing a communication context for the transfer (e.g. the receiver may want to know why the sender is sharing that file) and after the transfer has been accepted, the file transfer is presented to the receiver as a chat UX with a file being transferred. Please note that at the time the file is presented, the chat session is not started; the chat session will only start when if the receiver sends a chat message back to the sender.

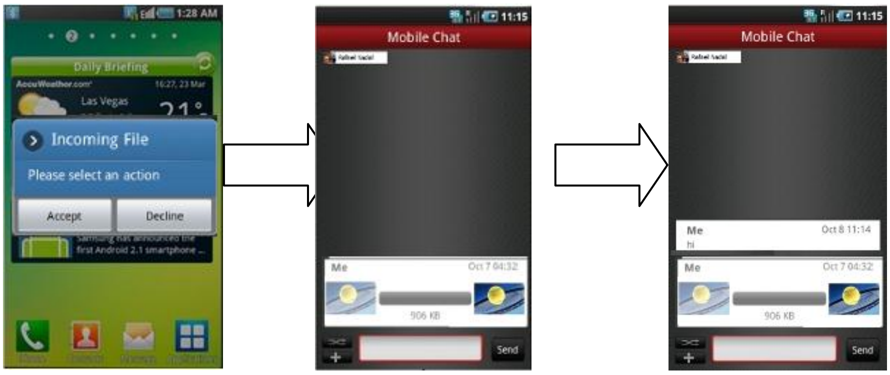


Figure 28. Reference UX file transfer on the receiver side

Please note section 3.4 covers the RCS-e file transfer service in detail.

3.2.4 1-to-1 Chat

A 1-to-1 Chat is a message exchange between two RCS-e users. Please note that where the specification describes the user interface, it should be taken as guidance.

3.2.4.1 Initiating a chat

A RCS-e user (A) initiates a chat by selecting one of his contacts (B) from the Address Book or IM/chat application in his mobile phone, or in the Contact List in the Broadband Access PC client.

Device A (either mobile or PC) will send a query for the real-time capabilities of contact B to ensure the IM service is available for that user at that time. If B is not available and there is no IM store and forward server on A's side and B's side, or if an answer to the query is not received in less than a time lapse (left to OEM User Experience criteria), then the contact will be shown as 'Not available for a Chat session', and SMS service could be offered as messaging option. Once the availability of the IM service is ensured end-to-end and the user performs the appropriate UI actions on the device, a message composer and an empty chat window will be opened.

When user A types the first message and presses the "Send" button, device A will initiate an IM session invitation toward B (for multidevice scenario see Multidevice handling in section 3.2.4.12). The IM session invitation is initiated according to the rules and procedures of [RCS2-OMA-SIMPLE-ENDORS][41] except that the message should be duplicated in a CPIM/IMDN[44] wrapper including the headers requesting an IMDN according to the rules and procedures of [RFC5438] [42] (if IM store and forward is enabled on the IM application server, see section 3.2.4.11). If there is no CPIM body carrying the actual INVITE message (e.g. a client implementing OMA-IM which is not an RCS-e client), then, even if there is an IMDN Disposition-Notification header requesting IMDNs, the message will not be stored in case of delivery failure, and there is no requirement that an IMDN will be generated, since there is no message.

When the device B receives IM session invitation, it will automatically send a SIP 180 answer toward A (if some kind of spam or black list is implemented on the device and user A is in the blacklist, the invitation is terminated following the procedure described in section 3.2.4.15). If the received IM session invitation contains an IMDN requesting 'delivered' notification, the device will send back a SIP MESSAGE containing the IMDN indicating successful delivery of the message sent by A according to the rules and procedure of [RFC5438] [42].

In the side B, a notification (UI dependant) will be displayed on device to inform about the incoming message. The user will be able to read the message and go to the chat window to answer the message.

User A can type additional messages before the chat is answered, i.e. before the IM session is established. The receiving client will send a 486 BUSY HERE response to the outstanding INVITE when a new INVITE arrives from the same user so that there is no more than one outstanding INVITE from one user. The IMDN for 'delivered' status is requested and sent similarly to the first session invitation. On B's side, a notification may be displayed for each received message (UI dependant).

3.2.4.2 Answering a chat

When B's device detects user activity relevant to the consumption of the message contained in the invitation (e.g. click on a pop-up to go to the IM window …) the 1-to-1 chat session is established according to three possible criteria:

1. Handset implementation client returns the 200 OK signalling the initiation on the remaining procedures to establish the chat when the receiver consumes the notification opening the chat window. Please note that this is the default criteria for RCS-e and, consequently, all the diagrams shown in this document reflect this behaviour.
2. The 200 OK is sent when the receiver starts to type a message. Please note this is the default criteria for RCS as described in [RCS2-OMA-SIMPLE-ENDORS][41].

3. The 200 OK is sent when the receiver sends a message. Please note the receivers' message will not generate an invite but instead will be buffered in the client until the MSRP session is successfully established in this case.

Please note that the behaviour can be configured via the IM START SESSION parameter as presented in Table 6 and covered in detail in Annex A section A.2.4.

If the IM session invitation from A contained an IMDN requesting 'displayed' notification, B generates an MSRP SEND request toward A that contains the IMDN 'displayed' status for the message received from A.

The rule and procedure of [RCS2-OMA-SIMPLE-ENDORS][41] are followed to handle the case where multiple IM sessions from A are pending on B's side. I.e. the last received IM session is established and the other pending sessions are answered with a 486 BUSY HERE response. In such cases, if the IM session invitations from A contained an IMDN requesting 'displayed' notification, B generates an MSRP SEND request toward A that contains the IMDN 'displayed' status for each message received from A

3.2.4.3 Messages exchanged in an established chat

As long as this IM session is established, further messages exchanged between A and B are transported in the MSRP session according to the rules and procedure of [RCS2-OMA-SIMPLE-ENDORS][41] except that, for the received MSRP SEND requests containing an IMDN 'displayed' and 'delivered' request, when the user message is delivered or displayed, the receiving device must generate and MSRP SEND request containing the IMDN status.

3.2.4.4 Display and local storage

All the messages will be stored in the device, together with some kind of time indication and an appropriate indication of the part that sent each one.

In the user's device, all the conversations held with the same contact will be displayed in a single thread, ordering stored messages on a timeline basis.

When storage limit is reached, deletion should happen on a FIFO queue policy. It is open to OEM criteria how to implement other opt-in deletion mechanisms (e.g., ask always, delete always, delete any conversation/message from specific contacts…).

3.2.4.5 Leaving the chat composing window

Once a 1-to-1 chat is established any of the two users can leave the composing window without closing the chat. For example, a user could move to his mobile home screen to check an incoming email, or make a phone call.

While the chat composing window is not shown (that is, it is not the foreground window) any incoming message corresponding to that chat will trigger a status notification (UI dependant) so the user is aware of the new message and, if he chooses so, get back to the chat composing window to answer it.

Also, the user could decide to get back to the chat composing window and send a new message without receiving one. The user would be able to do that via the IM/chat application, which will display the on-going chats, or via the Address Book by clicking on the contact with whom he has the chat session opened.

In both cases, when the user gets backs to the chat composing window, all the messages will be displayed.

3.2.4.6 'Is Composing' notification

When any user starts typing in the chat composition window, an *'Is Composing'* notification will be sent to the other user. His UI will then display an indication in the chat composing window to indicate it (UI dependant).

The *'Is Composing'* indication will be removed from the UI when a new message is received, when a timeout expires without receiving a new message, or when a new 'Is Composing' notification arrives.

The "*is Composing*" notification is handled according to the rules and procedure of [RCS2-OMA-SIMPLE-ENDORS][41]. Consequently, the 'is Composing' indication is not sent with CPIM headers, and a delivery and/or displayed notification shall not be requested.

3.2.4.7 Closing a chat / Re-opening a chat

Any of the two users can close his IM session associated with an established chat. This can be done from the chat composing window or in the IM/chat application.

The user would be able to re-open the chat however the resulting action at protocol level would depend on whether the IM session is still open or not.

Closing the IM session will not be notified to the remote user in the chat. The session is terminated, therefore, if the remote user sends a message, a process similar to the initiation of a chat is performed as described in 3.2.4.1.

3.2.4.8 Chat inactivity timeout

When a device or the network detects that there was no activity in a chat for a configurable period of time, it will close the established IM.

3.2.4.9 Chat abnormal interruption

If a user in a chat suffers an abnormal termination of the IM session, for example loss of coverage, it will be considered as it he had closed the chat and the mechanisms specified in section 3.2.4.7 (closing a chat) will apply, but in this case the "Send" button will be disabled. If the UE determines that a message could not be sent (e.g. MSRP SEND failed or received no response), it must inform the user that the chat message was not sent. If TCP connection is lost, client needs to resend them in a new chat session once reregistered.

In temporary interruption cases, for example the mobile phone gets network coverage again, the chat window will be enabled again and the re-opening chat mechanism explained in section 3.2.4.7 will be available.

3.2.4.10 Re-Opening a chat

An old chat conversation can be reopened. From the user perspective, it will be the same procedure as for initiating a chat (section 3.2.4.1), except that when the new message is sent, the new IM session will be established.

The device then will display the previously stored conversations with that contact preceding the current active one. If any displayed notifications need to be generated, they will be sent towards the sender outside a session if there is no session established with the sender using SIP MESSAGE as described in section 3.2.2.4. In a multidevice scenario, the same behaviour applies if there is an active session but the current session with the sender is with the wrong device of the sender."

3.2.4.11 Store and Forward Mode

Store and forward functionality is optional and it is up to each MNO to deploy it (i.e. to deploy an IM Server supporting store and forward because the client side implementation is mandatory in any case).

In order to provide store and forward functionality, an IM Server is required. There are three possible scenarios:

- Sender and receiver are on networks with an IM Server: In this case the receiver IM Server has the responsibility to store IM which are not delivered. The sender IM Server has the responsibility of storing the delivered/displayed notifications in case the sender is no longer online
- Only the sender is on a network with an IM Server: The sender's IM Server takes all the responsibility to store IM and/or delivered/displayed notifications in case they cannot be delivered. Because the sender IM Server cannot have information on when the destination is online, a retry mechanism will be employed instead.
- Only the destination is on a network with an IM Server: The receiver's IM Server takes all the responsibility to store IM and/or delivered/displayed notifications in case they cannot be delivered. Because the receiver IM Server cannot have information on when the sender is online, a retry mechanism will be employed instead.

In order to be able to deliver stored delivered/displayed notifications to a sender device that has become offline, without disrupting the user experience, the IM Server supporting store and forward functionality shall initiate a special IM session for the purpose of delivering these notification. This special IM session shall be automatically accepted by the device. It is recognized by the device thanks to the well-known URI (*rcse-standfw@<domain>*) uniquely identifying the store and forward service identity in the P-Asserted-Identity header field.

Note that the IM Server supporting store and forward is required to send the delivered/displayed notifications to the exact device that has previously sent the associated messages. Therefore the IM Server implementing multidevice handling shall support GRUU (see section 2.14).

Other aspects of the store and forward functionality implementation on the IM Server are out of scope of this specification. Please note additional diagrams are provided in ANNEX B for reference.

Finally, please note that store and forward functionality on the network side is optional, therefore there is a dedicated configuration setting (IM CAP ALWAYS ON, see section 2.1 Table 6 for further reference) which is used to configure the client to support or not this functionality and the implications on the user experience.

3.2.4.12 Multidevice handling

Multidevice happens when a user is able to have more than one device (PC and/or mobile) connected at the same time.

When a new 1-to-1 chat is initiated and a message is sent from user A to a user B with multiple devices registered at the same time, the network forks the IM session according to the rules and procedure of [RCS2-OMA-SIMPLE-ENDORS][41].

Each of B's devices that receives the session invitation generates a SIP MESSAGE to carry the delivered IMDN as per [RFC 5438]. In a multidevice scenario, if a sender receives more than one IMDN for a sent message, it shall discard all copies except the first one it receives.

The user B will be able to answer to the chat from any of his devices, but in the moment he sends a message from one of them, that device B will become the only active device and all the other IM sessions for the other devices will be closed. All the following messages sent to the user B will be received only in the active device B1 using the already established IM session.

Device switching (as per [RCS2-OMA-SIMPLE- ENDORS][41]):

a) If user B closes the IM session from the active device (either by closing the chat conversation from the chat window or due to an abnormal termination), any new message sent by user A through the chat will make the IM server establish again one IM session per connected device B and send the message to them all as explained before.

b) If user B changes from one device B1 to another B2 by just sending a new message to the chat from the new device B2. It will send a new INVITE with the message in the subject field as usual that will go to A's device. When A's device detects a new INVITE session from a user (B) which already has an established session it shall end it and accept the new one. All subsequent messages will be received only by device B2. Device B2 must then store the received messages and display them appropriately. If A still has delivery and displayed reports for Device B1, they should be sent before A's device tears down the old session."

The conversation history is implemented at device level. The intention for future release is reallocate back this functionality on the network.

3.2.4.13 Switching to 1-to-many Chat

A group chat could be only started from a user on a MNO which has deployed an IM-AS. It is optional for a MNO to provide the 1-to-many functionality, so from the terminal perspective, if there is not a configured IM conference-factory-URI, the terminal should not allow the user to add additional parties to the chat nor starting a multichat.

A 1-to-1 chat can be converted into a 1-to-many chat by any of the two users A and B adding new users to it. Users A, B will be given the option in their UI to select one or more contacts added to the conversation, only among the contacts known by their devices to be RCS-e Users.

A real time check of contacts capabilities will be performed as when initiating a chat (section 3.2.4.1). A new group chat composing window will be created in user A's device and the result of this check will be shown in it.

When user A sends the first message a new one-to-many chat will be opened between all the selected users, A and B as described in section 3.2.5.1.

For B user a new group chat composing window will be created in the user's device. It is recommended to the UX implementations not to close the already established one-to-one chat window but just switch the focus to the new created group chat windows.

Please note Store and Forward support for 1-to-many Chat is out of the scope of this specification and, therefore, this functionality is not required.

3.2.4.14 File transfer within 1-to-1 chat

During a one to one chat, any of the users will be able to initiate a file transfer from the chat composing window. The file transfer will be established using a new SIP session and carried in a new MSRP session which is different from the one used for the chat session.

The receiving user will get the file transfer invitation inside the chat window and will be able to accept or decline it.

If the user accepts the file transfer, the terminal will either ask the user the location to store the file or use a default directory. Once received, the user will be able to open the file from the chat composing window.

3.2.4.15 Spam/Blacklist filter

User will be allowed to qualify undesired incoming chat as spam. This will prevent subsequent messages from those originators to be shown or even notified to the user. Also, this undesired traffic will not be acknowledged to have been delivered.

From the technical implementation point of view, when receiving a message from a sender included in the spam sender list the client/handset implementation should:

- Terminate the transaction with a 486 BUSY HERE sent back to the sender.
- The receiver will still issue a delivery notification will be sent back to the sender.
- From the UX point of view, the receiver will not be notified on the reception of a message from a blacklisted sender and the message will be copied to the spam filter.

Please note that for clarification, the blacklist behaviour does not only apply to IM but also to the reception of files. If an invitation to receive a file is received from a blacklisted user, the client/handset implementation should:

- Terminate the transaction with a 603 DECLINE sent back to the sender.
- From the UX point of view, the receiver will not be notified on the reception of a file transfer invitation from a blacklisted sender however the event should be logged in the spam folder (e.g. "User A tried to send a file on TIME/DATE) and the message will be copied to the spam filter.

3.2.4.16 Emoticons

Selected emoticons will be displayed graphically but sent and received as text. The list of supported icons is defined in [RCS2-OMA-SIMPLE-ENDORS][41] Appendix N.

3.2.4.17 Chat message size limitations

In order to reduce the complexity at protocol level and avoid potential TCP switchover, it is recommended to set a limit the maximum size of a chat message to avoid the SIP INVITE to be longer than the PDU and, consequently, trigger the TCP switchover.

3.2.4.18 Clarifications on IM race conditions

3.2.4.18.1 Two simultaneous invites

Even unlikely, it can happen that two users decide to invite each other simultaneously for a chat. In this situation the behaviour of the clients should be the following:

- User A sends an invite to user B for IM/chat
- Before a final response for that invite is received, user A receives an invite from user B for IM/chat
- User A will send a 486 BUSY HERE response to user B. In addition to this, user A will send the correspondent delivery and read notification using SIP MESSAGE.
- From the UX point of view, the message sent by B will be displayed as received.

Please note this behaviour is consistent with the one described for RCS 2.0 ([RCS2-OMA-SIMPLE-ENDORS][41], section 7.1.2.1, bullet 6), however, the 486 BUSY HERE response is preferred to 487 BUSY EVERYWHERE because it allows a multidevice scenario.
For additional clarification, an explanatory diagram has been included in Annex B section B

3.2.4.18.2 New invite sent after a previous invite has been accepted

Even unlikely, the following scenario can take place:

- User A sends an invite for chat to user B
- User B accepts the chat a 200 OK response is sent back to user A
- In parallel and before receiving the 200 OK response, user A sends a new invite with a new message

To resolve the race condition:

- When user B receives the new invitation, it should terminate the current MSRP session (if established) by sending a SIP BYE
- Once the initial session is terminated, a new 200 OK response should be issued which will trigger the establishment of a new MSRP session.

Please note that for additional clarification, an explanatory diagram has been included in section B.10.

3.2.4.19 User experience regarding notifications when several store&forward messages arrive in a short period of time

Due to the fact a user may have several messages waiting in stored in the IM-AS to be delivered, the UX may be impacted if after getting registered again many IM message notifications appear when the messages are delivered.

To avoid this situation and, specifically, when receiving S&F messages (the INVITE carry a referred-by header with the sender's ID), the suggested experience is the following:

- Only the first message is shown in a notification. The rest of S&F messages are received but they do not cause a notification.
- If messages from several users are received, only one notification per user containing the first message is shown to the user.

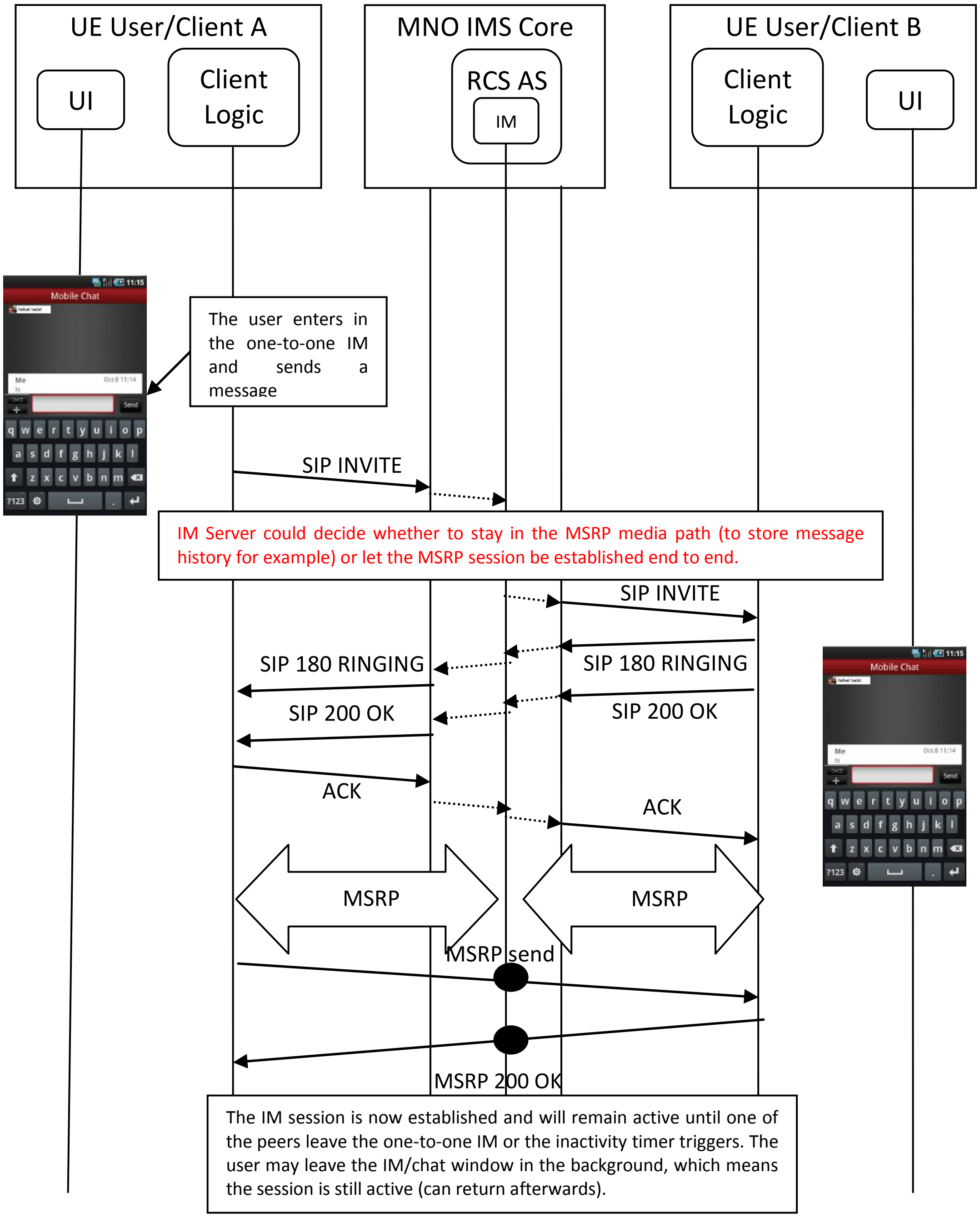
3.2.4.20 Protocol flow diagrams

Please note the diagrams presented in this section focus on a combination between the user experience and a high-level view on the signalling and media exchanges associated to chat. The detailed transactions together with store and forward and multidevice scenarios are covered in Annexes B and C.

3.2.4.20.1 General one-to-one chat

In case, user A wants to chat with user B. Consequently, user A enters in the chat composing window by one of the entry points presented in previous sections to the chat window and sends the first message.

In the following sequence we are assuming user B is currently registered, therefore, the chat can take place. Client A and B are aware of this because an OPTIONS request have been completed (send and receive capabilities from the other end) prior to enter to the chat (e.g. when selecting the contact in the address book).



The user enters in the one-to-one IM and sends a message

IM Server could decide whether to stay in the MSRP media path (to store message history for example) or let the MSRP session be established end to end.

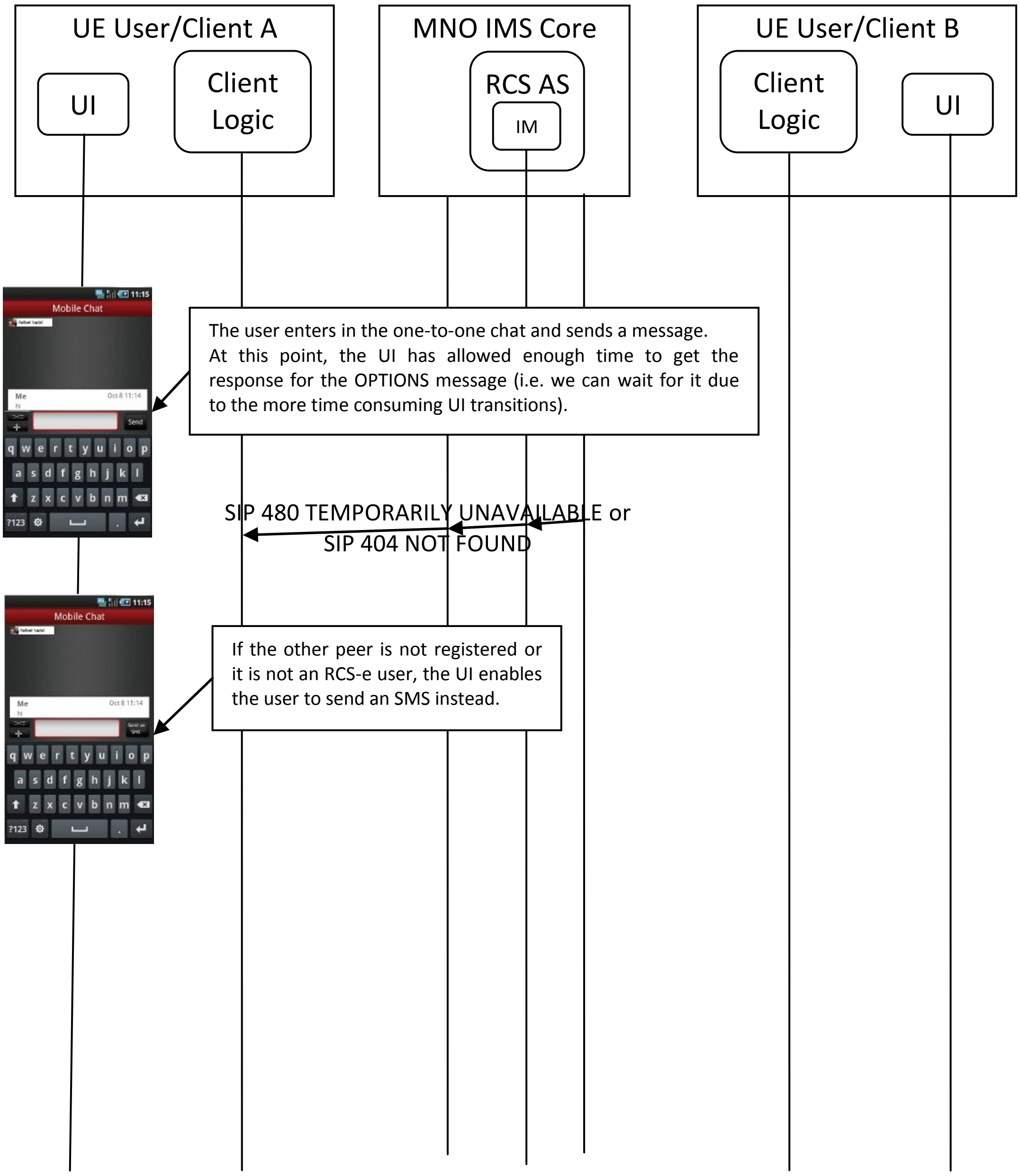
The IM session is now established and will remain active until one of the peers leave the one-to-one IM or the inactivity timer triggers. The user may leave the IM/chat window in the background, which means the session is still active (can return afterwards).

Figure 29. One-to-one chat

Note that MSRP is not only used to send messages but notifications (‘is composing’, displayed and delivered). Please note that prior to acceptance, SIP MESSAGE is also use for this purpose (only for displayed and delivered notifications in this case). In the previous diagram, the notifications were intentionally omitted for clarity. Please refer to Annex B (section B.1) for the complete sequence.

In contrast to the previous flow, there are cases where the chat originating user may have non-updated information about the capabilities from the other end. For example, a user was registered during the previous polling. We have selected the user in the address book, however there is some latency in getting the OPTIONS message response back quickly enough and the user decides to enter in the chat.

Although unlikely, the situation where a user (user A) enters in a chat and the other user(s) (user B in this case) is not registered (no chat possible) may happen. In this case, the proposed sequence is the following:



The user enters in the one-to-one chat and sends a message.
At this point, the UI has allowed enough time to get the response for the OPTIONS message (i.e. we can wait for it due to the more time consuming UI transitions).

If the other peer is not registered or it is not an RCS-e user, the UI enables the user to send an SMS instead.

Figure 30. One-to-one chat backup mechanism to send SMS

Please note the previous two diagrams do not cover the store and forward cases. Please refer to Annex B for detailed diagrams covering standard chat and the store and forward cases.

3.2.4.20.2 Store and Forward

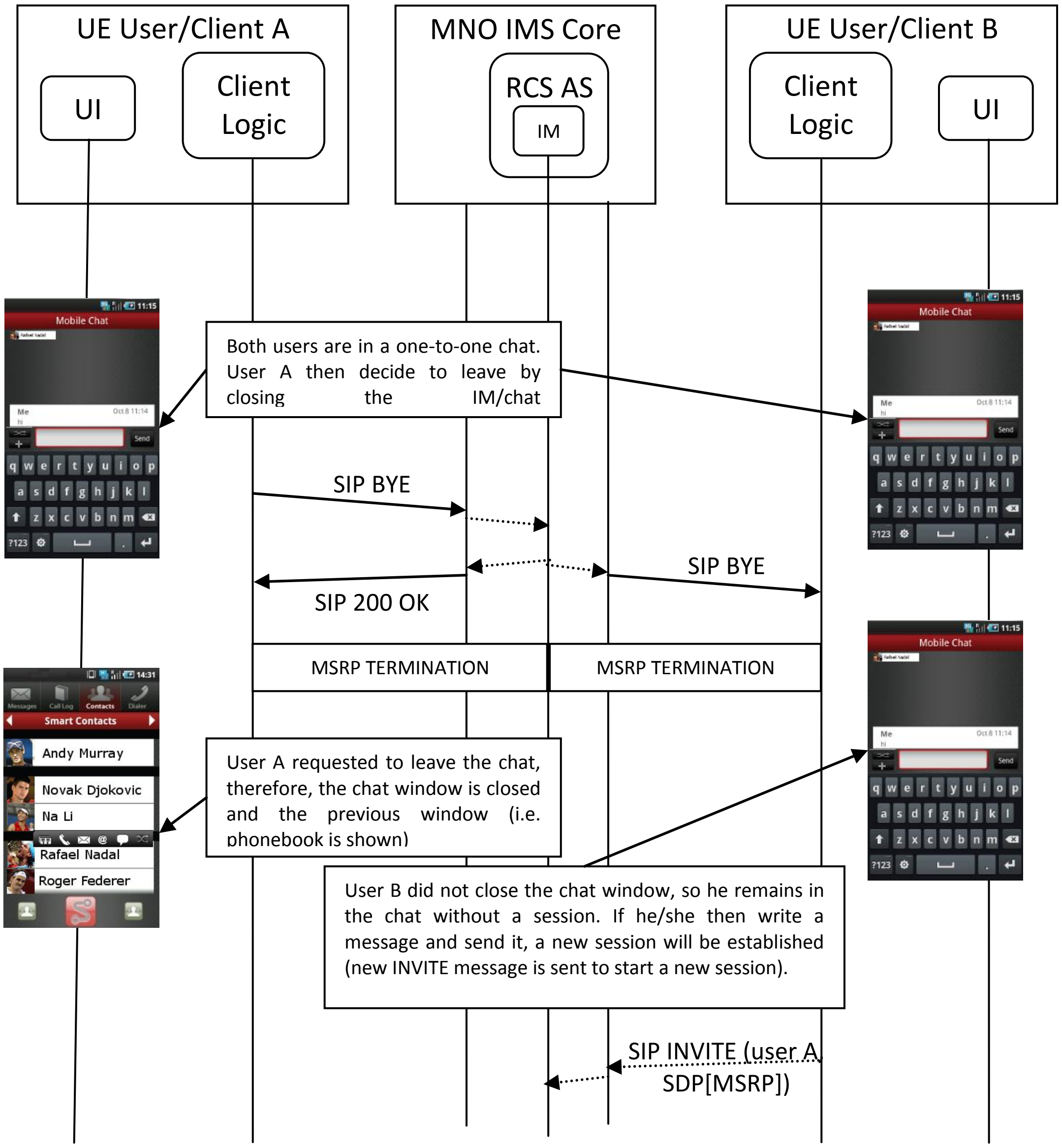
Due to the complexity of the store and forward scenarios, detailed diagrams are provided in Annex B.

3.2.4.20.3 Multidevice

Due to the complexity of the multidevice scenario, detailed diagrams are provided in Annex C.

3.2.4.20.4 Leaving a one-to-one chat

In this case, user A and B are in a chat, however A wants to leave it because, for example, the chat conversation is finished. The relevant UX and flow sequence is presented below:



Both users are in a one-to-one chat. User A then decide to leave by closing the IM/chat

User A requested to leave the chat, therefore, the chat window is closed and the previous window (i.e. phonebook is shown)

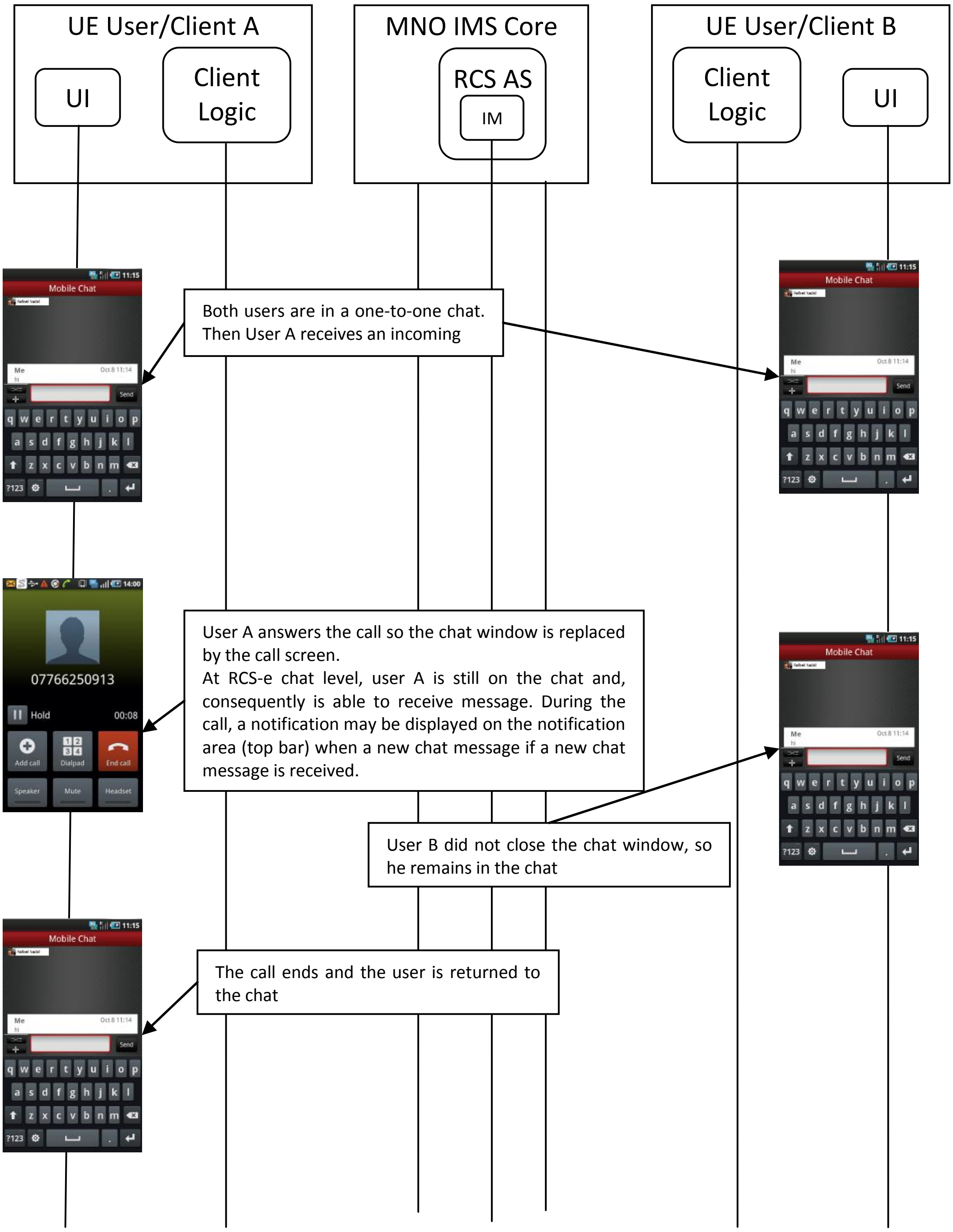
User B did not close the chat window, so he remains in the chat without a session. If he/she then write a message and send it, a new session will be established (new INVITE message is sent to start a new session).

Figure 31. Leaving a one-to-one chat session (chat terminated)

Please note that the IM Server, especially when store and forward is enabled could decide to leave the B's MSRP session open and start a new session with user A when user B sends a new message. No UI indication should be done reflecting that the underlying MSRP session has been closed.

In the next case, user A and B are in a chat, however A has to leave because an event (incoming e-mail, incoming call, etc.) or because it decides to put the chat task in the background. In this case, the chat conversation is not finished, so the session is kept active in the background.

The relevant UX and flow sequence is presented below:



Both users are in a one-to-one chat. Then User A receives an incoming

User A answers the call so the chat window is replaced by the call screen.
At RCS-e chat level, user A is still on the chat and, consequently is able to receive message. During the call, a notification may be displayed on the notification area (top bar) when a new chat message if a new chat message is received.

User B did not close the chat window, so he remains in the chat

The call ends and the user is returned to the chat

Figure 32. Leaving a one-to-one chat session (leaving chat in the background)

3.2.4.20.5 One-to-one chat forced termination

In this case, user A and B are in a chat, however user B client fails to keep the connection to the network (e.g. client error, IP reconfiguration due to a new data bearer, lost coverage, etc.):

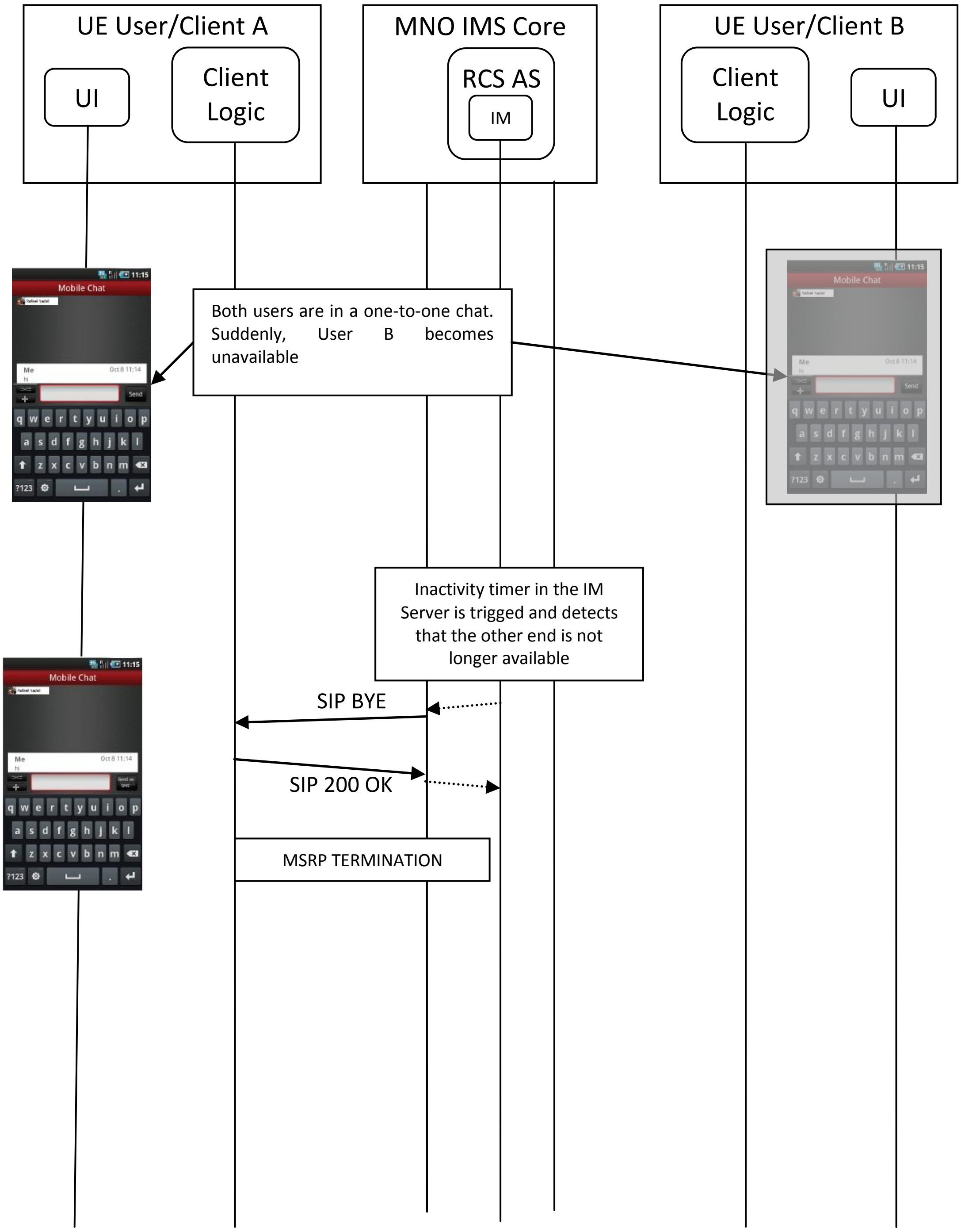

UE User/Client A
UI
Client Logic
MNO IMS Core
RCS AS
IM
UE User/Client B
Client Logic
UI
Both users are in a one-to-one chat. Suddenly, User B becomes unavailable
Inactivity timer in the IM Server is trigged and detects that the other end is not longer available
SIP BYE
SIP 200 OK
MSRP TERMINATION

Figure 33. One -to-one chat forced termination

3.2.4.20.6 Exchange capabilities during a 1-to-1 chat

The assumptions in this case are that user A and B are in a chat. The capabilities of one of the users change (e.g. different data carrier), however, the chat can continue. Even that chat can continue, the other end has to be informed using the OPTIONS message.

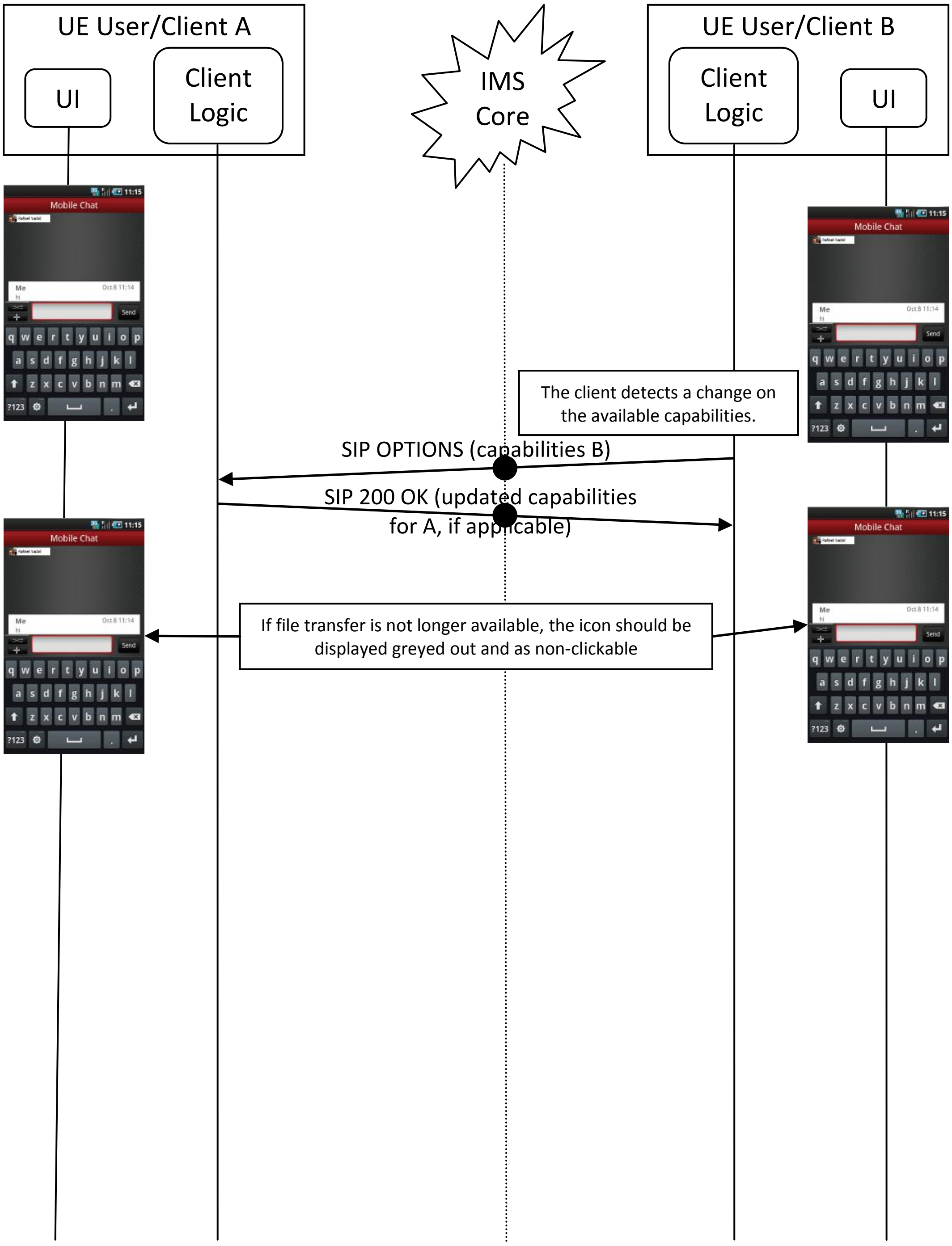

UE User/Client A
UI
Client Logic
IMS Core
UE User/Client B
Client Logic
UI
The client detects a change on the available capabilities.
SIP OPTIONS (capabilities B)
SIP 200 OK (updated capabilities for A, if applicable)
If file transfer is not longer available, the icon should be displayed greyed out and as non-clickable
Mobile Chat
Me
Send

Figure 34. Capabilities exchange during a chat session

3.2.5 1-to-many Chat

In order to implement the 1-to-many chat functionality an IM server is required, and consequently, the IM CONFERENCE FACTORY URI (see section 2.1 Table 6 for reference) configuration parameter should be correctly set.

It is optional for a MNO to provide the 1-to-many functionality, so from the terminal perspective, if there is not a configured IM CONFERENCE FACTORY URI, the terminal should not allow the user to add additional parties to the chat nor starting a multichat. Please note that the fact that starting a 1-to-many chat is not available in this scenario does not restrict the possibility to join a multichat session. Therefore, the OEM has to implement both the one-to-one and one-to-many chat experiences even for users without a configured IM CONFERENCE FACTORY URI.

Please note the following sections propose an experience which aimed to be employed as a reference for OEM implementations.

Support for store and forward in 1-to-many chat is not included in this version of the specification.

Finally, it should be taken into account that a group chat could be only started from a user on a MNO which has deployed an IM Server-AS.

3.2.5.1 Initiating a chat

User A initiates a chat by selecting some of his contacts (B, C… up to a limit OTA/remote-configured by the MNO) from the Address Book or from the IM/chat application in his mobile phone, or in the Contact List from the Broadband Access PC client, but only among the contacts known by his devices to be RCS-e users with IM capability. Device A (either mobile or PC) will send a query for the real-time capabilities of each contact B, C… (a query per intended contact) to ensure the IM service is available for those users at that time.

When user A types the first message and presses the “Send” button, device A will establish an IM session with the IM server and send the message through it. The IM server will establish IM Sessions with the other participant users.

When a user device receives a group chat invitation from the IM server, the recipient may accept or reject the invitation as would be done in a one to one case and subscribe to the conference event package to retrieve the list and status of the users in the one to many chat. User A’s device shall subscribe to the conference event package also. The identity of each user shall be matched against the contact list in the device to present a user friendly name.

The IM server will be opened A, B, C… up to a configured limit.

In the sides of the receivers a notification (UI dependant) will be displayed on device to inform about the incoming message. Notification must clearly state that it is a multichat, so the users are made aware

Unlike [RCS2-OMA-SIMPLE-ENDORS][41] once a 1-to-many chat is established, any participant is allowed to add more contacts, while the general limit is not reached.

3.2.5.2 General Behaviour

The same behaviour from one to one chat applies to 1-to-many chat except of:

- Displaying and local storage of an active conversation,
- Leaving the chat composing window (see section 3.2.4.5)
- Delivery and display notifications (see sections 3.2.2.3 and 3.2.2.4 respectively) are not required
- Store and forward mode (see section 3.2.4.11) is not required

In addition to this and consistently with the behaviour already endorsed [RCS2-OMA-SIMPLE-ENDORS], the UX associated a RCS-e group chat should provide the following functionality:

- Displaying the list of participants of the current group chat and notifications when a new participant is joining and when a participant is leaving the current group chat
- Invitation to group chat should list the participants to the group chat before accepting the invitation (e.g. "You're inviting to a group chat with A, B & C" instead of "A is inviting you to a group chat")

3.2.5.3 Closing multichat

Any of the participants can close his IM session associated with an established multichat. This can be done from the chat composing window or in the IM/chat application.

When user C closes his IM session it will be notified to the other users in the chat through a predefined indication “C has left the conversation”, and their devices will remove him from the displayed recipients. A new Conversation is created in user C’s device history with the messages associated to the chat up to the point he left.

A chat is closed when the less than the minimum number of RCS users defined for a group chat remain in the group chat all RCS users close their IM sessions, or when a chat inactivity timeout expires.

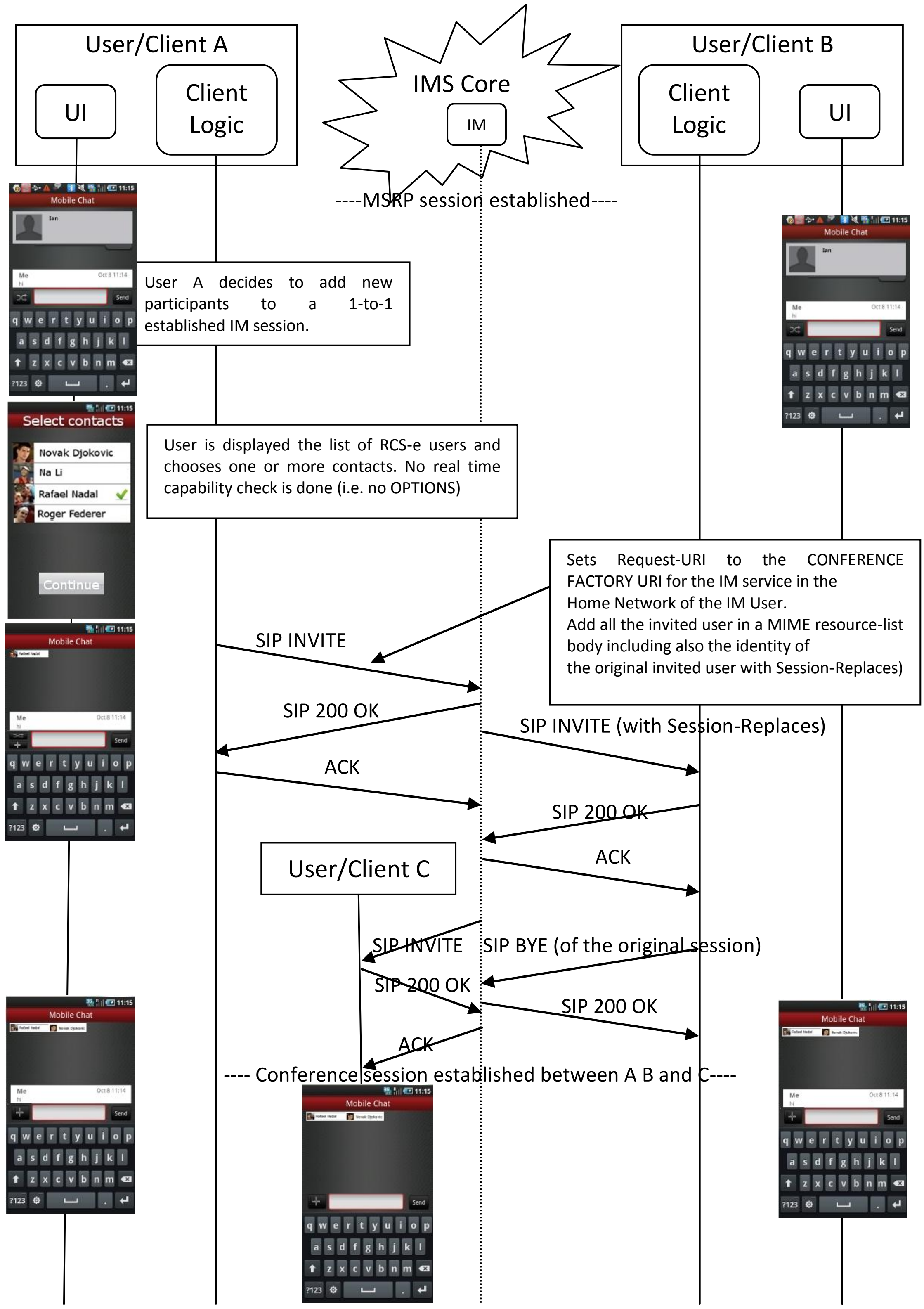
3.2.5.4 Chat message size limitations

As for the 1-to-1 chat and with the aim of reducing the complexity at protocol level and avoid potential TCP switchover, it is recommended to set a limit the maximum size of a chat message to avoid the SIP INVITE to be longer than the PDU and, consequently, trigger the TCP switchover.

3.2.5.5 Protocol flow diagrams

3.2.5.5.1 Start a multiple IM session from the IM composition window

In this case, user A and B are in a chat, and user A decides to add a third user (user C) to the chat session. The relevant UX and flow sequence is presented below:



User A decides to add new participants to a 1-to-1 established IM session.

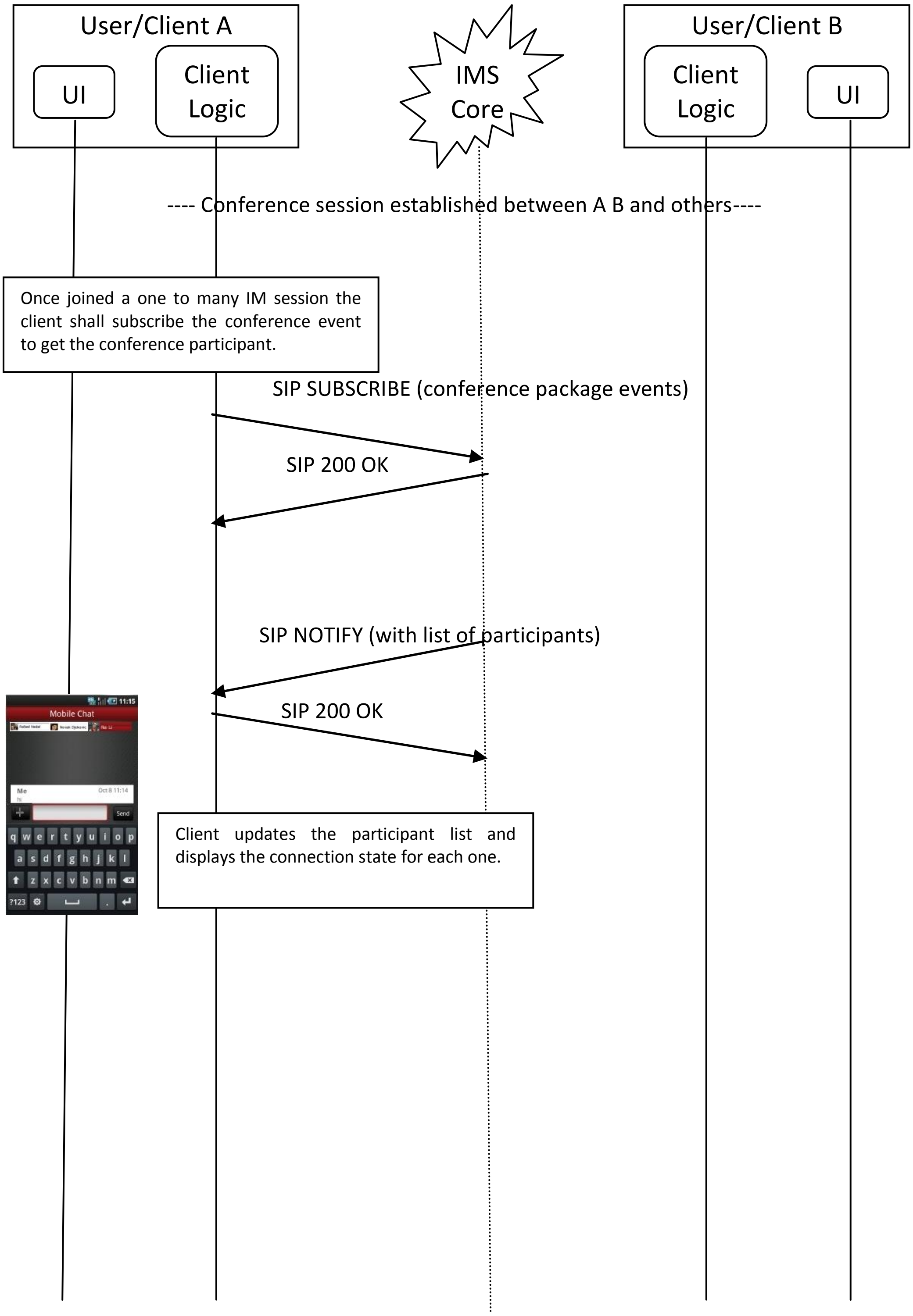
User is displayed the list of RCS-e users and chooses one or more contacts. No real time capability check is done (i.e. no OPTIONS)

Sets Request-URI to the CONFERENCE FACTORY URI for the IM service in the Home Network of the IM User.
Add all the invited user in a MIME resource-list body including also the identity of the original invited user with Session-Replaces)

Figure 35. Multichat session initiation

3.2.5.5.2 Get participants of multichat IM session

The following flow is complementary to the previous use case as it presents in details how to get information on the chat participants. Please note these exchanges were omitted in the previous diagram:

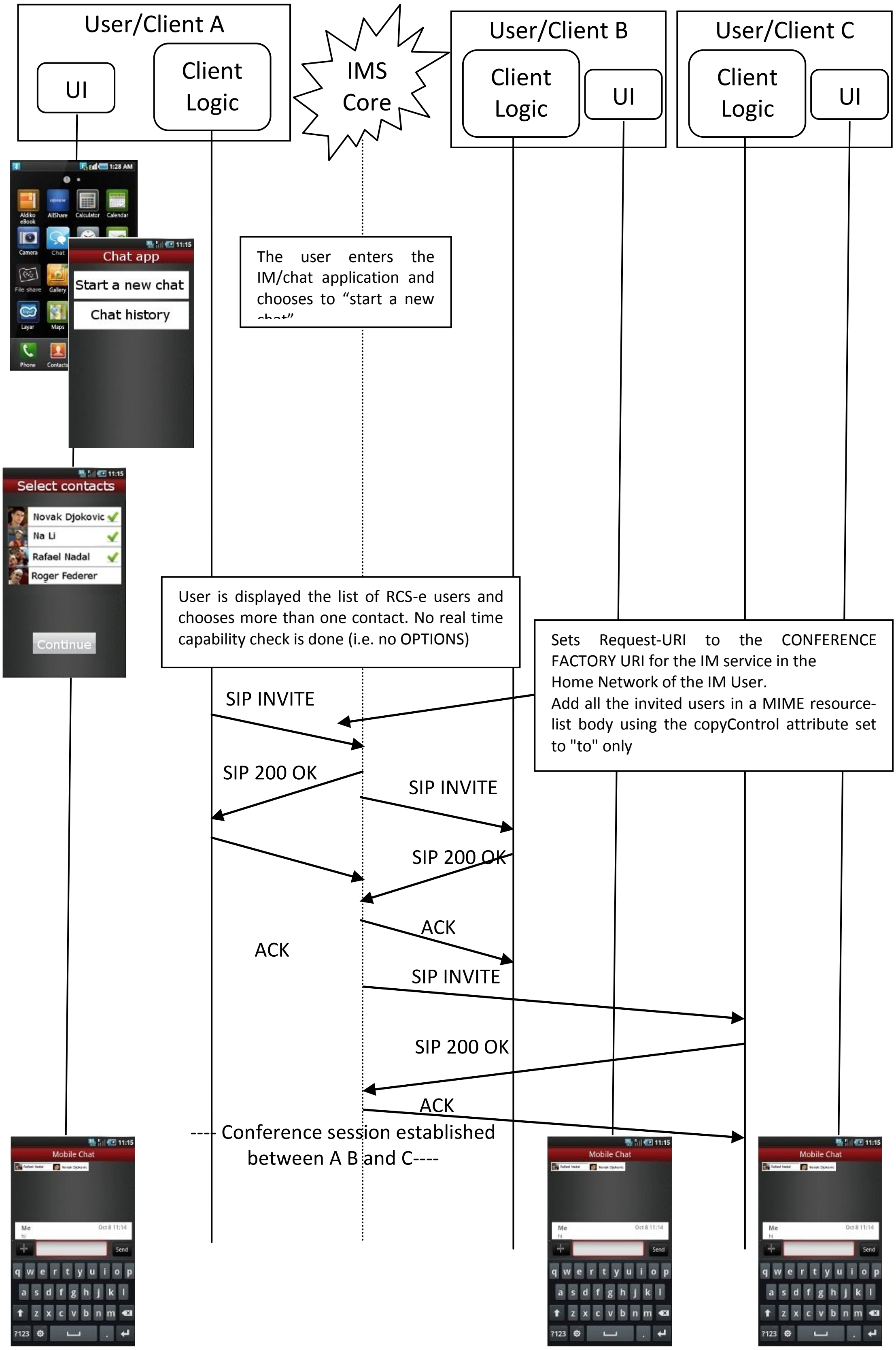

User/Client A
UI
Client Logic
IMS Core
User/Client B
Client Logic
UI
---- Conference session established between A B and others----
SIP SUBSCRIBE (conference package events)
SIP 200 OK
SIP NOTIFY (with list of participants)
SIP 200 OK
Mobile Chat

Once joined a one to many IM session the client shall subscribe the conference event to get the conference participant.

Client updates the participant list and displays the connection state for each one.

Figure 36. Multichat session initiation (II): Get participants

3.2.5.5.3 Start a group chat session from a IM/chat application



The user enters the IM/chat application and chooses to “start a new chat”

User is displayed the list of RCS-e users and chooses more than one contact. No real time capability check is done (i.e. no OPTIONS)

Sets Request-URI to the CONFERENCE FACTORY URI for the IM service in the Home Network of the IM User.
Add all the invited users in a MIME resource-list body using the copyControl attribute set to "to" only

---- Conference session established between A B and C----

Figure 37. Start a group chat from the IM/chat application

3.2.5.5.4 Add a participant to an already established one to many IM/chat session

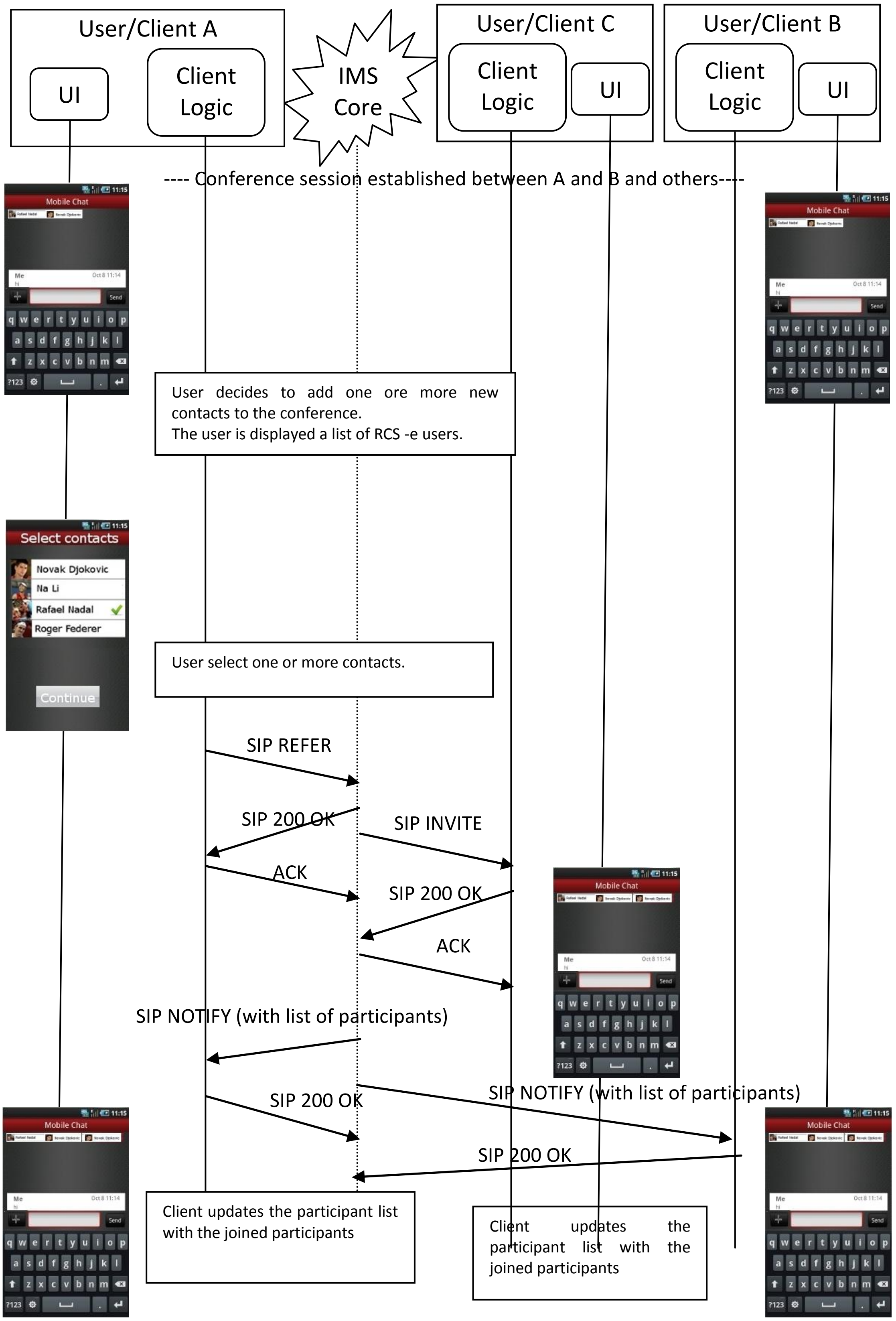
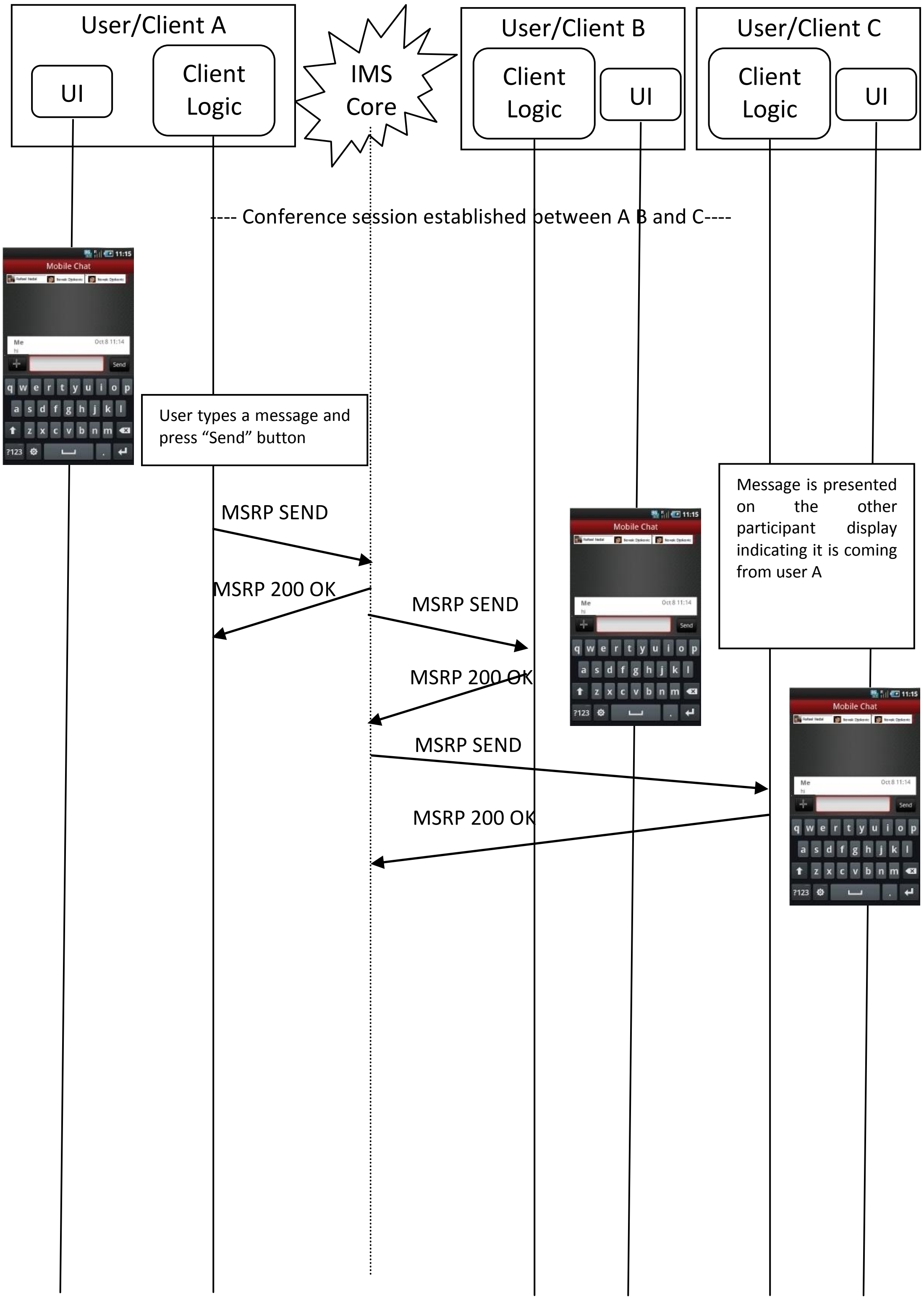

User/Client A
UI
Client Logic
IMS Core
User/Client C
Client Logic
UI
User/Client B
Client Logic
UI
---- Conference session established between A and B and others----
Mobile Chat
Send
User decides to add one ore more new contacts to the conference.
The user is displayed a list of RCS -e users.
Select contacts
Novak Djokovic
Na Li
Rafael Nadal
Roger Federer
Continue
User select one or more contacts.
SIP REFER
SIP 200 OK
SIP INVITE
ACK
SIP 200 OK
ACK
SIP NOTIFY (with list of participants)
SIP 200 OK
SIP NOTIFY (with list of participants)
SIP 200 OK
Client updates the participant list with the joined participants
Client updates the participant list with the joined participants

Figure 38. Adding new users to a multi-chat session

3.2.5.5.5 Sending a IM message from the IM multiple session window



User types a message and press "Send" button

Message is presented on the other participant display indicating it is coming from user A

Figure 39. Chat message sequence on a multi-chat session

3.2.5.5.6 User in a multiple IM session goes offline

In the following flow, users A and B are in a chat among others (multichat); suddenly User B goes offline (e.g. loses the connection to the network):

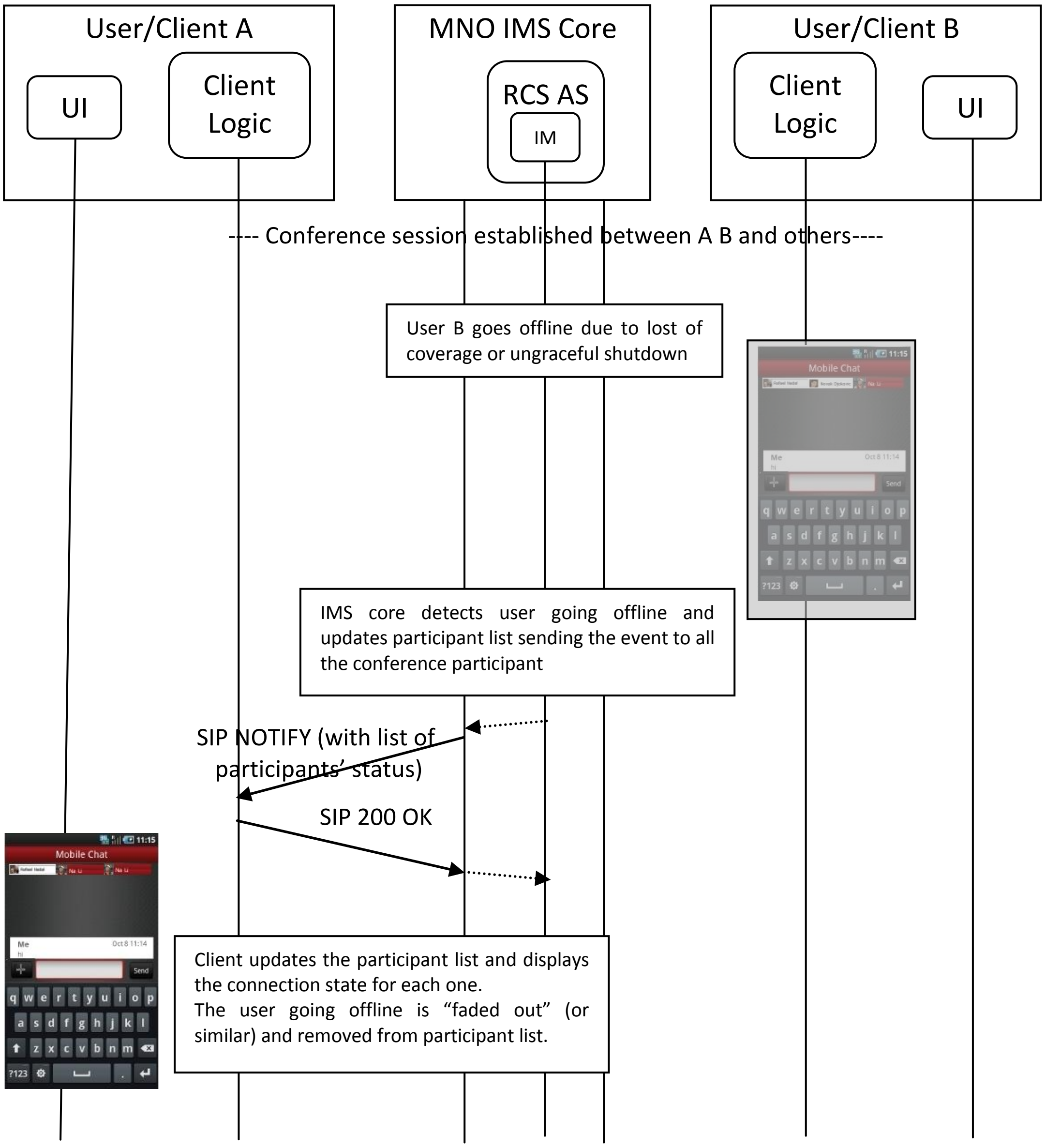
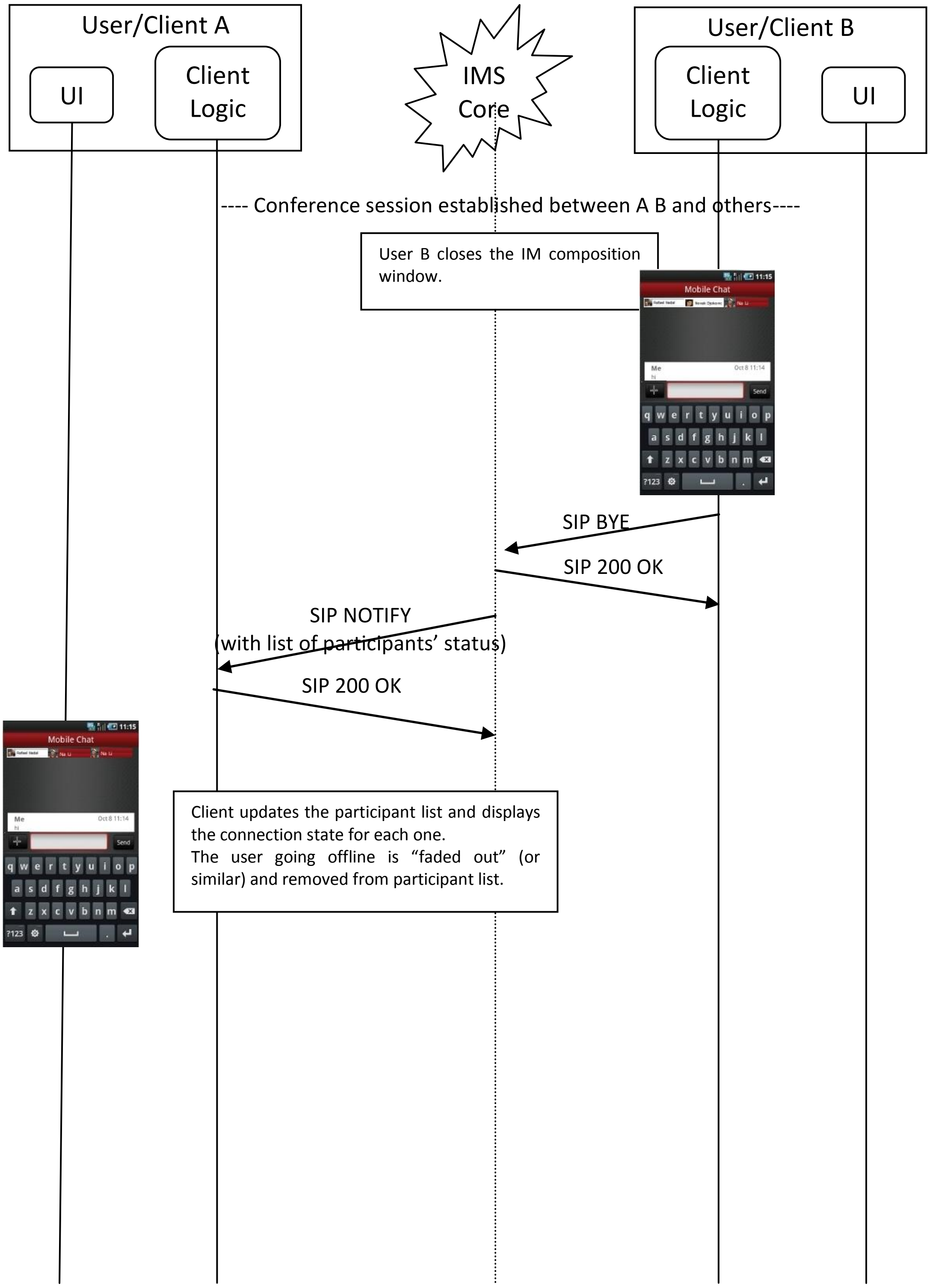

User/Client A
UI
Client Logic
MNO IMS Core
RCS AS
IM
User/Client B
Client Logic
UI
---- Conference session established between A B and others----
User B goes offline due to lost of coverage or ungraceful shutdown
IMS core detects user going offline and updates participant list sending the event to all the conference participant
SIP NOTIFY (with list of participants' status)
SIP 200 OK
Client updates the participant list and displays the connection state for each one.
The user going offline is "faded out" (or similar) and removed from participant list.
Mobile Chat
Mobile Chat

Figure 40. Forced chat termination in a multi-chat session

3.2.5.5.7 *Leaving a IM multiple session*

This case is equivalent to the previous one however in this case, User B leaves the chat intentionally:



User B closes the IM composition window.

Client updates the participant list and displays the connection state for each one.
The user going offline is "faded out" (or similar) and removed from participant list.

Figure 41. Leaving a multi-chat session

3.3 *RCS-e services during a call*

Among the different RCS-e services, during a call the user will be able to access the following:

- Share a video (video share, identical behaviour and version as defined in RCS Release 2 specifications): The video can be originated from:
    - The front camera (*"me"*)
    - The rear camera (*"what I see"*)
    - A file (*"video streaming"*)
- Share a picture (image share identical behaviour and version as defined in RCS Release 2 specifications): The picture can be:
    - A picture taken using the front camera (*"me"*)
    - A picture taken using the rear camera (*"what I see"*)
    - A file (*"send stored image")*

The user should be able to know whether one or both services are available during the call, therefore, both ends need to be updated of the respective capabilities of the other end to avoid showing a service as available when it is no longer the case.

Both video and image share are unidirectional however it is possible to establish simultaneous image and/or video share sessions in each direction. For example when referring to bidirectional video share, we mean that once user A is sharing video with user B and provide the right coverage conditions are in place, user B could also start to share video with A simultaneously. In this case each video share session is independent and should be handled separately. The same example would also apply to image share or to the combination of video and image share, each service in one direction.

For video share, the preferred media transport is RTP. For image share, MSRP is the preferred media transport.

3.3.1 General assumptions

In the following sections we will be showing the relevant message flows and reference user experience (UX). Please note that the following assumptions have been made:

- For simplicity, the internal mobile network interactions are omitted in the diagrams showed in the following sections.
- The terminal supports 2G DTM mode, therefore, it is always possible to gracefully terminate the transaction provide the terminal remains on. In case 2G DTM is not supported, the use case of one of the ends going to 2G would be equivalent to the client error one.
- The terminal comes with a front and rear camera. If one or both missing, the user should be notified only with the available options.
- Prior to the call, the user accessed its address book, call log or dial-pad to make the call. As described before, while these actions are performed an OPTIONS message is sent to double-check the available capabilities. In the following diagrams we are assuming that this exchange (OPTIONS and response) have already take place, and

therefore, both ends are aware of the capabilities and, consequently, the available RCS-e services. If that is not the case, the OPTIONS message should be send at the same time the call is being setup.

- In the diagrams we have assumed for simplicity that MSRP chunking is enabled. This is just for representation purposes and it is up to the OEM to make a decision on whether MSRP chunking is enabled or not.

3.3.2 Exchange capabilities during a call

The assumptions in this case are that user A and B are in a call. The capabilities of one of the users change (e.g. different data carrier), therefore, the other end has to be informed using the OPTIONS message.

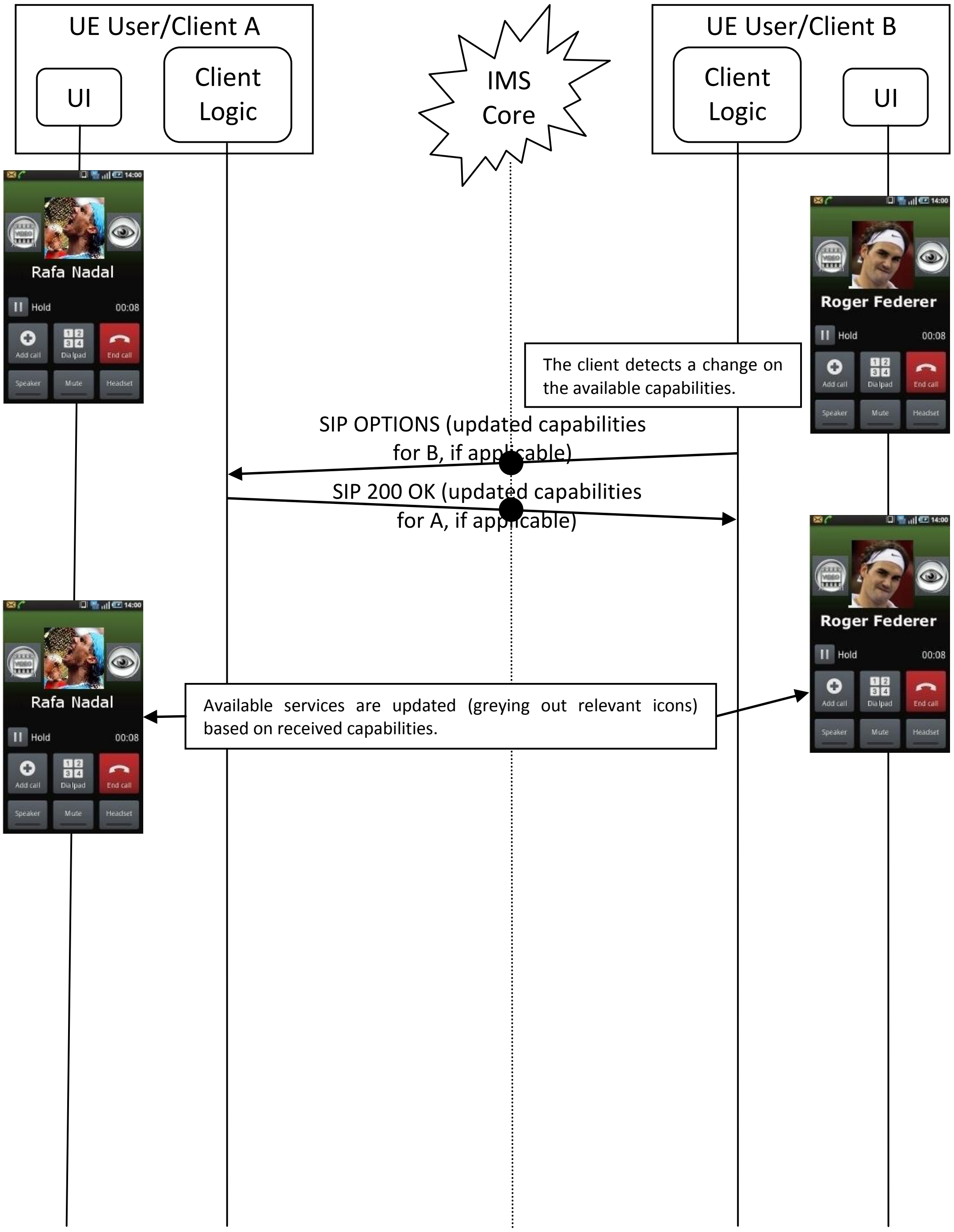
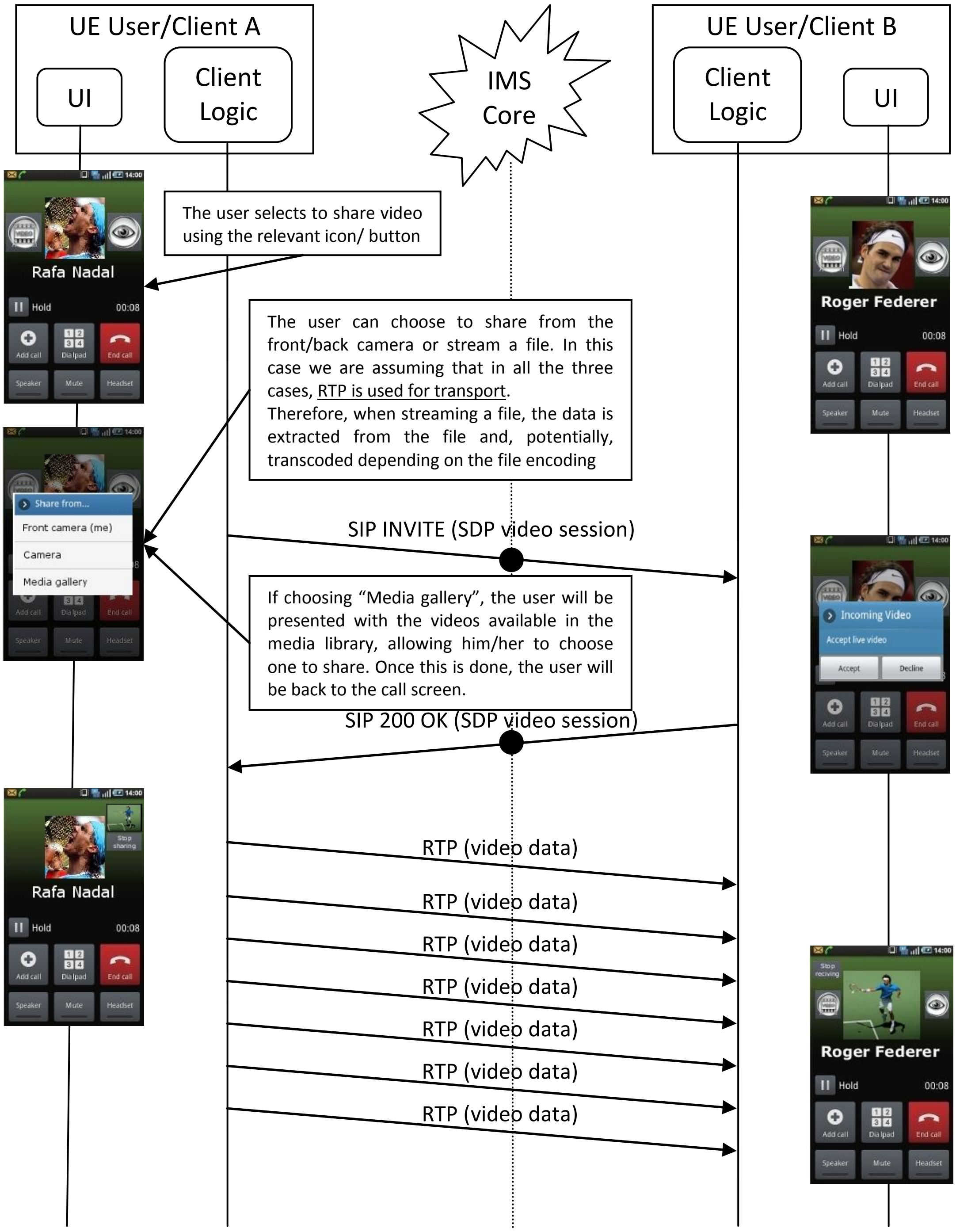

UE User/Client A
UI
Client Logic
IMS Core
UE User/Client B
Client Logic
UI
Rafa Nadal
Roger Federer
Hold
00:08
Add call
Dia lpad
End call
Speaker
Mute
Headset
The client detects a change on the available capabilities.
SIP OPTIONS (updated capabilities for B, if applicable)
SIP 200 OK (updated capabilities for A, if applicable)
Available services are updated (greying out relevant icons) based on received capabilities.

Figure 42. Capabilities exchange during a call

3.3.3 Share video during a call

The assumptions in this case are that both user A (wanting to share video) and user B (recipient wanting to receive it), have successfully exchanged the OPTIONS message, therefore, both clients are aware that video sharing is possible (both UEs on a 3G+ or Wi-Fi).

In this case RTP is the protocol used to stream the video data, so it can be reproduced in real-time on the other end.



The user selects to share video using the relevant icon/ button

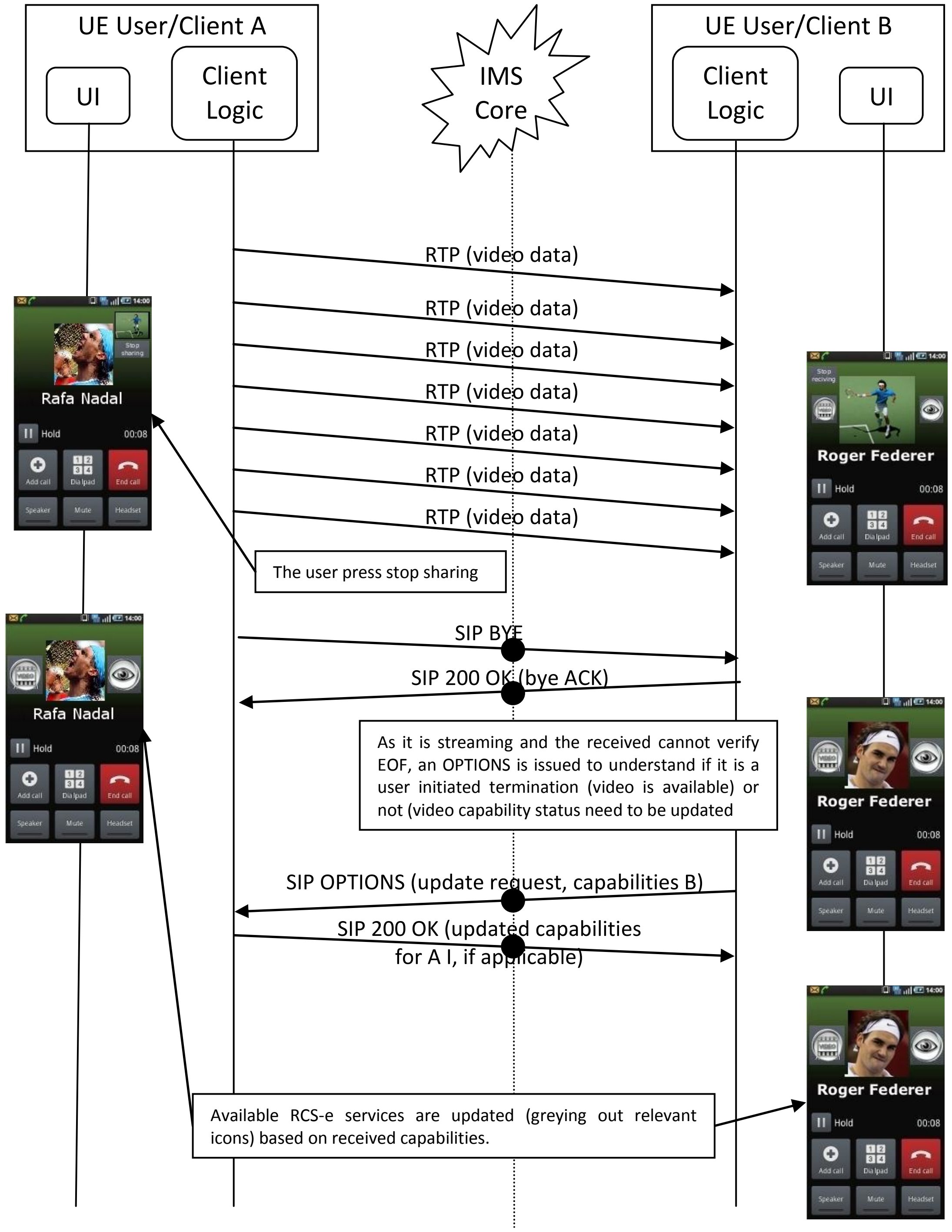
The user can choose to share from the front/back camera or stream a file. In this case we are assuming that in all the three cases, RTP is used for transport.
Therefore, when streaming a file, the data is extracted from the file and, potentially, transcoded depending on the file encoding

If choosing "Media gallery", the user will be presented with the videos available in the media library, allowing him/her to choose one to share. Once this is done, the user will be back to the call screen.

Figure 43. Share video during a call

3.3.4 Stop sharing video (RTP) during a call: Sender initiated

The assumptions in this case are that user A is sharing video (RTP) with user B, however user A does not longer want to keep sharing it.



The user press stop sharing

As it is streaming and the received cannot verify EOF, an OPTIONS is issued to understand if it is a user initiated termination (video is available) or not (video capability status need to be updated

Available RCS-e services are updated (greying out relevant icons) based on received capabilities.

Figure 44. Sender stops sharing video during a call

3.3.5 Stop sharing video (RTP) during a call: Receiver initiated

This case is equivalent to the previous one, however it is the receiver (user B) who does not longer want to keep receiving it.

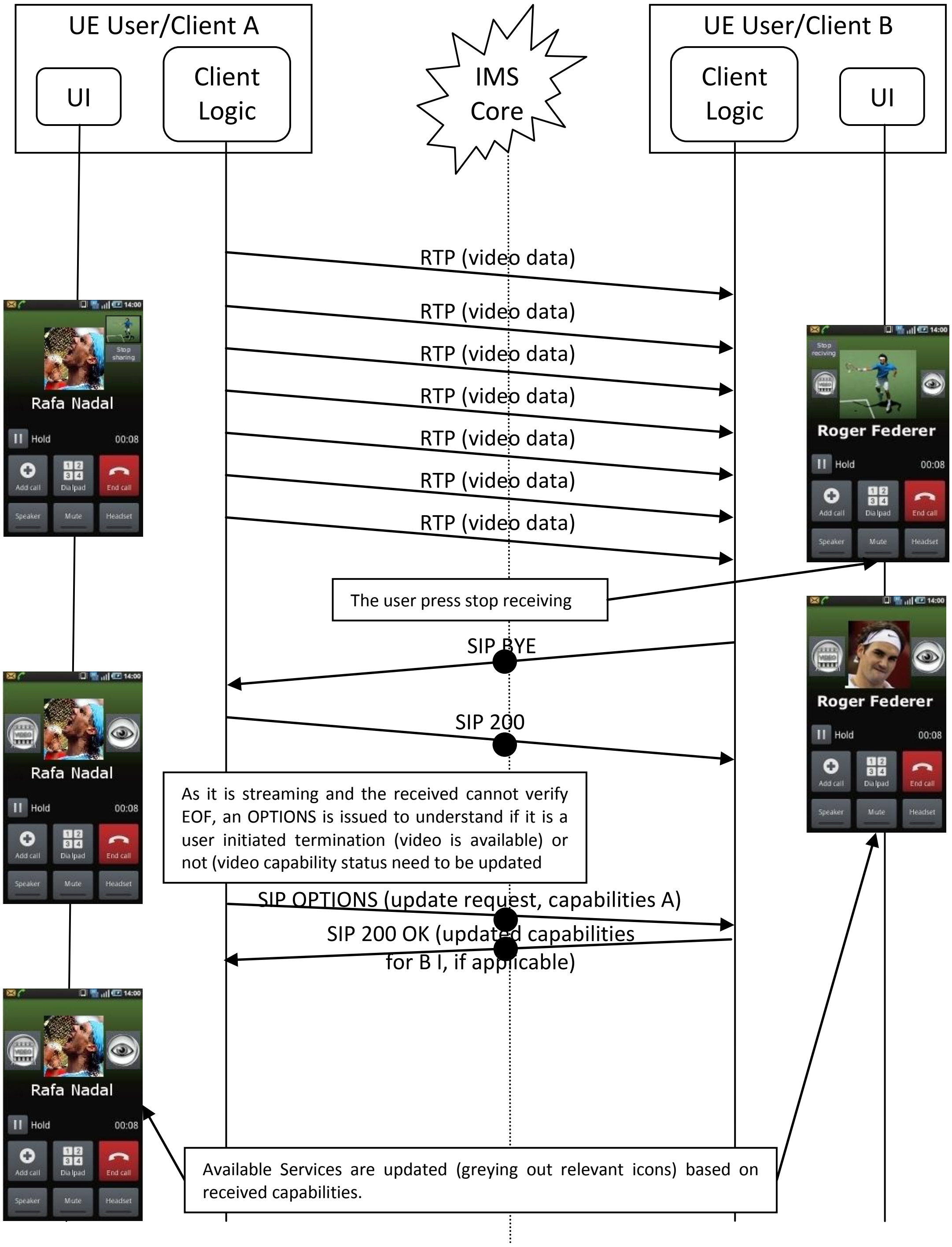

UE User/Client A
UI
Client Logic
IMS Core
UE User/Client B
Client Logic
UI
RTP (video data)
RTP (video data)
RTP (video data)
RTP (video data)
RTP (video data)
RTP (video data)
RTP (video data)
Rafa Nadal
Roger Federer
The user press stop receiving
SIP BYE
SIP 200
As it is streaming and the received cannot verify EOF, an OPTIONS is issued to understand if it is a user initiated termination (video is available) or not (video capability status need to be updated
SIP OPTIONS (update request, capabilities A)
SIP 200 OK (updated capabilities for B I, if applicable)
Available Services are updated (greying out relevant icons) based on received capabilities.

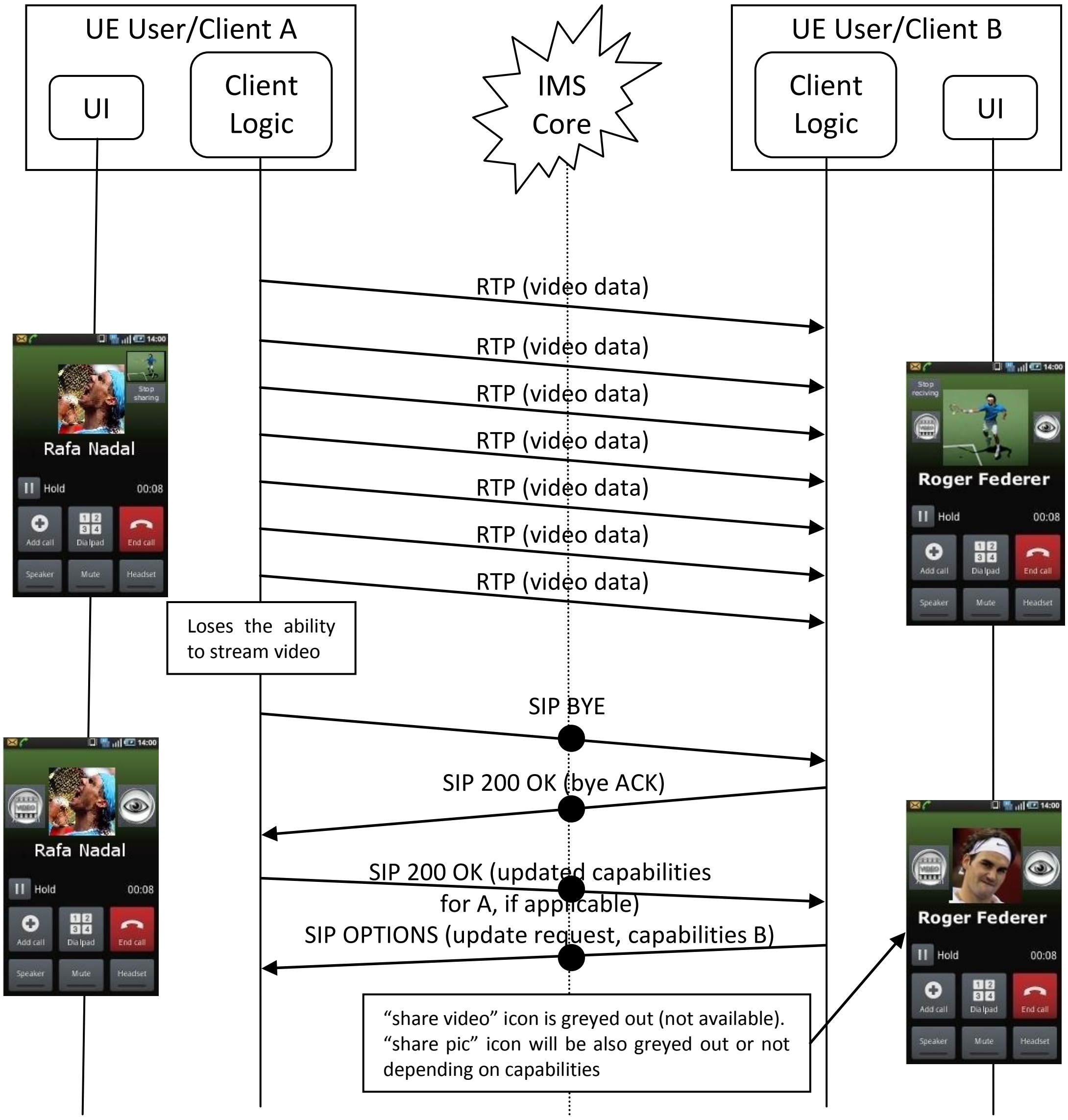
Figure 45. Receiver wants no longer to receive video during a call

3.3.6 Stop sharing video (RTP) during a call because the required capability is no longer available

The assumptions in this case are that user A is sharing video (RTP) with user B, and either A or B are no longer capable (e.g. the terminal is busy, no 3G+ or Wi-Fi coverage available suddenly however it does not trigger an IP reconfiguration or loss of connection) to send or receive video. Please note in the example, we assumed the sender (user A) is the one losing the capability. This sequence will be equivalent for:

- Sender (user A) loses the capability to receive video: The BYE and OPTIONS exchange would be initiated by the sender (user A) in this case.
- Both lose the capability to share video: The BYE and OPTIONS exchange message would be initiated by the first one to lose the capability in this case.

By losing the capability to send video, we are excluding the case there is an IP reconfiguration. Please note that particular case is covered under the "Client Error" section later in this chapter



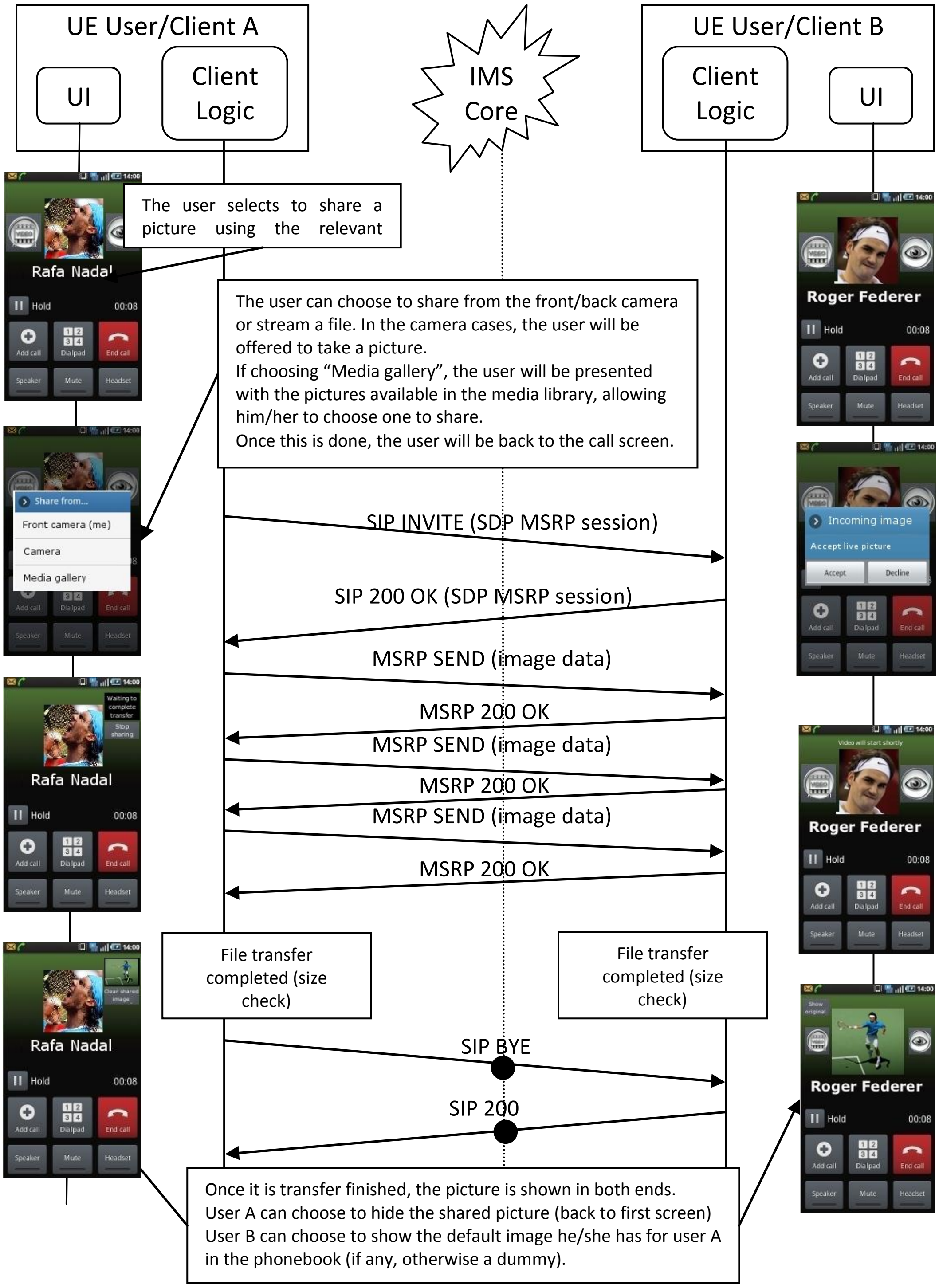
Loses the ability to stream video

"share video" icon is greyed out (not available). "share pic" icon will be also greyed out or not depending on capabilities

Figure 46. Video can no longer be shared during a call (capability not available)

3.3.7 Share pictures during a call

The assumptions in this case are that both user A (wanting to share picture) and user B (recipient wanting to receive it), have successfully exchanged the OPTIONS message, therefore, both clients are aware that file sharing is possible (both UEs on a 3G+ or Wi-Fi).



The user selects to share a picture using the relevant

The user can choose to share from the front/back camera or stream a file. In the camera cases, the user will be offered to take a picture.
If choosing "Media gallery", the user will be presented with the pictures available in the media library, allowing him/her to choose one to share.
Once this is done, the user will be back to the call screen.

File transfer completed (size check)

File transfer completed (size check)

Once it is transfer finished, the picture is shown in both ends.
User A can choose to hide the shared picture (back to first screen)
User B can choose to show the default image he/she has for user A in the phonebook (if any, otherwise a dummy).

Figure 47. Sharing a picture during a call

3.3.8 Stop sharing a picture during a call: Sender initiated

The assumptions in this case are that user A is sharing a picture with user B, the transfer is still on-going, and however user A does not longer want to keep sharing it.

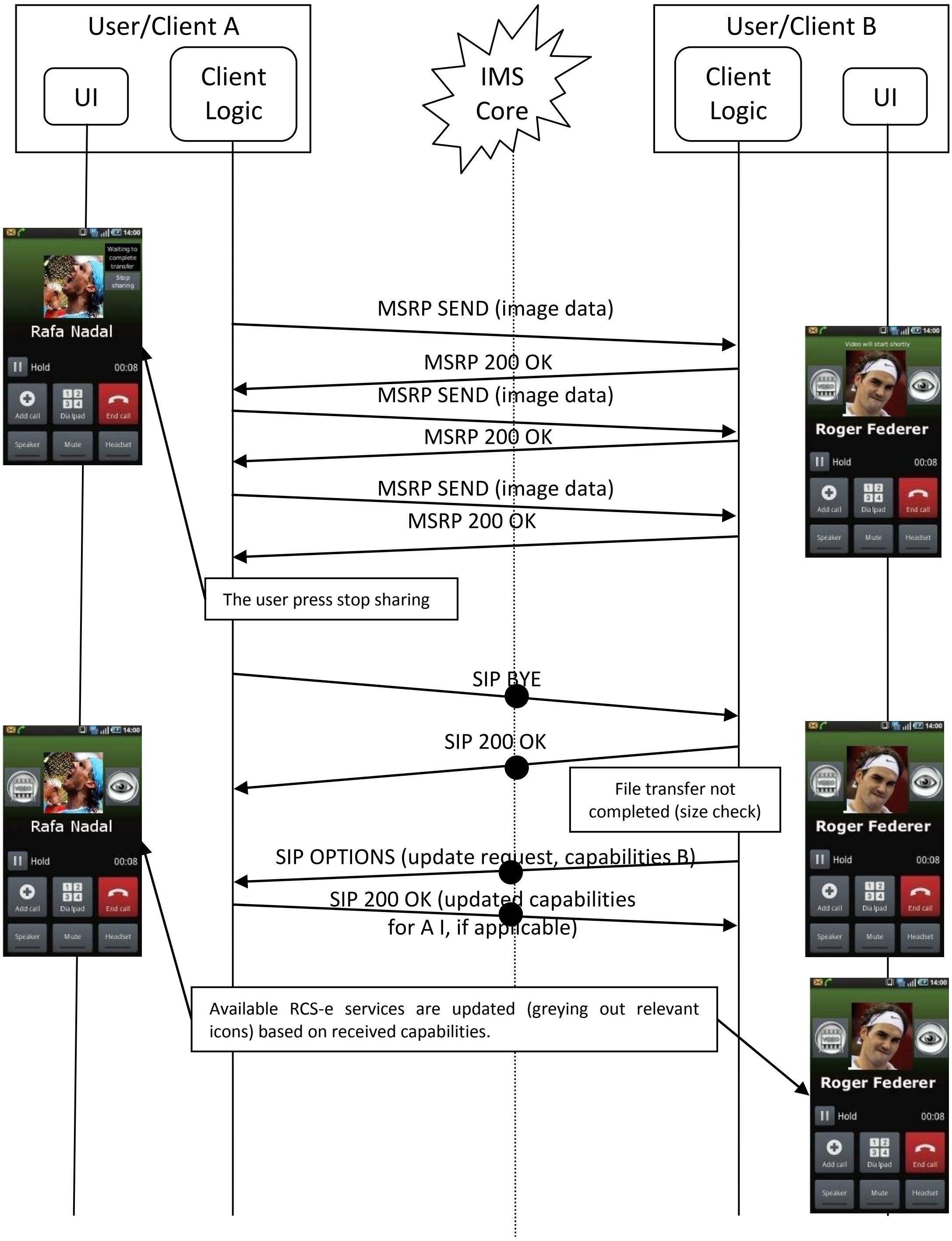

User/Client A
UI
Client Logic
IMS Core
User/Client B
Client Logic
UI
Waiting to complete transfer
Stop sharing
Rafa Nadal
Hold
00:08
Add call
Dia lpad
End call
Speaker
Mute
Headset
MSRP SEND (image data)
MSRP 200 OK
MSRP SEND (image data)
MSRP 200 OK
MSRP SEND (image data)
MSRP 200 OK
Video will start shortly
Roger Federer
The user press stop sharing
SIP BYE
SIP 200 OK
File transfer not completed (size check)
SIP OPTIONS (update request, capabilities B)
SIP 200 OK (updated capabilities for A I, if applicable)
Available RCS-e services are updated (greying out relevant icons) based on received capabilities.

Figure 48. Sender stops sharing a picture during a call

3.3.9 Stop sharing a picture during a call: Receiver initiated

This case is equivalent to the previous one, however it is the receiver (user B) who does not longer want to keep receiving it.

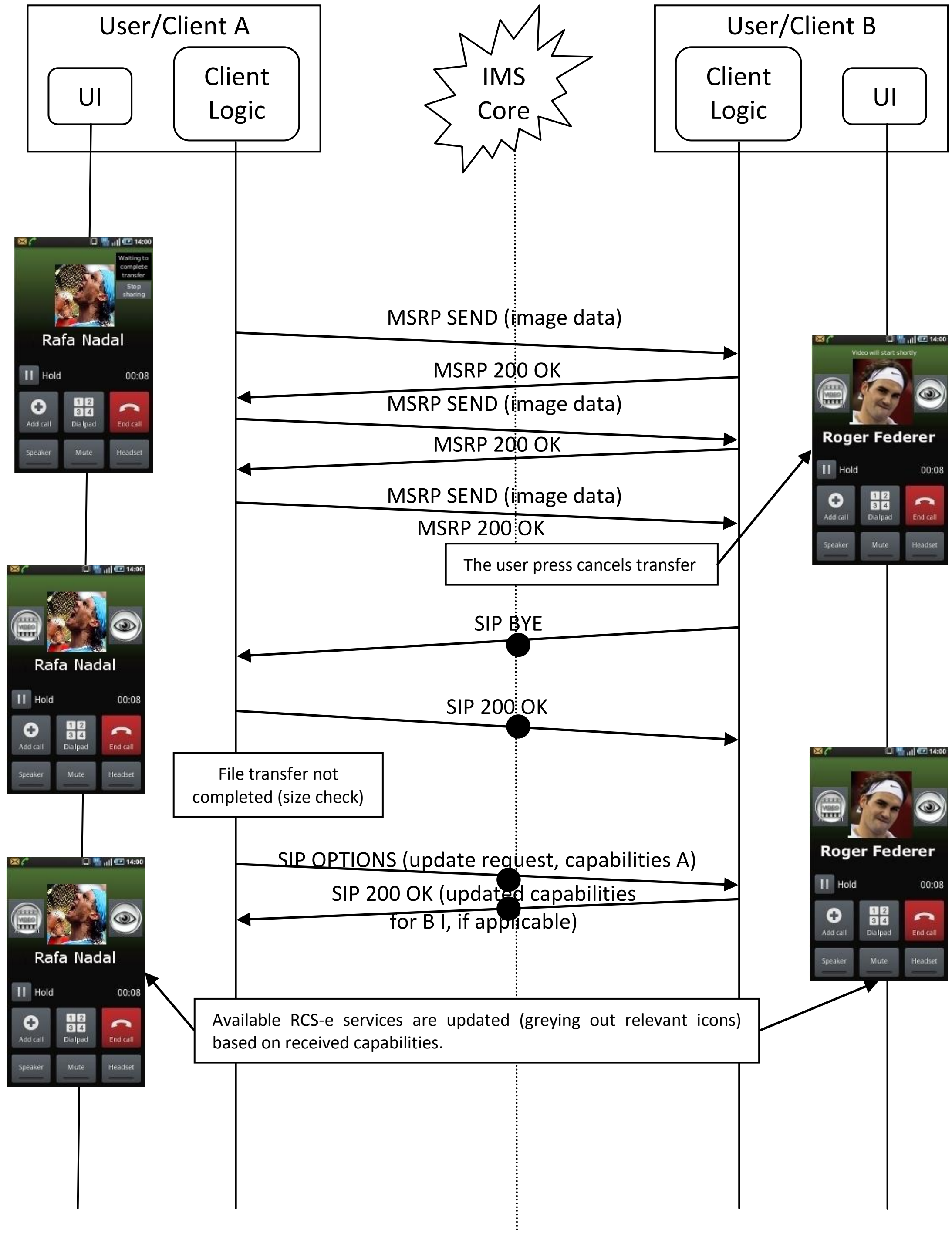

User/Client A
UI
Client Logic
IMS Core
User/Client B
Client Logic
UI
Rafa Nadal
Roger Federer
MSRP SEND (image data)
MSRP 200 OK
MSRP SEND (image data)
MSRP 200 OK
MSRP SEND (image data)
MSRP 200 OK
The user press cancels transfer
SIP BYE
SIP 200 OK
File transfer not completed (size check)
SIP OPTIONS (update request, capabilities A)
SIP 200 OK (updated capabilities for B I, if applicable)
Available RCS-e services are updated (greying out relevant icons) based on received capabilities.

Figure 49. Receiver stops picture sharing

3.3.10 Stop sharing a picture during a call because the required capability is no longer available

The assumptions in this case are that user A is sharing a picture with user B, the transfer has not yet finished, and either A or B are no longer capable (e.g. the terminal is busy) to keep sharing/receiving . Please note in the example, we assumed the sender (user A) is the one losing the capability, however, the sequence will be equivalent for:

- Receiver (user B) loses the capability to receive video: The BYE and OPTIONS exchange would be initiated by the received (user B) in this case.
- Both lose the capability to share video: The BYE and OPTIONS exchange would be initiated by the first one to lose the capability in this case.

Please note there is an exception to stop a file transfer due to capabilities. If one of the users is left with 2G coverage (DTM terminal) once a transfer has started and the handover did not trigger an IP bearer reconfiguration, the transfer may continue until completed. Once the transfer is completed, picture sharing will not be longer available as a service during the call.

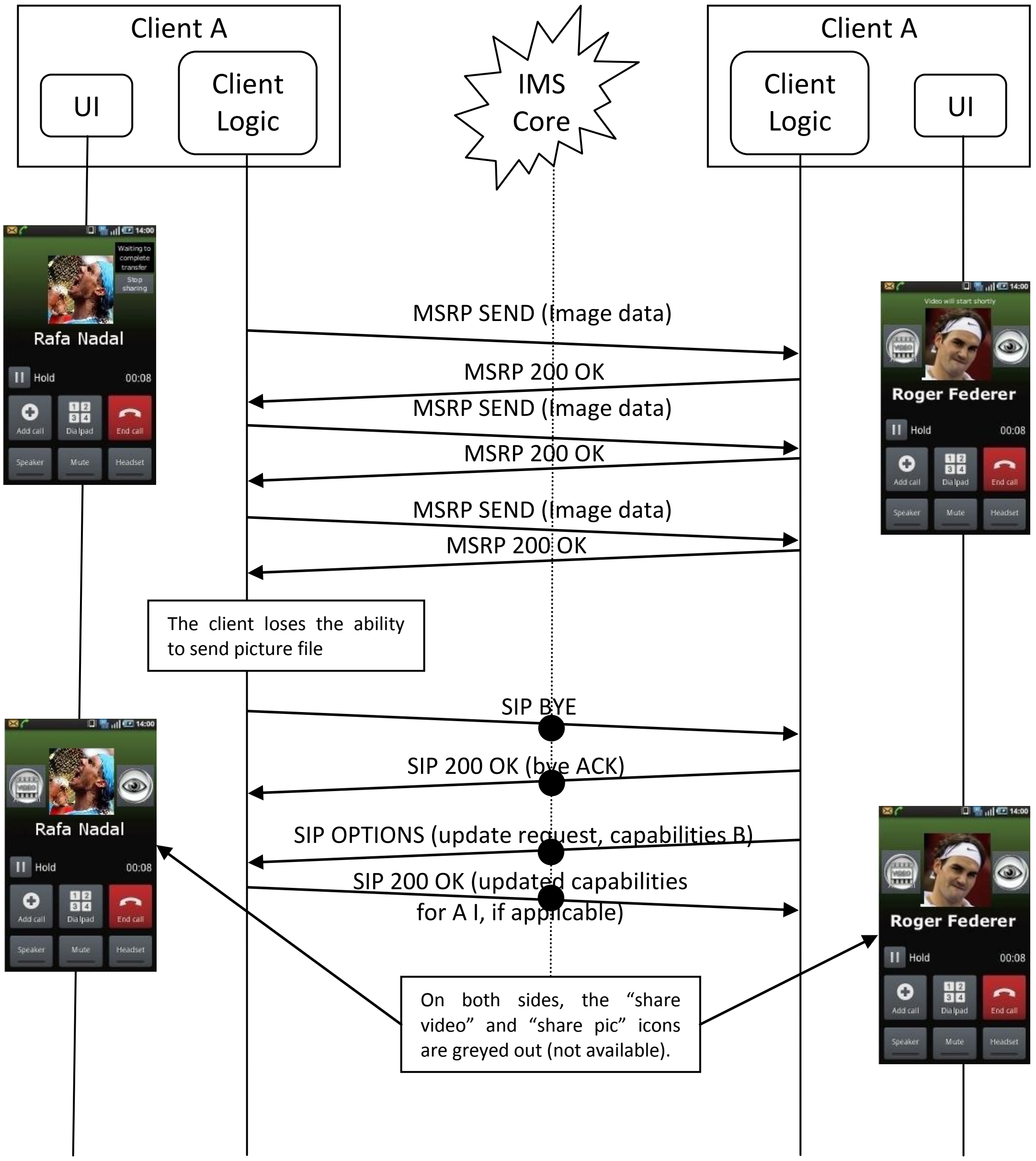
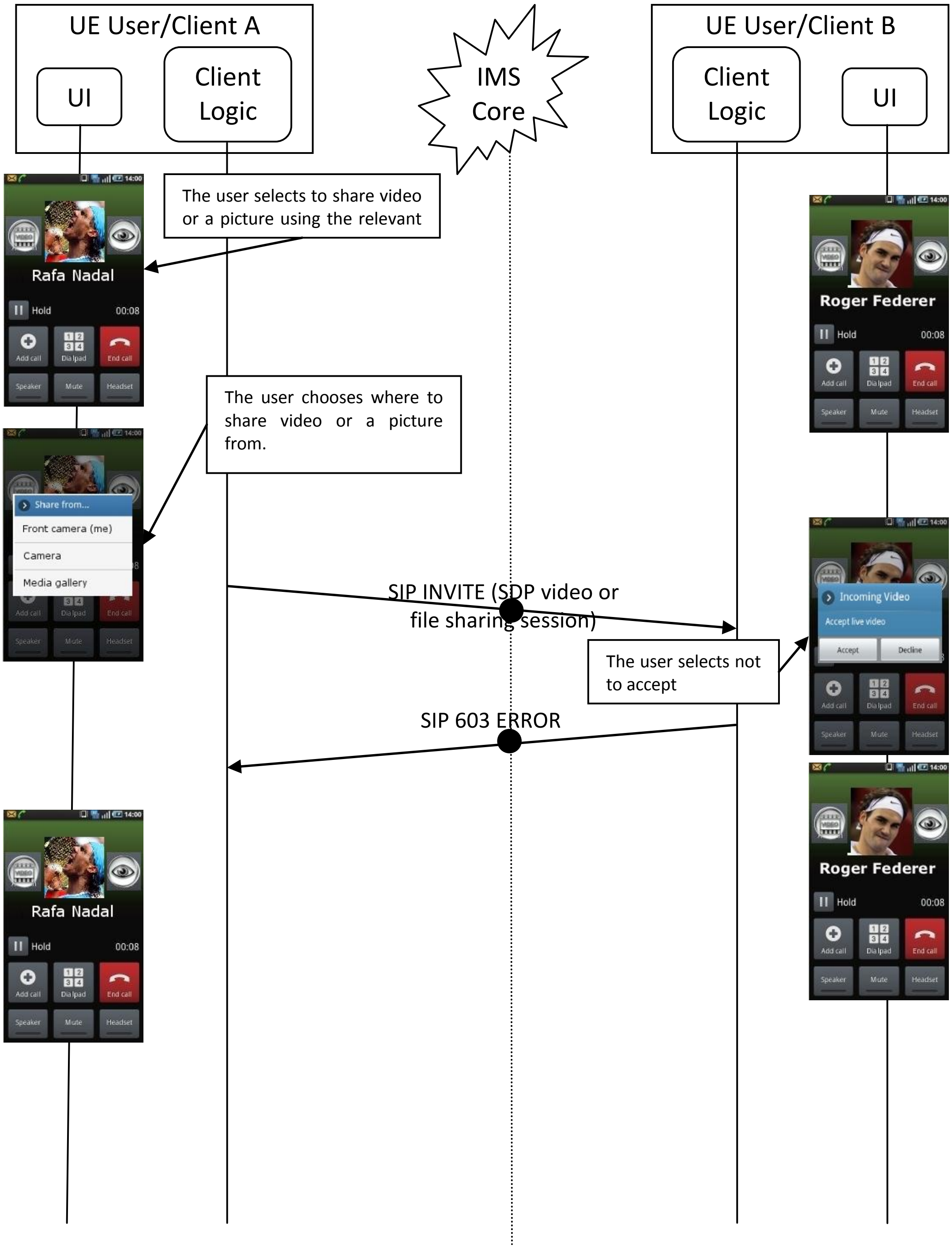


Figure 50. A picture can no longer be shared during a call (capability not available)

3.3.11 Decline share video or picture during a call

User A wants to share a video or picture with user B, however he/she does not want to receive it. Please note we are assuming that both video and image share is possible (right capabilities).



The user selects to share video or a picture using the relevant

The user chooses where to share video or a picture from.

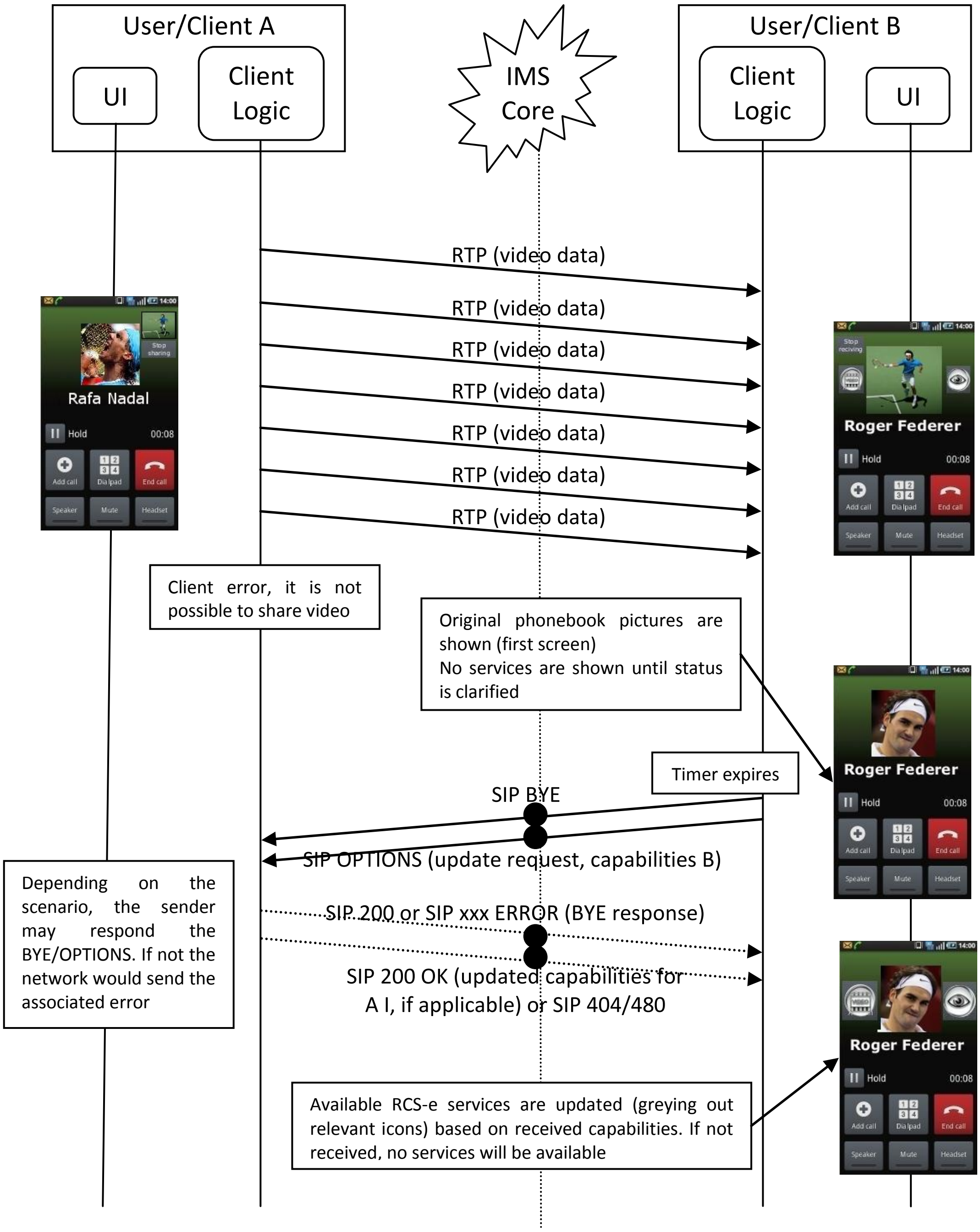
The user selects not to accept

Figure 51. User declines sharing a picture during a call

3.3.12 Non-graceful termination (sender): Video or picture sharing

User A is sharing video or a picture with user B. Suddenly, user A connection to the network fails (e.g. due to a client error, because the phone reboots, no data bearer, a switch in data carrier [e.g. 3G+ to 3G] causes an IP layer reconfiguration, etc.).

In the following flow, we are assuming a video transfer (RTP) was taking place but it will be equivalent to the case an MSRP (image or video sharing via file) was taking place (not finished):



Client error, it is not possible to share video

Original phonebook pictures are shown (first screen)
No services are shown until status is clarified

Depending on the scenario, the sender may respond the BYE/OPTIONS. If not the network would send the associated error

Available RCS-e services are updated (greying out relevant icons) based on received capabilities. If not received, no services will be available

Figure 52. Non-graceful termination (sender) for video

3.3.13 Non-graceful termination (receiver): Video or picture sharing

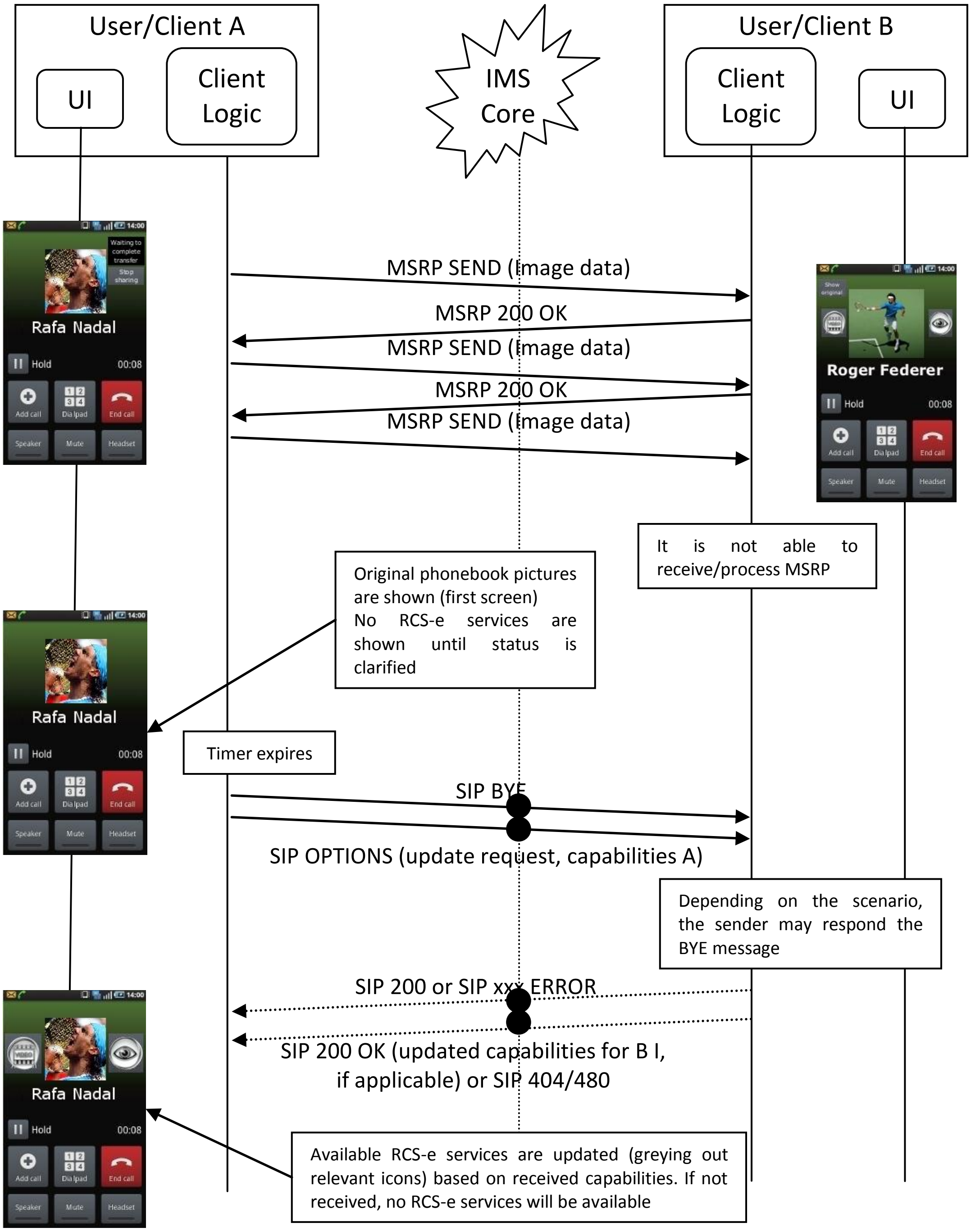
In order to protect the Core SIP network from cases where both the sender and the receiver become unresponsive or unreachable before any of them had the time to terminate the SIP session, the RCS-e Client shall use the procedure described in [RFC4028][47] in a similar way to the one mandated in [RCS2-OMA-SIMPLE-ENDORS][41]; i.e. the RCS-e client initiating a SIP session must request the role of refresher and the option tag 'timer' must be included in a Supported header.

The Session-Expires and Min-SE values announced by an RCS-e client must be configurable by the MNO.

This use case is identical to the previous one, except that in this case User B (receiver) loses the ability to receive/process MSRP (e.g. due to a client error, because the phone reboots, no data bearer, etc.).

In the first flow diagram we have assumed an image MSRP transaction was taking place:

[47] The Session Timers in the Session Initiation Protocol (SIP) IETF RFC is available at http://tools.ietf.org/html/rfc4028.



It is not able to receive/process MSRP

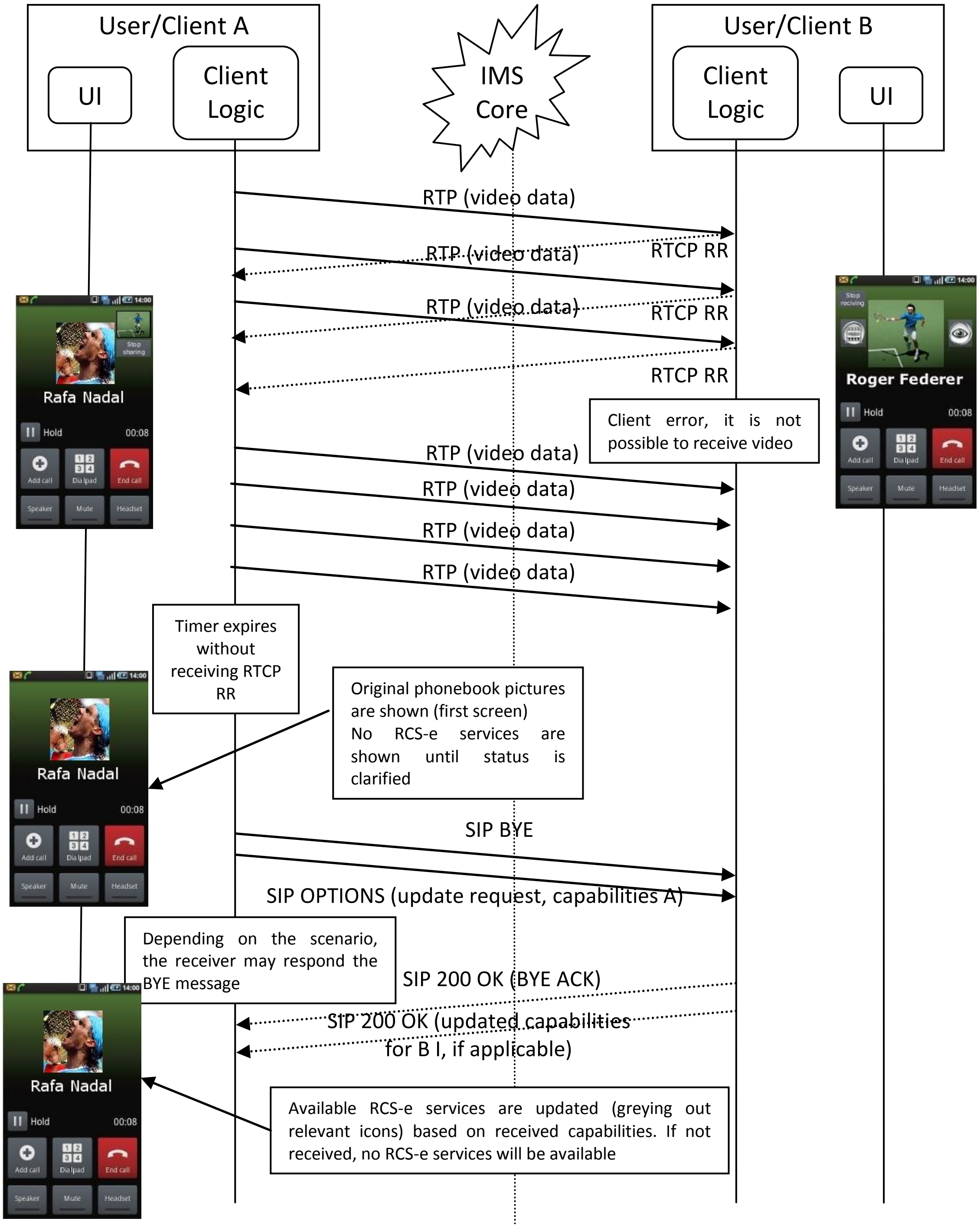
Original phonebook pictures are shown (first screen)
No RCS-e services are shown until status is clarified

Depending on the scenario, the sender may respond the BYE message

Available RCS-e services are updated (greying out relevant icons) based on received capabilities. If not received, no RCS-e services will be available

Figure 53. Non-graceful termination of video or picture sharing during a call

In the second flow we have assumed a video RTP transaction was taking place:



Client error, it is not possible to receive video

Timer expires without receiving RTCP RR

Original phonebook pictures are shown (first screen) No RCS-e services are shown until status is clarified

Depending on the scenario, the receiver may respond the BYE message

Available RCS-e services are updated (greying out relevant icons) based on received capabilities. If not received, no RCS-e services will be available

Figure 54. Non-graceful termination of video sharing during a call

3.3.14 Multiparty call and image/video share

Once a CS call is established between two users, it is possible for any of them to add another party to the call, and consequently, initiate a multiparty call. From RCS services point of view and as presented in section 2.7, the image and video share services are not available during a multiparty call, therefore, the terminal needs to manage the following scenarios:

- The users were in a CS call without using the image or video share services: In this case, switching to a multiparty call means that the end starting the process has to send an SIP OPTIONS message with a capability update (as described in section 3.3.2) indicating that image and video share services are no longer available (i.e. on-screen icons/layout updated accordingly).

- The users were in a CS call using video share: In this case, switching to a multiparty call means ending the video share service, either sender or receiver terminated upon circumstances as described in sections 3.3.4 and 3.3.5 respectively. In both cases, a capabilities exchange using SIP OPTIONS takes place and, consequently, the end initiating the multiparty call should report the image and video share services/capabilities are no longer available (i.e. on-screen icons/layout updated accordingly).

- The users were in a CS call using image share (transfer not completed): In this case, switching to a multiparty call means ending the image share service, either sender or receiver terminated upon circumstances as described in sections 3.3.8 and 3.3.9 respectively. In both cases, a capabilities exchange using SIP OPTIONS takes place and, consequently, the end initiating the multiparty call should report the image and video share services/capabilities are no longer available (i.e. on-screen icons/layout updated accordingly).

- The users were in a CS call using image share (completed): In this case, switching to a multiparty call means the picture is no longer shown in the call screen and that the end starting the process has to send an SIP OPTIONS message with a capability update (as described in section 3.3.2) indicating that image and video share services are no longer available (i.e. on-screen icons/layout updated accordingly).

It should be also noted that from the moment the users enter in a multiparty call, it is not necessary to perform the capability exchange described in section 3.3.2.

Finally, if the multiparty is again converted into a standard call (i.e. again a 1-to-1 call), this event should be treated as a new call establishment meaning that a capability exchange via OPTIONS needs to take place and, consequently, the relevant on screen icons need to be updated.

3.3.15 Call on hold and image/video share

Once a CS call is established between two users, it is possible for any of them to put the other party on hold. From RCS services point of view and as presented in section 2.7, the image and video share services are not available during a call which is not active, therefore, the terminal needs to manage the following scenarios:

- The users were in a CS call without using the image or video share services: In this case, putting the call on hold means that the end starting the process has to send an SIP OPTIONS message with a capability update (as described in section 3.3.2) indicating that image and video share services are no longer available (i.e. on-screen icons/layout updated accordingly).

- The users were in a CS call using video share: In this case, putting the call on hold means ending the video share service, either sender or receiver terminated upon circumstances as described in sections 3.3.4 and 3.3.5 respectively. In both cases, a capabilities exchange using SIP OPTIONS takes place and, consequently, the end initiating the multiparty call should report the image and video share services/capabilities are no longer available (i.e. on-screen icons/layout updated accordingly).

- The users were in a CS call using image share (transfer not completed): In this case, putting the call on hold putting the call on hold switching to a multiparty call means ending the image share service, either sender or receiver terminated upon circumstances as described in sections 3.3.8 and 3.3.9 respectively. In both cases, a capabilities exchange using SIP OPTIONS takes place and, consequently, the end initiating the multiparty call should report the image and video share services/capabilities are no longer available (i.e. on-screen icons/layout updated accordingly).

- The users were in a CS call using image share (completed): In this case, putting the call on hold switching to a multiparty call means the picture is no longer shown in the call screen and that the end starting the process has to send an SIP OPTIONS message with a capability update (as described in section 3.3.2) indicating that image and video share services are no longer available (i.e. on-screen icons/layout updated accordingly).

It should be also noted that from the moment the call is put on hold (i.e. call no active):

- It is not necessary to perform the capability exchange described in section 3.3.2, and,
- If there is another active call, the behaviour regarding to image and video share (capability exchange and the services itself) should not be affected by the fact another call is on hold.

Finally, if the call is again made active, this event should be treated as a new call establishment meaning that a capability exchange via OPTIONS needs to take place and, consequently, the relevant on screen icons need to be updated.

3.3.16 Waiting call and image/video share

A waiting call is a non-active call therefore, consequently with the information presented in section 2.7, it should not be possible to access the image and video share services between the caller and receiver.

Please note having a waiting call will not affect the behaviour for image and video share (capability exchange and the services itself) on the active call.

3.3.17 Calls from private numbers

When a call is received and the caller cannot be identified (e.g. hidden number), it should also not be possible to access the image and video share services between the caller and receiver.

3.3.18 Call divert/forwarding

If a user has call divert/forwarding active (e.g. forward calls to another number or to voicemail), it is not possible to access the image and video share services between the caller and receiver.

3.4 *File transfer*

The file transfer (FT) service enables the users to share files between one or more users instantaneously. As mentioned before, this service comes with some requirements (bandwidth, free space on the receiver's device); therefore, even if a RCS-e contact is registered, it may not be possible to share files.

From the UX experience point of view, there are five possible entry points to this service:

- Address book/Call-log: File share can be initiated with any registered contact providing the right capabilities are in place – contact oriented initiation. Following the address book interaction, the list of available files is displayed, so the user can select one or more to share. Once file transfer commences, the progress can be checked in the standard notification area.

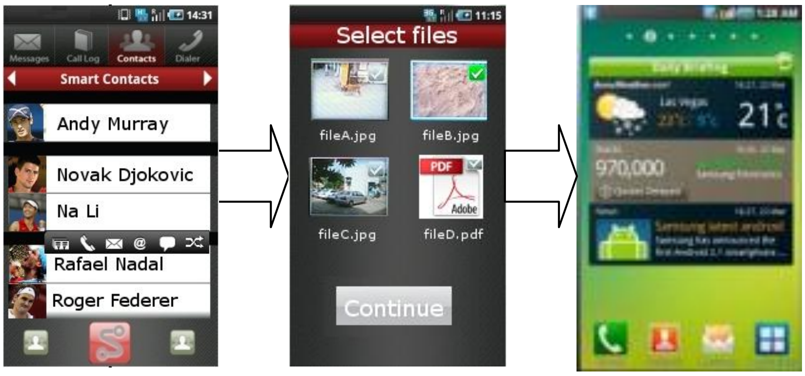


Figure 55. Reference UX for accessing file share from address book/call-log

- Media gallery/File browser: The user can browse, select a file (or multiple files) and then share with one or more RCS-e users – task contact oriented initiation. Only RCS-e capable users shall be displayed as candidate recipient of the file.

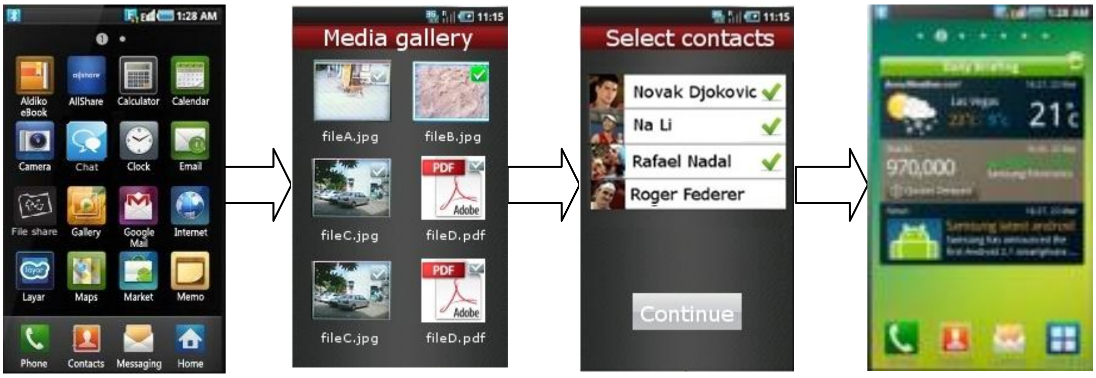


Figure 56. Reference UX for accessing file share from media gallery or file browser

In the previous figure, once file transfer is selected, the user will be presented with the complete list of RCS-e contacts (including contacts which are currently not registered).
In this case, an OPTIONS message is sent once a contact is selected from the list.

- Camera application: The experience is analogous to the media gallery/file browser experience with the difference that the user is able to only select the last picture or video (and, in some cases, one picture or video from the camera gallery) to be shared.
- IM/chat window: From the IM (one-to-one IM only) window a file can be shared using the relevant button/icon. The experience is identical to the address book/call-log. The user is redirected to the media gallery or file explorer where he/she can choose a file which then shared.

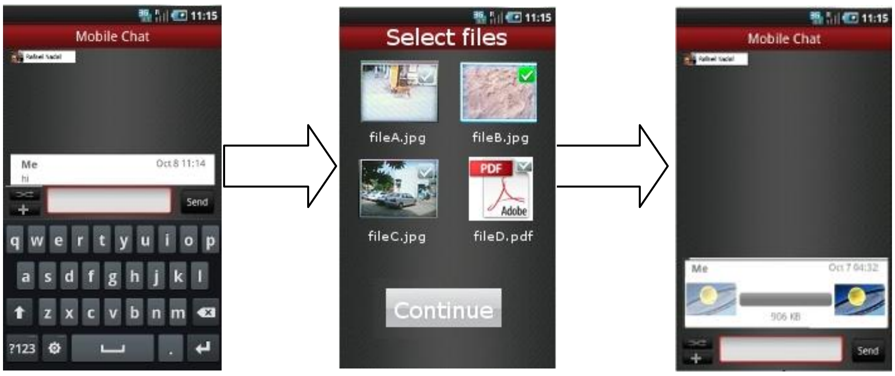


Figure 57. Reference UX for accessing file share from an IM window

- Call screen (image share): We can share a picture either by using the camera (front or back) or choosing a file from the media gallery. Please note this has been covered in detail in section 3.3.

When transferring a file whilst not in an existing session (i.e. when not in a call or IM) and after the transfer has commenced (i.e. the user accepted the incoming file) the file transfer is presented to the recipient in an IM UX. This establishes a communication context for the transfer as the recipient may want to know why the sender is sharing the file. Please note that at the time the file is presented, the IM session is not started; the IM session will only start if and when the receiver sends an IM message back to the sender.

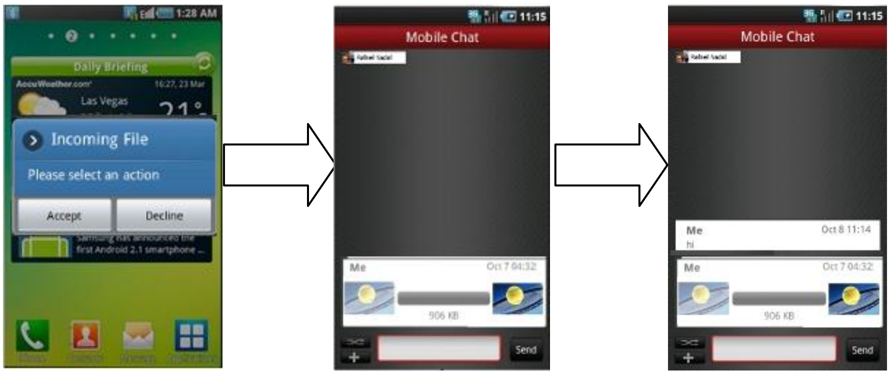


Figure 58. Reference UX for file transfer on the receiver side

3.4.1 General assumptions

In the proceeding sections we will be showing the relevant message flows and reference user experience (UX). These are based upon the following assumptions:

- For simplicity, the internal mobile network interactions are omitted in the diagrams showed in the following sections.
- It is assumed that by the time the file transfer begins, both sender and recipient have exchanged their capabilities using the OPTIONS message. Please note that if there is a UI flow which invalidates this assumption, OPTIONS messages should be exchanged between the sender and the receiver (bidirectional).
- All the file transfer service exchanges presented in this document follow the RCS GSMA[48] and OMA-IM specification[49] for file transfer. In other words, RCS-e makes use of RCS File Transfer service functionality without any modifications or additions.

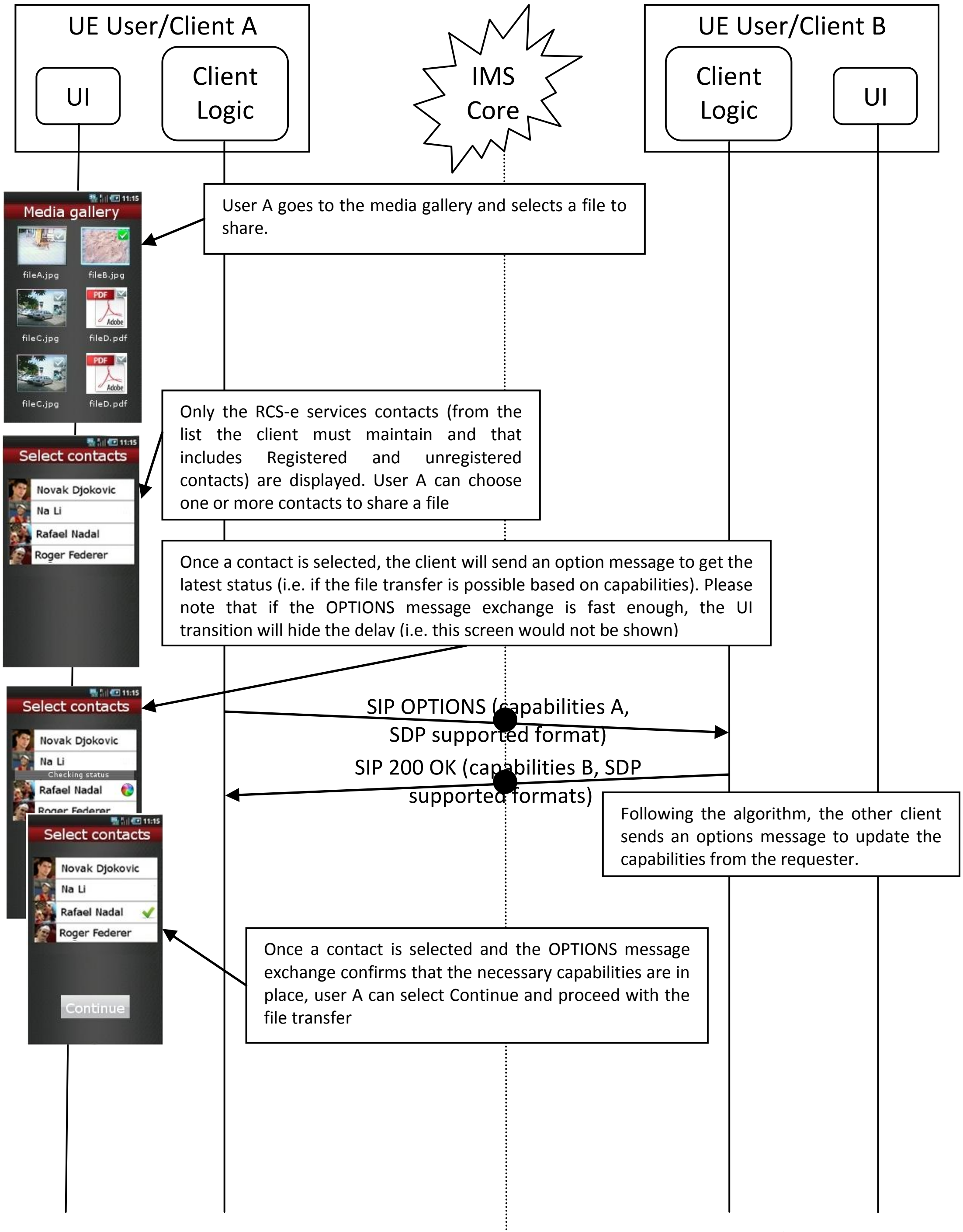
3.4.2 Selecting the file transfer recipient(s)

The first step for a user willing to share a file from the media gallery or file browser is to select the file and then choose the user or group of users the file will be shared with. Please note that the list which is presented to the user contains RCS-e contacts which may or may not be registered. In addition to this, the capabilities the client has for a contact may not have been updated.

Therefore, the first step is to determine whether the file can be shared with the selected user (i.e. should be registered and the right capabilities should be in place)

[48] By this reference we include both technical and functional references contained in the RCS Release 2 specifications (Technical Realization v2.0 [RCS2-TEC-REAL], Service Definition v2.0 [RCS2-SD] and Functional Description v2.0 [RCS2-FUN-DESC] available at www.gsmworld.com)

[49] Via GSMA RCS Release 2 OMA-IM endorsement [RCS2-OMA-SIMPLE-ENDORS]



User A goes to the media gallery and selects a file to share.

Only the RCS-e services contacts (from the list the client must maintain and that includes Registered and unregistered contacts) are displayed. User A can choose one or more contacts to share a file

Once a contact is selected, the client will send an option message to get the latest status (i.e. if the file transfer is possible based on capabilities). Please note that if the OPTIONS message exchange is fast enough, the UI transition will hide the delay (i.e. this screen would not be shown)

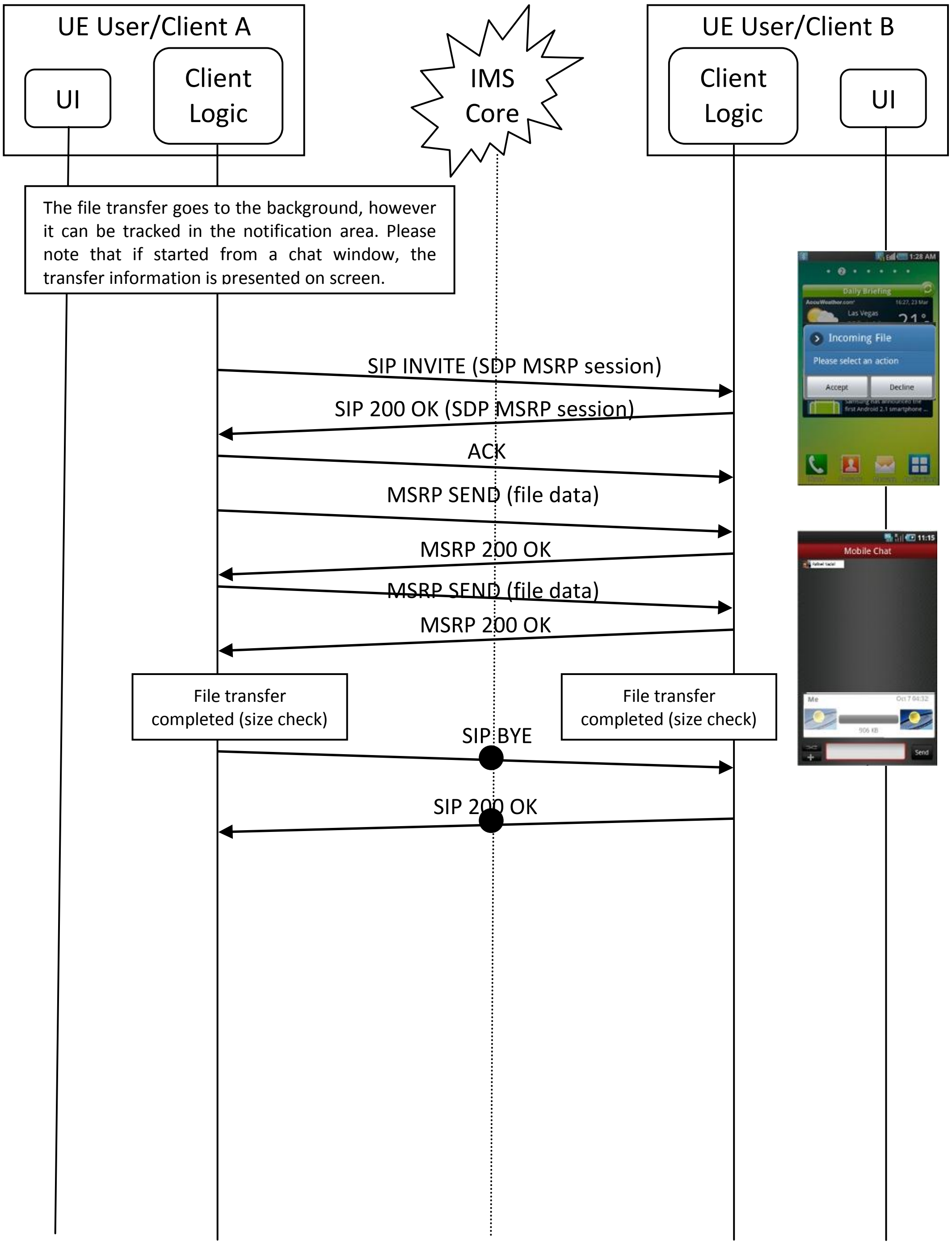
Following the algorithm, the other client sends an options message to update the capabilities from the requester.

Once a contact is selected and the OPTIONS message exchange confirms that the necessary capabilities are in place, user A can select Continue and proceed with the file transfer

Figure 59. Selecting users when sharing a file from the media gallery/file browser

3.4.3 Standard file share procedure

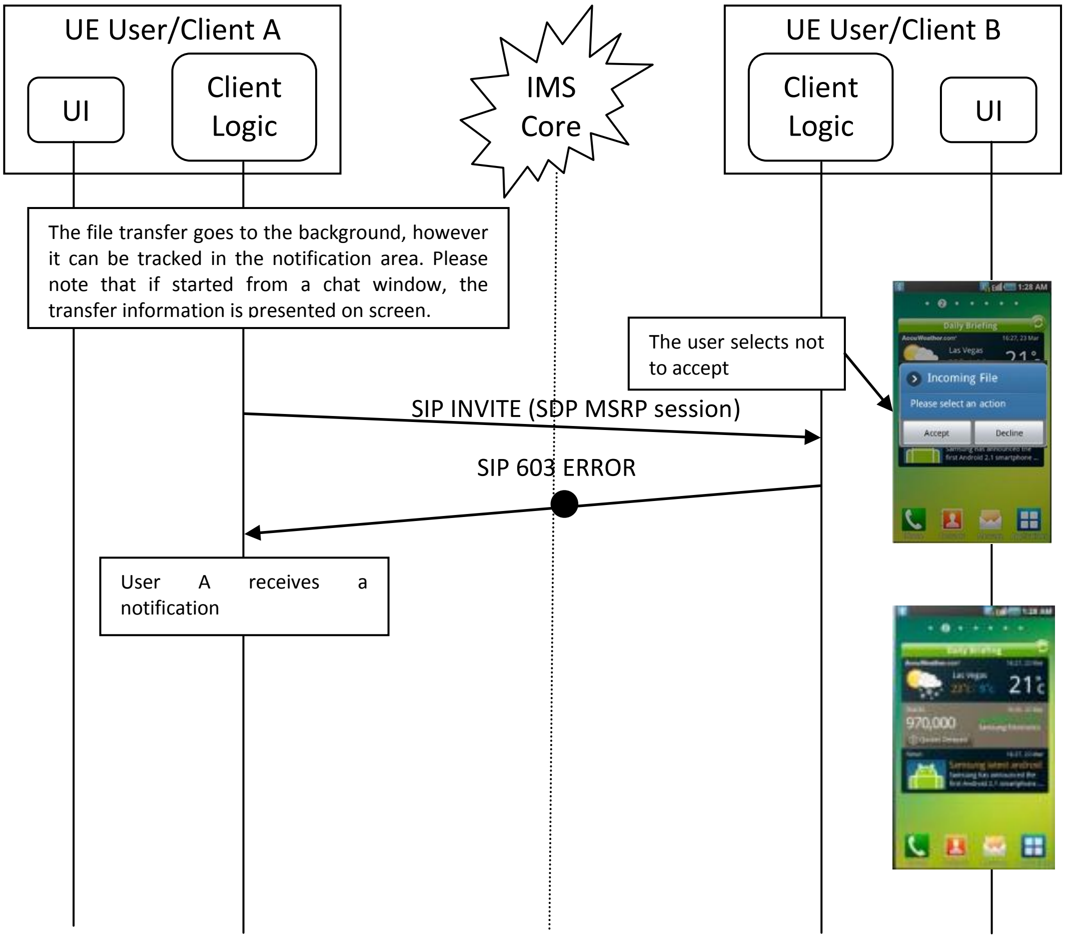
Independently of the file share UX entry point, once the files and users are selected, the transfer can start. Please note that if a user chooses to share several files with one or more users, each individual file transfer (1 file to 1 user only) are serialised (i.e. it is not supported to have simultaneous file sharing processes running in parallel).
In the following diagram, it is assumed the receiver accepts the transfer.



The file transfer goes to the background, however it can be tracked in the notification area. Please note that if started from a chat window, the transfer information is presented on screen.

Figure 60. Standard file transfer sequence diagram – Successful transfer

In the following diagram, User B rejects the transfer.



The file transfer goes to the background, however it can be tracked in the notification area. Please note that if started from a chat window, the transfer information is presented on screen.

The user selects not to accept

User A receives a notification

Figure 61. Standard file transfer sequence diagram – Receiver rejects the transfer

3.4.4 File share error cases

There are several scenarios in which a file transfer can result in an error. All these scenarios have been already covered in previous sections:

- Either the sender or the receiver decides to cancel the operation before the transfer is completed. The relevant sequences are equivalent to the diagrams presented for file sharing during a voice call in sections 3.3.8 and 3.3.9
- Either the sender or the receiver loses the connection to the network, before the transfer is completed. The relevant sequences are equivalent to those presented for file sharing during a voice call in sections 3.3.12 and 3.3.13

Finally, please note that if during a file transfer the capabilities of one of the ends changes, the file transfer may be affected:

- If the receiver runs out of space, the sequence should be equivalent to that presented in section 3.3.10.
- If one of the ends handovers into 2G (2G GPRS data coverage) without losing the IP configuration, the file transfer should continue until finished.

3.4.5 File share and file types

In principle, the RCS-e file transfer service comes without a limitation on the file sizes or types, meaning any kind of file can be transferred using this service. Taking this into account this and with the aim of providing all the necessary facts to the receiver to make an informed decision on whether to accept or reject the file, a user receiving a file transfer invitation should be informed at least of:

a) The size of the file: This is mainly to protect the user from unexpected charges and/or long transfers.
b) The file type: In this case and to make it more intuitive, the handset should present to the user whether the file which is being transferred can be handled/displayed by the device.

For example, if a user receives an invitation to receive a PDF document and his/her handset cannot process that sort of documents, an informative message with the size and the fact that the file type is not supported should be presented to the user prior to the decision of accepting or rejecting the file transfer.

Finally note that each individual MNO may introduce restrictions taking into account different consideration (e.g. security, intellectual property, etc.).

3.4.6 File size considerations

In order to prevent both the abuse of the file transfer functionality and protect customers from unexpected charges, a configurable size limitation (refer to FT WARN SIZE and FT MAX SIZE in Table 6 for reference) may be enabled.

From the user experience point of view and assuming the size limitation is in place (i.e. the values are different from 0):

- If a file transfer (send or receive) involves a file bigger than FT WARN SIZE, the terminal should warn the user of the potential associated charges and get confirmation from the user to go ahead.

- If the file is bigger than FT MAX SIZE, a warning message will be displayed when trying to send or receive a file larger that the mentioned limit and the transfer will be cancelled (i.e. at protocol level, the SIP INVITE will never be sent or a rejection response will be sent to the other end depending on the case).

A. ANNEX A: Extensions to the data model

As presented in section 1 and in section 2.1 Table 6, this specification proposes a set of extensions to the RCS data model part of the GSMA RCS Release 2 specification and described in detail in [RCS2-MO][50].

The aim of this section is to provide the necessary data to complement the mentioned GSMA RCS Release 2 specification documentation and, consequently, provide a complete configuration data model both for MNOs and OEMs reference.

A.1 Management objects parameter additions

Please note the information contained in this section is aimed to complement section 2 of [RCS2-MO][50] and, therefore, the parameters described in the following sections are additions to those already described in [RCS2-MO][50].

A.1.1 Presence related configuration

RCS-e specification includes the following additional presence related configuration parameters:

Configuration parameter	Description	RCS-e usage
USE PRESENCE	This parameter allows enabling or disabling the presence related features on the device. If set to 0, presence is disabled, if set to 1, presence is enabled and the parameters pertaining to presence defined in [RCS2_MO][50] apply.	Mandatory parameter

Table 27. RCS-e additional presence related configuration parameters

A.1.2 XDM related configuration

RCS-e specification does not include any additional XDM related parameters apart from those mentioned in [RCS2-MO][50]. Nevertheless, it should be noted that all the parameters become optional as they are only needed when employing presence-related functionality like presence discovery or profile information sharing.

A.1.3 IM related configuration

RCS-e specification includes the following additional IM related configuration parameters:

[50] Rich Communication Suite Release 2 Management Objects Version 2.0 14 February 2011 available at www.gsmworld.com

Configuration parameter	Description	RCS-e usage
IM CONFERENCE FACTORY URI	This is the parameter containing the URI for the IM server. The parameter is optional and if not configured, means that the MNO is not deploying an IM server. Consequently features requiring IM server (i.e. 1-to-many IM) will not be available for those customers.	Optional Parameter
IM CAP ALWAYS ON	This parameter configures the client to support store and forward when presenting the IM capability status for all the contacts. If set to **1**, the IM capability for all RCS-e contacts will be always reported as available. Otherwise (**0)**, the capability will be reported based on the algorithm presented in section 2.7. For example, this can be used in MNOs that are implementing the store and forward functionality for IM	Optional parameter (It is mandatory if IM CONFERENCE FACTORY URI is set)
IM WARN SF	In case, IM CAP ALWAYS ON is set to enabled (use of store and forward), a new parameter is used called IM WARN SF for UI purpose only. If IM WARN SF parameter is set to (1) then, when chatting with contacts which are offline (Store and Forward), the UI must warn the user of the circumstance (e.g. message on the screen). Otherwise (0), there won't be any difference at UX level between chatting with an online or offline (Store and Forward) user.	Optional parameter (It is mandatory if IM CONFERENCE FACTORY URI is set and IM CAP ALWAYS ON is set to 1)
IM SESSION START	This parameter defines the point in a chat when the receiver sends the 200 OK back to the sender so the MSRP session can be established: 0 (RCS-e default): The 200 OK is sent when the receiver consumes the notification opening the chat window. 1 (RCS default): The 200 OK is sent when the receiver starts to type a message back in the chat window. 2: The 200 OK is sent when the receiver sends a message (i.e. the message will not generate an invite but instead will be buffered in the client until the MSRP session is established.	Mandatory parameter

Table 28. RCS-e additional IM related configuration parameters

It should be also noted that the IM CONFERENCE FACTORY URI parameter should be configured using the *conf-fcty-uri* parameter as described in section 4.4 of [RCS2-MO][50]. Again, if set to 0, this limitation does not apply.

A.1.4 File transfer related configuration

RCS-e specification includes the following additional file transfer related configuration parameters:

Configuration parameter	Description	RCS-e usage
FT MAX SIZE	This is a file transfer size limit in KB. If a file is bigger than FT MAX SIZE, the transfer will be automatically cancelled. Please note that if set to 0, this limit will not apply.	Mandatory Parameter
FT WARN SIZE	This is a file transfer size limit in KB to warn the user that a file may end up in significant charges. Please note that if set to 0, the user will not be warned.	Mandatory Parameter

Table 29. RCS-e additional file transfer related configuration parameters

It should be also noted that the FT MAX SIZE parameter should be configured using the *MaxSizeFileTr* parameter as described in section 4.4 of [RCS2-MO][50]. Again, if set to 0, this limitation does not apply.

A.1.5 IMS Core /SIP related configuration

RCS-e specification includes no-specific additional IMS Core/SIP related configuration parameters. Nevertheless, it should be noted that:

- The USER and PASSWD parameters described in section 2.1 Table 6 map to the UserName and UserPwd parameters described in [RCS2-MO][50].
- The TEL-URI and SIP-URI parameters map to the Public_User_Identity parameters defined in [3GPP TS 24.167][51] [52] and endorsed in [RCS2-MO][50].
- The SIP PROXY parameter maps to the parameters hosted by the LBO_P-CSCF_Address sub-tree defined in [3GPP TS 24.167][51][52] and endorsed in the Managed Object document (version 1.1) part of the GSMA RCS Release 2

[51] 3GPP TS 24.167 version 10.2.0 (Mar-11) ,3rd Generation Partnership Project;Technical Specification Group Core Network and Terminals; 3GPP IMS Management Object (MO).

[52] The private identity (Private_User_Identity), public identity (Public_User_Identity_List/<X>/Public_User_Identity) and domain (Home_network_domain_name) objects mentioned in 3GPP TS 24.167 are defined as read-only and these parameters should be obtained by the UE using the procedures described in 3GPP TS 24.229. This specification makes and exception to that definition and consider them writable during the autoconfiguration process (OMA-DM, OMA-CP or the alternative HTTP mechanism).

specification. When the P-CSCF address has an "FQDN" type, the SIP transport protocol can be selected by the RCS-e client thanks to DNS SRV requests. When the P-CSCF address has an "IP Address" type, the SIP transport protocol should be selected based on MNO customized settings.

A.1.6 Configuration related with Address book Back-up/Restore

RCS-e specification does not include any additional address book back-up/restore related configuration parameters.

A.1.7 Configuration related with secondary device introduction

RCS-e specification does not include any additional secondary device introduction related configuration parameters.

A.1.8 Capability discovery related configuration

Although not covered in RCS Release 2, RCS-e specification includes the following additional capability discovery configuration parameters:

Configuration parameter	Description	RCS-e usage
POLLING PERIOD	This is frequency in seconds to run a periodic capabilities update for all the contacts in the phone address book whose capabilities are not available (e.g. non-RCS-e users) or are expired (see CAPABILITY INFO EXPIRY parameter. Please note that if set to 0, this periodic update is no longer performed.	Mandatory parameter
CAPABILITY INFO EXPIRY	When using the OPTIONS discovery mechanism and with the aim of minimizing the traffic, an expiry time is set in the capability information fetched using options. When performing a whole addressbook capability discovery (i.e. polling), an OPTIONS exchange takes place only if the time since the last capability update took place is greater than this expiration parameter	Optional parameter (It is mandatory if POLLING PERIOD is set to a value greater than 0)
PRESENCE DISCOVERY	This parameter allows enabling or disabling the usage of capabilities discovery via presence. If set to 0, the usage of discovery via presence is disabled. If set to 1, the usage of discovery via presence is enabled. This parameter will consequently influence the inclusion of the associated tag to presence discovery in OPTIONS exchanges.	Optional parameter (It is mandatory and becomes relevant only if USE PRESENCE is set to 1)

PRESENCE PROFILE	This parameter allows enabling or disabling the usage of the *social information via presence*. If set to 0, the usage of the *social information via presence* feature is disabled. If set to 1, the *social information via presence* feature is enabled. This parameter will consequently influence the inclusion of the associated tag to *social information via presence* in OPTIONS exchanges.	Optional parameter (It is mandatory and becomes relevant only if USE PRESENCE is set to 1)

Table 30. RCS-e additional capability discovery related configuration parameters

A.1.9 APN configuration

Although not covered in RCS Release 2, RCS-e specification includes the following additional configuration parameters targeting APN configuration (see sections 2.10 and 2.11):

Configuration parameter	Description	RCS-e usage
RCS-E ONLY APN	This is the reference/identifier to the APN configuration which should be used to provide PS connectivity ONLY to RCS-e as described in section 2.10.	Mandatory Parameter
ENABLE RCS-E SWITCH	As described in section 2.10, the user shall be able configure to allow or disallow RCS-e and/or internet traffic in the handset settings. If this parameter is set to 1, the setting is shown permanently. Otherwise it may be (MNO decision) only shown during roaming.	Mandatory Parameter

Table 31. RCS-e roaming configuration parameters

A.1.10 End user confirmation parameters

Although not covered in RCS Release 2, RCS-e specification includes the following additional configuration parameters targeting the End user confirmation configuration (see section 2.13):

Configuration parameter	Description	RCS-e usage
END USER CONF REQ ID	This is identity used for sending the end user confirmation request.	Optional Parameter

Table 32. RCS-e end user confirmation parameters

A.2 RCS Management trees additions

Please note the information contained in this section is aimed to complement section 4 of [RCS2-MO][50]. Please note that a common change to all the configuration sub trees described in this section is that the type property for the root nodes (i.e. /<X> nodes root) is *urn:gsma:mo:rcs:rcse* instead *urn:gsma:mo:rcs:2.0*.

A.2.1 IMS sub tree additions

The RCS-e specification does not include any additions to the RCS IMS sub tree defined in [RCS2-MO][50].

```
<characteristic type="APPLICATION">
      <parm name=”AppID” value=”X”/>
 </characteristic>
<characteristic type=”IMS”>
      <parm name=”Name” value=”X”/>
      <characteristic type=”ConRefs”>
            <parm name=”ConRef” value=”X”/>
      </characteristic>
      <parm name=”PDP_ContextOperPref” value=”X”/>
      <parm name=”Timer_T1” value=”X”/>
      <parm name=”Timer_T2” value=”X”/>
      <parm name=”Timer_T4” value=”X”/>
      <parm name=”Private_User_Identity” value=”X”/>
      <characteristic type=”Public_User_Identity_List”>
            <parm name=”Public_User_Identity” value=”X”/>
      </characteristic>
      <parm name=”Home_network_domain_name” value=”X”/>
      <characteristic type=”Ext”>
            <parm name=”NatUrlFmt” value=”X”/>
            <parm name=”IntUrlFmt” value=”X”/>
            <parm name=”Q-Value” value=”X”/>
            <characteristic type=”SecondaryDevicePar”>
                  <parm name=”VoiceCall” value=”X”/>
                  <parm name=”Chat” value=”X”/>
                  <parm name=”SendSms” value=”X”/>
                  <parm name=”FileTranfer” value=”X”/>
                  <parm name=” VideoShare” value=”X”/>
                  <parm name=”ImageShare” value=”X”/>
            </characteristic>
            <parm name=”MaxSizeImageShare” value=”X”/>
            <parm name=” MaxTimeVideoShare value=”X”/>
      </characteristic>
      <characteristic type=”ICSI_List”>
            <parm name=”ICSI” value=”X”/>
            <parm name=”ICSI_Resource_Allocation_Mode” value=”X”/>
      </characteristic>
      <characteristic type=”LBO_P-CSCF_Address”>
            <parm name=”Address” value=”X”/>
            <parm name=”AddressType” value=”X”/>
      </characteristic>
      <parm name=”Voice_Domain_Preference_E_UTRAN” value=”X”/>
      <parm name=”SMS_Over_IP_Networks_Indication” value=”X”/>
      <parm name=”Keep_Alive_Enabled” value=”X”/>
      <parm name=”Voice_Domain_Preference_UTRAN” value=”X”/>
```

Table 33. IMS sub tree associated OMA-CP configuration XML structure (1/2)[53]

[53] Please note the values marked in red refer to the objects described in [3GPP TS 24.167] as presented in section A.1.5.

```
-- follows from previous page –

      <parm name="Mobility_Management_IMS_Voice_Termination" value="X"/>
      <parm name="RegRetryBaseTime" value="X"/>
      <parm name="RegRetryMaxTime" value="X"/>
      <characteristic type="PhoneContext_List">
            <parm name="PhoneContext" value="X"/>
            <parm name="Public_User_Identity" value="X"/>
      </characteristic>
      <characteristic type="APPAUTH">
            <parm name="AuthType" value="X"/>
            <parm name="Realm" value="X"/>
            <parm name="UserName" value="X"/>
            <parm name="UserPwd" value="X"/>
      </characteristic>
</characteristic>
```

Table 34. IMS sub tree associated OMA-CP configuration XML structure

A.2.2 Presence sub tree additions

RCS-e specification includes the following additions to the presence sub tree:

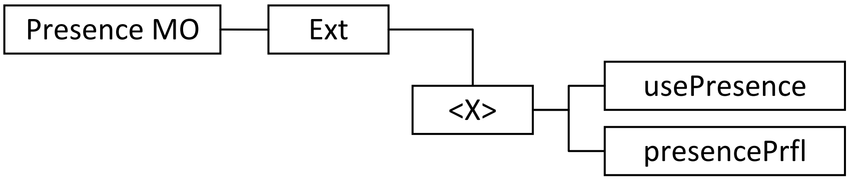


Figure 62. RCS-e additions to the presence MO sub tree

The associated OMA-CP configuration XML structure is presented in the table below. Please note that as RCS R2 specification does not cover OMA-CP configuration of RCS clients, both RCS (marked in blue) and RCS-e parameters are shown in this case (not only additions as for OMA-DM):

```
<characteristic type=”PRESENCE”>
      <parm name=”usePresence” value=”X”/>
      <parm name=”presencePrfl” value=”X”/>
      <parm name=”AvailabilityAuth” value=”X”/>
      <characteristic type=”FAVLINK”>
            <parm name=” AutMa” value=”X”/>
            <characteristic type=”LINKS”>
                  <parm name=” OpFavUrl1” value=”X”/>
                  <parm name=” OpFavUrl2” value=”X”/>
                  <parm name=” OpFavUrl3” value=”X”/>
                  …
            </characteristic>
      </characteristic>
      <parm name=”IconMaxSize” value=”X”/>
      <parm name=”NoteMaxSize” value=”X”/>
      <characteristic type=”SERVCAPWATCH”>
            <parm name=”FetchAuth” value=”X”/>
            <parm name=” ContactCapPresAut” value=”X”/>
      </characteristic>
      <characteristic type=”ServCapPresentity”>
            <parm name=”WATCHERFETCHAUTH” value=”X”/>
      </characteristic>
      <parm name=”client-obj-datalimit” value=”X”/>
      <parm name=”content-serveruri” value=”X”/>
      <parm name=”source-throttlepublish” value=”X”/>
      <parm name=”max-number-ofsubscriptions-inpresence-list
            ” value=”X”/>
      <parm name=”service-uritemplate” value=”X”/>
</characteristic>
```

Table 35. Presence sub tree associated OMA-CP configuration XML structure

Node: /<X>

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

Status	Occurrence	Format	Min. Access Types
Required	One	node	Get

Table 36. Presence MO sub tree addition presence node

- Values: N/A
- Type property of the Node is: *urn:gsma:mo:rcs:rcse:presence-ext*
- Associated OMA-CP characteristic type: “PRESENCE”

Node: /<X>/usePresence

Leaf node that describes whether the presence related features are enabled or disabled on the device.

Status	Occurrence	Format	Min. Access Types
Required	One	Bool	Get/Put

Table 37. Presence MO sub tree addition parameters (usePresence)

- Values: 1, the presence related features are enabled. 0, the presence related features are disabled.
- Post-reconfiguration actions: The client should be reset and should perform the complete first-time registration procedure following a reconfiguration (e.g. OMA-DM/OMA-CP) as described in section 2.2.2.1.
- Associated OMA-CP parameter ID: “usePresence”

Node: /<X>/presencePrfl

Leaf node that describes whether the social presence functionality is supported.

Status	Occurrence	Format	Min. Access Types
Required	One	Bool	Get/Put

Table 38. Capability MO sub tree addition parameters (presencePrfl)

- Values: If set to 1, it is supported. If set to 0, it is not supported.
- Post-reconfiguration actions: The client should be reset and should perform the complete first-time registration procedure following a reconfiguration (e.g. OMA-DM/OMA-CP) as described in section 2.2.2.1.
- Associated OMA-CP parameter: “presencePrfl”

A.2.3 XDMS sub tree additions

The RCS-e specification does not include any additions to the RCS XDMS sub tree defined in [RCS-MO][50].

As the RCS R2 specification does not cover OMA-CP configuration of RCS clients, the associated OMA-CP configuration XML structure for the parameters defined in the RCS R2 specification is presented in the table below:

```
<characteristic type=”XDMS”>
      <parm name=”RevokeTimer” value=”X”/>
      <parm name=”XCAPRootURI” value=”X”/>
      <parm name=”XCAPAuthenticationUserName” value=”X”/>
      <parm name=”XCAPAuthenticationSecret” value=”X”/>
      <parm name=”XCAPAuthenticationType” value=”X”/>
</characteristic>
```

Table 39. XDMS sub tree associated OMA-CP configuration XML structure

A.2.4 IM MO sub tree addition

RCS-e specification includes the following additions to the IM MO sub tree:

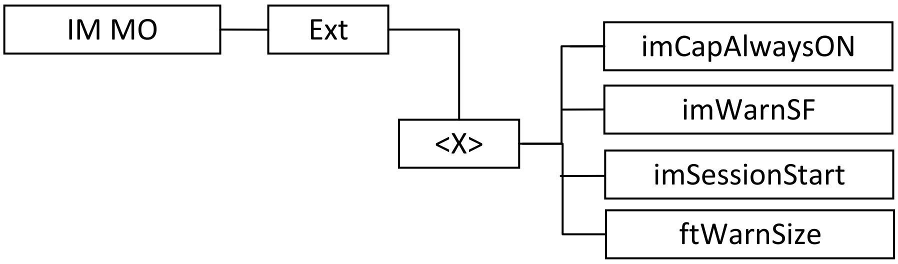


Figure 63. RCS-e additions to the IM MO sub tree

The associated OMA-CP configuration XML structure is presented in the table below. Please note that as RCS R2 specification does not cover OMA-CP configuration of RCS clients, both RCS (marked in blue) and RCS-e parameters are shown in this case (not only additions as for OMA-DM):

```
<characteristic type=”IM”>
      <parm name=” imCapAlwaysON” value=”X”/>
      <parm name=” imWarnSF” value=”X”/>
      <parm name=” imSessionStart” value=”X”/>
      <parm name=” ftWarnSize” value=”X”/>
      <parm name=”ChatAuth” value=”X”/>
      <parm name=”SmsFallBackAuth” value=”X”/>
      <parm name=”AutAccept” value=”X”/>
      <parm name=”MaxSize1to1” value=”X”/>
      <parm name=”MaxSize1toM” value=”X”/>
      <parm name=”TimerIdle” value=”X”/>
      <parm name=”MaxSizeFileTr” value=”X”/>
      <parm name=”pres-srv-cap” value=”X”/>
      <parm name=”deferred-msg-func-uri” value=”X”/>
      <parm name=”max_adhoc_group_size” value=”X”/>
      <parm name=”conf-fcty-uri” value=”X”/>
      <parm name=”exploder-uri” value=”X”/>
</characteristic>
```

Table 40. IM sub tree associated OMA-CP configuration XML structure

Node: /<X>

Under this interior node are placed the RCS parameters related to the IM configuration.

Status	Occurrence	Format	Min. Access Types
Required	One	node	Get

Table 41. IM MO sub tree addition IM node

- Values: N/A
- Type property of the Node is: *urn:gsma:mo:rcs:rcse:im-ext*
- Associated OMA-CP characteristic type: “IM”

Node: /<X>/imCapAlwaysON

Leaf node that describes whether the IM capability needs to be on independently on whether the other end is registered. For example this can be used in MNOs providing the store and forward functionality for IM

Status	Occurrence	Format	Min. Access Types
Optional	One	bool	Get/Put

Table 42. IM MO sub tree addition parameters (imCapAlwaysOn)

- Values: 1, RCS IM/chat server store and forward is enabled; 0, is disabled
- Post-reconfiguration actions: As the client remains unregistered during configuration, there are no additional actions apart from de-registering using the old configuration (section 2.2.2.4) and registering back (section 2.2.2.2) using the new parameter.
- Associated OMA-CP parameter: “imCapAlwaysOn”

Node: /<X>/imWarnSF

Leaf node that describes whether the UX should alert the user that messages are different when store and forward is available.

Status	Occurrence	Format	Min. Access Types
Optional	One	bool	Get/Put

Table 43. IM MO sub tree addition parameters (imWarnSF)

- Values: 1, the user is aware via UX on when the messages are deferred using S&F. 0, the user is not aware on when messages are differed.
- Post-reconfiguration actions: As the client remains unregistered during configuration, there are no additional actions apart from de-registering using the old configuration (section 2.2.2.4) and registering back (section 2.2.2.2) using the new parameter.
- Associated OMA-CP parameter: “imWarnSF”

Node: /<X>/imSessionStart

Leaf node that describes when the receiver client/handset implementation should return the 200 OK initiating the MSRP session associated to a 1-to-1 chat. Please note that this parameter is transparent to the user.

Status	Occurrence	Format	Min. Access Types
Optional	One	Int	Get/Put

Table 44. IM MO sub tree addition parameters (imSessionStart)

- Values: This parameter can have 3 possible values:
  - 0 (RCS-e default):
    - The 200 OK is sent when the receiver consumes the notification opening the chat window.
  - 1 (RCS default):
    - The 200 OK is sent when the receiver starts to type a message back in the chat window.
  - 2 (new option):
    - The 200 OK is sent when the receiver sends a message (i.e. the message will not generate an invite but instead will be buffered in the client until the MSRP session is established.

- Post-reconfiguration actions: As the client remains unregistered during configuration, there are no additional actions apart from de-registering using the old configuration (section 2.2.2.4) and registering back (section 2.2.2.2) using the new parameter.
- Associated OMA-CP parameter: “imSessionStart”

Node: /<X>/ftWarnSize

Leaf node that describes the file transfer size threshold (in KB) on when the user should be warned about the potential charges associated to the transfer of a large file.

Status	Occurrence	Format	Min. Access Types
Required	One	Int	Get/Put

Table 45. IM MO sub tree addition parameters (ftWarnSize)

- Values: The file size threshold (in KB) or 0 to disable the warning
- Post-reconfiguration actions: As the client remains unregistered during configuration, there are no additional actions apart from de-registering using the old configuration (section 2.2.2.4) and registering back (section 2.2.2.2) using the new parameter.
- Associated OMA-CP parameter: “ftWarnSize”

A.2.5 Capability discovery MO sub tree

RCS-e specification includes the following additions of a new configuration sub tree, the capability discovery MO sub tree. Please note this sub tree is not included in RCS Release 2 specification, so no other nodes from previous specifications need to be added:

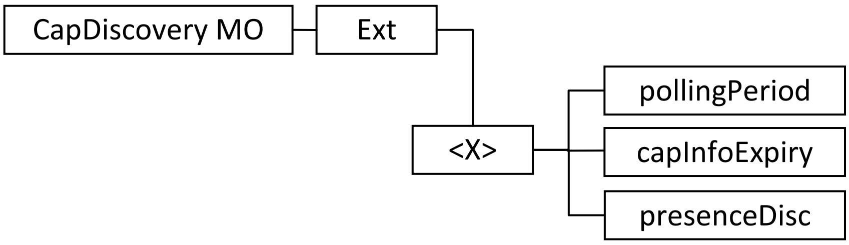


Figure 64. RCS-e additions, capability sub tree

The associated OMA-CP configuration XML structure is presented in the table below:

```
<characteristic type=”CAPDISCOVERY”>
      <parm name=”pollingPeriod” value=”X”/>
      <parm name=”capInfoExpiry” value=”X”/>
      <parm name=”presenceDisc” value=”X”/>
</characteristic>
```

Table 46. Capability sub tree associated OMA-CP configuration XML structure

Node: /<X>

Under this interior node are placed the RCS-e parameters related to capability discovery.

Status	Occurrence	Format	Min. Access Types
Required	One	node	Get

Table 47. Capability MO sub tree addition capability discovery node

- Values: N/A
- Type property of the Node is*: urn:gsma:mo:rcs:rcse:icapdis-ext*
- Associated OMA-CP characteristic type: “CAPDISCOVERY”

Node: /<X>/pollingPeriod

Leaf node that describes the timer in seconds between querying all the contacts in the address book to update the capabilities.

Status	Occurrence	Format	Min. Access Types
Required	One	Int	Get/Put

Table 48. Capability MO sub tree addition parameters (pollingPeriod)

- Values: The time in seconds. If set to 0, the periodic capability update (polling) is not performed
- Post-reconfiguration actions: As the client remains unregistered during configuration, there are no additional actions apart from de-registering using the old configuration (section 2.2.2.4) and registering back (section 2.2.2.2) using the new parameter.
- Associated OMA-CP parameter: “pollingPeriod”

Node: /<X>/capInfoExpiry

Leaf node that describes the validity of the capability information stored in the terminal in seconds.

Status	Occurrence	Format	Min. Access Types
Optional	One	Int	Get/Put

Table 49. Capability MO sub tree addition parameters (capInfoExpiry)

- Values: The time in seconds.
- Post-reconfiguration actions: As the client remains unregistered during configuration, there are no additional actions apart from de-registering using the old configuration (section 2.2.2.4) and registering back (section 2.2.2.2) using the new parameter.
- Associated OMA-CP parameter: “capInfoExpiry”

Node: /<X>/presenceDisc

Leaf node that describes whether the capability discovery using presence is supported.

Status	Occurrence	Format	Min. Access Types
Required	One	Bool	Get/Put

Table 50. Capability MO sub tree addition parameters (presenceDisc)

- Values: If set to 1, it is supported. If set to 0, it is not supported.
- Post-reconfiguration actions: The client should be reset and should perform the complete first-time registration procedure following a reconfiguration (e.g. OMA-DM/OMA-CP) as described in section 2.2.2.1.
- Associated OMA-CP parameter: “presenceDisc”

A.2.6 APN configuration MO sub tree

RCS-e specification includes the following additions of a new configuration sub tree, the roaming MO sub tree. Please note this sub tree is not included in RCS Release 2 specification, so no other nodes from previous specifications need to be added:

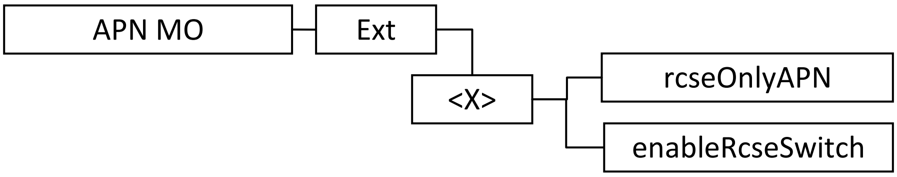


Figure 65. RCS-e additions, roaming sub tree

The associated OMA-CP configuration XML structure is presented in the table below:

```
<characteristic type=”APN”>
      <parm name=”rcseOnlyAPN” value=”X”/>
      <parm name=”enableRcseSwitch” value=”X”/>
</characteristic>
```

Table 51. APN sub tree associated OMA-CP configuration XML structure

Node: /<X>

Under this interior node are placed the RCS parameters related to roaming.

Status	Occurrence	Format	Min. Access Types
Required	One	node	Get

Table 52. APN MO sub tree addition node

- Values: N/A
- Type property of the Node is: *urn:gsma:mo:rcs:rcse:apn-ext*
- Associated OMA-CP characteristic type: “APN”

Node: /<X>/rcseOnlyAPN

Leaf node that describes the APN to be used as the RCS-e roaming APN as described in section 2.10.

Status	Occurrence	Format	Min. Access Types
Required	One	chr	Get/Put

Table 53. Roaming MO sub tree addition parameters (rcseOnlyAPN)

- Values: The APN name or the identifier used on the phone for the RCS-e only APN
- Post-reconfiguration actions: As the client remains unregistered during configuration, there are no additional actions apart from de-registering using the old configuration (section 2.2.2.4) and registering back (section 2.2.2.2) using the new parameter.
- Associated OMA-CP parameter: “rcseOnlyAPN”

Node: /<X>/enableRcseSwitch

Leaf node that describes whether to show the RCS-e enabled/disabled switch permanently as described in section 2.10.

Status	Occurrence	Format	Min. Access Types
Required	One	chr	Get/Put

Table 54. Roaming MO sub tree addition parameters (enableRcseSwitch)

- Values: If set 1, the setting is shown permanently. Otherwise it may (MNO decision) be only shown during roaming.
- Post-reconfiguration actions: As the client remains unregistered during configuration, there are no additional actions apart from de-registering using the old configuration (section 2.2.2.4) and registering back (section 2.2.2.2) using the new parameter.
- Associated OMA-CP parameter: “enableRcseSwitch”

A.2.7 Other RCS-e configuration sub tree

RCS-e specification includes the following additions of a new configuration sub tree, containing the remaining RCS-e configuration parameters. Please note this sub tree is not included in RCS Release 2 specification, so no other nodes from previous specifications need to be added:

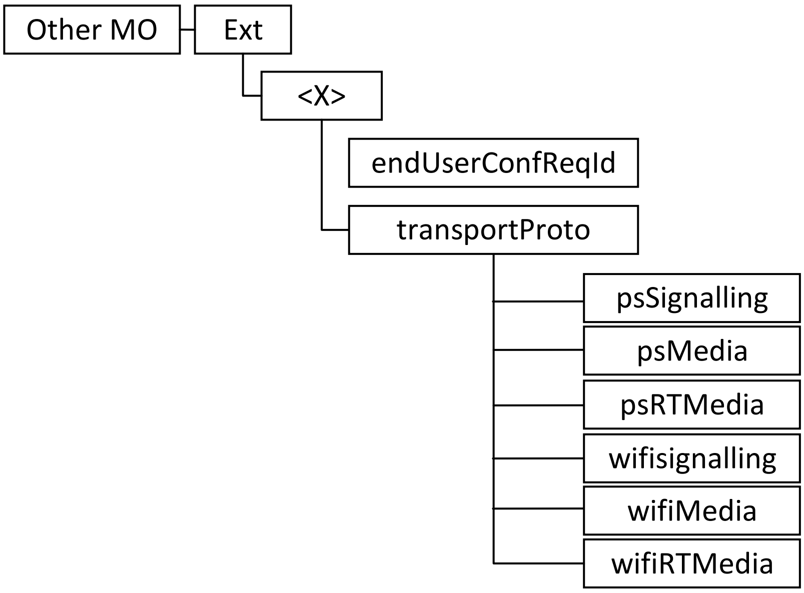


Figure 66. RCS-e additions, other sub tree

The associated OMA-CP configuration XML structure is presented in the table below:

```
<characteristic type=”OTHER”>
      <parm name=”endUserConfReqId” value=”X”/>
      <characteristic type=” transportProto”>
            <parm name=”psSignalling” value=”X”/>
            <parm name=”psMedia” value=”X”/>
            <parm name=”psRTMedia” value=”X”/>
            <parm name=”wifiSignalling” value=”X”/>
            <parm name=”wifiMedia” value=”X”/>
            <parm name=”wifiRTMedia” value=”X”/>
      </characteristic>
</characteristic>
```

Table 55. Other sub tree associated OMA-CP configuration XML structure

Node: /<X>

Under this interior node are placed the RCS-e parameters which does not fit in other categories.

Status	Occurrence	Format	Min. Access Types
Required	One	node	Get

Table 56. Other MO sub tree addition node

- Values: N/A
- Type property of the Node is: *urn:gsma:mo:rcs:rcse*:*other-ext*
- Associated OMA-CP characteristic type: “OTHER”

Node: /<X>/ endUserConfReqId

Leaf node that describes the identity (p-asserted-id) used for sending the end user confirmation request.

Status	Occurrence	Format	Min. Access Types
Required	One	chr	Get/Put

Table 57. Other MO sub tree addition parameters (endUserConfReqId)

- Values: The identity (p-asserted-id) used for sending the end user confirmation request
- Post-reconfiguration actions: As the client remains unregistered during configuration, there are no additional actions apart from de-registering using the old configuration (section 2.2.2.4) and registering back (section 2.2.2.2) using the new parameter.
- Associated OMA-CP parameter: “endUserConfReqId”

Node: /<X>/transportProto

Under this interior node are placed the RCS-e parameters related to the transport protocols which are employed to carry the signalling and media data required for RCS-e.

Status	Occurrence	Format	Min. Access Types
Required	One	node	Get

Table 58. Transport Protocol sub tree node

- Values: N/A
- Type property of the Node is: *urn:gsma:mo:rcs:rcse*:*other-ext:transportProto*
- Associated OMA-CP characteristic type: “transportProto”

Node: /<X>/ transportProto/psSignalling

Leaf node that describes the transport protocol used to carry signalling when connecting over PS.

Status	Occurrence	Format	Min. Access Types
Required	One	chr	Get/Put

Table 59. Other MO sub tree addition parameters (psSignalling)

- Values: The possible values are:
  - SIPoUDP
  - SIPoTCP
  - SIPoTLS

- Post-reconfiguration actions: As the client remains unregistered during configuration, there are no additional actions apart from de-registering using the old configuration (section 2.2.2.4) and registering back (section 2.2.2.2) using the new parameter.
- Associated OMA-CP parameter: “psSignalling”

Node: /<X>/ transportProto/psMedia

Leaf node that describes the transport protocol used to carry media (e.g. IM, file transfer and image share services) when connecting over PS.

Status	Occurrence	Format	Min. Access Types
Required	One	chr	Get/Put

Table 60. Other MO sub tree addition parameters (psMedia)

- Values: The possible values are:
  - MSRP
  - MSRPoTLS

- Post-reconfiguration actions: As the client remains unregistered during configuration, there are no additional actions apart from de-registering using the old configuration (section 2.2.2.4) and registering back (section 2.2.2.2) using the new parameter.
- Associated OMA-CP parameter: “psMedia”

Node: /<X>/ transportProto/psRTMedia

Leaf node that describes the transport protocol used to carry real time media (e.g. video share) when connecting over PS.

Status	Occurrence	Format	Min. Access Types
Required	One	chr	Get/Put

Table 61. Other MO sub tree addition parameters (psRTMedia)

- Values: The possible values are:
  - RTP
  - SRTP

- Post-reconfiguration actions: As the client remains unregistered during configuration, there are no additional actions apart from de-registering using the old configuration (section 2.2.2.4) and registering back (section 2.2.2.2) using the new parameter.
- Associated OMA-CP parameter: “psRTMedia”

Node: /<X>/ transportProto/wifiSignalling

Leaf node that describes the transport protocol used to carry signalling when connecting over WiFi.

Status	Occurrence	Format	Min. Access Types
Required	One	chr	Get/Put

Table 62. Other MO sub tree addition parameters (wifiSignalling)

- Values: The possible values are:
  - SIPoUDP
  - SIPoTCP
  - SIPoTLS

- Post-reconfiguration actions: As the client remains unregistered during configuration, there are no additional actions apart from de-registering using the old configuration (section 2.2.2.4) and registering back (section 2.2.2.2) using the new parameter.
- Associated OMA-CP parameter: “wifiSignalling”

Node: /<X>/ transportProto/wifiMedia

Leaf node that describes the transport protocol used to carry media (e.g. IM, file transfer and image share services) when connecting over WiFi.

Status	Occurrence	Format	Min. Access Types
Required	One	chr	Get/Put

Table 63. Other MO sub tree addition parameters (wifiMedia)

- Values: The possible values are:
  - MSRP
  - MSRPoTLS

- Post-reconfiguration actions: As the client remains unregistered during configuration, there are no additional actions apart from de-registering using the old configuration (section 2.2.2.4) and registering back (section 2.2.2.2) using the new parameter.
- Associated OMA-CP parameter: “wifiMedia”

Node: /<X>/ transportProto/wifiRTMedia

Leaf node that describes the transport protocol used to carry real time media (e.g. video share) when connecting over WiFi.

Status	Occurrence	Format	Min. Access Types
Required	One	chr	Get/Put

Table 64. Other MO sub tree addition parameters (wifiRTMedia)

- Values: The possible values are:
  - RTP
  - SRTP

- Post-reconfiguration actions: As the client remains unregistered during configuration, there are no additional actions apart from de-registering using the old configuration (section 2.2.2.4) and registering back (section 2.2.2.2) using the new parameter.
- Associated OMA-CP parameter: “wifiRTMedia”

A.3 OMA-CP specific configuration and behaviour

A.3.1 OMA-CP configuration XML structure

In addition to the parameters and characteristics type correspondences presented in the previous section, it is necessary to define the following mandatory configuration XML elements[54]:

```
<?xml version="1.0"?>
      <wap-provisioningdoc version="1.1">
            <characteristic type="APPLICATION">
                  <parm name=”AppID” value=”ap2001”/>
                  <parm name=”Name” value=”IMS Settings”/>
                  <parm name=”AppRef” value=”IMS-Settings”/>
                        …  -- see section A.2.1
            </characteristic>
            <characteristic type="APPLICATION">
                  <parm name=”AppID” value=”ap2002”/>
                  <parm name=”Name” value=”RCS-e settings”/>
                  <parm name=”AppRef” value=”RCSe-Settings”/>
                  <characteristic type=”IMS”>
                        <parm name=”To-AppRef” value=”IMS-Settings”/>
                  </characteristic>
                  <characteristic type=”PRESENCE”>
                        …       -- See section A.2.2
                  </characteristic>
                  <characteristic type=”XDMS”>
                        …       -- See section A.2.3
                  </characteristic>
                  <characteristic type=”IM”>
                        …       -- See section A.2.4
                  </characteristic>
                  <characteristic type=”CAPDISCOVERY”>
                        …       -- See section A.2.5
                  </characteristic>
                  <characteristic type=”APN”>
                        …       -- See section A.2.6
                  </characteristic>
                  <characteristic type=”OTHER”>
                        …       -- See section A.2.7
                  </characteristic>
            </characteristic>
      </wap-provisioningdoc>
```

Table 65. Complete RCS-e OMA-CP configuration XML structure

[54] Please note the application ids used in the example are just provided for reference as they have not been reserved.

A.4 Autoconfiguration XML sample

```
<?xml version="1.0"?>
   <wap-provisioningdoc version="1.1">
        <characteristic type="VERS">
               <parm name=”version” value=”1”/>
               <parm name=”validity” value=”1728000”/>
        </characteristic>
        <characteristic type="MSG">                              -- This section is OPTIONAL
               <param name=”title” value=”Example”/>
               <param name=”message” value=”Hello world”/>
               <param name=”Accept_btn” value=”X”/>
               <param name=”Reject_btn” value=”X”/>
        </characteristic>                                        -- This section is OPTIONAL
        <characteristic type="APPLICATION">
               <parm name=”AppID” value=”ap2001”/>
               <parm name=”Name” value=”IMS Settings”/>
               <parm name=”AppRef” value=”IMS-Settings”/>
               <characteristic type=”ConRefs”>
                      <parm name=”ConRef” value=”X”/>
               </characteristic>
               <parm name=”PDP_ContextOperPref” value=”X”/>
               <parm name=”Timer_T1” value=”X”/>
               <parm name=”Timer_T2” value=”X”/>
               <parm name=”Timer_T4” value=”X”/>
               <parm name=”Private_User_Identity” value=”X”/>
               <characteristic type=”Public_User_Identity_List”>
                      <parm name=”Public_User_Identity” value=”X”/>
               </characteristic>
               <parm name=”Home_network_domain_name” value=”X”/>
               <characteristic type=”Ext”>
                      <parm name=”NatUrlFmt” value=”1”/>
                      <parm name=”IntUrlFmt” value=”1”/>
                      <parm name=”Q-Value” value=”0.5”/>
                      <characteristic type=”SecondaryDevicePar”>
                             <parm name=”VoiceCall” value=”0”/>
                             <parm name=”Chat” value=”0”/>
                             <parm name=”SendSms” value=”0”/>
                             <parm name=”FileTranfer” value=”0”/>
                             <parm name=”VideoShare” value=”0”/>
                             <parm name=”ImageShare” value=”0”/>
                      </characteristic>
                      <parm name=”MaxSizeImageShare” value=”0”/>
                      <parm name=”MaxTimeVideoShare” value=”0”/>
               </characteristic>
               <characteristic type=”ICSI_List”>
                     <parm name=”ICSI” value=”0”/>
                      <parm name=”ICSI_Resource_Allocation_Mode” value=”X”/>
               </characteristic>
               <characteristic type=”LBO_P-CSCF_Address”>
                      <parm name=”Address” value=”X”/>
                      <parm name=”AddressType” value=”X”/>
               </characteristic>
               <parm name=”Voice_Domain_Preference_E_UTRAN” value=”X”/>
               <parm name=”SMS_Over_IP_Networks_Indication” value=”X”/>
               <parm name=”Keep_Alive_Enabled” value=”X”/>
               <parm name=”Voice_Domain_Preference_UTRAN” value=”X”/>
               <parm name=”Mobility_Management_IMS_Voice_Termination” value=”X”/>
               <parm name=”RegRetryBaseTime” value=”X”/>
               <parm name=”RegRetryMaxTime” value=”X”/>
               <characteristic type=”PhoneContext_List”>
                      <parm name=”PhoneContext” value=”X”/>
                      <parm name=”Public_User_Identity” value=”X”/>
               </characteristic>
               <characteristic type=”APPAUTH”>
                      <parm name=”AuthType” value=”X”/>
                      <parm name=”Realm” value=”X”/>
                      <parm name=”UserName” value=”X”/>
                      <parm name=”UserPwd” value=”X”/>
               </characteristic>
        </characteristic>
```

Table 66. Complete RCS-e autoconfiguration XML structure (1/3)

```
        -- Follows from previous table –

        <characteristic type="APPLICATION">
                <parm name=”AppID” value=”ap2002”/>
                <parm name=”Name” value=”RCS-e settings”/>
                <parm name=”AppRef” value=”RCSe-Settings”/>
                <characteristic type=”IMS”>
                        <parm name=”To-AppRef” value=”IMS-Settings”/>
                </characteristic>
                <characteristic type=”PRESENCE”>
                        <parm name=”usePresence” value=”X”/>
                        <parm name=”presencePrfl” value=”X”/>
                        <parm name=”AvailabilityAuth” value=”X”/>
                        <characteristic type=”FAVLINK”>
                        </characteristic>
                        <parm name=”IconMaxSize” value=”X”/>
                        <parm name=”NoteMaxSize” value=”X”/>
                        <characteristic type=”SERVCAPWATCH”>
                                <parm name=”FetchAuth” value=”X”/>
                                <parm name=”ContactCapPresAut” value=”X”/>
                        </characteristic>
                        <characteristic type=”ServCapPresentity”>
                                <parm name=”WATCHERFETCHAUTH” value=”X”/>
                        </characteristic>
                        <parm name=”client-obj-datalimit” value=”X”/>
                        <parm name=”content-serveruri” value=”X”/>
                        <parm name=”source-throttlepublish” value=”X”/>
                        <parm name=”max-number-ofsubscriptions-inpresence-list
” value=”X”/>
                        <parm name=”service-uritemplate” value=”X”/>
                </characteristic>
                <characteristic type=”XDMS”>
                        <parm name=”RevokeTimer” value=”X”/>
                        <parm name=”XCAPRootURI” value=”X”/>
                        <parm name=”XCAPAuthenticationUserName” value=”X”/>
                        <parm name=”XCAPAuthenticationSecret” value=”X”/>
                        <parm name=”XCAPAuthenticationType” value=”X”/>
                </characteristic>
                <characteristic type=”IM”>
                        <parm name=”imCapAlwaysON” value=”X”/>
                        <parm name=”imWarnSF” value=”X”/>
                        <parm name=”ftWarnSize” value=”X”/>
                        <parm name=”ChatAuth” value=”X”/>
                        <parm name=”SmsFallBackAuth” value=”X”/>
                        <parm name=”AutAccept” value=”X”/>
                        <parm name=”MaxSize1to1” value=”X”/>
                        <parm name=”MaxSize1toM” value=”X”/>
                        <parm name=”TimerIdle” value=”X”/>
                        <parm name=”MaxSizeFileTr” value=”X”/>
                        <parm name=”pres-srv-cap” value=”X”/>
                        <parm name=”deferred-msg-func-uri” value=”X”/>
                        <parm name=”max_adhoc_group_size” value=”X”/>
                        <parm name=”conf-fcty-uri” value=”X”/>
                        <parm name=”exploder-uri” value=”X”/>
                </characteristic>
                <characteristic type=”CAPDISCOVERY”>
                        <parm name=”pollingPeriod” value=”X”/>
                        <parm name=”capInfoExpiry” value=”X”/>
                        <parm name=”presenceDisc” value=”X”/>
                </characteristic>
                <characteristic type=”APN”>
                        <parm name=”rcseOnlyAPN” value=”X”/>
                        <parm name=”enableRcseSwitch” value=”X”/>
                </characteristic>

        -- Continues in the next table --
```

Table 67. Complete RCS-e autoconfiguration XML structure (2/3)

```
      -- Follows from previous table –

              <characteristic type=”OTHER”>
                      <parm name=”endUserConfReqId” value=”X”/>
                      <parm name=”endUserConfReqId” value=”X”/>
                      <characteristic type=” transportProto”>
                              <parm name=”psSignalling” value=”X”/>
                              <parm name=”psMedia” value=”X”/>
                              <parm name=”psRTMedia” value=”X”/>
                              <parm name=”wifiSignalling” value=”X”/>
                              <parm name=”wifiMedia” value=”X”/>
                              <parm name=”wifiRTMedia” value=”X”/>
                      </characteristic>
              </characteristic>
      </characteristic>
  </wap-provisioningdoc>
```

Table 68. Complete RCS-e autoconfiguration XML structure (3/3)

B. ANNEX B: IM and store and forward diagrams

B.1 IM without store and forward

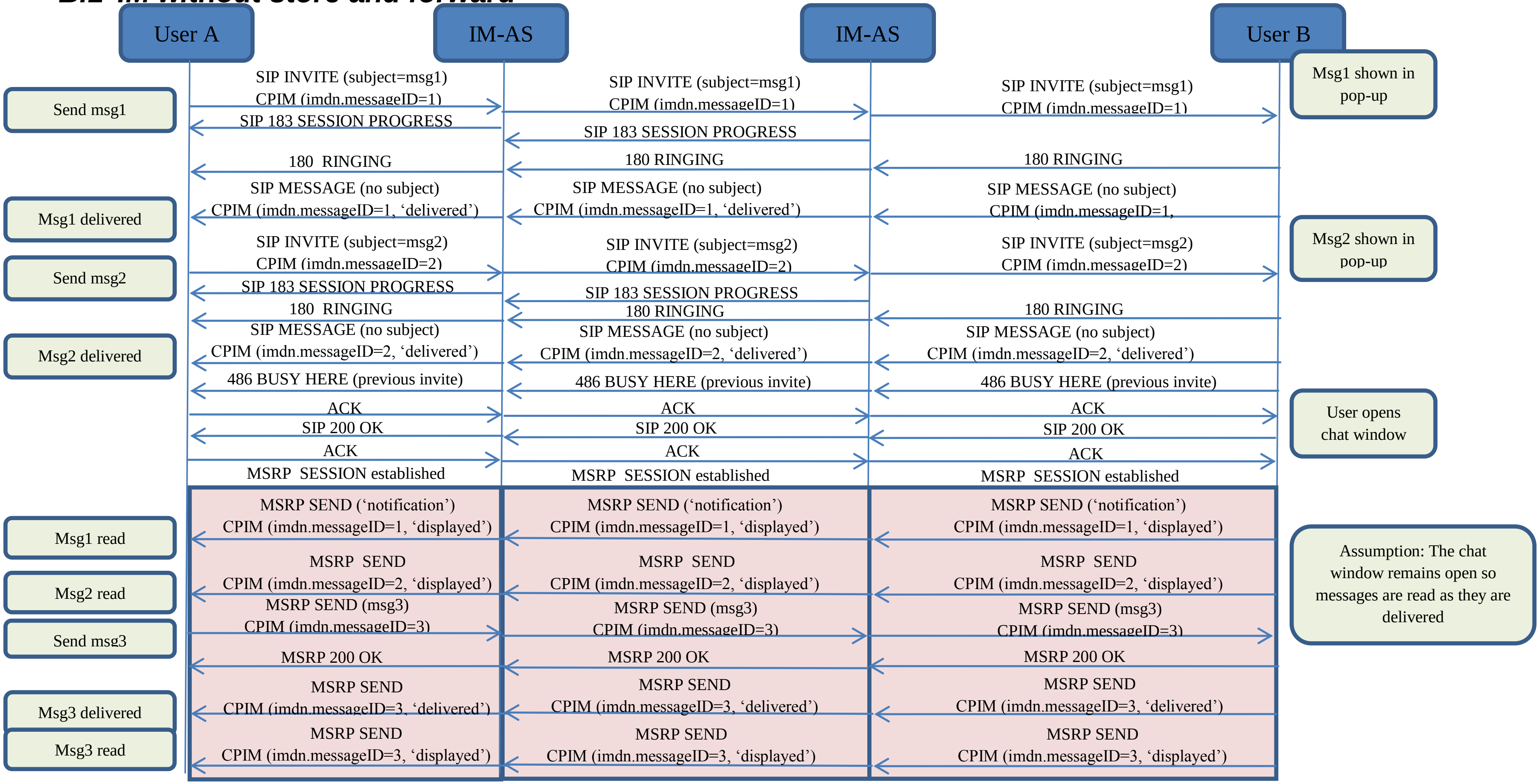

User A
IM-AS
IM-AS
User B
Send msg1
SIP INVITE (subject=msg1)
CPIM (imdn.messageID=1)
SIP INVITE (subject=msg1)
CPIM (imdn.messageID=1)
SIP INVITE (subject=msg1)
CPIM (imdn.messageID=1)
Msg1 shown in pop-up
SIP 183 SESSION PROGRESS
SIP 183 SESSION PROGRESS
180 RINGING
180 RINGING
180 RINGING
Msg1 delivered
SIP MESSAGE (no subject)
CPIM (imdn.messageID=1, 'delivered')
SIP MESSAGE (no subject)
CPIM (imdn.messageID=1, 'delivered')
SIP MESSAGE (no subject)
CPIM (imdn.messageID=1,
Send msg2
SIP INVITE (subject=msg2)
CPIM (imdn.messageID=2)
SIP INVITE (subject=msg2)
CPIM (imdn.messageID=2)
SIP INVITE (subject=msg2)
CPIM (imdn.messageID=2)
Msg2 shown in pop-up
SIP 183 SESSION PROGRESS
SIP 183 SESSION PROGRESS
180 RINGING
180 RINGING
180 RINGING
Msg2 delivered
SIP MESSAGE (no subject)
CPIM (imdn.messageID=2, 'delivered')
SIP MESSAGE (no subject)
CPIM (imdn.messageID=2, 'delivered')
SIP MESSAGE (no subject)
CPIM (imdn.messageID=2, 'delivered')
486 BUSY HERE (previous invite)
486 BUSY HERE (previous invite)
486 BUSY HERE (previous invite)
ACK
ACK
ACK
User opens chat window
SIP 200 OK
SIP 200 OK
SIP 200 OK
ACK
ACK
ACK
MSRP SESSION established
MSRP SESSION established
MSRP SESSION established
Msg1 read
MSRP SEND ('notification')
CPIM (imdn.messageID=1, 'displayed')
MSRP SEND ('notification')
CPIM (imdn.messageID=1, 'displayed')
MSRP SEND ('notification')
CPIM (imdn.messageID=1, 'displayed')
Msg2 read
MSRP SEND
CPIM (imdn.messageID=2, 'displayed')
MSRP SEND
CPIM (imdn.messageID=2, 'displayed')
MSRP SEND
CPIM (imdn.messageID=2, 'displayed')
Assumption: The chat window remains open so messages are read as they are delivered
Send msg3
MSRP SEND (msg3)
CPIM (imdn.messageID=3)
MSRP SEND (msg3)
CPIM (imdn.messageID=3)
MSRP SEND (msg3)
CPIM (imdn.messageID=3)
MSRP 200 OK
MSRP 200 OK
MSRP 200 OK
Msg3 delivered
MSRP SEND
CPIM (imdn.messageID=3, 'delivered')
MSRP SEND
CPIM (imdn.messageID=3, 'delivered')
MSRP SEND
CPIM (imdn.messageID=3, 'delivered')
Msg3 read
MSRP SEND
CPIM (imdn.messageID=3, 'displayed')
MSRP SEND
CPIM (imdn.messageID=3, 'displayed')
MSRP SEND
CPIM (imdn.messageID=3, 'displayed')

Figure 67. IM flow without store and forward *

***:** Check NOTE 1 in section B.12

B.2 Store and forward: Receiver offline

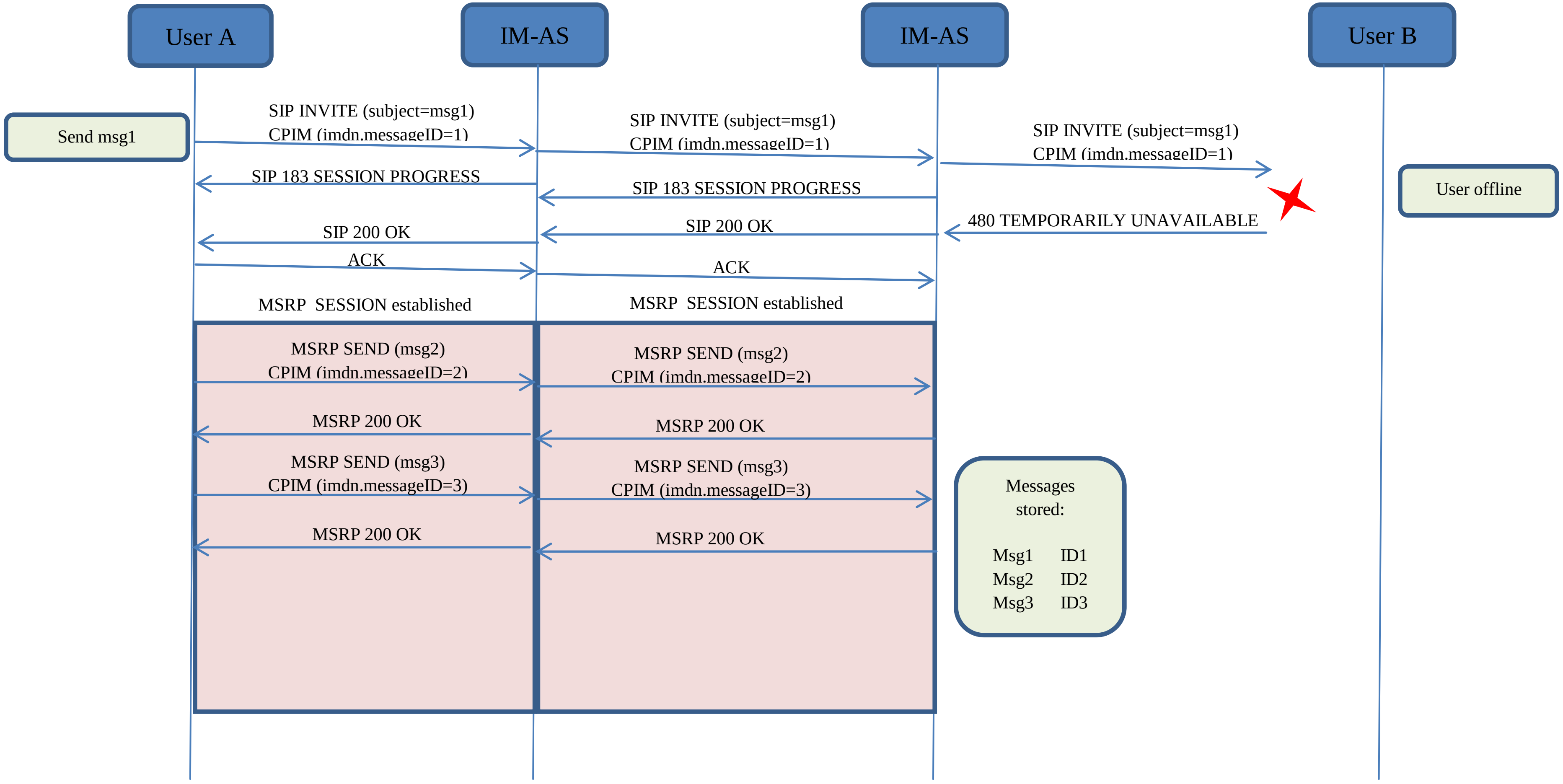


Figure 68. Store and forward: Receiver offline*

***:** Check NOTE 1 and 6 and in section B.12

B.3 Store and forward: Message deferred delivery with sender still on an active IM session

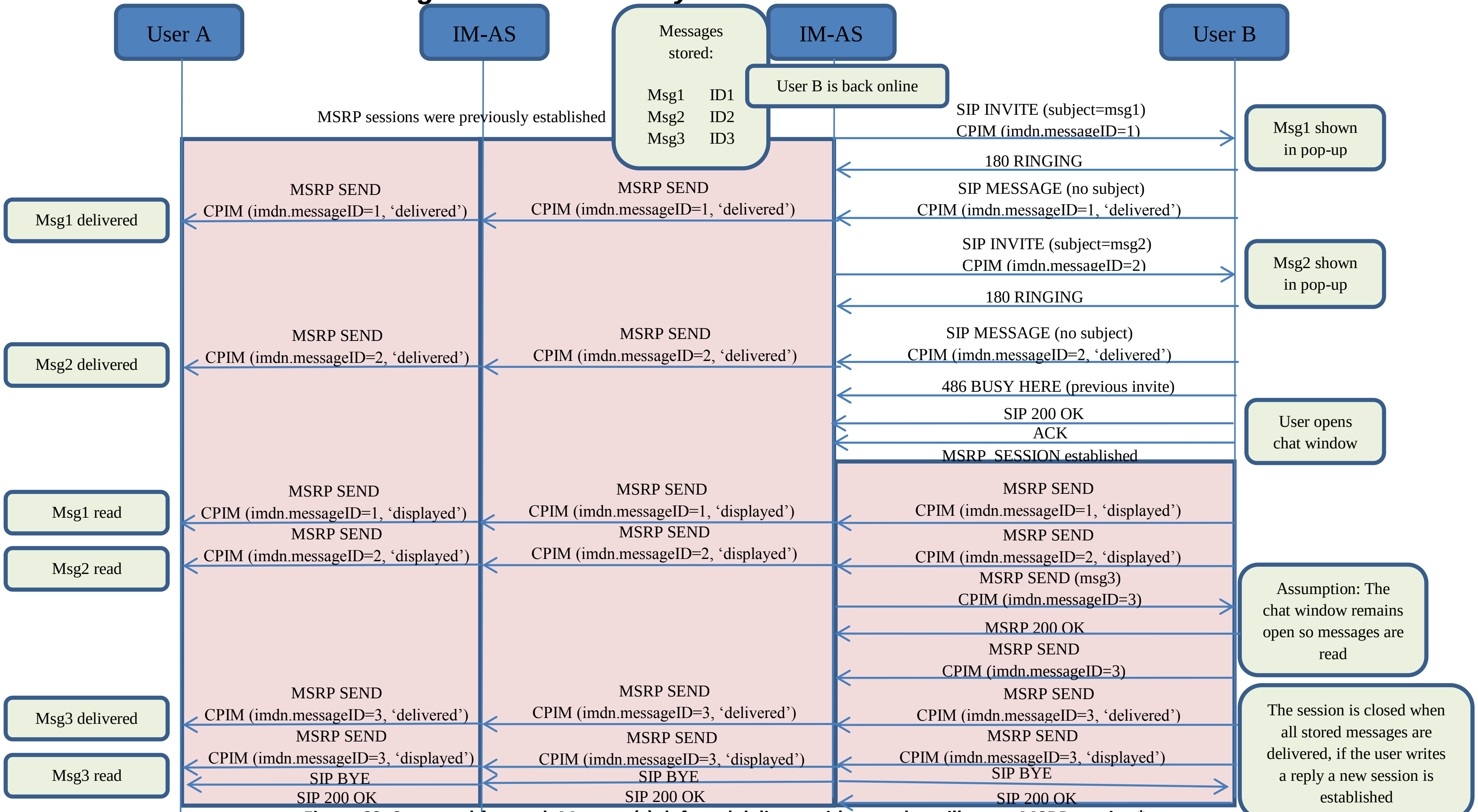

User A
IM-AS
Messages stored:
Msg1 ID1
Msg2 ID2
Msg3 ID3
IM-AS
User B
User B is back online
MSRP sessions were previously established
SIP INVITE (subject=msg1)
CPIM (imdn.messageID=1)
Msg1 shown in pop-up
180 RINGING
SIP MESSAGE (no subject)
CPIM (imdn.messageID=1, 'delivered')
MSRP SEND
CPIM (imdn.messageID=1, 'delivered')
MSRP SEND
CPIM (imdn.messageID=1, 'delivered')
Msg1 delivered
SIP INVITE (subject=msg2)
CPIM (imdn.messageID=2)
Msg2 shown in pop-up
180 RINGING
SIP MESSAGE (no subject)
CPIM (imdn.messageID=2, 'delivered')
MSRP SEND
CPIM (imdn.messageID=2, 'delivered')
MSRP SEND
CPIM (imdn.messageID=2, 'delivered')
Msg2 delivered
486 BUSY HERE (previous invite)
SIP 200 OK
ACK
User opens chat window
MSRP SESSION established
MSRP SEND
CPIM (imdn.messageID=1, 'displayed')
MSRP SEND
CPIM (imdn.messageID=1, 'displayed')
MSRP SEND
CPIM (imdn.messageID=1, 'displayed')
Msg1 read
MSRP SEND
CPIM (imdn.messageID=2, 'displayed')
MSRP SEND
CPIM (imdn.messageID=2, 'displayed')
MSRP SEND
CPIM (imdn.messageID=2, 'displayed')
Msg2 read
MSRP SEND (msg3)
CPIM (imdn.messageID=3)
Assumption: The chat window remains open so messages are read
MSRP 200 OK
MSRP SEND
CPIM (imdn.messageID=3)
MSRP SEND
CPIM (imdn.messageID=3, 'delivered')
MSRP SEND
CPIM (imdn.messageID=3, 'delivered')
MSRP SEND
CPIM (imdn.messageID=3, 'delivered')
Msg3 delivered
The session is closed when all stored messages are delivered, if the user writes a reply a new session is established
MSRP SEND
CPIM (imdn.messageID=3, 'displayed')
MSRP SEND
CPIM (imdn.messageID=3, 'displayed')
MSRP SEND
CPIM (imdn.messageID=3, 'displayed')
Msg3 read
SIP BYE
SIP 200 OK
SIP BYE
SIP 200 OK
SIP BYE
SIP 200 OK

Figure 69. Store and forward: Message(s) deferred delivery with a sender still on an MSRP session*

***:** Check NOTES 1, 2, 3, 5, 7 and 11 in section B.12

B.4 Store and forward: Message deferred delivery with sender online

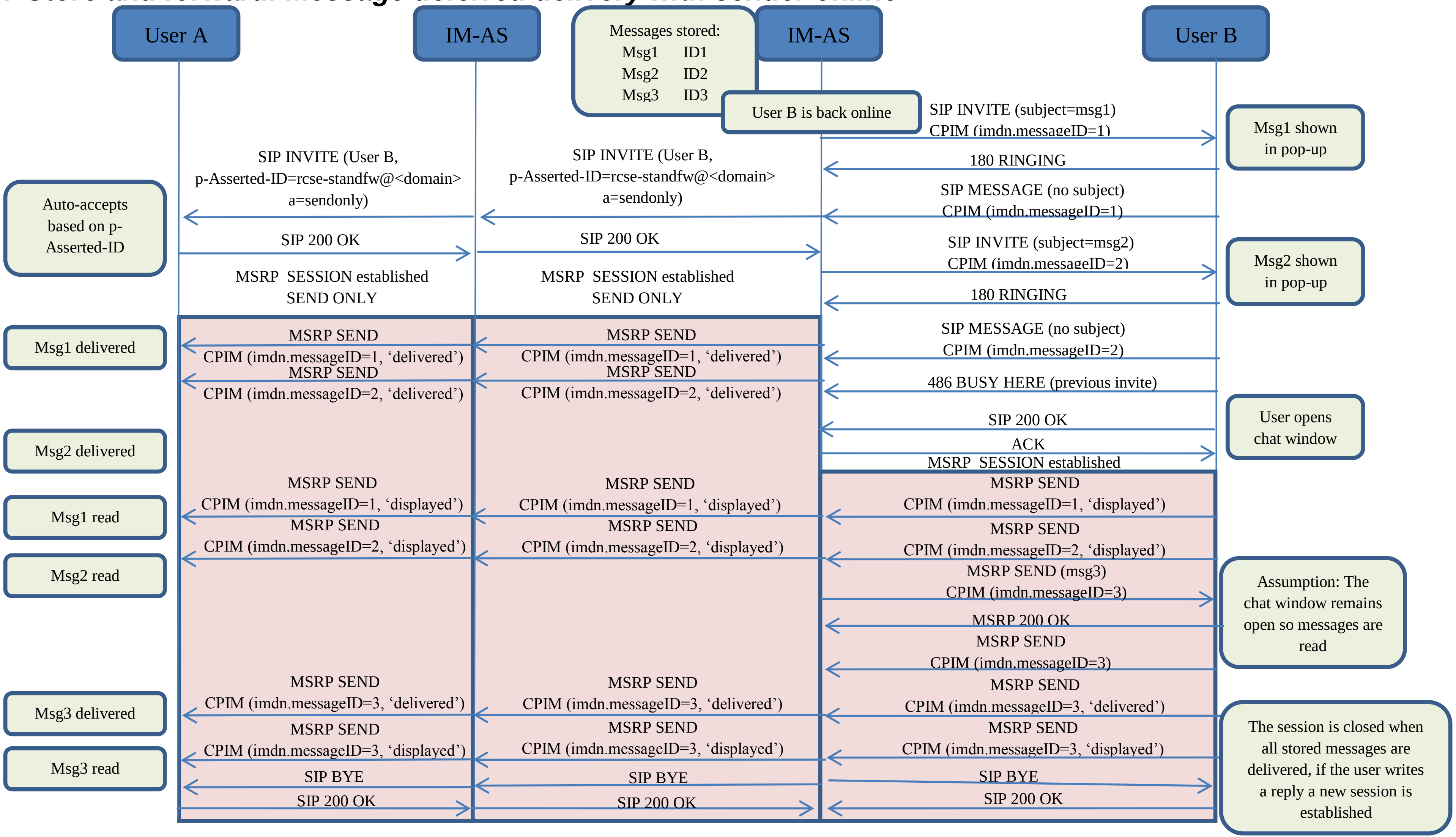

User A
IM-AS
Messages stored:
Msg1 ID1
Msg2 ID2
Msg3 ID3
IM-AS
User B
User B is back online
SIP INVITE (subject=msg1)
CPIM (imdn.messageID=1)
Msg1 shown in pop-up
180 RINGING
SIP INVITE (User B, p-Asserted-ID=rcse-standfw@<domain> a=sendonly)
SIP INVITE (User B, p-Asserted-ID=rcse-standfw@<domain> a=sendonly)
SIP MESSAGE (no subject)
CPIM (imdn.messageID=1)
Auto-accepts based on p-Asserted-ID
SIP 200 OK
SIP 200 OK
SIP INVITE (subject=msg2)
CPIM (imdn.messageID=2)
Msg2 shown in pop-up
MSRP SESSION established SEND ONLY
MSRP SESSION established SEND ONLY
180 RINGING
SIP MESSAGE (no subject)
CPIM (imdn.messageID=2)
Msg1 delivered
MSRP SEND
CPIM (imdn.messageID=1, 'delivered')
MSRP SEND
CPIM (imdn.messageID=2, 'delivered')
MSRP SEND
CPIM (imdn.messageID=1, 'delivered')
MSRP SEND
CPIM (imdn.messageID=2, 'delivered')
486 BUSY HERE (previous invite)
Msg2 delivered
SIP 200 OK
ACK
User opens chat window
MSRP SESSION established
MSRP SEND
CPIM (imdn.messageID=1, 'displayed')
MSRP SEND
CPIM (imdn.messageID=1, 'displayed')
MSRP SEND
CPIM (imdn.messageID=1, 'displayed')
Msg1 read
MSRP SEND
CPIM (imdn.messageID=2, 'displayed')
MSRP SEND
CPIM (imdn.messageID=2, 'displayed')
MSRP SEND
CPIM (imdn.messageID=2, 'displayed')
Msg2 read
MSRP SEND (msg3)
CPIM (imdn.messageID=3)
Assumption: The chat window remains open so messages are read
MSRP 200 OK
MSRP SEND
CPIM (imdn.messageID=3)
MSRP SEND
CPIM (imdn.messageID=3, 'delivered')
MSRP SEND
CPIM (imdn.messageID=3, 'delivered')
MSRP SEND
CPIM (imdn.messageID=3, 'delivered')
Msg3 delivered
MSRP SEND
CPIM (imdn.messageID=3, 'displayed')
MSRP SEND
CPIM (imdn.messageID=3, 'displayed')
MSRP SEND
CPIM (imdn.messageID=3, 'displayed')
Msg3 read
The session is closed when all stored messages are delivered, if the user writes a reply a new session is established
SIP BYE
SIP BYE
SIP BYE
SIP 200 OK
SIP 200 OK
SIP 200 OK

Figure 70. Store and forward: Message(s) deferred delivery with a sender online*

***:** Check NOTES 1, 3, 4, 5,7 and 11 in section B.12

B.5 Store and forward: Message deferred delivery with sender offline (delivery notifications)

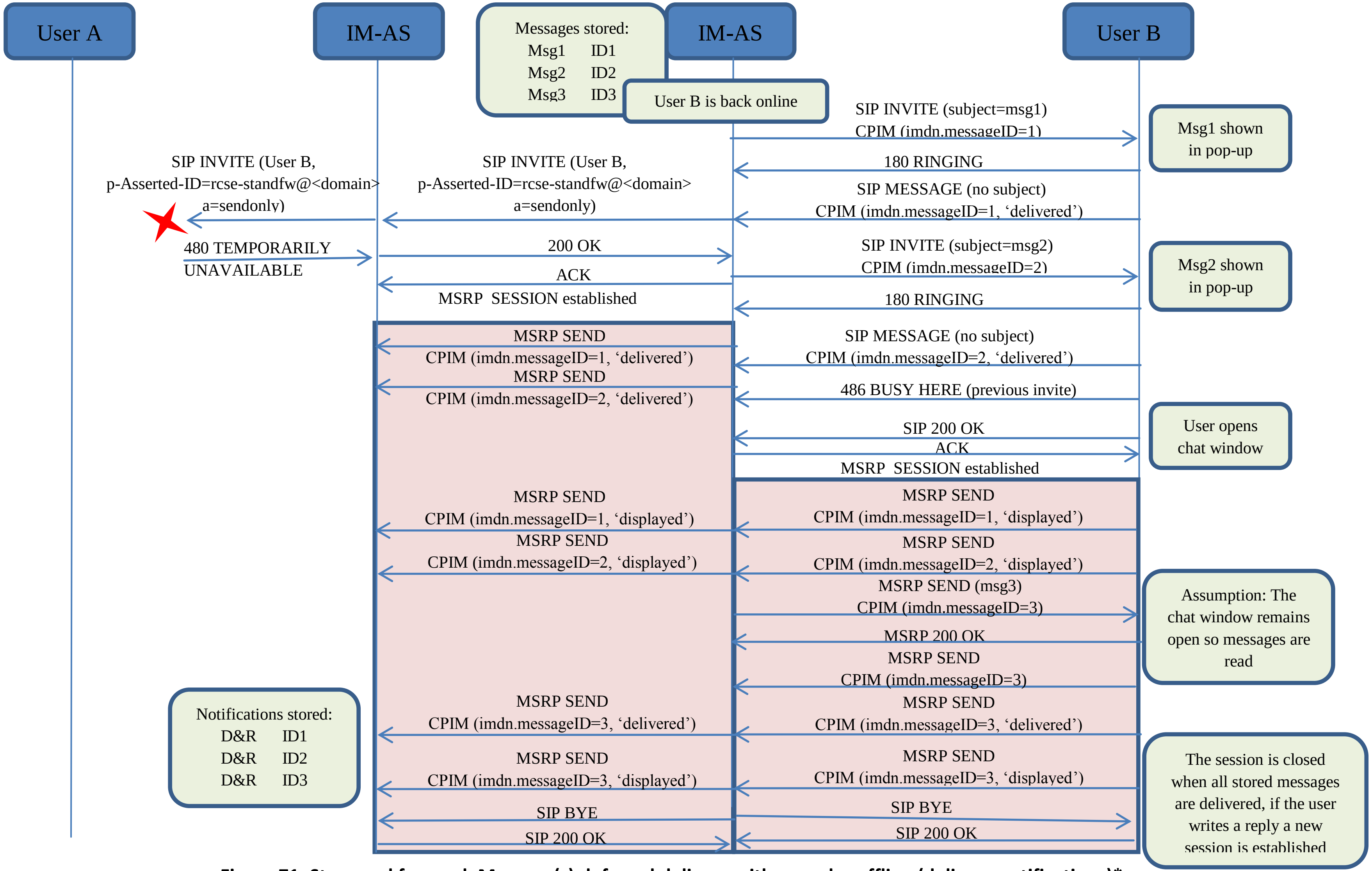

User A
IM-AS
Messages stored:
Msg1 ID1
Msg2 ID2
Msg3 ID3
IM-AS
User B
User B is back online
SIP INVITE (subject=msg1)
CPIM (imdn.messageID=1)
Msg1 shown in pop-up
180 RINGING
SIP INVITE (User B, p-Asserted-ID=rcse-standfw@<domain> a=sendonly)
SIP INVITE (User B, p-Asserted-ID=rcse-standfw@<domain> a=sendonly)
SIP MESSAGE (no subject)
CPIM (imdn.messageID=1, 'delivered')
480 TEMPORARILY UNAVAILABLE
200 OK
SIP INVITE (subject=msg2)
CPIM (imdn.messageID=2)
Msg2 shown in pop-up
ACK
MSRP SESSION established
180 RINGING
MSRP SEND
CPIM (imdn.messageID=1, 'delivered')
SIP MESSAGE (no subject)
CPIM (imdn.messageID=2, 'delivered')
MSRP SEND
CPIM (imdn.messageID=2, 'delivered')
486 BUSY HERE (previous invite)
SIP 200 OK
User opens chat window
ACK
MSRP SESSION established
MSRP SEND
CPIM (imdn.messageID=1, 'displayed')
MSRP SEND
CPIM (imdn.messageID=1, 'displayed')
MSRP SEND
CPIM (imdn.messageID=2, 'displayed')
MSRP SEND
CPIM (imdn.messageID=2, 'displayed')
MSRP SEND (msg3)
CPIM (imdn.messageID=3)
Assumption: The chat window remains open so messages are read
MSRP 200 OK
MSRP SEND
CPIM (imdn.messageID=3)
Notifications stored:
D&R ID1
D&R ID2
D&R ID3
MSRP SEND
CPIM (imdn.messageID=3, 'delivered')
MSRP SEND
CPIM (imdn.messageID=3, 'delivered')
MSRP SEND
CPIM (imdn.messageID=3, 'displayed')
MSRP SEND
CPIM (imdn.messageID=3, 'displayed')
The session is closed when all stored messages are delivered, if the user writes a reply a new session is established
SIP BYE
SIP BYE
SIP 200 OK
SIP 200 OK

Figure 71. Store and forward: Message(s) deferred delivery with a sender offline (delivery notifications)*

***:** Check NOTE 1, 5, 7 and 11 in section B.12

B.6 Store and forward: Notifications deferred delivery

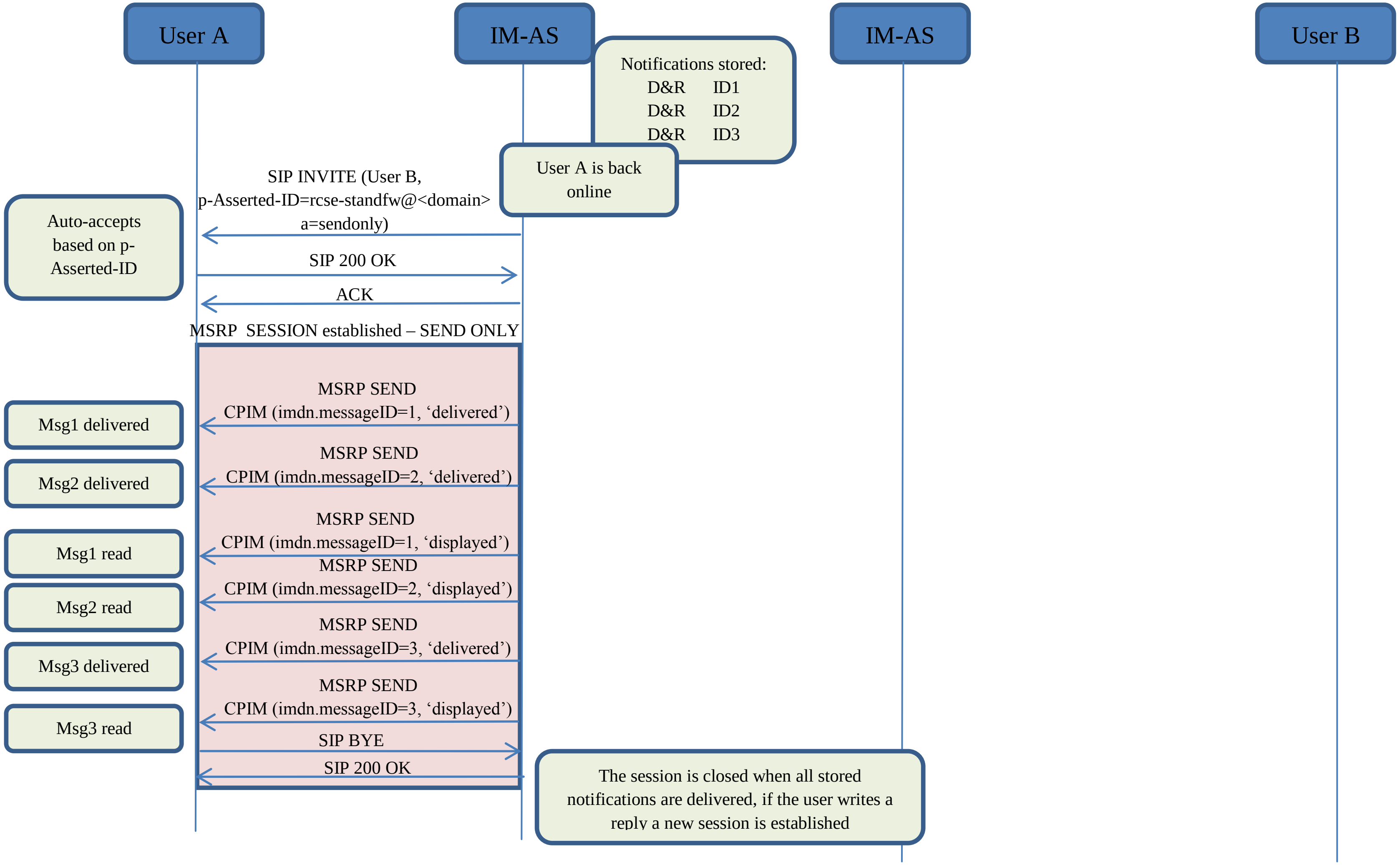

User A
IM-AS
IM-AS
User B
Notifications stored:
D&R ID1
D&R ID2
D&R ID3
User A is back online
SIP INVITE (User B, p-Asserted-ID=rcse-standfw@<domain> a=sendonly)
Auto-accepts based on p-Asserted-ID
SIP 200 OK
ACK
MSRP SESSION established – SEND ONLY
MSRP SEND CPIM (imdn.messageID=1, 'delivered')
Msg1 delivered
MSRP SEND CPIM (imdn.messageID=2, 'delivered')
Msg2 delivered
MSRP SEND CPIM (imdn.messageID=1, 'displayed')
Msg1 read
MSRP SEND CPIM (imdn.messageID=2, 'displayed')
Msg2 read
MSRP SEND CPIM (imdn.messageID=3, 'delivered')
Msg3 delivered
MSRP SEND CPIM (imdn.messageID=3, 'displayed')
Msg3 read
SIP BYE
SIP 200 OK
The session is closed when all stored notifications are delivered, if the user writes a reply a new session is established

Figure 72. Store and forward: Notification(s) deferred delivery*

***:** Check NOTES 1, 4 and 11 in section B.12

B.7 Delivery of displayed notifications in an unanswered chat (without store and forward)

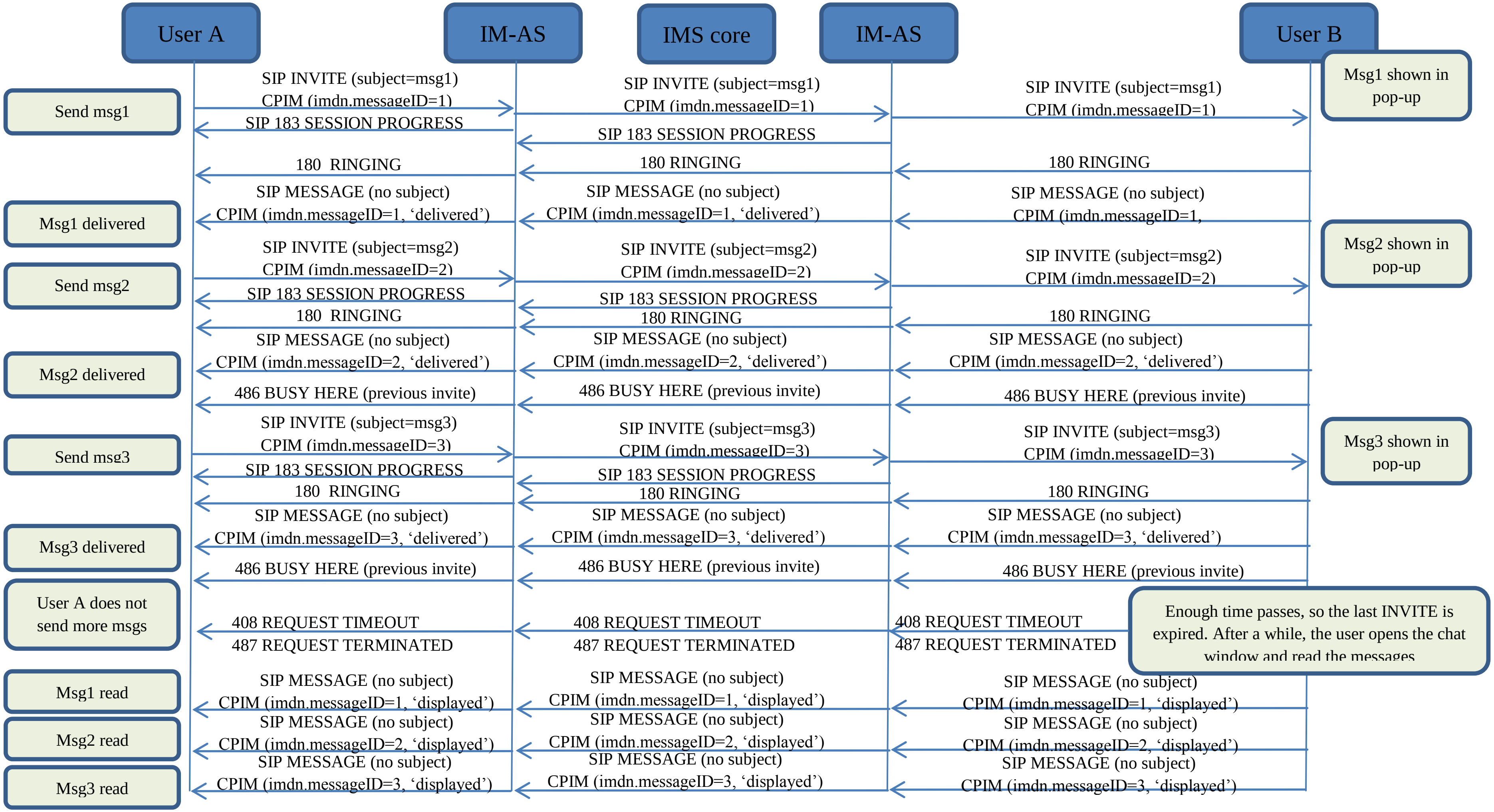
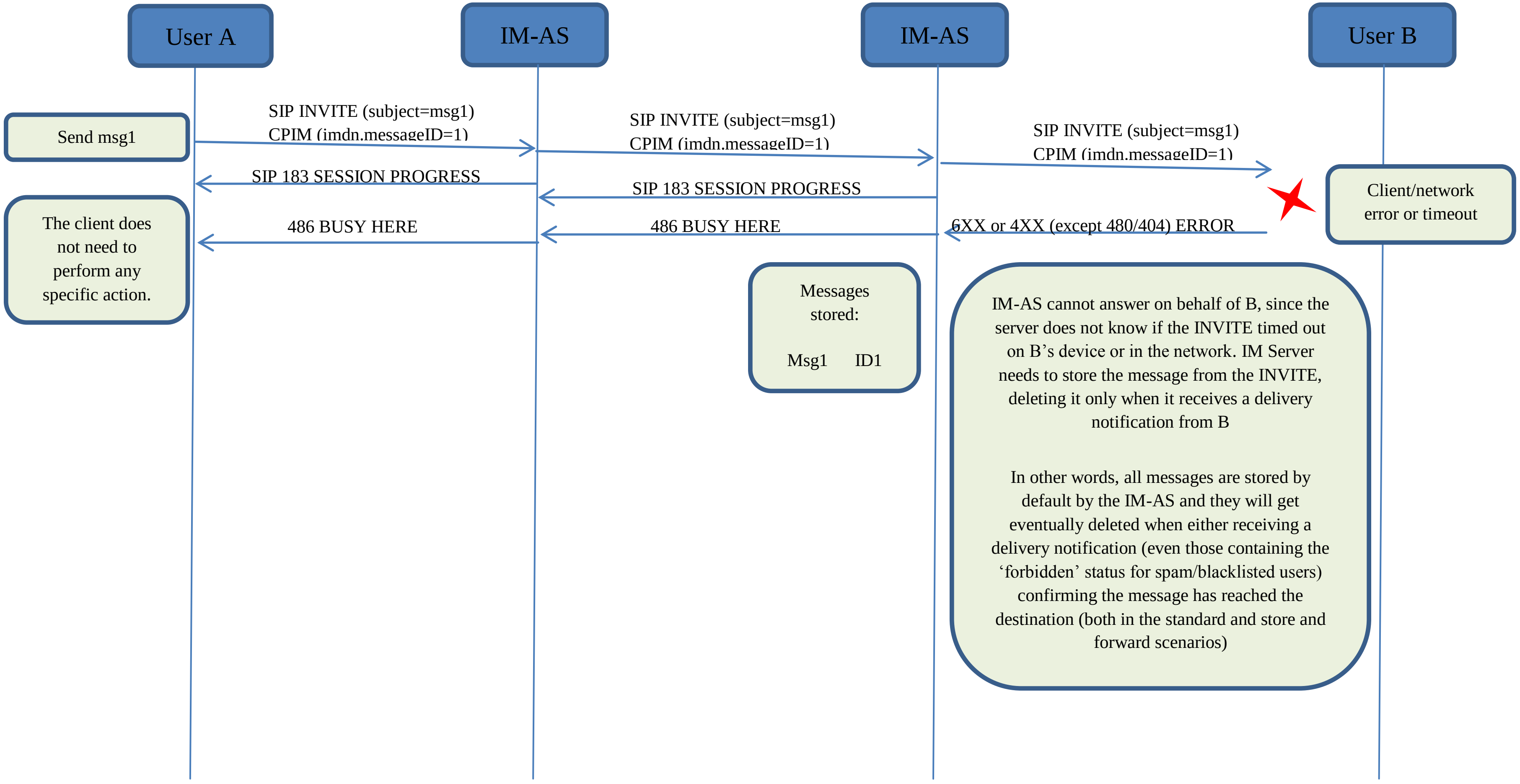


Figure 73. Delivery of displayed notifications in an unanswered chat (without store and forward)*

***: Check NOTE 1 and 10 in section B.12

B.8 Store and forward: Handling errors in the receiver's side



IM-AS cannot answer on behalf of B, since the server does not know if the INVITE timed out on B's device or in the network. IM Server needs to store the message from the INVITE, deleting it only when it receives a delivery notification from B

In other words, all messages are stored by default by the IM-AS and they will get eventually deleted when either receiving a delivery notification (even those containing the 'forbidden' status for spam/blacklisted users) confirming the message has reached the destination (both in the standard and store and forward scenarios)

Figure 74. Store and forward: Handling errors in the receiver's side

B.9 Race conditions: Simultaneous INVITEs

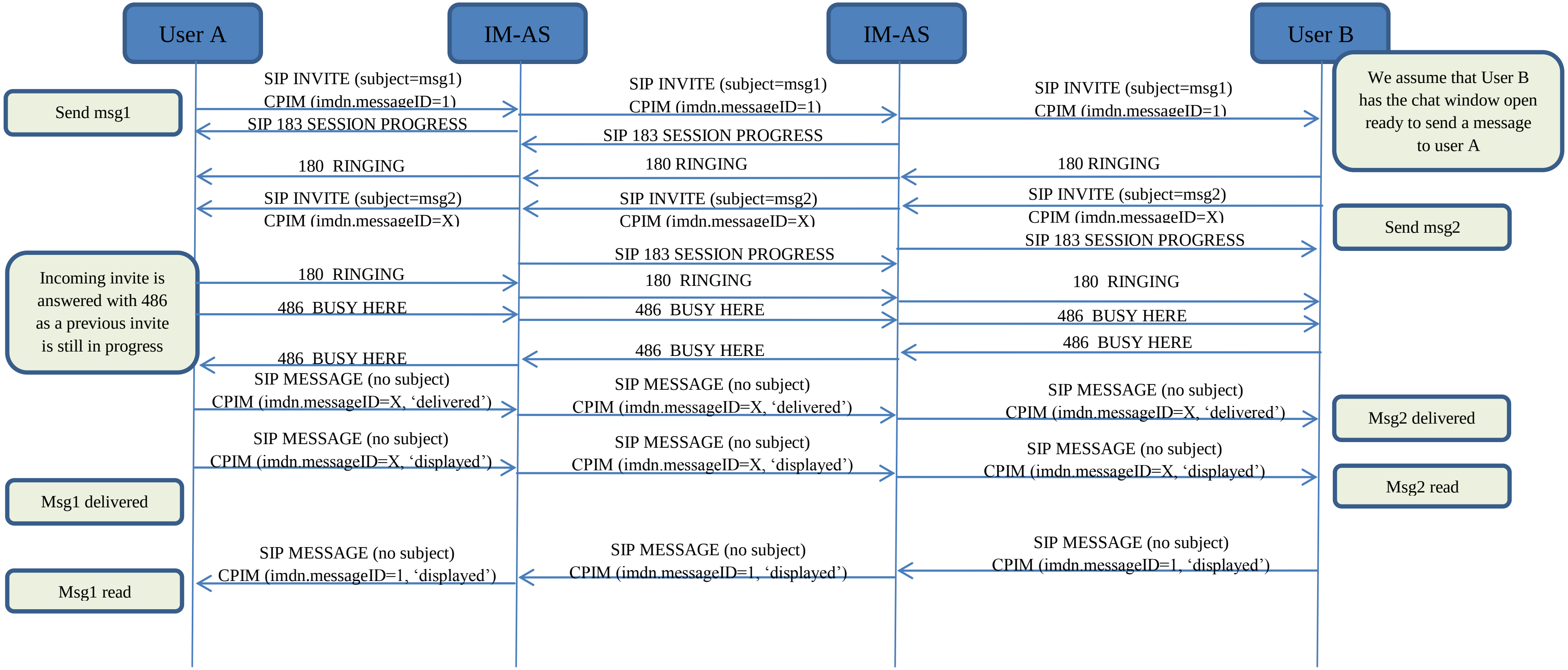


Figure 75. Store and forward race conditions: Simultaneous INVITEs*

*: Check NOTE 1 in section B.12

B.10 Race conditions: New INVITE after a session is accepted

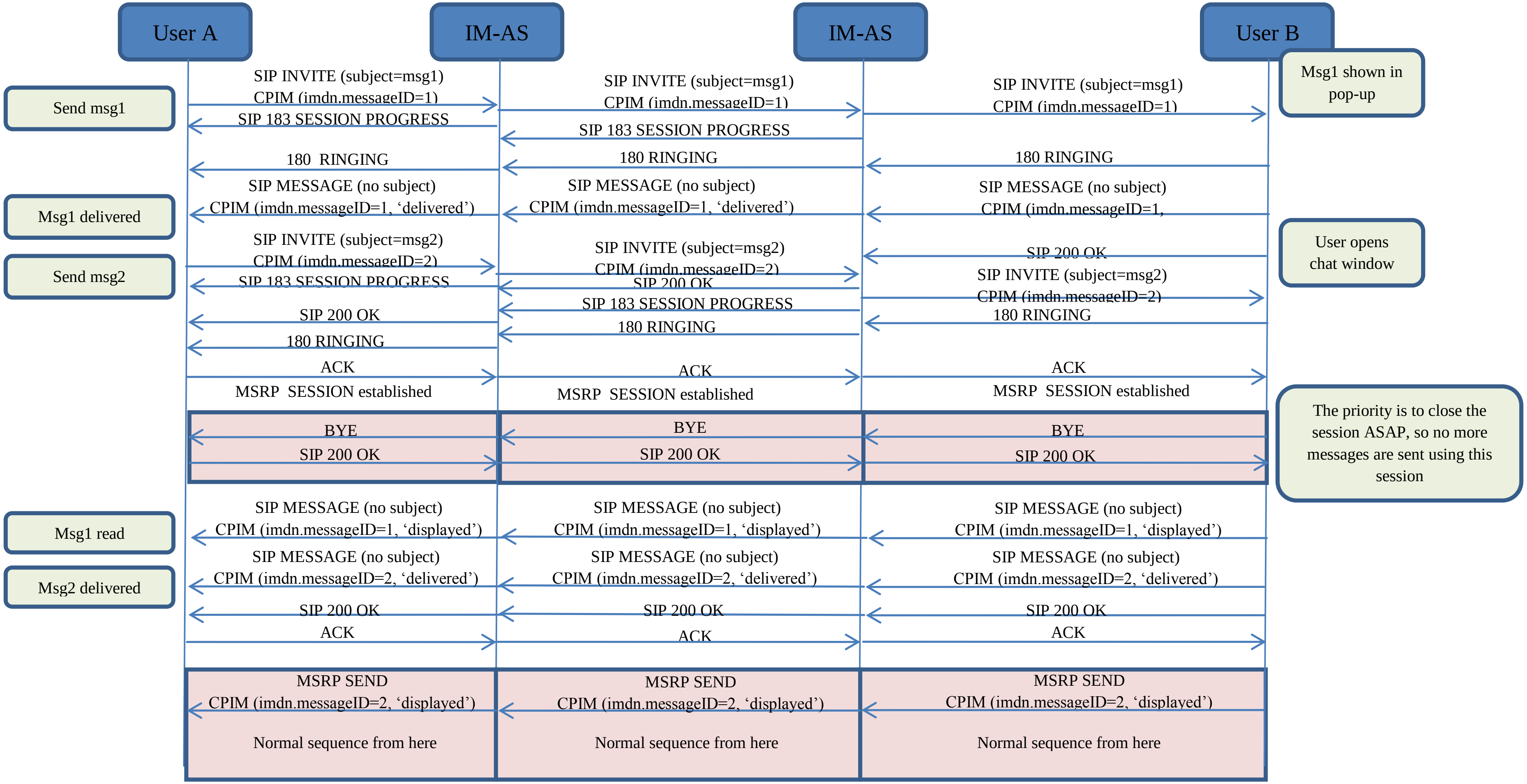


Figure 76. Store and forward race conditions: New INVITE after a session is accepted

B.11 Store and forward: Message(s) displayed notifications via SIP MESSAGE with sender offline

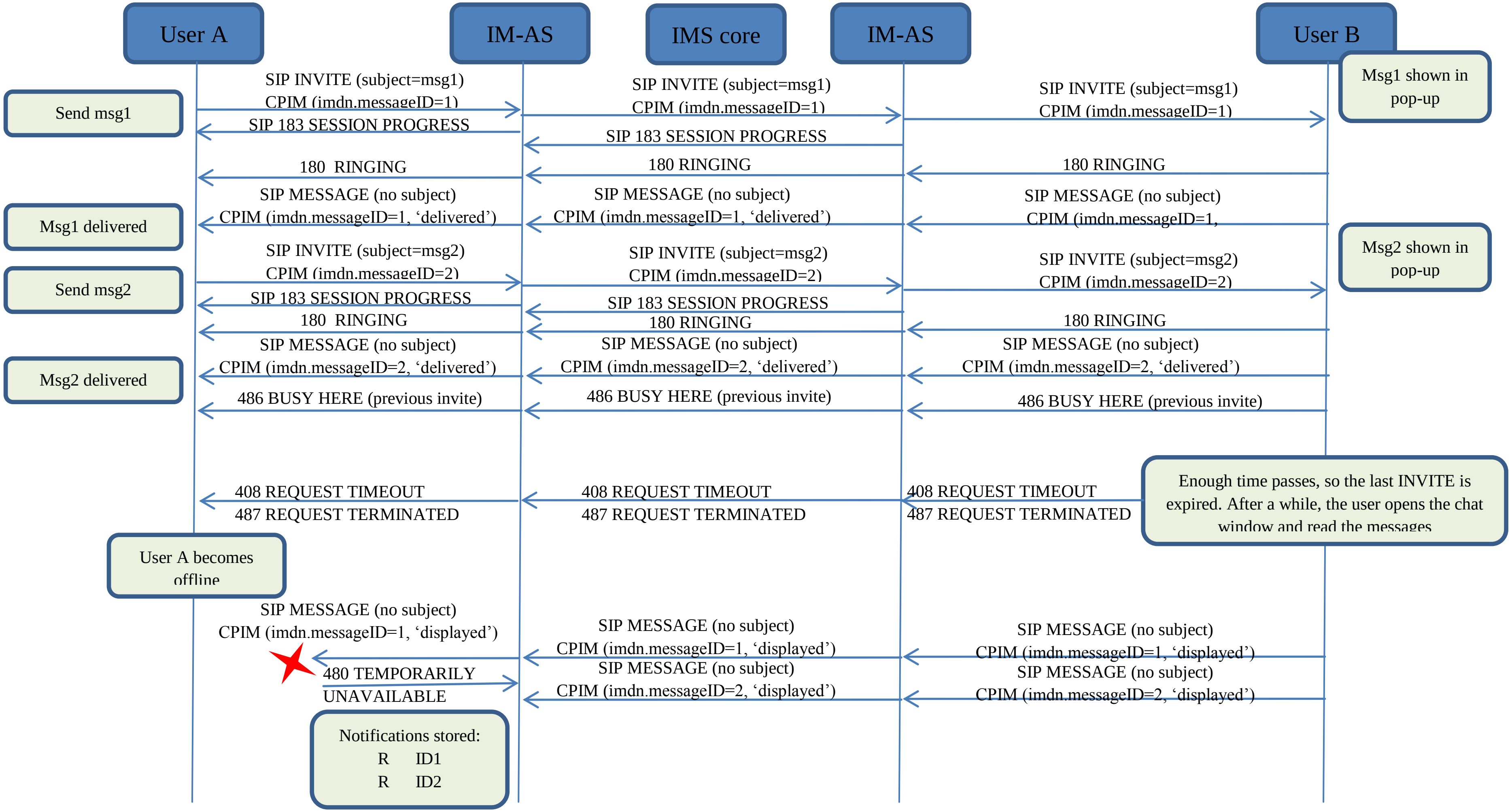


Figure 77. Store and forward: Message(s) displayed notifications via SIP MESSAGE with sender offline*

***:** Check NOTES 1, 8, 9 and 10 in section B.12

B.12 IM and store and forward diagrams: Notes

Please note the following notes apply to diagrams in Annex B:

- NOTE 1 (B.1, B.2, B.3, B.4, B.5, B.6, B.7, B.9, B.10 and B.11): 200 OK responses to SIP MESSAGE and MSRP SEND messages are omitted for clarity.

- NOTE 2 (B.3): In a multidevice scenario, if the device public GRUU in a delivery notification received from User B is different from the value for User A's device used in the on-going MSRP session, a new SIP INVITE using the new device public GRUU and P-Asserted-Identity set to standfwd@sip.rcse.com needs to be sent towards A.

- NOTE 3 (B.4): In a multidevice scenario, if the device public GRUU in a delivery notification a delivery notification received after the first INVITE is sent to User A is different from the value in the first one, a new SIP INVITE with the new device public GRUU needs to be sent towards A.

- NOTE 4 (B.3, B.4 and B.6): Clarify that B could have to handle two incoming INVITEs, one from the IM server on behalf of A to deliver stored messages and notifications, and a second one directly from A who happens to want to chat with B at the same time. B should recognize the INVITE from the IM server on behalf of A and not tear it down when the new INVITE directly from A arrives. Please note that the same applies to the case the order the INVITEs arrive is inversed.
  The INVITE from the IM server on behalf of A would have P-Asserted-Identity set to the IM server (e.g. IMserver@<domain>, and Referred-By set to A).

- NOTE 5 (B.3, B.4 and B.5): The session established by the IM-AS to deliver deferred messages to the destination only allows the receiver (client/phone) to send back notifications (i.e. an INVITE with referred-by header will only allow message/imdn+xml in the CPIM part). If the user replies with a new message, then a separate session shall be established (i.e. if user B (MT) wants to reply a new INVITE should be used) after all the deferred messages have been delivered.

- NOTE 6 (B.2): In the diagram we have represented one of the possible mechanisms to detect that the user is not online (wait for the 480 response), however, there are alternative mechanisms (triggers, 3rd party registration) that can be also used by the IM-AS for the purpose.

- NOTE 7 (B.3, B.4 and B.5): Note that in the scenario the MSRP socket is closed between IM-AS and mobile Terminating (B) in a deferred message delivery (e.g. small connectivity loss but PDP context is active) and no re-registration takes place, if there are notifications pending (delivery or displayed) and all the deferred messages have been already sent to B (no need to open a new MSRP session), SIP MESSAGE can be used to confirm the pending delivery/display that could not be sent over MSRP.

- NOTE 8 (B.11): Note that the deferred delivery of the displayed notifications stored in the IM-AS will be performed as shown in section B.6.

- NOTE 9 (B.11): In the absence of an IM-AS and in the case the display notification fail to be delivered because the sender is offline, these notifications will be discarded and the receiver does not need to retry sending them. In any case, the next time user A manages to establish a chat session with user B, all the previous messages pending to receive the displayed notification will be marked as displayed/read.

- NOTE 10 (B.7 and B.11): In those scenarios where an IM-AS is not available on both sender and receiver end, there is a chance displayed notifications carried via SIP MESSAGE may be lost if the original sender is offline when the receiver sends the mentioned displayed notifications (last three messages in the diagram). In order to overcome this limitation, a terminal or client implementation should mark all the previous messages as displayed when a new chat message is received from the receiver in the future.

- NOTE 11 (B.3, B.4, B.5 and B.6): The session established by the IM-AS server to deliver differed messages or notification should be terminated once the all the messages or notifications have been delivered as a general rule. In more details:

    - When delivering differed messages, the session should be terminated (sending a BYE) either (whatever is shorter) the displayed notification correspondent to the last differed message has been received by the IM-AS or, after a timer started on the reception of the delivered notification for the last message expires. This timer is to be defined by the MNO.

C. ANNEX C: RCS-e IM/Chat and multidevice

C.1 Delivery prior to acceptance

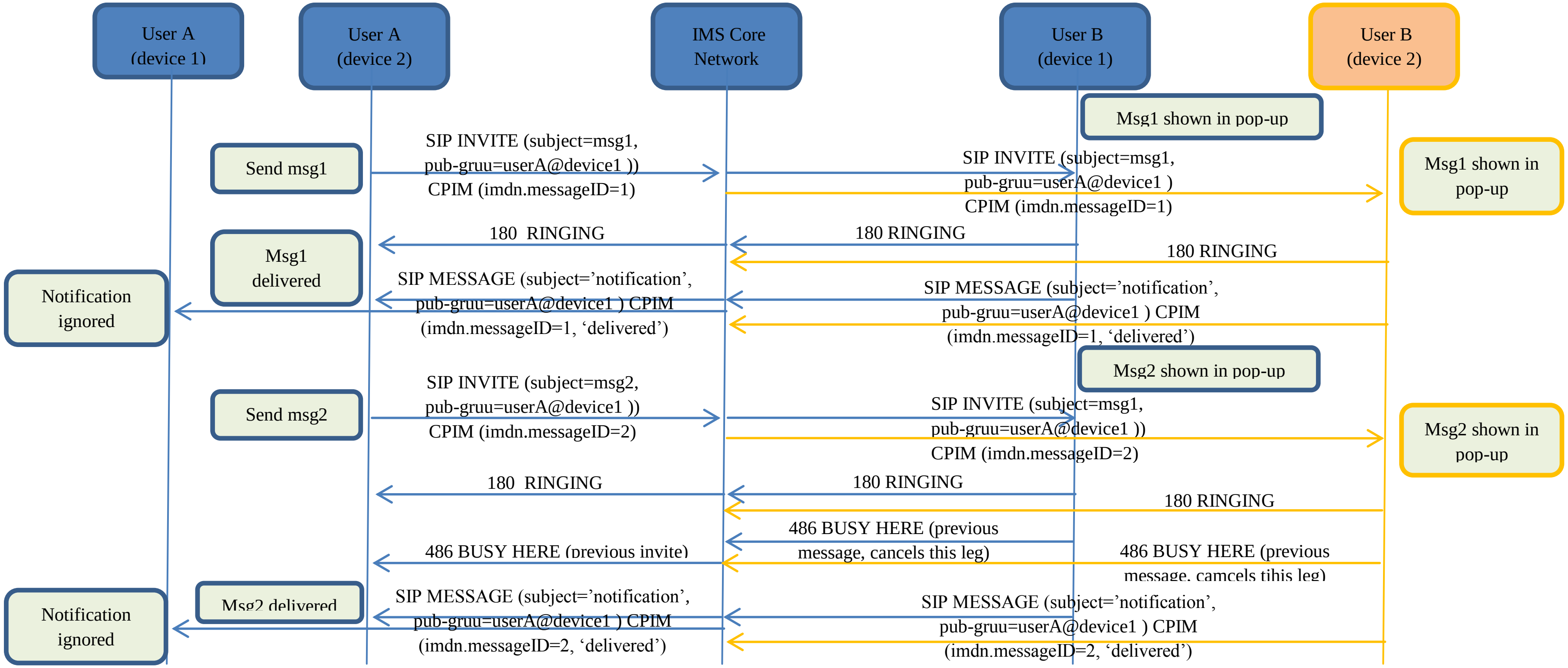

User A (device 1)
User A (device 2)
IMS Core Network
User B (device 1)
User B (device 2)
Msg1 shown in pop-up
Send msg1
SIP INVITE (subject=msg1, pub-gruu=userA@device1)) CPIM (imdn.messageID=1)
SIP INVITE (subject=msg1, pub-gruu=userA@device1) CPIM (imdn.messageID=1)
Msg1 shown in pop-up
180 RINGING
180 RINGING
180 RINGING
Msg1 delivered
Notification ignored
SIP MESSAGE (subject='notification', pub-gruu=userA@device1) CPIM (imdn.messageID=1, 'delivered')
SIP MESSAGE (subject='notification', pub-gruu=userA@device1) CPIM (imdn.messageID=1, 'delivered')
Msg2 shown in pop-up
Send msg2
SIP INVITE (subject=msg2, pub-gruu=userA@device1)) CPIM (imdn.messageID=2)
SIP INVITE (subject=msg1, pub-gruu=userA@device1)) CPIM (imdn.messageID=2)
Msg2 shown in pop-up
180 RINGING
180 RINGING
180 RINGING
486 BUSY HERE (previous message, cancels this leg)
486 BUSY HERE (previous invite)
486 BUSY HERE (previous message, camcels tihis leg)
Msg2 delivered
Notification ignored
SIP MESSAGE (subject='notification', pub-gruu=userA@device1) CPIM (imdn.messageID=2, 'delivered')
SIP MESSAGE (subject='notification', pub-gruu=userA@device1) CPIM (imdn.messageID=2, 'delivered')

Figure 78. IM and multidevice: Delivery prior to acceptance*

***:** Check NOTES 1 and 2 in section C.3

C.2 Post-acceptance behaviour

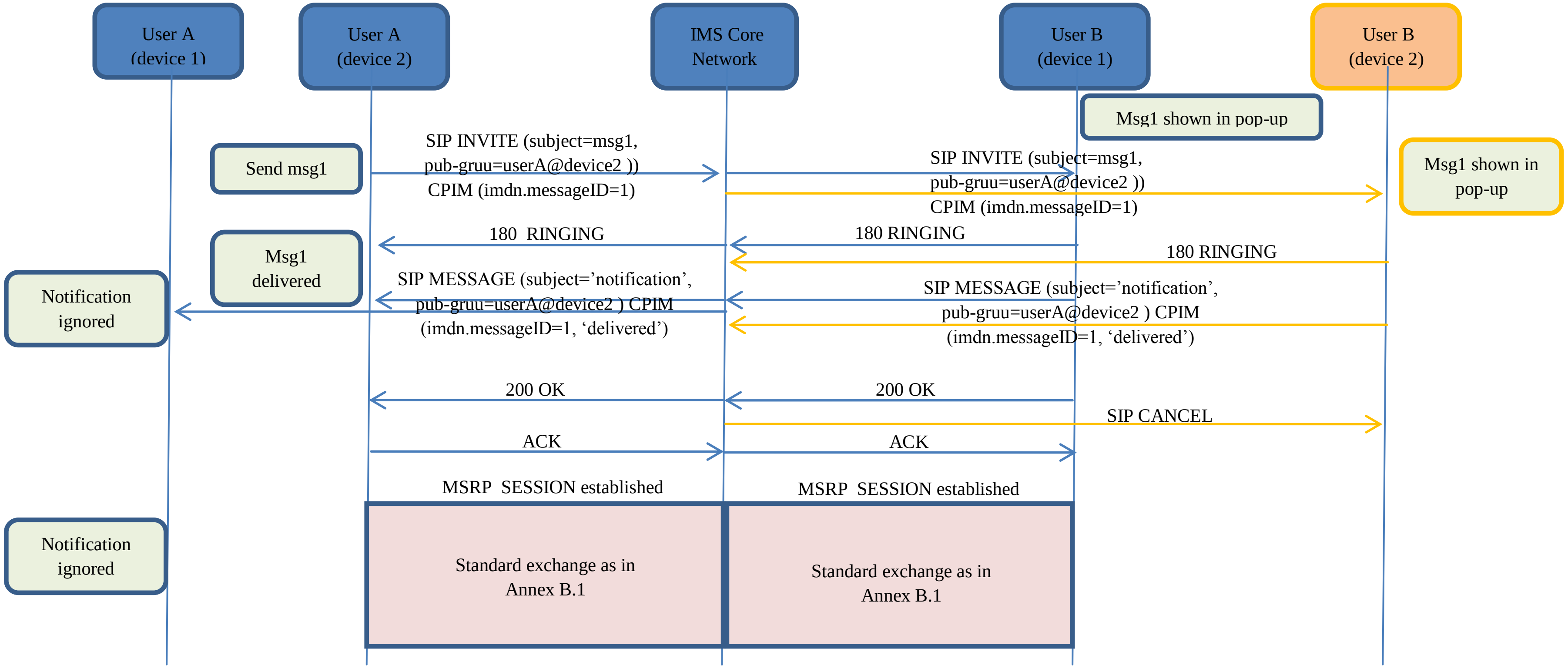

User A (device 1)
User A (device 2)
IMS Core Network
User B (device 1)
User B (device 2)
Msg1 shown in pop-up
Send msg1
SIP INVITE (subject=msg1, pub-gruu=userA@device2)) CPIM (imdn.messageID=1)
SIP INVITE (subject=msg1, pub-gruu=userA@device2)) CPIM (imdn.messageID=1)
Msg1 shown in pop-up
180 RINGING
180 RINGING
180 RINGING
Msg1 delivered
Notification ignored
SIP MESSAGE (subject='notification', pub-gruu=userA@device2) CPIM (imdn.messageID=1, 'delivered')
SIP MESSAGE (subject='notification', pub-gruu=userA@device2) CPIM (imdn.messageID=1, 'delivered')
200 OK
200 OK
SIP CANCEL
ACK
ACK
MSRP SESSION established
MSRP SESSION established
Notification ignored
Standard exchange as in Annex B.1
Standard exchange as in Annex B.1

Figure 79. IM and multidevice: Post-acceptance behaviour*

*: Check NOTES 1 and 2 in section C.3

C.3 RCS-e IM/Chat and multidevice: Notes

Please note the following notes apply to diagrams in Annex B:

- NOTE 1 (C.1 and C.2): 200 OK responses to SIP MESSAGE and MSRP SEND messages are omitted for clarity.
- NOTE 2 (C1 and C.2): As presented in section 2.14, the diagrams display the solution in a network supporting the *pub-gruu* generation. For a network supporting the *sip.instance* tag only, would be equivalent but changing the relevant mechanism to carry the device ID (*sip.instance* instead *pub-gruu*).

D. ANNEX D: Authors

This document defines the RCS-e specification jointly developed France Télécom, Telefónica, Telecom Italia, Deutsche Telekom and Vodafone (group also known as MNO G5). This specification will be shared with other operators and suppliers with a view to launching a commercial service in 2011.

Contributors:

Javier Arenzana Arias (Telefónica)
Phillip Carter (Vodafone)
Enrique Collado López (Vodafone)
Fazli Erbas (Deutsche Telekom)
Patrick Froeller (Deutsche Telekom)
Óscar Gallego Gómez (Vodafone, RCE Technical Specification Group Lead)
Sergio Garcia Murillo (Telefónica)
Yann Gestraud (France Télécom/Orange)
Gonzalo Gómez Acebo (Telefónica)
Alfonso Gómez Díaz (Vodafone)
Marion Le Gléau (France Télécom/Orange)
Carlos Andrés Loaiza (Deutsche Telekom)
Juan José Lozano Lozano (Telefónica)
Jonathon Marchant (Vodafone)
Rogelio Martínez Perea (Vodafone)
Thibaud Mienville (France Télécom/Orange)
Antonia Napolitano (Telecom Italia)
Séverin Pasquereau (France Télécom/Orange)
Jean Paul Rodrigues (France Télécom/Orange)
Martin Söhn (Deutsche Telekom)
Silvia Tessa (Telecom Italia)
Vincent Trocme (France Télécom/Orange)
Stéphane Tuffin(France Télécom/Orange)
Francesco Vadala (Telecom Italia)
Tom Van Pelt (GSMA, document editor)

Finally and from this group, we would also like to thank the valuable contribution that many network, application and terminal/OEM vendors have provided via reviews, technical advisory and comments.