RCS-e - Advanced Communications: Services and Client Specification

Version 1.2

28 November 2011

*This is a **Non Binding** Permanent Reference Document of the GSMA.*

This document does not replace any documents related to Rich Communications Suite Release 2-4.

The purpose of this document is to provide detailed specifications that are based on the current RCS Release 2 specification in order to set the initial reference implementation of the RCS-e services that are planned to be implemented by a number of operators throughout the world.

This RCS-e Version 1.2 Service and client Specification document is supported by the following operators: Deutsche Telecom, Orange, Telecom Italia, SKT, Telefonica & Vodafone

Security Classification – NON CONFIDENTIAL GSMA MATERIAL

Table of Contents

Table of Figures

List of Tables

1 Introduction

The purpose of this document is to provide the detailed specifications that are based on the current Rich Communication Suite (RCS) Release 2 specification in order to set the initial reference implementation of the Rich Communication suite enhanced (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 to accelerate time to market and simplify the customer proposition. This renewed focus is based on results from customer trials to date and offers further insight for Mobile Network Operators (MNOs) in where they can further enhance their data network offering to deliver more value to customers and complement established 3rd party services.

As indicated in Figure 1, the current document does not detail the "*social information via presence*"[1] and the network address book 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 and/or network address book outlined in the 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. For these device implementations the same possibilities are offered for accessing the operator core network as in RCS Release 2.

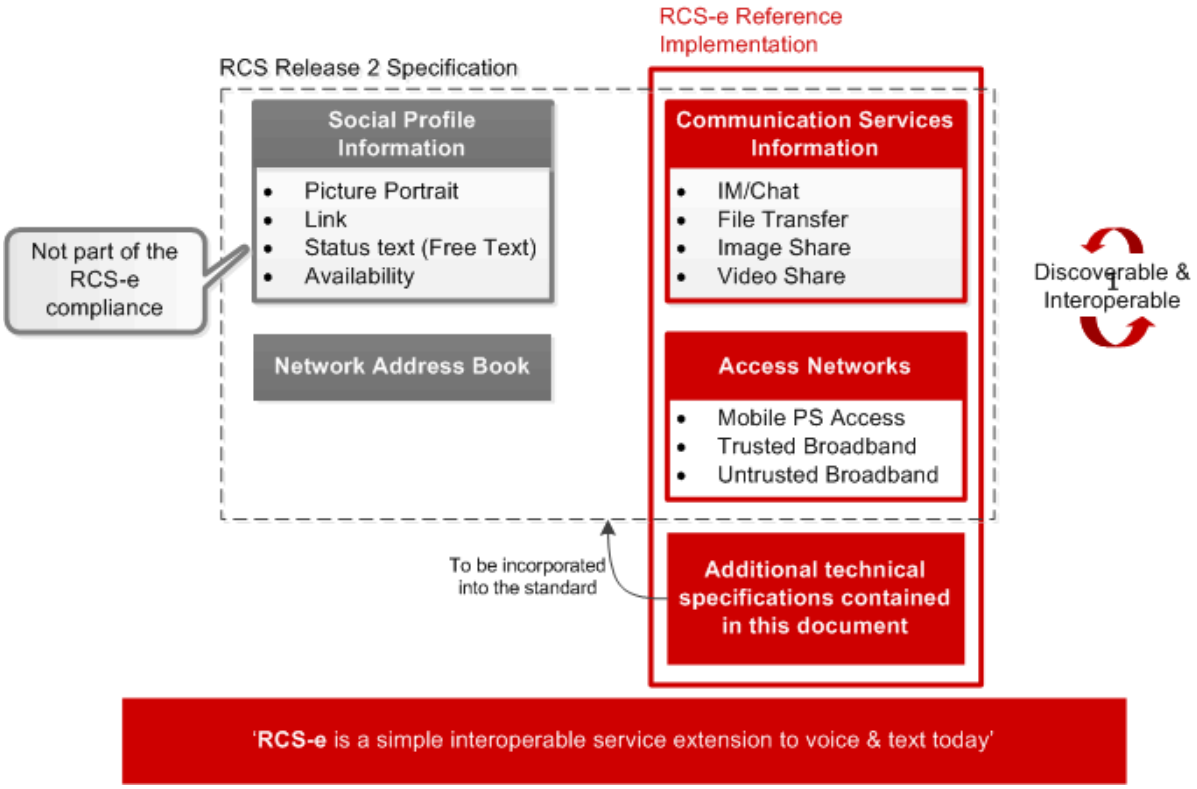

Figure 1: RCS-e positioning

[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.

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).

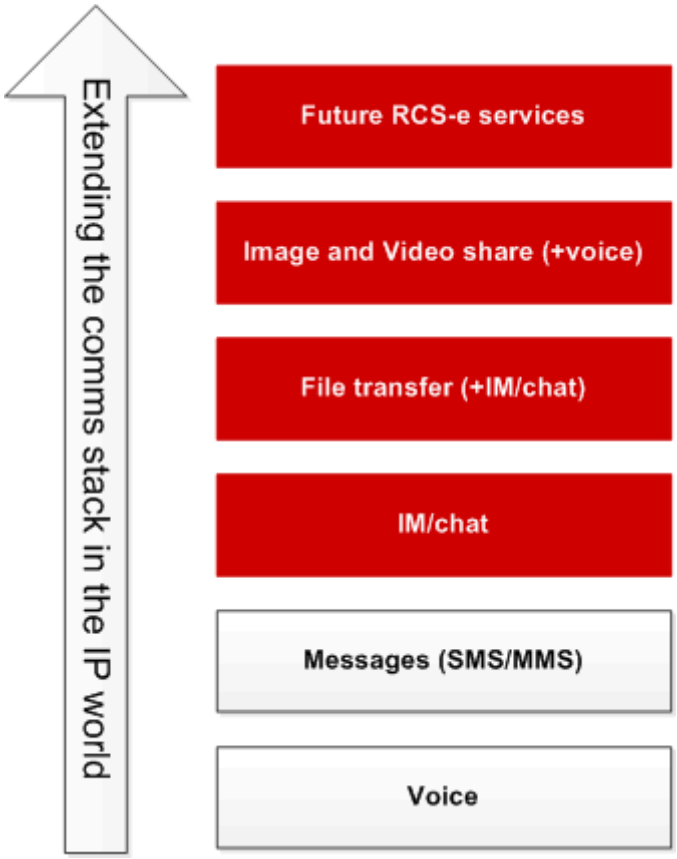

Figure 2: RCS-e Industry Proposition – '*extending the communications stack*'

1.1 RCS-e Principles

The fundamental mechanism that enables RCS-e is service or capability discovery. For example, when User A, scrolls through their Address Book and selects an 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 the Session Initiation Protocol's (SIP) OPTIONS request. SIP OPTIONS is a peer-to-peer request routed by the network that will generate one of two 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 as 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 within an address book when the user first registers for the service.

Figure 3: RCS-e capability discovery

1.2 Scope

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.

Finally, it should be noted that the aim of this document is to only specify functionality which can be validated in standard Internet Protocol (IP) Multimedia Subsystem (IMS)/RCS Release 2 pre-production and production environments without major customisation or changes apart from those that MNOs may introduce to optimise or differentiate their networks.

1.2.1 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.

1.2.2 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 Instant Messaging (IM)/chat functionality (covered in detail in section 3.2).

The rest of the 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 the RCS-e specification can be summarized in the following terms[2]:

- All the necessary procedures to provision and register with the core network elements (like IMS, RCS Application Servers (ASs) and so on) **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, an RCS-e handset **SHALL**[2] try to support all the feasible RCS-e services taking into account the relevant hardware and software limitations.

[2] Please note the terms SHALL and MAY contained in the conformance summary are used as described in [RFC2119]

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

Please note that although outside the conformance and consistently with section 1.1, an 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.

1.2.3 Future Evolution

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

- RCS Home Services (fixed line, Personal Computer (PC) and mobile)
- Additional capabilities and services (e.g. High Definition (HD) voice, advanced geo-location services, etc.)
- Enhanced network address book services

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

1.3 Definition of Terms

Term	Description
2G	2nd Generation of Global System for Mobile Communications (GSM)
ACK	Acknowledgement
ACL	Access Control List
APN	Access Point Name
AS	Application Server
ASAP	As Soon As Possible
AVC	Advanced Video Codec
Bool	Boolean
bps	Bits per second (used with Mbps: Mega-, kbps: kilo-)
CPIM	Common Profile for Instant Messaging
CRLF	Carriage Return Line Feed
CS	Circuit Switched
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DNS SRV	DNS Service record
DTM	Dual Transfer Mode
EOF	End Of File
FIFO	First IN First Out
FQDN	Fully Qualified Domain Name
GIBA	GPRS-IMS-Bundled Authentication
GPRS	General Packet Radio Service
GRUU	Globally Routable User agent URI
GSMA	GSM Association
HD	High-Definition (voice or video)
HPLMN	Home Public Land Mobile Network
HTTP	Hyper-Text Transfer Protocol
HTTPS	HTTP Secure
HW	HardWare
Hz	Hertz
IARI	IMS Application Reference Identifier
IM	Instant Messaging. The term chat is also applied in this document to the same concept.
IM-AS	IM Application Server

[3] 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.

IMDN	Instant Message Disposition Notification
IMEI	International Mobile Station Equipment Identity
IMS	IP Multimedia Subsystem
IMSI	International Mobile Subscriber Identity
IMS AKA	IMS Authentication and Key Agreement
Int	Integer
IP	Internet Protocol
KB	KiloByte
LTE	Long Term Evolution
MIME	Multipurpose Internet Mail Extensions
MNO	Mobile Network Operator
MO	Management Object
MPEG	Moving Pictures Experts Group
ms	milliseconds
MSISDN	Mobile Subscriber Integrated Services Digital Network Number
MSRP	Message Session Relay Protocol
MTU	Maximum Transmission Unit
NAT	Network Address Translation
NW	NetWork
OEM	Original Equipment Manufacturer
OFDM	Orthogonal Frequency Division Multiplex
OMA	Open Mobile Alliance
OMA-CP	OMA Client Provisioning
OMA-DM	OMA Device Management
OS	Operating System
OTA	Over The Air
PCO	Protocol Configuration Options
P-CSCF	Proxy-Call Session Control Function
PC	Personal Computer
PDP	Packet Data Protocol
PS	Packet Switched
QoS	Quality of Service
RADIUS	Remote Authentication Dial In User Service
RCS	Rich Communication Suite
RCS-e	RCS enhanced
RR	Receiver Report
RTCP	RTP Control Protocol
RTP	Real-time Transport Protocol
SDP	Session Description Protocol
SIM	Subscriber Identity Module
SIP	Session Initiation Protocol
SMS	Short Message Service
SRTP	Secure RTP
SSO	Single Sign On (type of IMS authentication)
STUN	Simple Traversal of UDP through NATs
SW	SoftWare
TCP	Transmission Control Protocol
TEL URI	TELephone URI
TLS	Transport Layer Security
UC	Use Case
UDP	User Datagram Protocol
UE	User Equipment
UI	User Interface
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
UUID	Universally Unique IDentifier
UX	User Experience
vCard	A format for electronic business cards

VoLTE	Voice over LTE
VoIP	Voice over IP
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
XSD	XML Schema Definition

1.4 Document Cross-References

Ref	Document Number	Title
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) http://www.3gpp.org
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) http://www.3gpp.org
3	[IETF-DRAFT-SIMPLE-MSRP-SESSMATCH 10]	IETF Simple MSRP sessmatch draft version 10 http://tools.ietf.org/html/draft-ietf-simple-msrp-sessmatch-10
4	[PRD-IR.74]	GSMA PRD IR.74 - "Video Share Interoperability Specification" 1.4 20 December 2010 http://www.gsmworld.com
5	[PRD-IR.79]	GSMA PRD IR.79 - "Image Share Interoperability Specification" 1.4 29 March 2011 http://www.gsmworld.com
6	[PRD-IR.92]	GSMA PRD IR.92 - "IMS Profile for Voice and SMS" 4.0 22 March 2011 http://www.gsmworld.com
7	[RCS1-FUN-DESC]	Rich Communication Suite Release 1 Functional Description Version 2.0 14 February 2011 http://www.gsmworld.com
8	[RCS1-TEC-REAL]	Rich Communication Suite Release 1 Technical Realization Version 2.0 14 February 2011 http://www.gsmworld.com
9	[RCS2-FUN-DESC]	Rich Communication Suite Release 2 Functional Description Version 2.0 14 February 2011 http://www.gsmworld.com
10	[RCS2-MO]	Rich Communication Suite Release 2 Management Objects Version 2.0 14 February 2011 http://www.gsmworld.com
11	[RCS2-TEC-REAL]	Rich Communication Suite Release 2 Technical Realization Version 2.0 14 February 2011 http://www.gsmworld.com
12	[RCS2-SD]	Rich Communication Suite Release 2 Service Definition Version 2.0 14 February 2011 http://www.gsmworld.com
13	[RCS2-OMA-SIMPLE-ENDORS]	Rich Communication Suite Release 2 Endorsement of OMA SIP/SIMPLE IM 1.0 Version 2.0 14 February 2011

		http://www.gsmworld.com
14	[RCS3-OMA-SIMPLE-ENDORS]	Rich Communication Suite Release 3 Endorsement of OMA SIP/SIMPLE IM 1.0 Version 2.0 14 February 2011 http://www.gsmworld.com
15	[RCS4- TEC-REAL]	Rich Communication Suite Release 4 Technical Realization Version 1.0 14 February 2011 http://www.gsmworld.com
16	[RCS4-IR92-ENDORS]	GSMA RCS Release 4 Endorsement of [PRD-IR.92] Version 1.0 14 February 2011 http://www.gsmworld.com
17	[RFC2119]	Key words for use in RFCs to Indicate Requirement Levels IETF RFC http://tools.ietf.org/html/rfc2119
18	[RFC3261]	SIP (Session Initiation Protocol) IETF RFC http://tools.ietf.org/html/rfc3261
19	[RFC3264]	An Offer/Answer Model Session Description Protocol IETF RFC http://tools.ietf.org/html/rfc3264
20	[RFC3711]	The Secure Real-time Transport Protocol (SRTP) IETF RFC http://tools.ietf.org/html/rfc3711
21	[RFC3966]	The TEL-URI for Telephone Numbers IETF RFC http://tools.ietf.org/html/rfc3966
22	[RFC4028]	The Session Timers in the Session Initiation Protocol (SIP) IETF RFC http://tools.ietf.org/html/rfc4028
23	[RFC4122]	The Universally Unique IDentifier (UUID) URN Namespace IETF RFC http://tools.ietf.org/html/rfc4122
24	[RFC4483]	A Mechanism for Content Indirection in Session Initiation Protocol (SIP) Messages IETF RFC http://tools.ietf.org/html/rfc4483
25	[RFC4961]	Symmetric RTP / RTP Control Protocol (RTCP) IETF RFC http://tools.ietf.org/html/rfc4961
26	[RFC5438]	Instant Message Disposition Notification (IMDN) IETF RFC http://tools.ietf.org/html/rfc5438
27	[RFC5626]	Managing Client-Initiated Connections in the Session Initiation Protocol (SIP) IETF RFC http://tools.ietf.org/html/rfc5626
28	[RFC5627]	Using Globally Routable User Agent URIs (GRUUs) in the Session Initiation Protocol (SIP) IETF RFC http://tools.ietf.org/html/rfc5627
29	[RFC6135]	Alternative Connection Model for the Message Session Relay Protocol (MSRP) IETF RFC http://tools.ietf.org/html/rfc6135
30	[RFC6223]	Indication of Support for Keep-Alive IETF RFC http://tools.ietf.org/html/rfc6223
31	[IMCR090017]	OMA-IM-2009-0017-CR_Replaces_Correction http://member.openmobilealliance.org/ftp/Public_documents/COM/IM/2009/OMA-IM-2009-0017-CR_Replaces_Correction.zip

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 Unique Resource Identifier (URI), that is a TEL-URI and/or a SIP-URI) is correctly provisioned to access the RCS-e services.

To give the end user the impression that the new services are working out of the box and to minimise the operational impact on MNOs both processes are performed automatically.

A mobile network implementing RCS-e should be able to detect when a user attaches to the network with an 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 table focuses within RCS-e specific parameters. Please note that all the parameters describing the configuration can only be modified by the MNO (via MNO customization settings or one of the procedures described in section 2.2.2.1.2) and are not accessible to the terminal user:

Configuration parameter	Comments	RCS-e usage
SIP proxy	P-CSCF address	Mandatory parameter
XDM server	extensible Markup Language (XML) Document Management Server (XDMS) address	Mandatory parameter It is mandatory and becomes relevant only if USE PRESENCE is set to 1
TEL-URI	User's Telephone URI (TEL-URI)	Optional parameter
SIP-URI	User's SIP-URI	Mandatory parameter[4]
SIP USER / PASSWORD	For alternative digest authentication to Single Sign On based on General Packet Radio Service-IMS-Bundled Authentication (SSO/GIBA)	Mandatory parameter
DEVICE ID	This controls the identity provided in the sip.instance parameter during registration (see chapter 2.15). It is only relevant in case the client has access to the device's International Mobile Station Equipment Identity (IMEI). Then handling will be as follows:	Optional parameter

[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). At least the SIP-URI configuration parameter must be configured and optionally a TEL URI may also be configured. The configured parameters are used to select the URI which must be used by the RCS-e client during non-REGISTER transactions as specified in section 2.9.3.2. If both TEL-URI and SIP-URI are defined, the TEL-URI should be used.

Also when using Digest, at least a SIP-URI must be configured. This URI is used for REGISTER transactions. For non-REGISTER transactions the behaviour is the same as when using GIBA: the TEL-URI is used when it has been configured.

	1: a Universally Unique IDentifier (UUID) or hashed value of the IMEI is provided 0: the value is set to the device's IMEI Please note that if not provided the device should use the IMEI. The value of 0 is thus the default.	

Table 1: Summary of IMS registration related configuration parameters

Configuration parameter	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 an IM server (that is Group chat) will not be available for those customers.	Optional parameter
IM CAP ALWAYS ON	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
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 setup procedure when the receiver sends the 200 OK response back to the sender allowing the MSRP session to 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 presses the button to send a message (that is the message will be buffered in the client until the MSRP session is established). Note: as described in section 3.2, the parameter only affects the behaviour for 1-to-1 sessions in case no session between the parties has been established yet.	Mandatory parameter
POLLING PERIOD	This is the frequency in seconds to run a periodic capabilities update for all the contacts in the phone's address book whose capabilities are not available (like for example 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 SIP OPTIONS requests. When performing a whole address book capability discovery (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 tag associated 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 tag associated 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 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 Access Point Name (APN) configuration which should be used to provide Packet-Switched (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 KiloByte (KB). It is used to warn the user that a file may end up in significant charges. Please note that if this parameter is 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 this parameter is set to 0, this limit will not apply	Mandatory parameter
END USER CONF REQ ID	This is the identity used for sending the end user confirmation requests.	Optional parameter

Table 2: Summary of RCS-e client configuration parameters

Please note that the detailed information on the extended managed objects for RCS-e is provided 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 later by the MNO by pushing new configuration documents using the Open Mobile Alliance's (OMA) Device Management (DM) enabler or the other configuration mechanisms defined in section 2.2.2.1.2.

Finally, please note that with the aim of reducing the complexity, the Proxy-Call Session Control Function (P-CSCF) address used by the RCS-e client is selected from the list in the IMS Management Object. The other auto-configuration mechanisms (that can for example

be based on the Dynamic Host Configuration Protocol (DHCP) or on the Protocol Configuration Options (PCO) info received during Packet Data Protocol (PDP) context activation) are left out of the scope of this specification. A MNO may request an Original Equipment Manufacturer (OEM) to implement such functionality as a customization. The validation of this functionality will remain outside of the RCS-e compliance however.

2.1.1 RCS-e client configuration storage

The RCS-e and, by extension, the IMS configuration should be stored securely on the handset and should not be accessible to the user unless it is an explicit requirement of the 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 2) must be configured correctly. If any of the parameters are not configured or configured with an unexpected value, the RCS-e functionality should be disabled and not be presented or accessible to the user (that is the phone behaves as it would be a non-RCS-e enabled phone). In this state, the RCS-e functionality can only be 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 an RCS-e configured device is reset, the RCS-e client should securely back up the configuration in the device together with the associated International Mobile Subscriber Identity (IMSI) prior to the reset. Please note that this also applies in the event of swapping Subscriber Identity Module (SIM) cards. The configuration associated to the old SIM should then 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. In that case instead of 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 a policy where a SIM swap causes the deletion of the contacts), the associated RCS-e information (that is the cached capabilities per contact and the RCS-e contact list) should also be 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 1). 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 Wireless Local Area Network (Wi-Fi)), then digest authentication will be performed. This authentication mechanism is based on a challenge that the network sends to the client and should be responded to using the configured username/password pair (see Table 1 for reference).

Please note that in this document in the flow diagrams 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, the client must register again.

Finally note that a precondition to register is that all the mandatory parameters presented in Table 2 are correctly configured. In addition to this and if RCS-e is the only IMS based functionality available on the phone (that is no other IMS services like Voice over Internet Protocol (VoIP) are incorporated), the precondition is extended to have also all the mandatory parameters presented in Table 1 correctly configured.

2.2.1 Additional message authentication

Depending on the network configuration, also other SIP messages (apart from SIP REGISTER) may 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 Authentication and Key Agreement (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). A MNO may request to add additional authentication mechanisms as a customization. This functionality is outside the scope of this specification however and, consequently, the associated verification is also 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 (as for example in Wi-Fi scenarios).

In addition to the SIP messages, XML Configuration Access Protocol (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 assumption in this case is that user A has already been provisioned to access the RCS-e services (because for example the tariff includes the service) however they have never used an 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 correct settings. Once the auto provisioning and client configuration is completed, the first time registration procedure takes place. Once the client is provisioned, the first step is to register and to find the subset among the existing contacts (if any) who are also RCS-e users

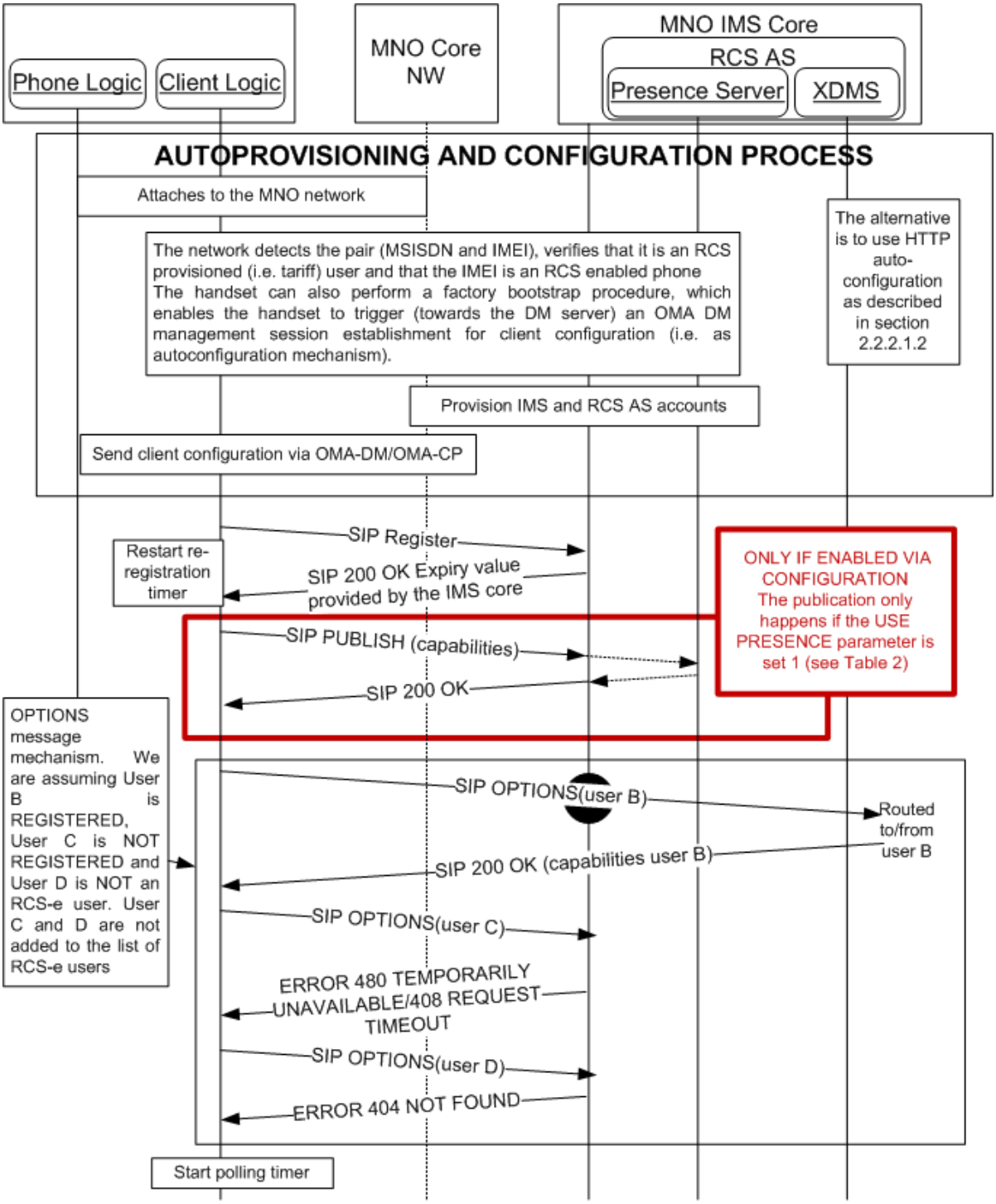

Figure 4: First time registration sequence diagram

Note that if the terminal is configured to handle presence related functionality (USE PRESENCE set 1 as presented in Table 2), this process will be used to identify those contacts supporting the “social information via presence” and capability discovery via presence functionalities.

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 can use RCS-e services and, as a consequence, trigger the relevant handset configuration. This triggering process is network specific and outside the scope of this specification. The handset may also be able to perform a customized bootstrap (also named factory bootstrap)

operation in order to trigger a client-initiated OMA DM management session towards the DM server for client configuration purposes.

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 the same sequence applies:

- When the customer changes to another RCS-e enabled device: In this case, the sequence is identical and the only difference is that the IMS provisioning (i.e. provision IMS and RCS AS accounts) is not required as it was performed previously.
- When the customer changes the SIM card: In this case, the sequence is identical to the one described in the previous section.
- A Configuration update implying changes in the user's IMS identity (that is 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. This parameter is 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 to perform the autoconfiguration of the RCS-e functionality in terminals:

- OMA-DM[5]: This is the same mechanism as the one proposed for RCS based on the managed object configuration proposed in ANNEX A, section A.2. All RCS-e capable handsets (incl. open-market devices) shall support the following requirements for OMA-DM:
    - Multiple management authorities where operator DM accounts are persistent, not editable and not visible to the user (e.g. Software (SW) updates don't delete/overwrite DM accounts) and accessible by the respective active operator DM account only (protected by OMA DM Access Control List (ACL) mechanism).
    - The active operator's 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).
    - The active operator's RCS-e management sub-tree needs to be visible, selected and activated on SIM card change.
    - The provided settings are active/updated and used on RCS-e client after successful configuration.
    - The handset shall support the customized bootstrap (also named factory bootstrap, that is the operator DM account, including DM server address, is loaded in the handset at factory phase) procedure (as specified in section 5.1.2.1 of OMA Device Management Bootstrap specification v1.2.1) in order to trigger a client-initiated

[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.

management session towards the DM server (operated by the network operator which the handset is subscribing to (that is the Home Public Land Mobile Network (HPLMN))) allowing the DM client to initiate and perform a client configuration procedure for RCS-e configuration parameters.

    - The handset shall be able to perform the factory bootstrap procedure:
        - When device is switched on for the first time
        - When the user changes the SIM card on the device
    - After successfully processing the bootstrap, the DM client of the handset SHALL automatically initiate a management session to the DM server configured in the bootstrap at the next practical opportunity (that is when network connectivity and other factors would allow such a connection).

- OMA-CP[6]: This is an alternative mechanism (that is OMA-DM is considered as the preferred standards based 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 the auto-detection mechanism complexity on network infrastructure

Note: Although RCS-e provides different mechanisms to perform the auto-configuration, the configured parameters remain the same and are independent of the mechanism that is used. The used mechanism therefore only determines the used protocol and the encoding of the parameters between the client and the network.

The new mechanism is based on a Hyper-text Transfer Protocol (HTTP) secure (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 details 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 ensure the network can implement the necessary procedures to resolve the user's Mobile Subscriber Integrated Services Digital Network Number (MSISDN) (that is RADIUS requests, header enrichment and so on), the configuration can only occur if connected using an MNO PS[7] data network and,

[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 Wi-Fi. The decision to implement this mechanism is up to the discretion of each MNO.

therefore, the handset should have the necessary APN configuration to perform the connection.

- As some of the mechanisms presented in the previous paragraphs require an initial HTTP request, the proposal is to first perform an HTTP request:
  - The handset/client shall perform a HTTP request to the RCS-e autoconfiguration server's 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 a HTTP 200 OK response. Then the client will then perform a second request, this time HTTPS (towards the same Uniform Resource Locator (URL) with 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 provide 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 User Experience (UX) perspective, the customer is not aware of the configuration process (it is background process with no pop-ups or notifications shown on the screen) unless the provisioned data includes a message for the end user.

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

RCS-e Initial configuration request:

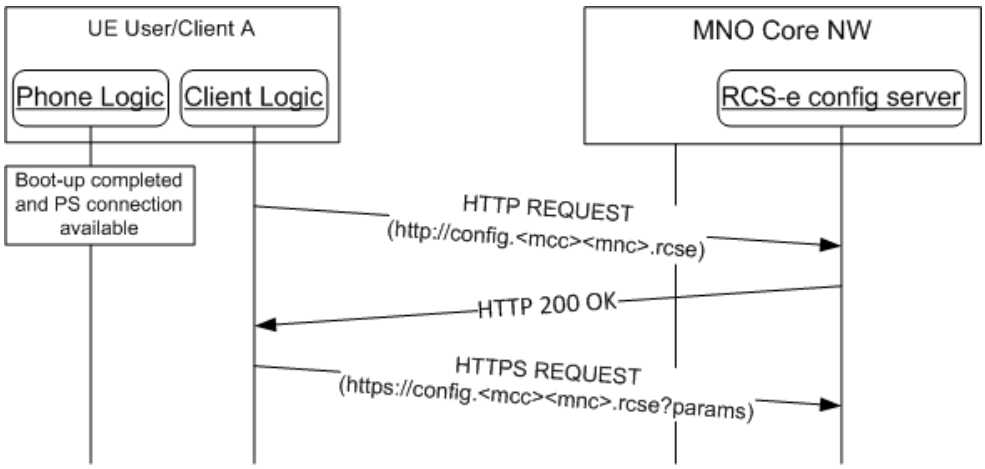

Figure 5: RCS-e alternative configuration: Initial request

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 an update is required.	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, if available to the RCS-e implementation.	N if the OS platform allows it, it shall be included	String (15 digits)

Table 3: 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 Mobile Country Code (MCC) and Mobile Network Code (MNC) in the IMSI and complete the prior name depending on the MNO.
- Please note that this URL is only routable from the PS domain so the autoconfiguration can only happen via PS.
  If a handset is employed by a MNO that does not support RCS-e, this domain will not be resolved. Therefore the application will handle it as a "client not valid" scenario.

RCS-e configuration server response:

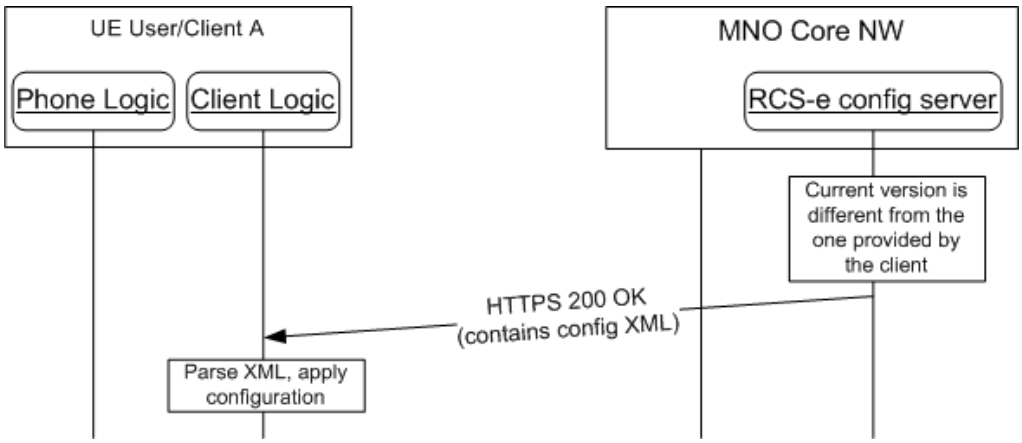

Figure 6: RCS-e alternative configuration: Server response

- 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 4: 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 5: RCS-e alternative configuration empty XML (reset RCS-e client)

- Please note that if RCS-e is disabled on the phone, the phone should perform the autoconfiguration query every time it 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 an XML containing only the version and the validity set to -1:

- Note that if the SIM is swapped or the terminal reset, 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 6: RCS-e alternative configuration empty XML (reset RCS-e client and stop autoconfiguration query)

- When the server has an updated configuration, the response will contain a configuration XML (i.e. content-type text/xml) document that the client needs to parse and apply:
  - The XML format of this document 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 if a validity=version 0 response was received).

Please note, that an "RCS-e Info" Management Object (MO) sub tree shall be included into the RCS-e management tree that contains the configuration parameter as described in Table 3, except "vers", "IMEI".

User messages delivered within autoconfiguration

As an optional addition (that is 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">
                <parm name=”title” value=”Example”/>
                <parm name=”message” value=”Hello world”/>
                <parm name=”Accept_btn” value=”1”/>
                <parm name=”Reject_btn” value=”0”/>
        </characteristic>
        …
</wap-provisioningdoc>
```

Table 7: 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 and 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 kinds of responses:

1. The one containing the full configuration settings.
2. 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 is required to send the language locale settings to the server as the language the message is served depends on this parameter. To achieve this, the client should use the HTTP Accept-Language header in all the requests and set the value consistently with the handset locale.

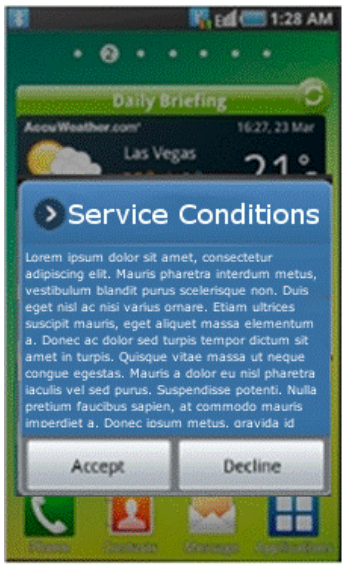

Figure 7: Autoconfiguration server notification example

Use cases review

Although it has already been introduced, in this chapter we have compiled the different use cases to indicate what the device behaviour will be for each scenario.

1. **First detection**: is the first time a user uses an RCS-e device. If the process is successful the device will receive the correct configuration XML. One of the parameters sent is the validity period. If the device has no issues in the registration process, it will not contact the server again until the validity has expired. As mentioned previously, 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, the device will send a request to check if the configuration it has is the correct one. If the device already has the latest version, the client will receive an XML containing only the same version with the validity reset to the value specified in the server. Meaning that the configuration the handset/client currently has is correct and, consequently, the validity is renewed.

3. **Version checking: new version available.** If the server has a new version of some of the fixed parameters (such as for example the registration IP address) 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 customers are not 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 (that is vanilla behaviour).**
5. **SIM change**: If the SIM changes, the previous configuration should be backed up and the handset/client should behave as if no configuration were available (that is first-time configuration) and, therefore, the handset implementation or client shall make a request for a new configuration. Please note 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 of making a new request.
6. **User with different RCS-e devices.** If the client is using multiple RCS-e devices, the same configuration will be valid for all of them. The described process will ensure the device they currently use has the latest version.
7. **User asks Customer Care to disable the RCS-e service.** In this case the user will be un-provisioned on the IMS network, and when the application asks for a reconfiguration it will always receive an XML with the version and validity set to 0. The process will remain that way until 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 (that is vanilla behaviour).**

Please notice that all the scenarios described comply 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 correct configuration (version 0 or it is not able to complete registration process), it 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 (for instance being unable 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 if it has 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).
  - If the SIM is swapped or the terminal reset, the terminal should again query for configuration settings on every boot.

Finally, (including error cases), please find below all 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 un-provisioned 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 un-provisioned 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 8: Summary of RCS-e autoconfiguration responses and scenarios

Security considerations:

Since the connection is done over PS, the current design ensures that it is not possible to perform a man-in-the-middle attack where a 3rd party can impersonate the configuration server.

To secure interoperability between MNOs and to reduce the complexity on the handset/client implementation, it is encouraged to use public root certificates issued by a recognized CA (similar to 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

In this case it is assumed that User A is provisioned for service and the first/time registration has already taken place.

The user was not registered and is trying to perform a registration using PS, and therefore assuming that SSO/GIBA authentication is available the flow would be as shown in Figure 8.

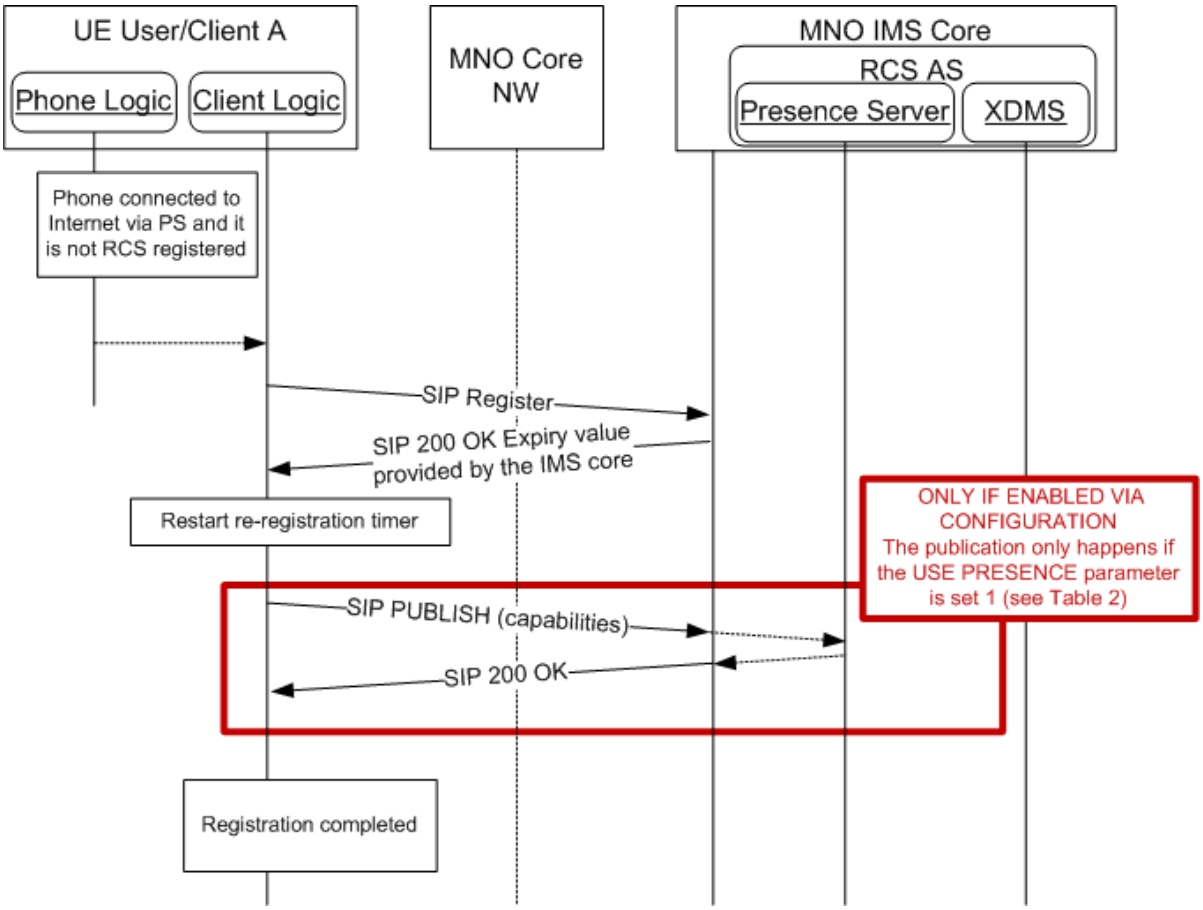

Figure 8: Registration from offline over PS (assuming SSO/GIBA)

If the initial authentication (SSO/GIBA) fails (that is 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). This leads to the flow in Figure 9:

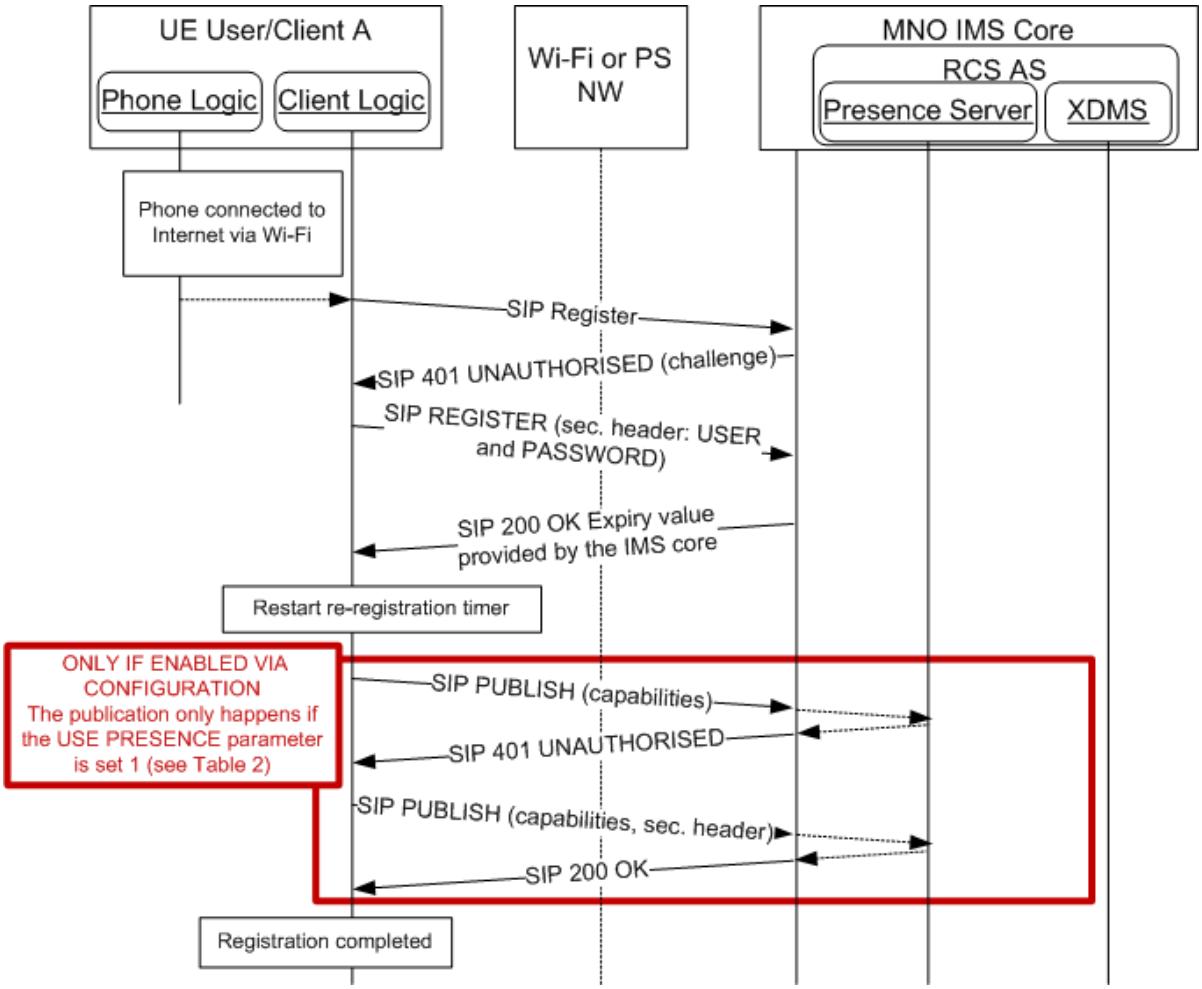

Figure 9: Registration from offline over Wi-Fi or PS networks without SSO/GIBA authentication support

In the same scenarios and provided the terminal is configured to handle presence related functionality (USE PRESENCE set 1 as presented in Table 2), it should be noted that:

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

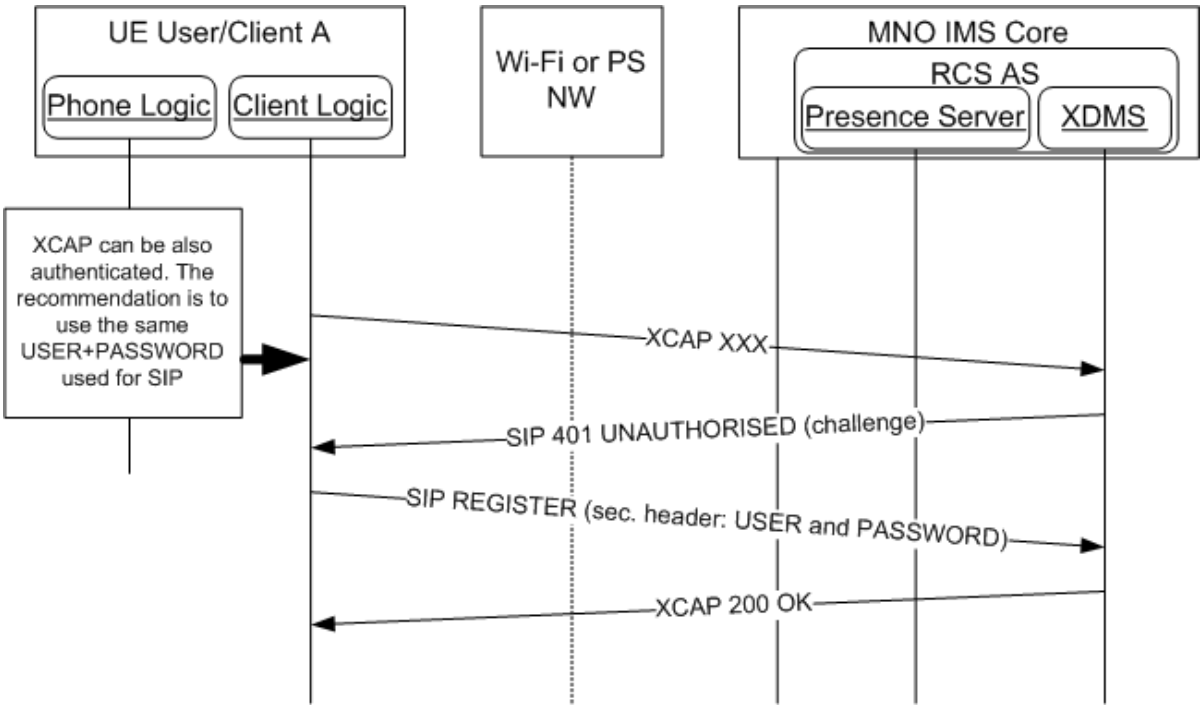

Figure 10: XCAP exchanges when using digest authentication

2.2.2.3 Re-registration

In this case it is assumed that User A is already registered. The registration expires however (that is the timer started at the last registration reaches the expiry value provided by the network). In this case, the client needs to re-register following the flow presented in Figure 11. Please note that for simplicity, in the diagram it has been assumed that SSO/GIBA authentication is available.

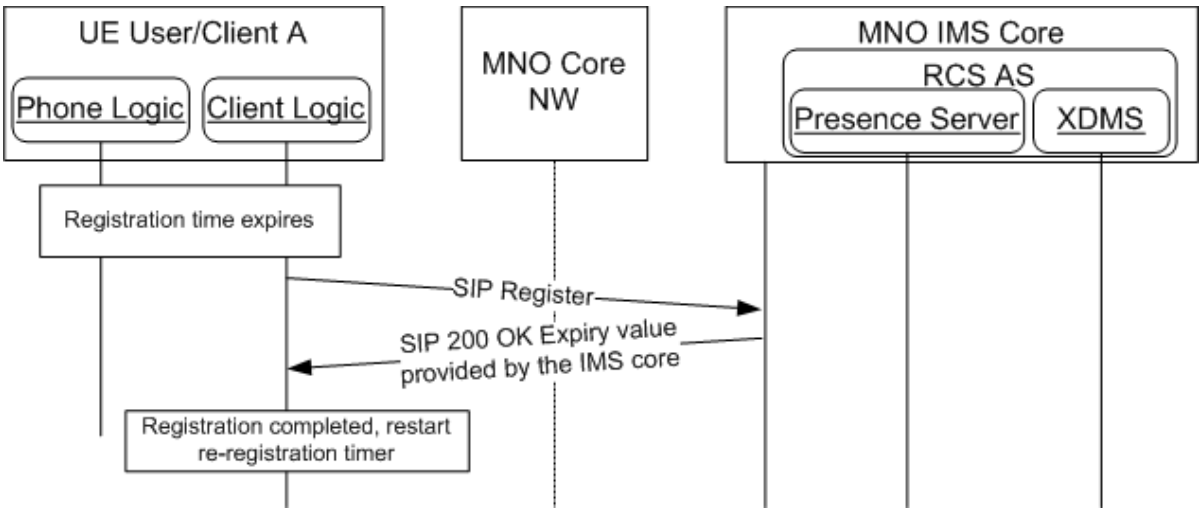

Figure 11: Re-registration

2.2.2.4 Deregistration

In this case it is assumed that User A is registered, but that based on the phone logic, the connection to the service is no longer possible or needed. Among the possible reasons, we have listed the most relevant: Powering down, battery low and so on.

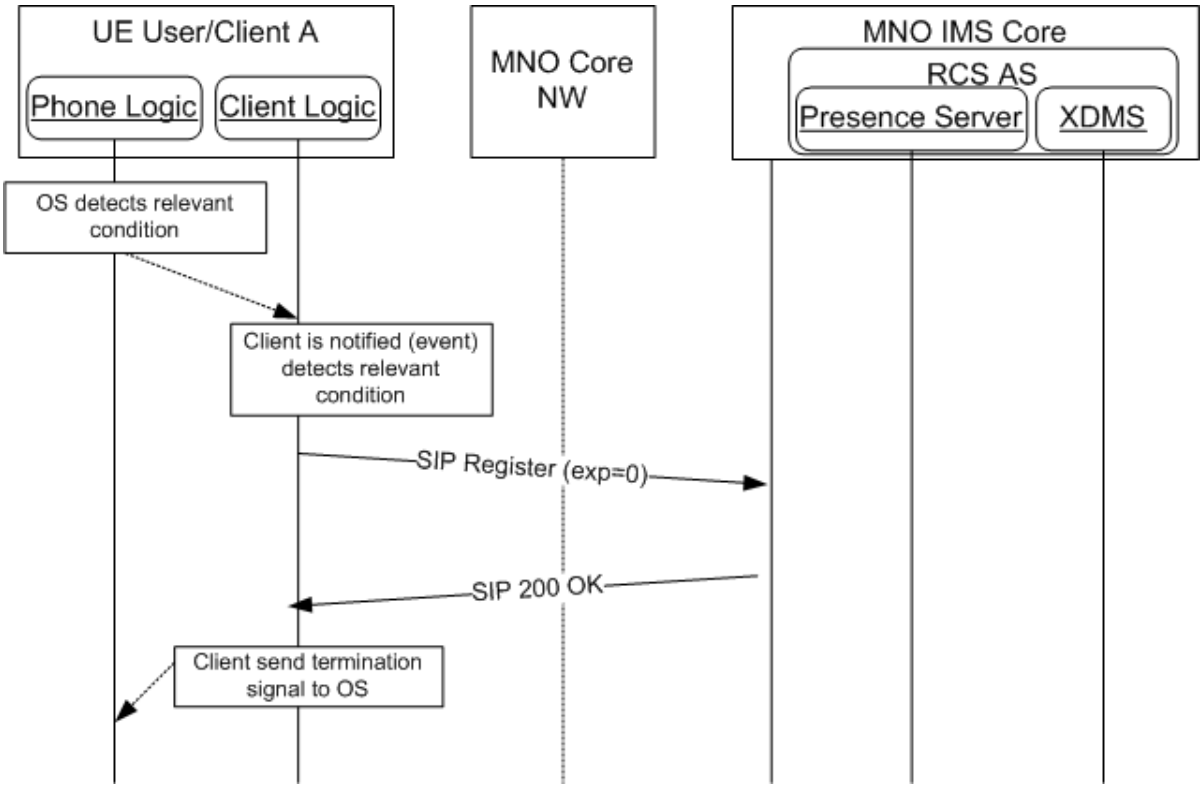

Figure 12: Deregistration

2.2.2.5 Registration status and available capabilities

If 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 (the IM CAP ALWAYS ON setting presented in Table 2 is ignored for instance).

2.2.2.6 Registration frequency optimization

RCS-e client shall not send more register requests 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 a 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 of RCS-e services that is available to access and/or communicate with other contacts at certain points .

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 include the 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 (the phone is off for instance), then the network will respond with one of the following error messages: 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 an error message: 404 NOT FOUND[8].

Note that from a user experience perspective response 2[9] 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:

- After first time registration to obtain the registration state and default set of capabilities for each contact in the phone's address book (note one SIP OPTIONS is sent per IMS identity [that is TEL-URI/MSISDN or SIP-URI] stored in the address book)[10],
- 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 2) 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 2 for reference),
- 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 an 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 established voice call to obtain the real-time capabilities for the call or IM session provided this has not been performed before (see previous bullet) or content sharing during a call is supported,
- 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.

[8] Please note that the response provided may depend on the network configuration. A useful 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.

[9] Please note that in this case if IM CAP ALWAYS ON (see Table 2) is enabled, the IM/chat should still be reported to the user as available even the other end is not registered.

[10] 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.

Please note that in some cases sending an OPTIONS request is not required as the last SIP OPTIONS exchange took place just before the communication was set up (e.g. to send a Short Message Service (SMS) message, the user went to the address book, selected a user [SIP OPTIONS exchange takes place] and chooses to send a SMS message).

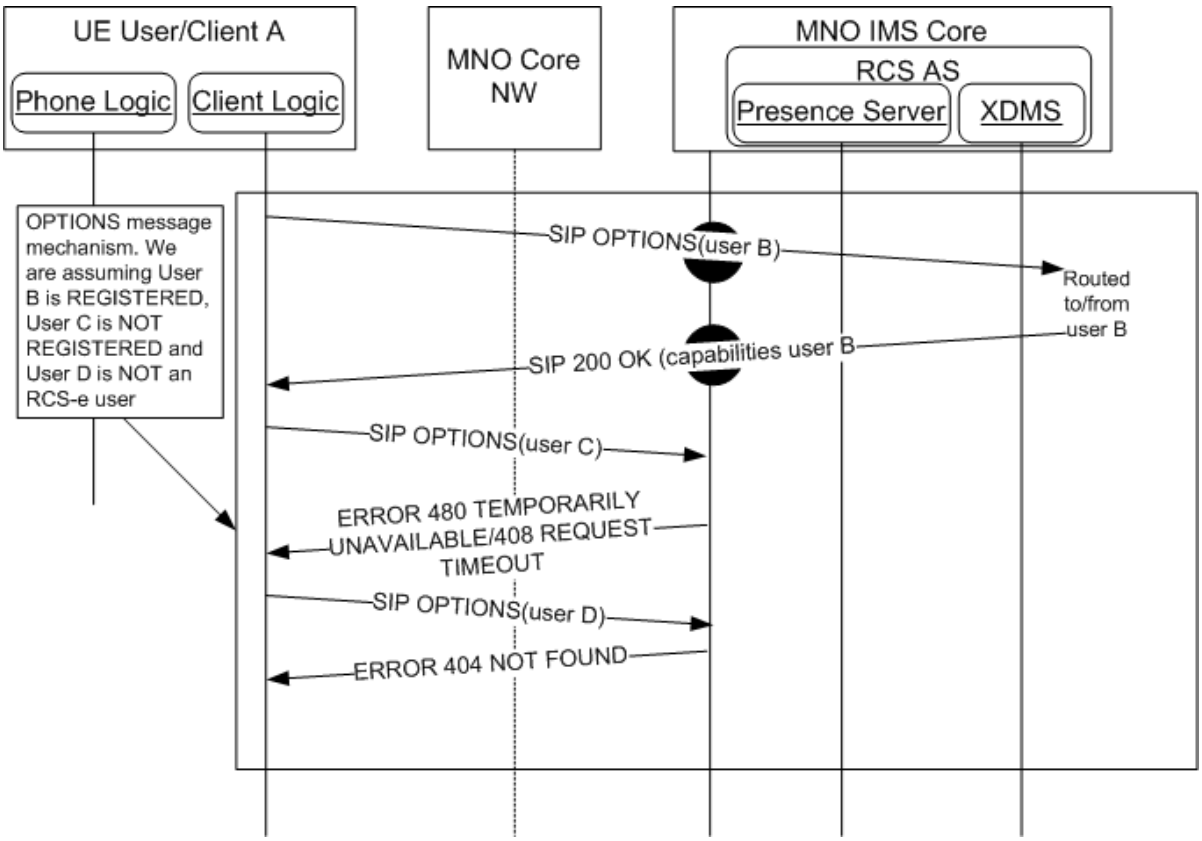

Figure 13: Capabilities discovery via SIP OPTIONS message

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 on a SIP OPTIONS exchange) related to the image and video share services during a call. This mechanism is based on the use of tags 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 9: Standard RCS Release 2 SIP OPTIONS tags

Please note that the image and video share capabilities can only be sent in SIP OPTIONS exchanges during an active call and are included only if the exchange takes place between

the users in the active call[11]. In this case as specified in [PRD-IR.74], a 200 OK response to the SIP OPTIONS request shall also contain a Session Description Protocol (SDP) body in which the available codecs are indicated. The SIP OPTIONS request itself may contain such a body. The service shall be considered as available only if such a body contains codecs that are also supported by the client.

In order to support the full service discovery functionality 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[12], 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 10: Additional tags to cover the remaining RCS-e services

- For those clients supplementing the RCS-e functionality with the *"social information via presence"*[13] functionality (that is the PRESENCE PROFILE parameter is set to 1; see Table 2), a new tag is defined to represent such features:
  - 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 2), 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.

[11] These restrictions are not fully applicable to a broadband access client. As in [RCS2-TEC-REAL], such a client shall always (and to everyone) respond on a SIP OPTIONS request indicating that it supports these services. For these services it may also accept a SIP INVITE request whatever be its origin if the user indicates that he wants to accept the session. As in [RCS2-TEC-REAL], the restrictions remain valid for the SIP OPTIONS queries and SIP INVITE requests sent by the client itself.

[12] 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.

[13] 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.

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 11: Complete SIP OPTIONS tag proposal for RCS-e

Please note that the new tags defined in this section should ONLY be 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 also the *+g.oma.sip-im* feature tag may be listed during this SIP OPTIONS exchange.

Finally, it should be taken into account that when several IMS Application Reference Identifier (IARI) tags are included in an OPTIONS request, 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 12: 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 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>"
- 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's 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 13: SIP OPTIONS tag proposal for future lines of work

2.3.1.3 SIP OPTIONS exchange optimisations

As presented in section 2.3.1, there are several scenarios where the SIP OPTIONS message is 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 (in case of very frequent GPRS bearer changes for instance).

To avoid the overhead and increase the efficiency, the client may implement a mechanism to reduce the number of requests in 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 (that is 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 (that is 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 distinguishes 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 to the discovery mechanism integration on the User Interface (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 (for instance during first time registration or when polling), it is recommended to employ a non-aggressive strategy and allow time between each exchange to:
    - Minimize potential network impact
    - Avoid any impact on the user experience (like for instance a slower UI, blockings and so on)

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 distinguishes their products from competitors.

2.3.1.5 SIP OPTIONS and multidevice support

Ultimately, the choice of supporting multiple devices for a single user 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 to the IMS CORE with various devices using the same IMS identity (that is a TEL-URI and/or a SIP-URI), the OPTIONS exchange will return incomplete information:

- The capabilities contained in the OPTIONS message refer only to the originating device (that is the originating user may be logged in with the same URI in several devices).
- The IMS Core, depending on the configuration, either sends the OPTIONS message to the device that first registered to 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 from only one of the devices of the user.

The preferred implementation for handling the OPTIONS in a multidevice environment is left to the MNO's discretion with the only requirement being, that it should not impact the terminal side (that is there will be 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 RCS-e user's registered devices and will aggregate all the capabilities returned into one OPTIONS response in case the forking is not already implemented by the IMS core network.
- Once the responses from the different devices are received, the AS will aggregate all the capabilities from the replies and send them back to the caller.
- Even if not all of 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 (a Globally Routable User agent URI (GRUU)) is covered in section 2.15.

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[14]

In addition to the SIP OPTIONS mechanism defined in section 2.3.1, a 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 (that is the *+g.3gpp.iari-ref="urn%3Aurn-7%3A3gpp-application.ims.iari.rcse.dp"* tag was included either in the OPTIONS request or in its response).

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 (storing it as a property in the address book for instance).

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
- When querying, the client polls each contact's 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 see [RCS1-TEC-REAL] section 4.2 and [RCS2-TEC-REAL] section 6.3.

[14] 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.

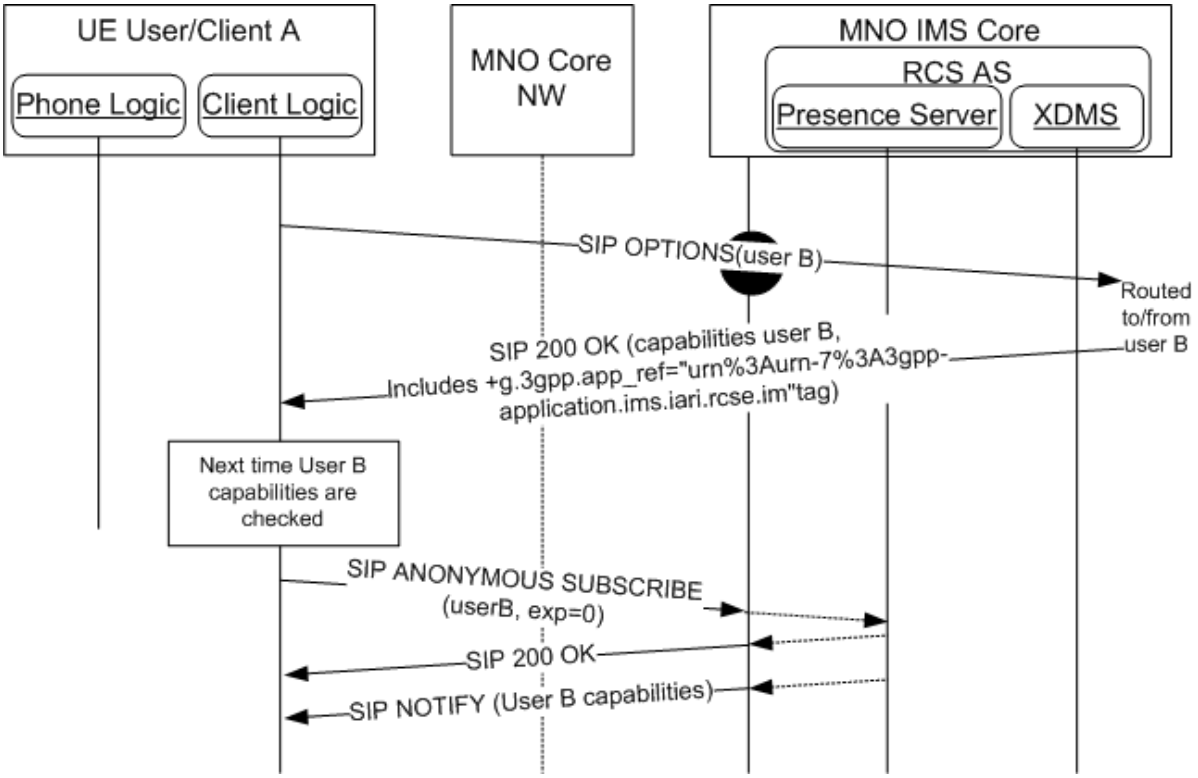

Figure 14: Capabilities discovery via PRESENCE

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 none registered contacts; in contrast, it does not include not provisioned contacts.

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

In order to keep this list up-to-date, when a new contact is added to the phonebook it is necessary to evaluate whether the contact is a RCS-e capable is 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 or not a contact is an RCS-e user, independently of whether the contact 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 include the 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 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 an 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. SIP OPTIONS request or a complete 200 OK response with the capabilities was received from the user 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[15]. 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 request with capabilities from user A, user B identifies user A as an RCS-e user.
5. If User B was identified as an RCS-e user and the response to the OPTIONS message indicates that User B is no longer an 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 enabled contacts which is maintained in the handset or device.
6. Please note there is a possibility an RCS-e user who is not within the address book 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 an RCS-e user and the cached capabilities) in case the user decides to add a new address book 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 is required to verify whether the contact is an RCS-e user and, therefore, add them to the list the terminal maintains.

[15] Please note that the response provided may depend on the network configuration. A useful 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-e. 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.

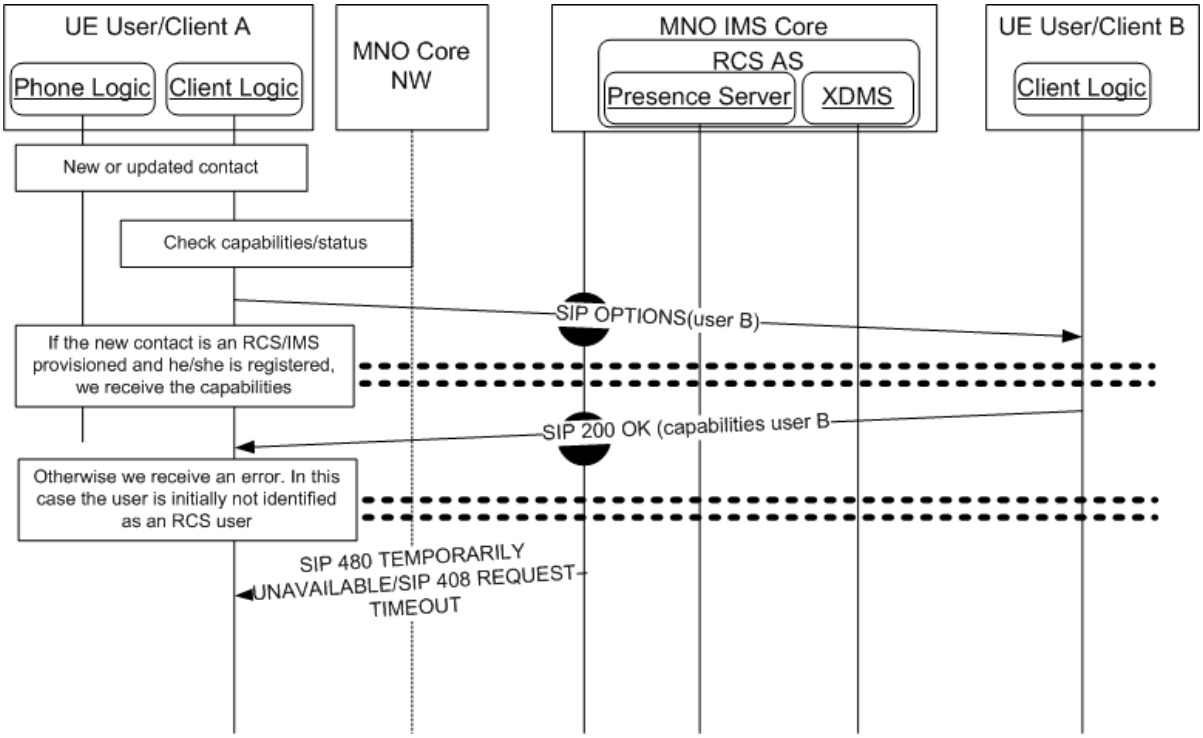

Figure 15: Adding/Editing a contact

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 PROFILE is set to 1 (see Table 2), 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.

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 on the phone. In that case the next time the RCS-e client completes the registration process, the process described in Figure 15 shall be used to verify the capabilities of those contacts.

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, this specification provides a mechanism, capability polling, consisting in polling the status/capabilities of all the contacts in the address book whose capabilities are not available (such as non-RCS-e users) or have expired (see CAPABILITY INFO EXPIRY parameter in section 2.1 Table 2 for reference).

It should be noted that the capability polling mechanism is optional and will be only performed if the related configuration settings have been provisioned (that is if the POLLING_PERIOD parameter presented in Table 2 is set to 0, this polling mechanism will not be used).

Assuming the POLLING_PERIOD is configured to be greater than 0 and after the polling timer expires, the client will use 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 2 for further reference)[16].

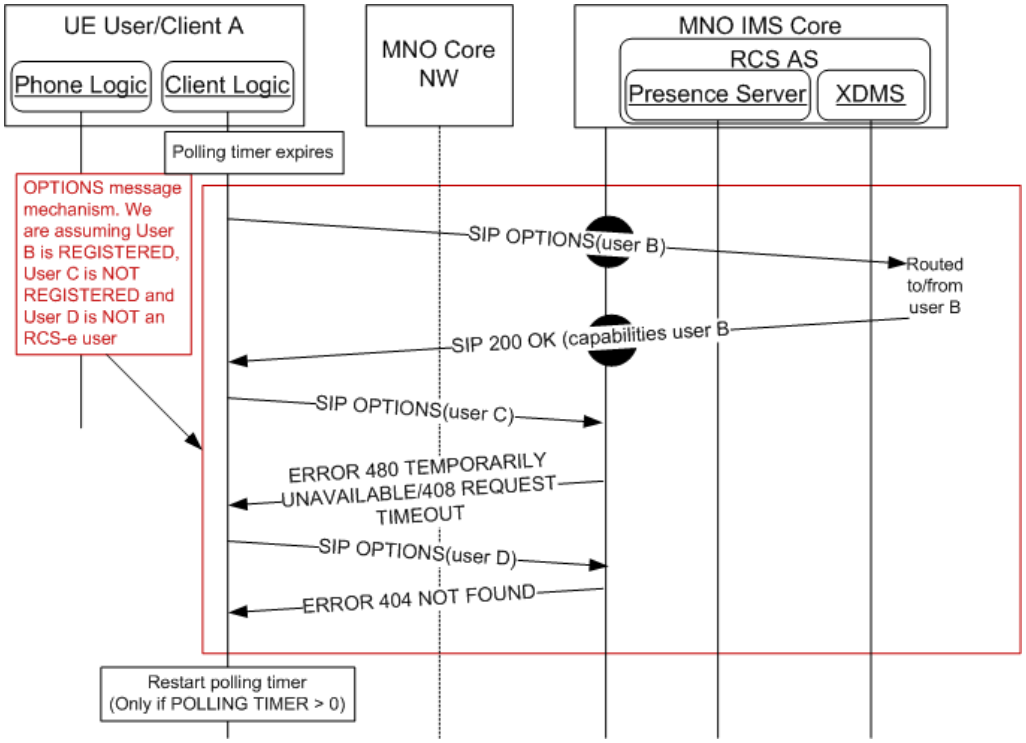

Figure 16: Capabilities polling via OPTIONS message

When PRESENCE DISCOVERY is set to 1 (see Table 2), anonymous presence SUBSCRIBE requests are used for those contacts supporting the capability discovery via presence.

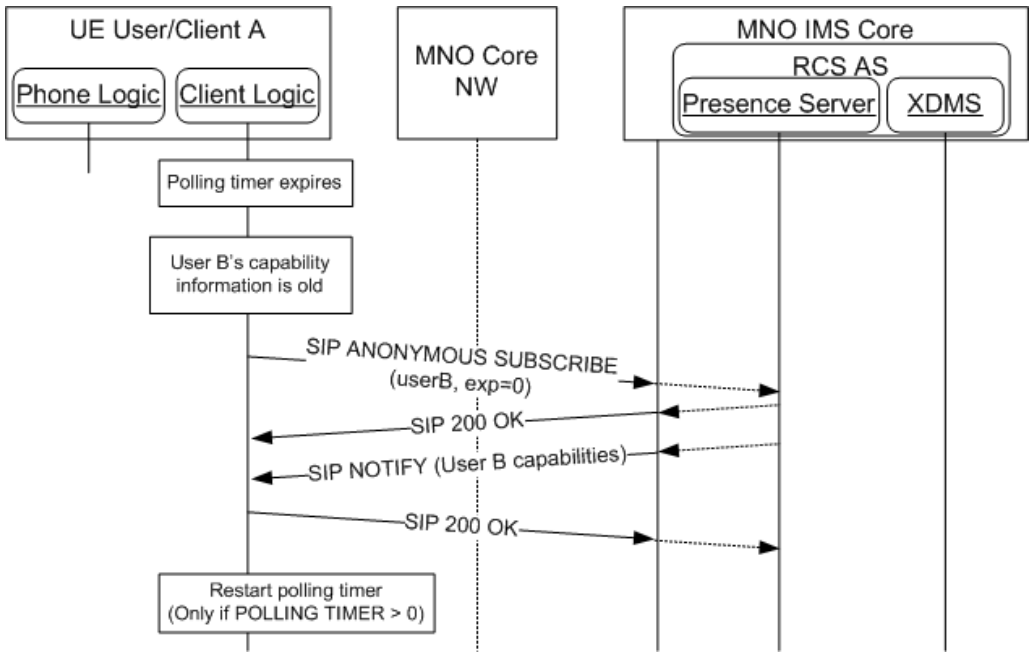

Figure 17: Capabilities polling via anonymous fetch

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

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

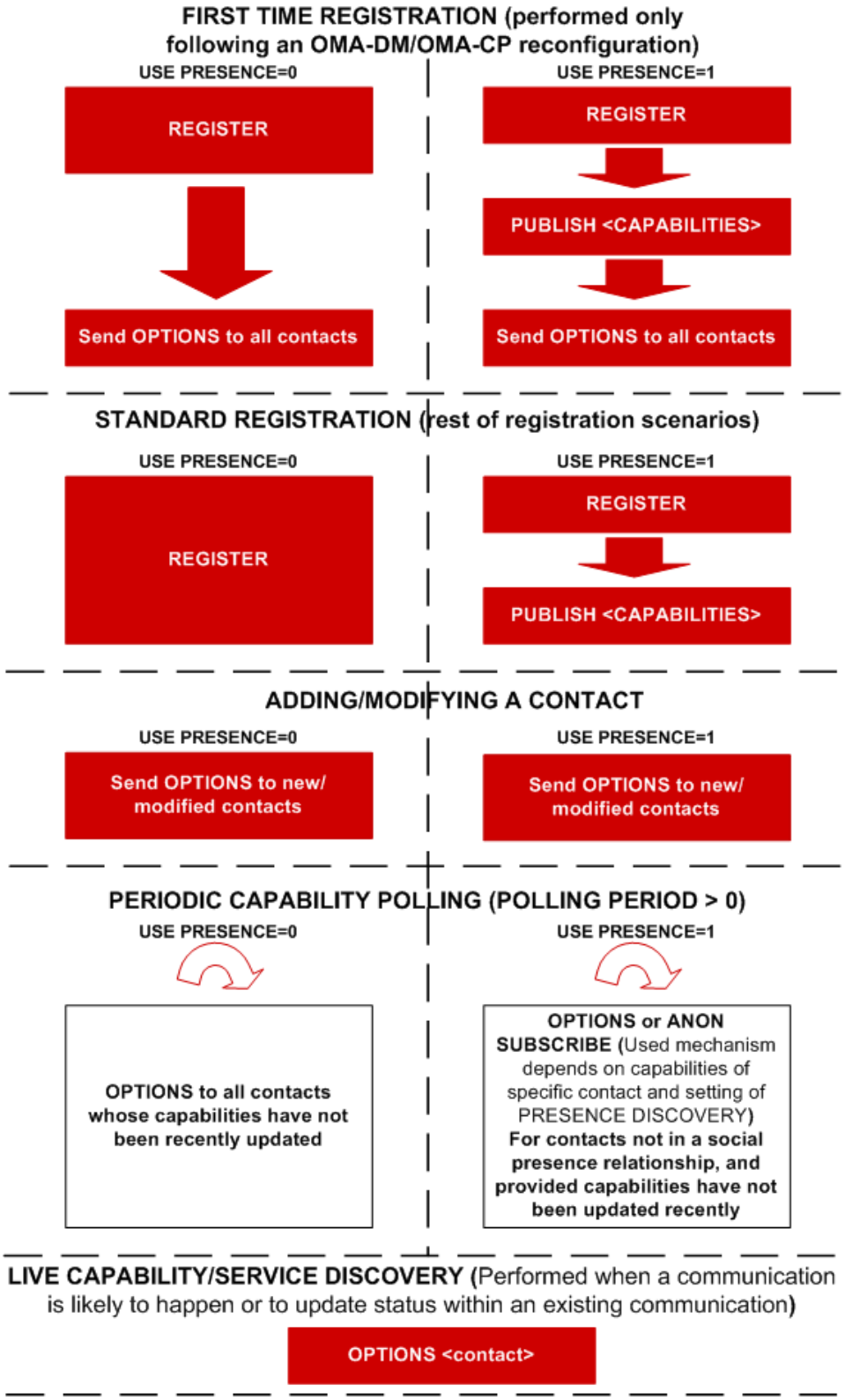

Figure 18: RCS-e capability and new user discovery mechanisms[17]

[17] The red boxes represent mandatory procedures. Meanwhile the clear boxes represent optional procedures.

2.6 Management of supplementary RCS functionality

As mentioned in the introduction, an RCS-e deployment (terminal and network) can be supplemented with the "*social information via presence*"[18] functionality (that is presence invitation and social information sharing features) included in RCS Release 2 specifications. This is not part of the RCS-e compliance however. For those clients implementing this set of functionalities, the following procedure is proposed to ensure interoperability[19]:

- Prior to being able to send an invitation to a contact (e.g. from the address book), the terminal will use the OPTIONS mechanism to determine if the other end also supports this set of features (that is 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 which 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 polling defined in section 2.5.

2.7 RCS-e and capabilities

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

1. 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)
2. 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
3. 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)
4. Connectivity status: Certain services may require a certain level of network QoS. For example, streaming video over a 2G GPRS does not provide the adequate user experience.

[18] Please note that by the term "social profile information" is 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 availability 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.

[19] 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.

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[20] 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[21] with the user the video is willing to be shared with. It is not available in multiparty calls.	N	N	One way only	Y[22]	Y[22]

Table 14: RCS-e services HW and data bearer requirements

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

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

- The phone is working adequately. In the event the terminal detects an issue that prevents 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 reaches a certain threshold. 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 points previously mentioned, the following assumptions are made for the image and video share cases:

[20] 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. This limitation is not applicable for broadband access devices for the handling of a received capability request or an incoming invitation. The restrictions fully apply for outgoing requests.

[21] 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. This limitation is not applicable for broadband access devices for the handling of a received capability request or an incoming invitation. The restrictions fully apply for outgoing requests. That is OPTIONS and INVITE requests.

[22] 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.

- Both the sharing and receiving end are in a call (that may for instance be Circuit Switched (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

Meaning 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.

Also for clarification, provided the IM and file transfer services are available (e.g. the conditions of coverage and space are met and the handset UI supports these services simultaneously with the call), also the IM and FT tags should be included with the image and video share tags (again, if applicable according to coverage and space status).

As a consequence of the information presented above, an 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. user A may support video encode and user B may support decode, but both need to be under 3G or better data coverage for the service to operate).

In addition to the information presented above, it should also be taken into account that some terminals do not support 2G DTM (dual-transfer mode). When such devices are within a 2G data coverage (meaning that no services are available during the call), the PS connection will automatically drop once they engage in 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 11), however, given the extensibility of the service framework further capabilities may be added (i.e. following the proposal given in Table 13 or agreeing on additional common services and the associated tags in future versions of this specification).

2.7.2 IM store and forward

As presented in Table 2 (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 consists of storing 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	Not 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 15 : Store and forward possible scenarios

The store and forward functionality and behaviour on the client are controlled by a couple of configuration parameters (see Table 2 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 enable. 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 15).
  - 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 15).

  As a summary: IM CAP ALWAYS ON is enabled when store and forward functionality is provided in the network, otherwise it is disabled
- Additionally and assuming IM CAP ALWAYS ON is enabled, there is a 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 (for instance after switching on the phone or regaining network 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 of whether the messages are being stored or are delivered directly 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.

To guarantee the interoperability of RCS-e clients during video share scenarios, 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

Note: In SDP exchanges this corresponds to the use of a profile-level-id set to 42f00b

Please note that including this, it is highly recommended to support also the H.263-2000 codec with profile 0 Level 45 which is mandatory in RCS Release 2 Video Share that is based on [PRD-IR.74].

Next to these mandatory codecs, 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. As specified in [RFC3264], formats must be listed in order of preference in the SDP media description. As such additional codecs providing better quality than the mandatory ones should be listed before the mandatory codecs.

Note that as for H.264 only one level and profile can be indicated in the SDP, a client supporting other H.264 encodings (like for instance the level 1.3 specified in section 2.12.2) should indicate the highest level and profile that it supports.

Should an RCS-e terminal support several profiles, the final choice should be based on the outcome of the SDP media negotiation where both ends (sender and receiver) will present the supported video formats at that particular point (that is taking into account 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 among the options presented will not impact MNO interoperability:

Protocol name	Description	Transport layer	Secure transport layer/protocol
Session initiation protocol (SIP)	Client-IMS core signalling protocol	User Datagram Protocol (UDP) over IP or Transmission Control Protocol (TCP) over IP	SIP over Transport Layer Security (TLS) or IP Security (IPsec)
Message 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) (see [RFC3711]) or IPsec

Table 16: 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 Network Address Translation (NAT) traversal in the different protocols involved in RCS-e, the following considerations shall be taken into account:

- Regarding the SIP protocol:
  - Carriage Return Line Feed (CRLF) keep-alive [RFC6223] support is MANDATORY when SIP/TCP or SIP/TLS is used by the RCS-e client.
  - Simple Traversal of UDP through NATs (STUN) keep-alive [RFC6223] support is RECOMMENDED when SIP/UDP is used by the RCS-e client as it allows network capacity optimization.
  - An RCS-e client using SIP/UDP and not supporting [RFC6223]:

    - SHALL support symmetric signalling (That is the IP and port combination used to send SIP messages is the same as the one used to receive SIP messages).
    - SHALL perform TCP switchover for large SIP messages.
- For handling MSRP sessions, the RCS-e client SHALL support:
    - [RFC6135]: The Alternative Connection Model for the Message Session Relay Protocol (MSRP)
    - [IETF-DRAFT-SIMPLE-MSRP-SESSMATCH10]
- 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 IPsec based protocols to secure the signalling and media exchanges is RECOMMENDED particularly for those scenarios where the data is 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 the way in which interoperability between RCS-e clients and MNOs can be achieved is left for further studies.

Finally, please note that to ensure interoperability of devices across different MNO networks (that is 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).

2.8.1 RTP and NAT traversal

As mentioned previously, an 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 scarcity 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 keep-alive (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 (that is use the same port number for sending and receiving packets) as defined in [RFC4961] 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.

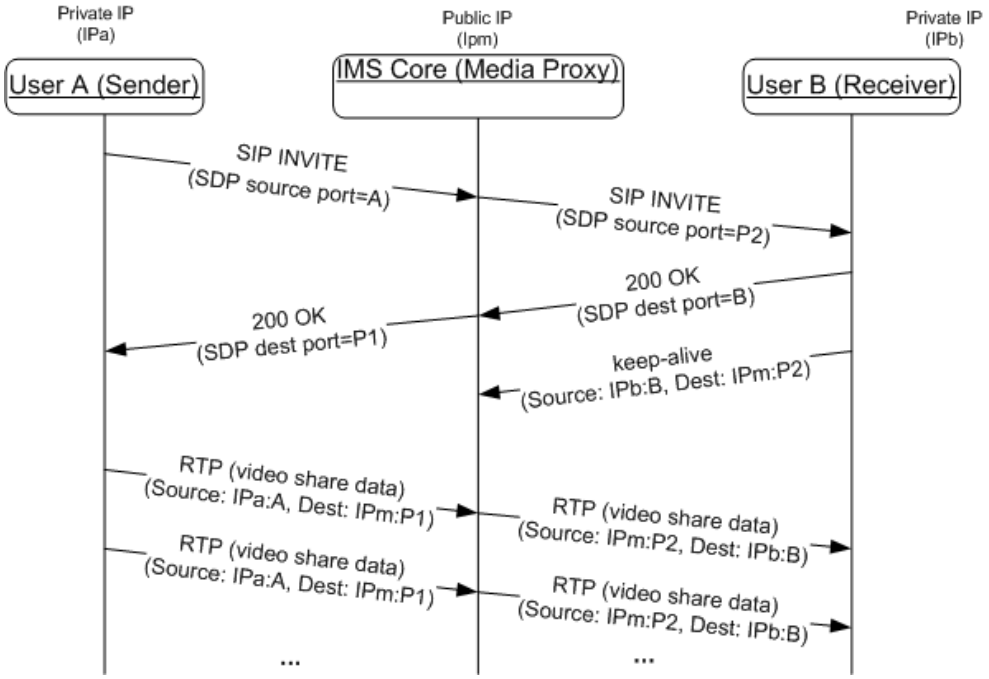

Figure 19: RTP symmetric media path establishment

- SHALL use the RTP Control Protocol (RTCP)
  The symmetric media procedure described for the RTP protocol is, in general, applicable to any UDP stream. As the usage of RTCP is also mandatory, an analogous mechanism shall be implemented in order to prevent any RTCP stream from being blocked. Therefore, the symmetric media procedure described in this section for RTP is also applicable to RTCP and shall be employed (that is a dummy packet is sent by the receiver to secure the RTP flow and a second one is used to secure RTCP flow). Also the sender handset/client shall send a dummy packet when the session is established to secure the RTCP flow on their side and ensure the reception of any RTCP RR sent by the receiving side. The dummy packet format recommended for establishing the RTCP flow is an empty RTCP RR (receiver report) or empty RTCP SR (sender report).

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

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 in that case be provisioned with only the appropriate SIP URI parameter as seen in Table 1, leaving the TEL-URI parameter empty.

Consequently, an RCS-e enabled terminal's 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 exception to this rule is when the request includes a Referred-By header, in which case 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 URIs (for example tel:+1234578901, or tel:2345678901;phone-context=<phonecontextvalue>)
- SIP URIs with a "user=phone" parameter, the contact's phone number will be provided in the user part (for example 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 [3GPP TS 24.229]) for 1-to-1 communication, as well as 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 [RFC3966] and SIP-URI (for example sip:+12345678901@domain;user=phone) with the user parameter set to "phone" as defined in [RFC3261]. 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 (the 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 value set as defined in [3GPP TS 24.229] 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 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 they can receive more information than just the MSISDN in case the originating user is not in the receiver's Address Book. This case will probably very common in group chats.

This alias information will be set in the From header of the SIP request as the display name and also in the Common Profile for Instant Messaging (CPIM) From header as the formal name. 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 while 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 major handset platforms only support one active APN at the time. To overcome these difficulties and to allow the final user to have greater control over the behaviour of the handset regarding data traffic, RCS-e handsets can be configured with two different APNs:

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

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 17: 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 2.

This approach can be used not only for roaming but also to protect the user from unexpected charges. Therefore, a MNO can decide to display this setting permanently (covering home network scenarios). The behaviour of whether or not to show the setting permanently is controlled by the configuration parameter ENABLE RCS-E SWITCH (see Table 2). If enabled, the setting is permanent. If disabled, the setting is only proposed during roaming.

Finally note that the use of 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 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 once 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 18: 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 18) individually to each of the following connections:

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

Regarding 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 ("always connect" for the "home" connections and "always ask" for the "roaming" connections)

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

2.11 Privacy considerations

Currently, (that is when this version of the specification is published), work to establish a set of guidelines to address the user privacy issues associated to RCS-e is not completed yet. This section is 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 also be used for privacy

purposes. This refers particularly to making the RCS-e switch permanently accessible to the user (that is, not only use it for roaming cases) via the device configuration by setting the ENABLE RCS-E SWITCH configuration parameter to 1 (see Table 2 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 Long Term Evolution (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 yet , therefore, this section only contains references to those areas where that work has already been completed allowing future versions of the specification to include the elements remaining for a complete integration.

2.12.1 LTE and Voice over LTE

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

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

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

2.12.2 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.

As specified in [PRD-IR.74], an RCS-e device shall support the H.264 video codec with baseline profile and level 1.3[23] in order to provide 384/768 kilobits per second (kbps) video over an LTE bearer or over a similar high bitrate bearer. Please note that this is an addition to the mandatory formats specified in section 2.7.3.

The assumption for the use of a high bitrate bearer is that the connectivity and video parts of both terminals support it and have LTE or another 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 Other Access Networks

Next to the Mobile PS access networks that are assumed in sections like 2.10 and 2.12, like RCS Release 2 RCS-e can be used over any IP access over which the MNO's IMS core and application servers can be reached, provided that it offers sufficient bandwidth and an acceptable latency. As specified in [RCS2-TEC-REAL] this can be both trusted and untrusted networks where for the latter more elaborate security measures may be needed to guarantee privacy and authenticity of the signalling and media traffic. The specifics of the deployment environment will determine how that can be achieved.

2.14 End User Confirmation Requests

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

[23] The support for this level of H.264 encoded content is indicated in the SDP as profile-level-id=42C00D

there has not been a standardised mechanism that allows the MNO to directly ask the End User in this scenario.

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 asking the user to confirm or decline the proposed request.

The end user confirmation request is implemented using an SIP MESSAGE[24] method containing a XML payload type “application/end-user-confirmation-request+xml” that will be sent by the MNO serving the End User to his RCS-e handset/client. A specific device can be addressed using GRUU (see section 2.15). If the user is required to answer from every device, the devices should be addressed individually using GRUU.

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 2 and extract the request information from the XML payload body. A dialog or notification will be displayed to the End User (UX dependent) showing the confirmation request and related information.

The End User confirmation response will be encapsulated in an XML body with a payload type “application/end-user-confirmation-response+xml” and returned back to the MNO 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:
    1. *Volatile*, the answer shall be returned inside of a new SIP MESSAGE request. The request may time out without end user input, in which case it will be discarded.
    2. *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 than 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 clients shall check the language attribute and display the text data of the element that matches the current language used by the user. If there is no language matching the users, the first node of Subject and Text shall be used.

If the type of 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

[24] 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 traverse 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 by the MNO in the initial confirmation request and/or ack using content-indirection as specified in [RFC4483]. Therefore, this shall be supported by the handsets/clients.

encapsulated in an XML body with a payload type “application/end-user-confirmation-ack+xml” and returned in a separate SIP MESSAGE. If the acknowledgement refers to the message which is currently displayed, it shall be discarded even if no answer was sent. This allows sending a message to all active devices of a user also in case a response from a single device is sufficient. For that reason it is also possible to send acknowledgements without Subject or textual content.

The following table specifies the XML Schema Definition (XSD) 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"
        xmlns:xml=”http://www.w3.org/XML/1998/namespace”
        elementFormDefault="qualified">
        <xs:import namespace=http://www.w3.org/2001/XMLSchema
                schemaLocation="http://www.w3.org/2009/01/xml.xsd"/>
        <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" use="optional"/>
                </xs:complexType>
      </xs:element>
      <xs:element name="Subject">
                <xs:complexType>
                        <xs:simpleContent>
                                <xs:extension base=”xs:string”>
                                        <xs:attribute ref="xml:lang"/>
                                </xs:extension>
                        </xs:simpleContent>
                </xs:complexType>
      </xs:element>
      <xs:element name="Text">
                <xs:complexType>
                        <xs:simpleContent>
                                <xs:extension base=”xs:string”>
                                        <xs:attribute ref="xml:lang"/>
                                </xs:extension>
                        </xs:simpleContent>
                </xs:complexType>
        </xs:element>
</xs:schema>
```

Table 19: 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 20: End User Confirmation Response XSD

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

- **Id**: Unique identifier of the original request. If the ID matches the ID of the currently shown message, this message shall be discarded even if no answer was sent from the receiving device.
- **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"
        xmlns:xml=”http://www.w3.org/XML/1998/namespace”
        elementFormDefault="qualified">
        <xs:import namespace=http://www.w3.org/2001/XMLSchema
                schemaLocation="http://www.w3.org/2009/01/xml.xsd"/>
        <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:simpleContent>
                                <xs:extension base=”xs:string”>
                                        <xs:attribute ref="xml:lang"/>
                                </xs:extension>
                        </xs:simpleContent>
                </xs:complexType>
        </xs:element>
        <xs:element name="Text">
                <xs:complexType>
                        <xs:simpleContent>
                                <xs:extension base=”xs:string”>
                                        <xs:attribute ref="xml:lang"/>
                                </xs:extension>
                        </xs:simpleContent>
                </xs:complexType>
        </xs:element>
</xs:schema>
```

Table 21: End User Confirmation Acknowledgement XSD

2.14.1 Example UC1: Accepting terms and conditions

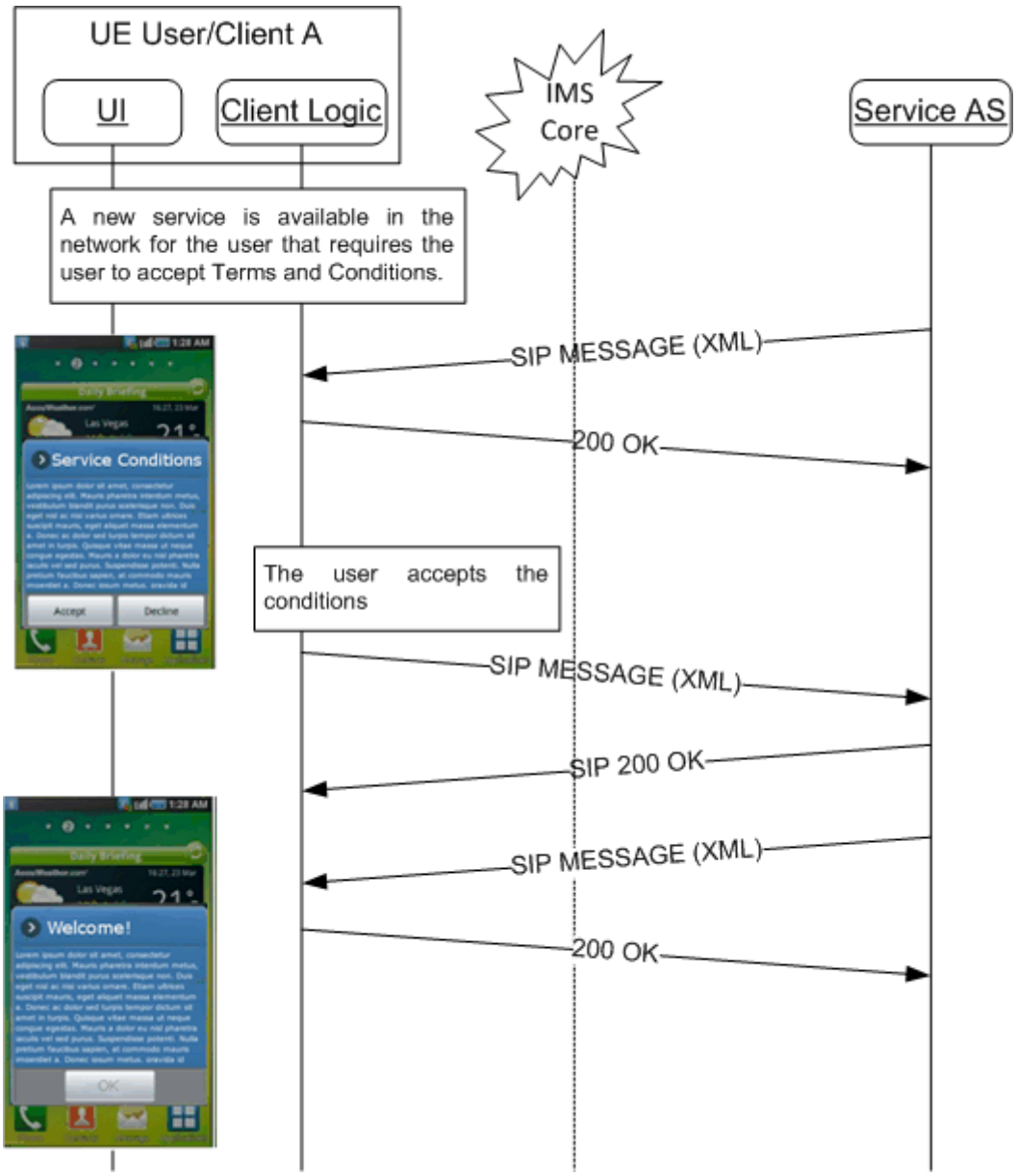

Figure 20: Terms and Condition UC example

2.14.2 Example UC2: Accepting Extra Charges

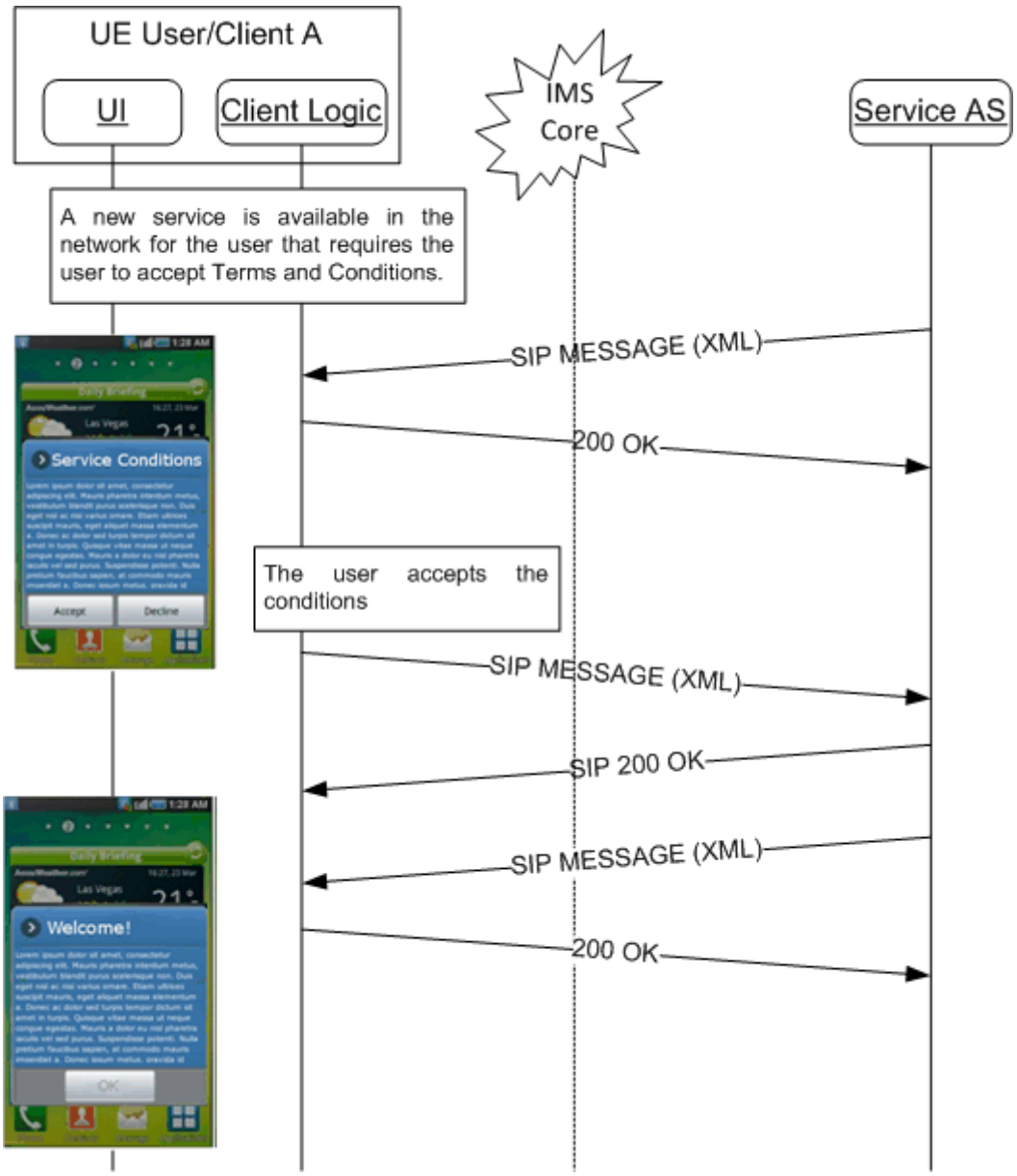

Figure 21: Extra Charge UC example

2.15 GRUU and multidevice support

RCS-e clients and terminals SHALL support GRUU as specified in [RFC5627]. 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. As network support for GRUU is not mandatory, a configuration parameter DEVICE ID is used for the RCS-e client to know how to set the sip.instance value. If not provided or set to 0, the sip.instance SHALL be the IMEI value. If set to 1, then to avoid potential privacy issues, IMEI SHALL NOT be used as the device-id value of *sip.instance* instead this device-id value either must be an UUID (generated by the handset as specified in [RFC4122]) or must be a hashed value of the IMEI and in all cases, must not be modified

over time. A client that has no access to the IMEI shall provide a UUID. If the REGISTER response is a 2xx and the network supports GRUU, 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 MNOs 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 where the GRUU will be included in the Contact Header.

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 simplicity and because the long-term standard [RFC5627] 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*).

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 (that is the receiver may want to clarify why the sender is sharing that file). The chat session will not 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 an 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 the one-to-one or, optionally, also the group chat (selecting/inviting more than one user). The user can also access the chat history and continue a previous chat.
- File browser, media gallery and camera application: The user can access the file transfer service. Note that the file transfer is combined with chat at the UX layer on the receiver to create a communication context (the receiver may want to clarify for instance why the sender is sharing that file). Even though once the incoming file is accepted the transfer is presented in a chat window on the receiver side, the chat session will not begin until the receiver sends the first message.
- Chat window: It is possible to add new contacts to an existing chat session. In addition to this, file transfers are also available in a one-to-one chat. Even though from the protocol perspective, it is necessary to use a new SIP invitation and MSRP transfer (that is the file transfer occurs in a separate MSRP session, 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 in the UI.
- Call screen: Video and image transfer (live video, stored video or picture). Please note that the communication context is already established so it is not necessary to implement any additional actions in the UI.

Finally, it should be noted that a precondition to provide access to the RCS-e functionality is that all the mandatory parameters described in section 2.1 (Table 2) must be correctly configured. Where some of the parameters are not configured or configured with an unexpected value, the RCS-e functionality should be disabled and not be presented nor accessible to the user (that is 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 by extension 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

The following sections describe the relevant chat message flows and reference user experiences (UX). Please note that the following assumptions have been made:

- For simplicity, the internal mobile network interactions are omitted in the diagrams shown 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 an RCS-e contact which is registered. Please note the capabilities are only updated in 1-to-1 chats. In group chat sessions, there are no other services available and the ultimate responsibility to maintain and report the status of the session lies at the IM application server.

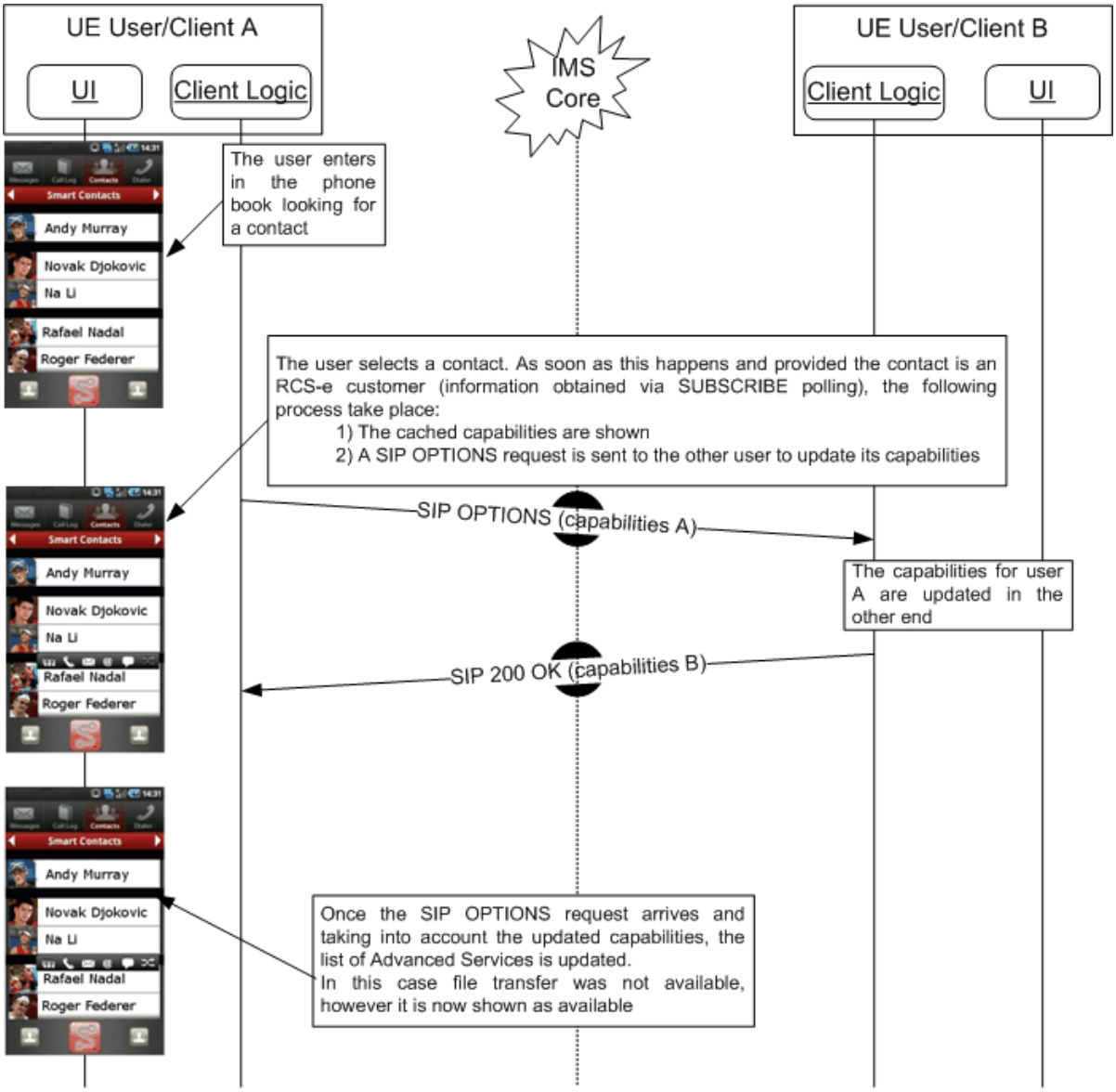

Figure 22: Address book: Capabilities update

If User B is either not an RCS-e user or 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, User A's client will assume that no services are available to communicate with User B[25].

[25] It should be noted that in this case if IM CAP ALWAYS ON (see Table 2) is enabled, the IM/chat should still be reported to the user as available even if the other end/user is not registered.

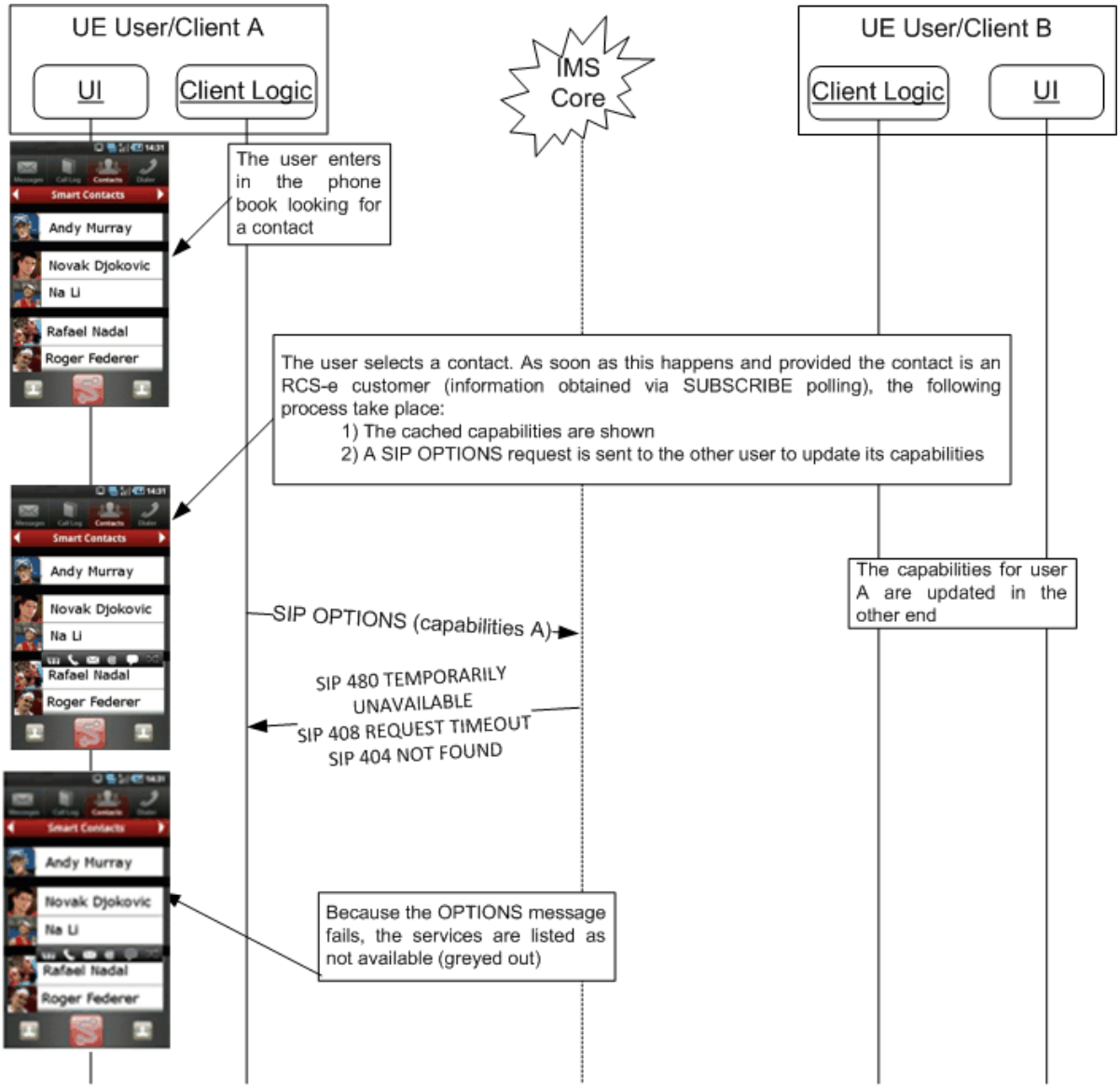

Figure 23: Address book: Capabilities update (II)

3.2 IM/chat service

The IM service enables users to exchange messages between one or more users instantly. 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] as a specification basis. As new optional features are introduced (such as store and forward and "displayed" notifications), some adjustments, clarifications or modifications need to be brought to [RCS2-OMA-SIMPLE-ENDORS]. The delta between RCS Release 2 IM and RCS-e IM is 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 comes online again (i.e. store and forward).

- "Displayed" message disposition
  This new disposition allows the sender of a message to be notified when a 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 of whether the MSRP session associated to a chat is established or not. When delivering these notifications outside of a MSRP session, SIP MESSAGE is used instead as described later in this section.
- Local Black List
  The terminal/Client shall support a locally stored IM Black List. Basic guidance on the use of this list 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.
- 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 new features, some of the existing 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 transfer of files while a chat is taking place shall be performed in a separate session (note that this is only at protocol level, from the user experience perspective, the user should be able to transfer files while in chat), irrespective of the type or nature of the file.
- 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 to signal an explicit rejection of the session by the user of a 1-to-1 session, instead the terminating side will ignore the invitation and wait for the request to expire. Note that as described in section 3.2.4.1 the terminal will reject the invitation with a 486 Busy Here error response in case a second invite request is received from the same user.

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]
  RCS-e relies on the support of Instant Message Disposition Notification (IMDN) as defined in [RFC5438] to request and forward dispositions of all the exchanged messages.
- Device identification using the mechanisms described in section 2.15.
- 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
  - When an IM session is initiated by a Client, the SIP INVITE should still convey the message in the "subject" Header. In addition in RCS-e, the message is replicated in a CPIM/IMDN[2627] wrapper including the DateTime, Message-ID and Disposition-Notification header fields. The deviceID shall be carried using the mechanisms described in section 2.15.
  - The client is able to identify that an IM-AS is pushing stored messages because the invite originated from the IM-AS is for a 1-to-1 chat and contains a Referred-by header (consistent with the explanation provided in section 2.9.1). Using this mechanism the handset/client implementation is able to differentiate a session for delivering deferred messages and will only send notifications back. If the user replies with a new message, 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-Identity header is set to a known value (*rcse-standfw@<domain>*) and a Referred-By header is included with the identity of the user that sent the notifications.
  - GRUU (GRUU public identities, pub-gruu, as presented in section 2.15) 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>*)[28].
  - Contribution-ID and Session-Replaces headers: As described in [IMCR090017], RCS-e requires that each 1-to-1 chat session invitation generated from the client shall include a Contribution-ID and when client A extends a 1-to-1 chat session with client B to a group chat, the value of the Contribution-ID used for the 1-to-1 chat session shall be included in the Session-Replaces header added to the URI-list entry for client B in order for client B to tear down the 1to-1 chat session. If a client receiving a chat session invitation with a Session-Replaces header does not find a corresponding chat session with the value in the Session-Replaces header, it shall respond with a 481 Call/Transaction Does Not Exist. The Contribution-ID and Session-Replaces headers and the procedures summarized here are defined in [IMCR090017]. Note that the procedures in [IMCR090017] are used instead of the Replaces header as in [RCS2-OMA-SIMPLE-ENDORS], with the clarification that the format of the original participant should be with “Session-Replaces=”, (i.e., <entry uri=”bob@biloxi.com:method=INVITE?Session-Replaces=abcdef-1234-5678-90ab-cdef01234567f” />)
    Note: the value used for the Contribution-ID shall not contain any information that allows to identify the client that generated it (such as an IP Address).The IM-AS should set the CPIM DateTime header in the chat messages it receives in an INVITE request if no valid date/time setting is included yet. The IM-AS may set the IMDN DateTime element in notifications in case no valid element is included yet.

---

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

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

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

- SIP MESSAGE
  RCS-e relies on SIP MESSAGE requests to carry notifications (delivery and display) of messages sent prior to the establishment of a media session or when a previously established session has timed out. Again, the SIP MESSAGE shall carry a CPIM/IMDN[27] wrapper including the DateTime, Message-ID and 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 be transported following the mechanisms described in section 2.15.

  The Accept-Contact header of the SIP MESSAGE used for IMDN shall carry the +g.oma.sip-im feature tag[29].
  The use of SIP MESSAGE for Pager Mode messages is still not supported (consistently with RCS Release 2).
- MSRP SEND
  In RCS-e, all messages (IM) are conveyed in CPIM/IMDN[27] wrappers, which are strictly forbidden in RCS Release 2.
  When applicable, these MSRP SEND requests with CPIM/IMDN[27] wrappers are used by the sender to request IMDN 'delivered' and 'displayed' notifications and by the receiver to provide the same IMDN 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'.
  The IM-AS should set the CPIM DateTime header in the chat messages it receives if no valid date/time setting is included yet. The IM-AS may set the IMDN DateTime element in notifications in case no valid element is included yet.
  If present, a client may use these timestamps to indicate to the user when a message or notification was sent. If the element is not provided the client should assume that the message was delivered immediately.

Finally, in order to support the use of aliases, the limitation added in [RCS2-OMA-SIMPLE-ENDORS] for the use of a display-name is removed in RCS-e. 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. In more detail, the CPIM/IMDN[27] wrapper should carry a 'delivered' notification as described in [RFC5438] section 7.2.1.1 including the same message-id contained in the original message .
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[27] wrapper with a 'delivered' notification as described in [RFC5438] section 7.2.1.1 and previously stated in this section. Again, the original message CPIM/IMDN[27] message-id shall be carried to identify the message this notification is associated to.

[29] This ensures that initial filter criteria already in place in GSMA RCS Release 1, 2 or 3 environments will route these SIP MESSAGEs to the OMA SIMPLE IM server.

The sender's 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 the need for a pop-up or information message when the user is outside of the IM application.

When the recipient of a 'delivery' notification is not available and in those cases where an IM-AS with enabled Store and Forward functionality is available (either at the sender's or at the receiver's side), the IM-AS should be able to store and forward this notification independently of whether they are delivered within a MSRP session or outside of such a session 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 should ensure that they are not forwarded to the current device in the IM session if that is not the device that sent the message which has been delivered. In this case, the delivery notifications should be sent to the device that sent the original message.

The Request-URI of the SIP MESSAGE requests carrying a delivery notification shall be composed based on the SIP INVITE request carrying the message for which the notification is sent or if that message was received within a session, on the SIP INVITE request or 200 OK response received during the setup of that session. The Request-URI shall be composed as follows:

- The client shall use as Request-URI either the URI in the P-Asserted-Identity header of the SIP INVITE request or 200 OK response or, if present in the SIP INVITE request, the URI in the Referred-By header;
- If the SIP INVITE request or 200 OK response contains a pub-gruu in the Contact header, the client shall add the pub-gruu from the Contact header in a "gr=" parameter to the Request-URI;
- If the SIP INVITE request or 200 OK response contains no pub-gruu in the Contact header, but includes a sip.instance parameter, the client shall include the sip.instance parameter and its value in the SIP MESSAGE request as a separate Accept-Contact header along with the require;explicit tags.

An IM Server setting up a session to deliver stored notifications shall compose the Request-URI of the INVITE request in a similar way:

- The IM Server shall set the Request-URI to the identity of the recipient;
- If a pub-gruu is available as the device-id, the "gr=" parameter containing the pub-gruu shall be added to the Request-URI;
- If no pub-gruu is available but a sip.instance parameter is available, the sip.instance parameter and its value shall be included in the SIP INVITE request as a separate Accept-Contact header along with the require;explicit tags.

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[27] wrapper carrying a 'displayed' notification as described in [RFC5438] (section 7.2.1.2). Again the original message CPIM/IMDN[27] Message-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. In more detail, the CPIM/IMDN[27] wrapper should carry a 'displayed' notification as described in [RFC5438] section 7.2.1.1 including the same msg-ID contained in the original message.

The sender's client side shall support both scenarios, process the display notification and display this information to the user. Regarding the display 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 display notification is optional meaning the user (receiver of the original message) shall have access to a configuration parameter to enable or disable this notification via UI (i.e. a user can disable sending back display notifications to the sender).

When the recipient of a 'display' notification is not available and in those cases where an IM-AS with enabled Store and Forward functionality is available (either at the sender's or at receiver's side), 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 display notifications start to arrive for stored messages, the IM server should ensure that they are not forwarded to the current device in the IM session if that is not the device that sent the message which has been displayed. In that case the display notifications will be sent to the device that sent the original message.

The Request-URI and Accept-Contact headers of a SIP MESSAGE request carrying a display notification shall be composed in the same way as a delivery notification as described in chapter 3.2.2.3. Since the SIP INVITE request for pushing stored notifications is not specific to delivery notifications, the same procedures as in chapter 3.2.2.3 for the Request-URI and Accept-Contact headers of that request also apply.

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 shown in the following sections.
- Each MNO MAY deploy an IM Server (that is the use of an IM server is optional in RCS-e deployments), to manage all messages from its customers.
- Prior to the chat, the user accessed their address book or IM/chat application to start the communication. As described previously, while these actions are performed an OPTIONS request is sent to double-check the available capabilities. In the following diagrams it is assumed that this exchange (OPTIONS request and response) has already taken place, and therefore, both ends are aware of the capabilities and the available RCS-e services. If that is not the case, the OPTIONS request should be sent at the same time the chat is being setup.
- All the IM service exchanges presented in this document follow the GSMA RCS Release 2 specification [RCS2-OMA-SIMPLE-ENDORS] 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] and adapted to the context of session-mode instant messaging.
    - The terminal UI must be implemented in such 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 at which the message was originally sent shall be also presented.

- Procedures, based on the IMDN disposition 'display' have been introduced at the sender side to request 'display' notifications and at the receiver side to provide 'display' 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 combining multidevice support with Store and Forward mode have been introduced to ensure consistent delivery of deferred delivered and display 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 towards a user of a MNO that doesn't support store and forward, the messages can be stored in the sender's IM server.

From the UX experience perspective, 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.

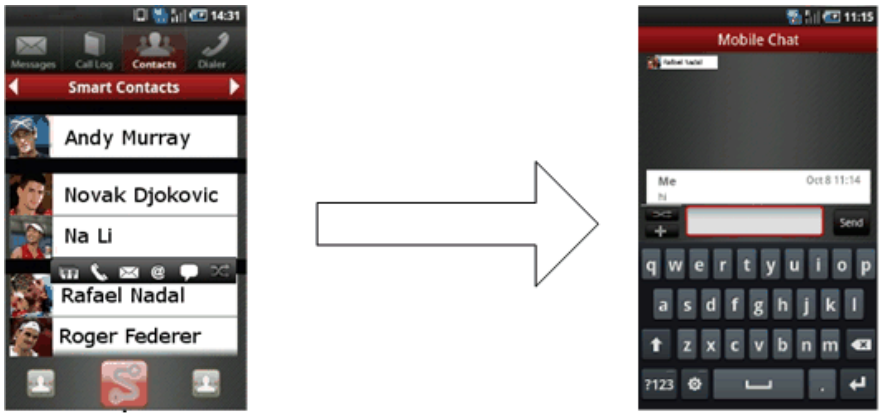

Figure 24: Reference UX for accessing chat from address book/call-log

- 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.

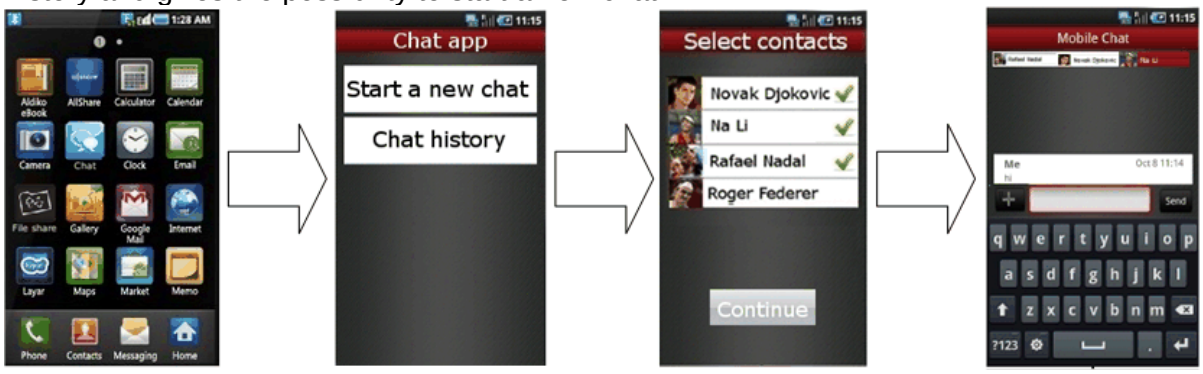

Figure 25: Reference UX for starting a chat from the IM/chat application

Once the IM/chat application is opened, the user will be presented with the complete list of RCS-e contacts with IM capability. Whether or not contacts which are currently not registered will be shown depends 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 group chat sessions:

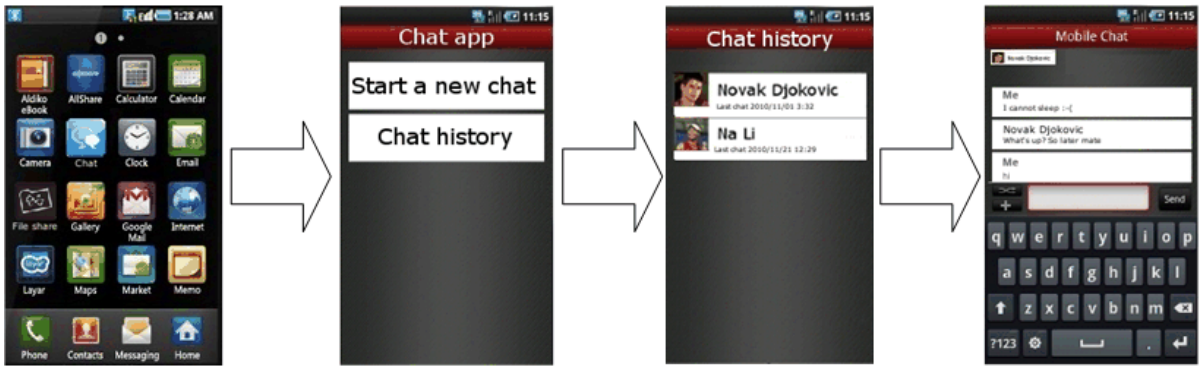

Figure 26: Reference UX for starting chat from the IM/chat application history

- File transfer (receiver): When transferring a file and with the aim of establishing a communication context for the transfer (the receiver may want to know for instance why the sender is sharing that file), 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 this file transfer 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 27: Reference UX for 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

An 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 the SMS service could be offered as a 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 the 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] except that the message should be duplicated in a

CPIM/IMDN[27] wrapper including the headers requesting an IMDN according to the rules and procedures of [RFC5438] (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 (for instance 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 the case of delivery failure, and there is no requirement that an IMDN will be generated, since there is no message.

When device B receives an IM session invitation, it will automatically send a SIP 180 answer toward A (if a spam filter or a black list is implemented on the device and user A is in the black list, 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].

On the user B side, a notification (UI dependent) will be displayed on the device to inform the user 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, that is 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 not more than one outstanding INVITE from one user. The IMDN for 'delivered' status is requested and sent similarly to the first session invitation. On user B's side, a notification may be displayed for each received message (UI dependent).

3.2.4.2 Answering a chat

When user 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. The client returns the 200 OK signalling the initiation on the remaining procedures to establish the chat when the receiver reacts to the notification by 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].
3. The 200 OK is sent when the receiver sends a message. Please note that in this case the receivers' message will not generate an invite but will be buffered in the client until the MSRP session is successfully established.

Please note that the behaviour is configured via the IM SESSION START parameter as presented in Table 2 and formally defined in ANNEX A section A.2.4.

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

The rules and procedures of [RCS2-OMA-SIMPLE-ENDORS] are followed to handle the case where multiple IM sessions from A are pending on B's side. that is 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 a IMDN Disposition-Notification header requesting a 'display' notification, B generates an MSRP SEND request toward A that contains the IMDN 'display' 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] except that, for the received MSRP SEND requests containing an IMDN 'displayed' and ‘delivered’ request, the receiving device must generate an MSRP SEND request containing the IMDN status, when the user message is delivered or displayed.

3.2.4.4 Display and local storage

All the messages will be stored in the device, together with the time indication and an appropriate indication of that part of the message exchange that each user sent.

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 the storage limit is reached, deletion should occur on a first in/first out (FIFO) queue policy. It is open to OEM criteria how to implement other opt-in deletion mechanisms (such as ask always, delete always, delete any conversation/message from specific contacts and so on).

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 dependent) so the user is aware of the new message and, may return to the chat composing window to answer it.

Also, the user could decide to return 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 is involved in the chat session.

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. That user’s UI will then display an indication in the chat composing window to indicate it (UI dependent).

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 generated and processed according to the rules and procedure of [RCS2-OMA-SIMPLE-ENDORS]. 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 the IM session associated with an established chat. This can be achieved 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. At protocol level, the session is terminated though. 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 Session.

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 that they 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 the TCP connection is lost, the client should resend it in a new chat session once reregistered.

In temporary interruption cases, for example the mobile phone is within network coverage, 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 an older chat

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

The device will then display the previously stored conversations with that contact preceding the current active one. If any displayed notifications still need to be generated , they will be sent towards the sender outside of a session using SIP MESSAGE as described in section 3.2.2.4, since there is no session established with the sender. As specified in section 3.2.2.4 in a multidevice scenario, if there is an active session but that session is with a device of the sender other than the one that was used to send the message to which this notification relates, the IM server will ensure that these notifications are delivered outside of that session.

3.2.4.11 Store and Forward Mode

The store and forward functionality is optional and it is up to each MNO to deploy it (that is to deploy an IM Server supporting store and forward as the client side implementation is mandatory).

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

1. Sender and receiver are on networks with an IM Server: In this case the receiver's side IM Server has the responsibility to store IMs which are not delivered. The sender's side IM Server has the responsibility of storing the delivered/displayed notifications in case the sender is no longer online
2. Only the sender is on a network with an IM Server: The sender's side IM Server has all the responsibility to store IM and/or delivered/displayed notifications if they cannot be delivered. As it is in the sender's network, the IM Server will not have information on when the destination is online. Therefore a retry mechanism will be employed.
3. Only the destination is on a network with an IM Server: The receiver's side IM Server has all the responsibility to store IM and/or delivered/displayed notifications in if they cannot be delivered. As the it is at the receiver's side, that IM Server will not have information on when the sender is online. Therefore a retry mechanism will be employed to deliver stored notifications.

The IM Server will store the messages for a period that is determined by local server policy. If at the end of this period the messages have not been delivered, the IM Server will discard them.

To be able to deliver stored delivered/displayed notifications to a sender's device that has become offline, without disrupting the user experience, the IM Server supporting the 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 by means of the well-known URI (*rcse-standfw@<domain>*) uniquely identifying the store and forward service identity that is provided in the P-Asserted-Identity header field.

Note that the IM Server supporting the store and forward functionality 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 2.15).

An IM Server supporting store and forward will behave as a back-to-back user agent handling the SIP INVITE requests that are used to establish the chat session. While doing so it may have to return a different response to the INVITE request on the originating leg than the one it received on the INVITE request on the terminating leg. The mappings shown in Table 22 will be applied

Response received on terminating leg	Response sent on originating leg	Store the message
480 Temporarily unavailable	200 OK	Y
408 Request Timeout	486 Busy Here	Y
487 Request Terminated	486 Busy Here	Y
500 Server Internal Error	486 Busy Here	Y
503 Service Unavailable	486 Busy Here	Y
504 Server Timeout	486 Busy Here	Y
600 Busy Everywhere	486 Busy Here	Y
603 Decline	486 Busy Here	Y
Any other response (including 404 Not Found and 200 OK)	Received response (that is no mapping is done)	N

Table 22: Mapping of received Error Responses by the IM Server[30]

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 2 for further reference) which is used to configure the client to support or not support 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 simultaneously.

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-TEC-REAL] and [RCS2-OMA-SIMPLE-ENDORS].

[30] These mapping means that the semantics of 486 Busy Here are that the chat session cannot be accepted, but that the message has been stored by the entity that sent the original 486 response.

Each of user B's devices that receive the session invitation generates a SIP MESSAGE to carry the delivered IMDN as per [RFC5438]. 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.

User B will be able to answer to the chat from any of his devices, when they send a message from one of the devices, that device (B1) will become the only active device for user B and all the other IM sessions towards the other devices will be closed. All the following messages sent to user B will be received only by the active device B1 using the already established IM session.

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

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 messages sent by user A through the chat will make the IM server establish the chat again using one IM session per connected device of user B and send the message to them all.
b) If user B changes from one device B1 to another B2 by 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 that will go to user A's device. When user A's device detects a new INVITE session from a user B which already has an established session it shall end that session 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 closes the old session."

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

3.2.4.13 Switching to Group Chat

A group chat can only be initiated from a user on a MNO which has deployed an IM-AS. It is optional for a MNO to provide the group chat functionality. Therefore from the terminal perspective, if there is no IM conference-factory-URI configured, the terminal should not allow the user to add additional parties to the chat or start a group chat.

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

A real time check of contacts capabilities will be performed 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 visible there.

When user A sends the first message a new group chat will be opened between all the selected users, and 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 to switch the focus to the new created group chat windows. However, user B's device will close the one-to-one chat session once the Group Chat has been accepted.

Please note that the Store and Forward support for Group 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 there.

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

Users 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 read.

From the technical implementation perspective, 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 with status “delivered” which 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 receipt 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 receipt 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).

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] Appendix N.

3.2.4.17 Chat message size limitations

To reduce the complexity at protocol level and avoid potential TCP switchover, it is recommended to limit the maximum size of a chat message to avoid the SIP INVITE to be longer than the path MTU and, consequently, trigger the TCP switchover. This maximum size will be controlled through the MaxSize1To1 configuration parameter defined in [RCS2-MO].

If the user attempts to send a message larger than this limit, they should be informed in the conversation that messages of that size cannot be sent.

3.2.4.18 Clarifications on IM race conditions

3.2.4.18.1 *Two simultaneous invites*

Even if unlikely, it may be possible 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 that as both parties initiate a session, this behaviour is the same on both sides and consistent with the one described for RCS Release 2 ([RCS2-OMA-SIMPLE-ENDORS], section 7.1.2.1, bullet 6), however, the 486 BUSY HERE response is preferred to 600 BUSY EVERYWHERE because it allows a multidevice scenario.

For additional clarification, an explanatory diagram has been included in ANNEX B section B.9

3.2.4.18.2 *New invite sent after a previous invite has been accepted*

Even if 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 and forward messages arrive in a short period of time

Due to the fact that a user may have several messages waiting in storage 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 stored messages (the INVITE carry a referred-by header with the sender's ID and not containing an "isfocus" tag in the Contact header), the suggested experience is the following:

- Only the first message is shown in a notification to the user. The remaining stored 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.

Note: the described behaviour does refer to notifications shown on screen to the user and does not affect the behaviour with regard to the sending of Delivery notifications. Those are still sent for all received messages for which such a notification was requested.

3.2.4.20 Protocol flow diagrams

Please note that 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 ANNEX B and ANNEX C.

3.2.4.20.1 *General one-to-one chat*

In this scenario 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 and sends the first message.

In the following sequence we are assuming that user B is currently registered, therefore, the chat can take place. Client A and B are aware of this because an OPTIONS exchange has been completed (providing the capabilities from the other end) prior to entering into the chat

(This exchange may for instance have happened when selecting the contact in the address book).

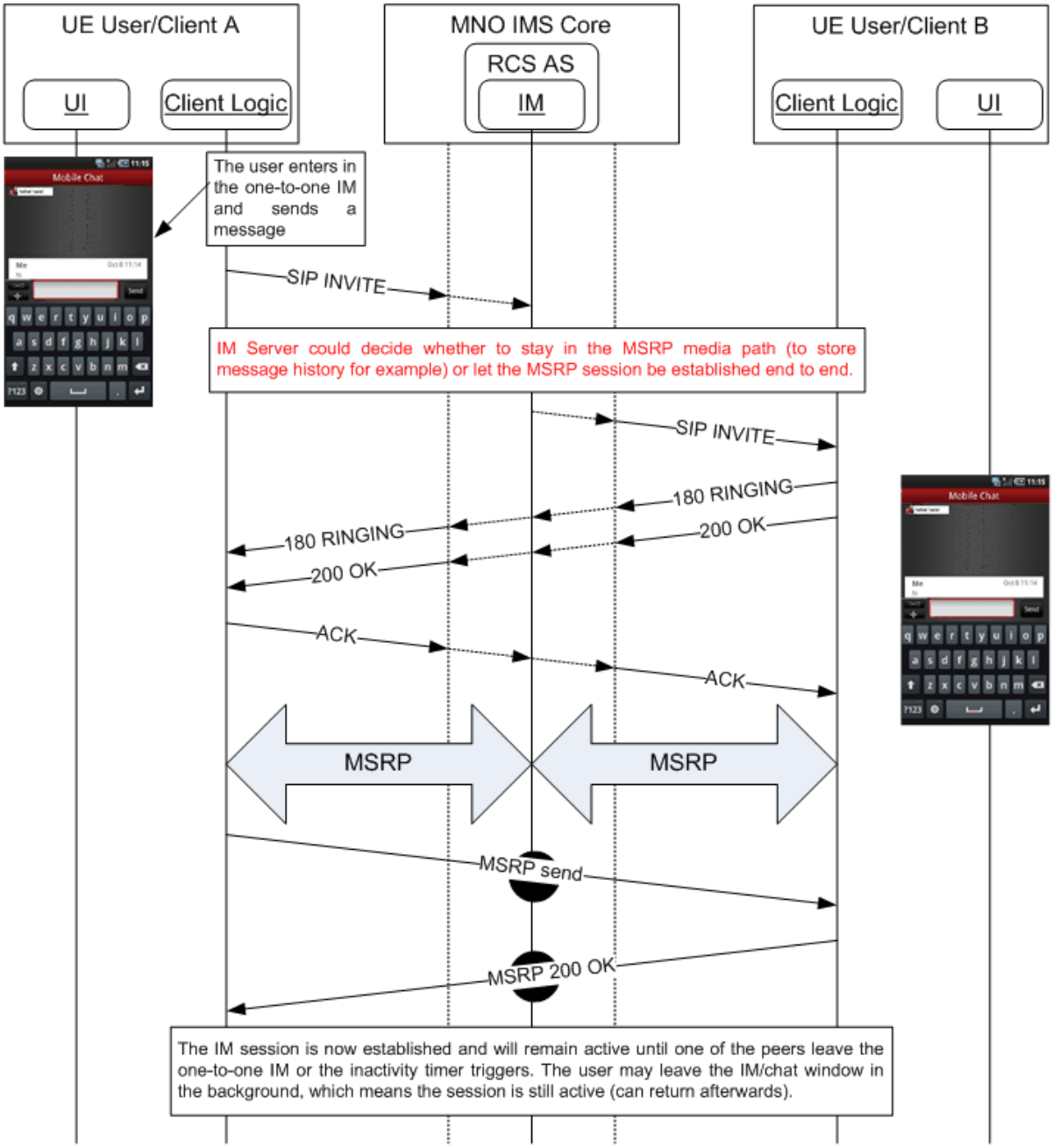

Figure 28: One-to-one chat

Note that MSRP is not only used to send messages but it is also used for notifications ('is composing', display and delivered). Please also note though that prior to the establishment of the session, SIP MESSAGE is used 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 information about the capabilities from the other end that is not up-to-date. For example, the other user was registered during the previous polling. User A has selected the user in the address book. There is some latency however 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 anymore (no chat possible) may happen. In this case, the proposed sequence is the following:

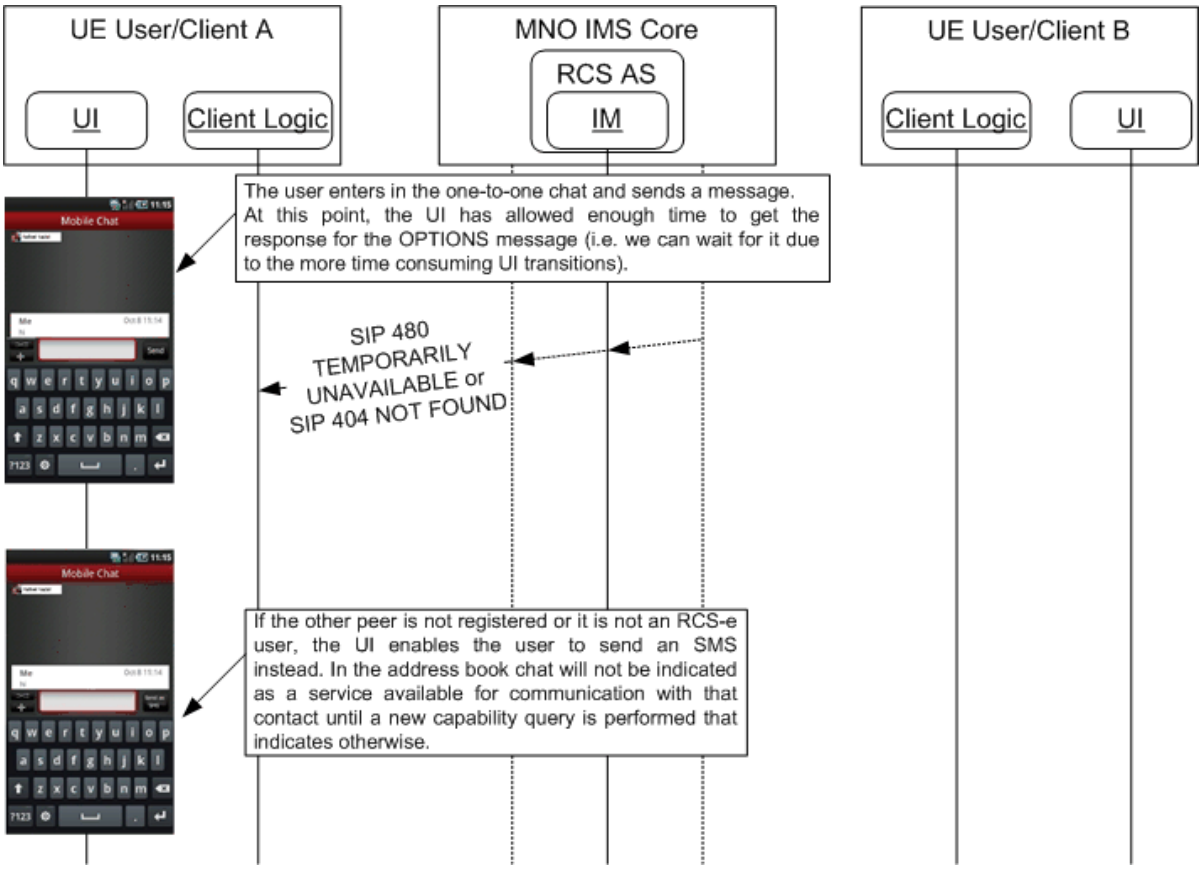

Figure 29: One-to-one chat backup mechanism to send SMS

Please note that 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.

Note also that according to section 2.3.1 the SMS messages will trigger capability queries of their own. This will allow the device to indicate that normal chat is available again in case it was not available due to a temporary problem.

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 as, for example, the chat conversation is finished. The relevant UX and flow sequence is presented below:

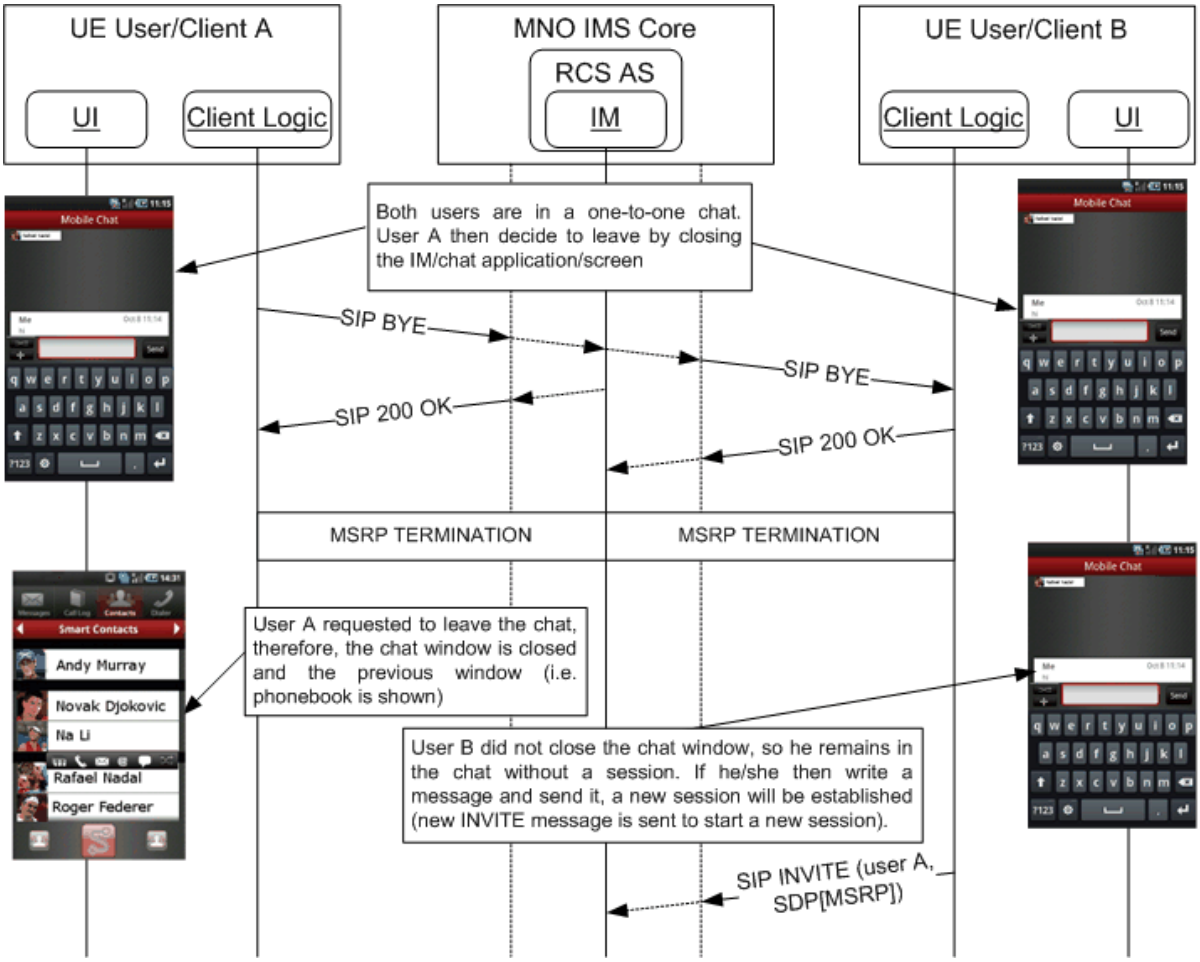

Figure 30: Leaving a one-to-one chat session (chat terminated)

Please note that the IM Server, especially when store and forward is enabled could decide to leave the user 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 shown reflecting that the underlying MSRP session has been closed.

In the next case that is discussed, user A and B are in a chat. User A has to leave however because an incoming event (incoming e-mail, incoming call, etc.) or other reason results in the user deciding 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:

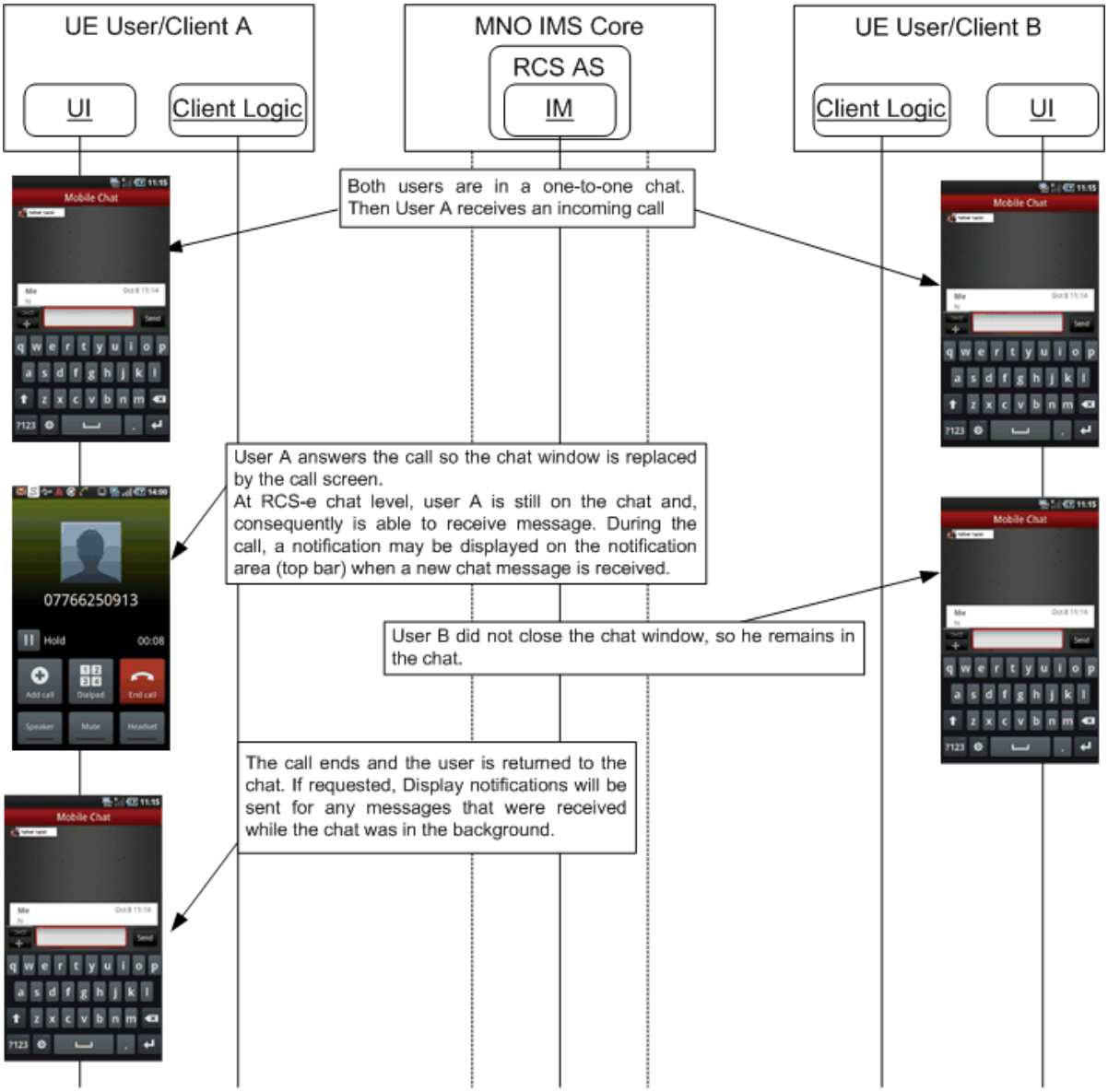

Figure 31: Leaving a one-to-one chat session (leaving chat in the background)

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 fails to keep the connection to the network (due to for instance a client error, an IP reconfiguration due to a new data bearer, lost coverage and so on):

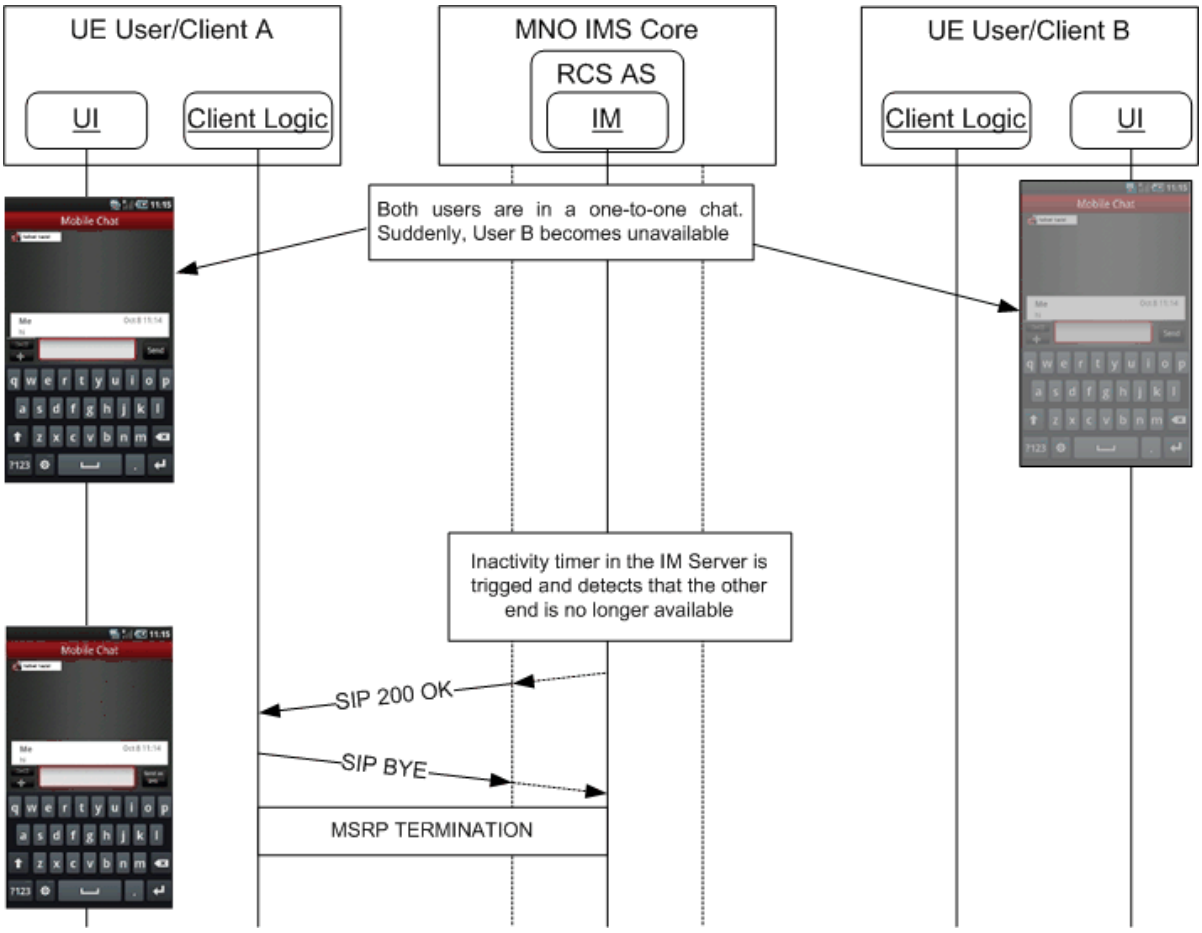

Figure 32: One -to-one chat forced termination

Note: If user A sends a message while user B is unavailable before the expiry of the inactivity timer, the IM server will detect that the TCP connection used for the MSRP session towards user B is no longer available. In this case the IM server will use that as a trigger to terminate the session. Depending on the availability of a store and forward function along the path towards user A, either the message will be accepted or an appropriate MSRP error response will be returned.

It should be noted that in most cases the IMS core will be aware that user B has become unavailable in which case it can terminate all on-going sessions for user B including the chat session which means that it is unlikely that anything is still sent within the session.

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 (a handover to a different data carrier for instance) and the chat can continue. However, even if the chat can continue, the other end is informed of a change in the capabilities using the OPTIONS message.

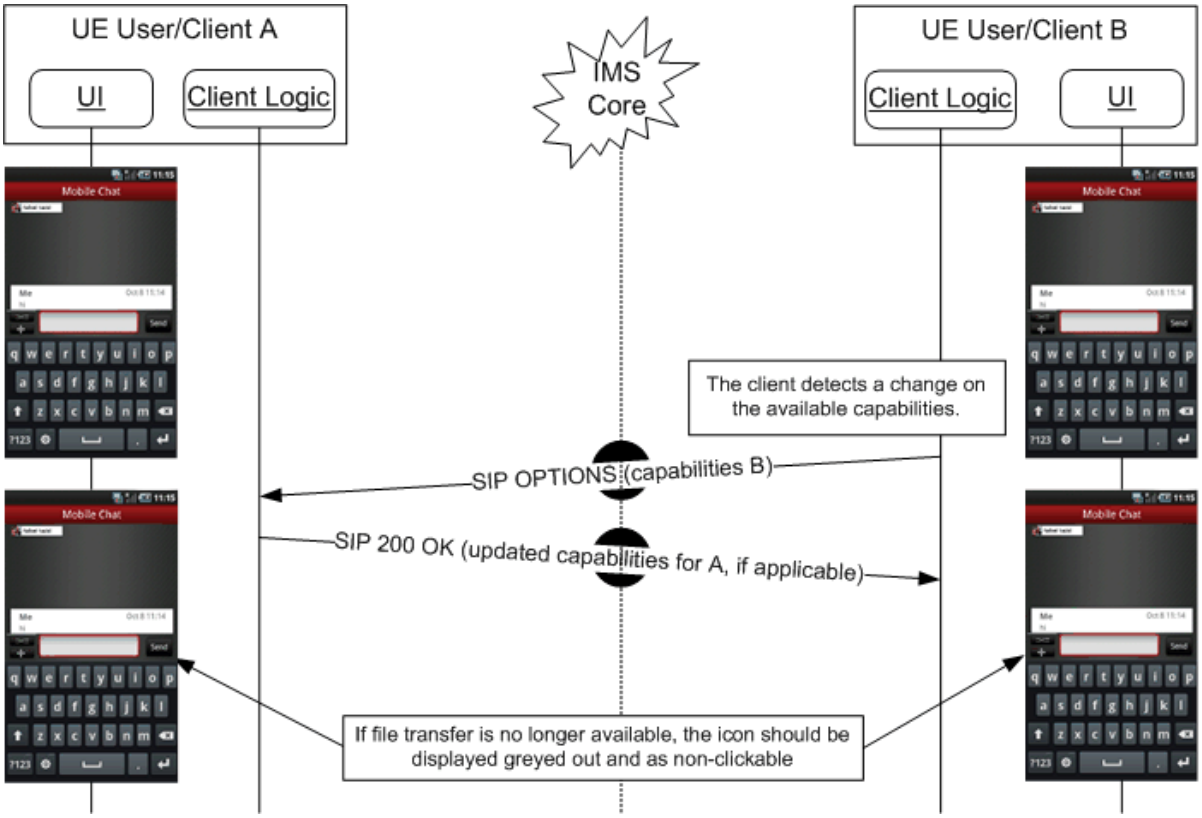

Figure 33: Capabilities exchange during a chat session

3.2.5 Group Chat

To implement the group chat functionality an IM server is required, and consequently, the IM CONFERENCE FACTORY URI (see section 2.1 Table 2 for reference) configuration parameter should be correctly set.

It is optional for a MNO to provide the group chat functionality, so from the terminal perspective, if there is no IM CONFERENCE FACTORY URI configured, the terminal should neither allow the user to add additional parties to the chat nor allow to start a group chat. Please note that even if starting a group chat is not available in this scenario, it does not restrict the possibility to join a group chat session. Therefore, the OEM should implement both the one-to-one and group chat experiences even for those users without a configured IM CONFERENCE FACTORY URI.

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

Support for the store and forward functionality in group chat is not included in this version of the specification.

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

3.2.5.1 Initiating a chat

User A initiates a chat by selecting some of his contacts (B, C and so on up to a limit Over The Air (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. This choice will be offered 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 and so on (a query per intended contact) to ensure that the IM service is available for those users at that time.

When user A types the first message, which is used as subject for the conversation, 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’s client receives a group chat invitation from the IM server, the user may accept or reject the invitation and after acceptance the client shall subscribe to the conference event package to retrieve the list and status of the users in the group 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 open sessions to users A, B, C and so on up to a configured limit.

In the interfaces of the receivers’ clients a notification (UI dependent) will be displayed to inform about the incoming invitation. This notification must clearly state that it is a group chat making the users aware of this fact.

Unlike [RCS2-OMA-SIMPLE-ENDORS] once a group chat is established, any participant is allowed to add more contacts, as long as the general limit has not been reached.

3.2.5.2 General Behaviour

The same behaviour from the one to one chat applies to group chat with following changes:

- 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
- As specified in [RCS2-OMA-SIMPLE-ENDORS], the invitation for a group chat is explicitly shown to the user who can accept or decline to participate

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

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

  Note: This requires the IM server to send along the list of invitees in the group chat invitation. Therefore an IM server shall follow section 7.2.2.2 of [RCS3-OMA-SIMPLE-ENDORS] instead of the same section in [RCS2-OMA-SIMPLE-ENDORS]. For the clients clarification 8 of section 7.1.2.1 of [RCS3-OMA-SIMPLE-ENDORS] applies instead of clarification 8 in the same section of [RCS2-OMA-SIMPLE-ENDORS]. In case

the invitation does not include the list of invitees, it shall thus still be possible for the user to accept the session.

3.2.5.3 Closing Group Chat

Any of the participants can close his IM session associated with an established group chat. 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 less than the minimum number of RCS users defined for a group chat remain in the group chat, all RCS users close their IM session, 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 limit the maximum size of a chat message to avoid the SIP INVITE to be longer than the path MTU and, consequently, trigger the TCP switchover. This maximum size will be controlled through the MaxSize1ToM configuration parameter defined in [RCS2-MO].

In case the user attempts to send a message larger than this limit, the user should be informed that messages of that size cannot be sent in the conversation.

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:

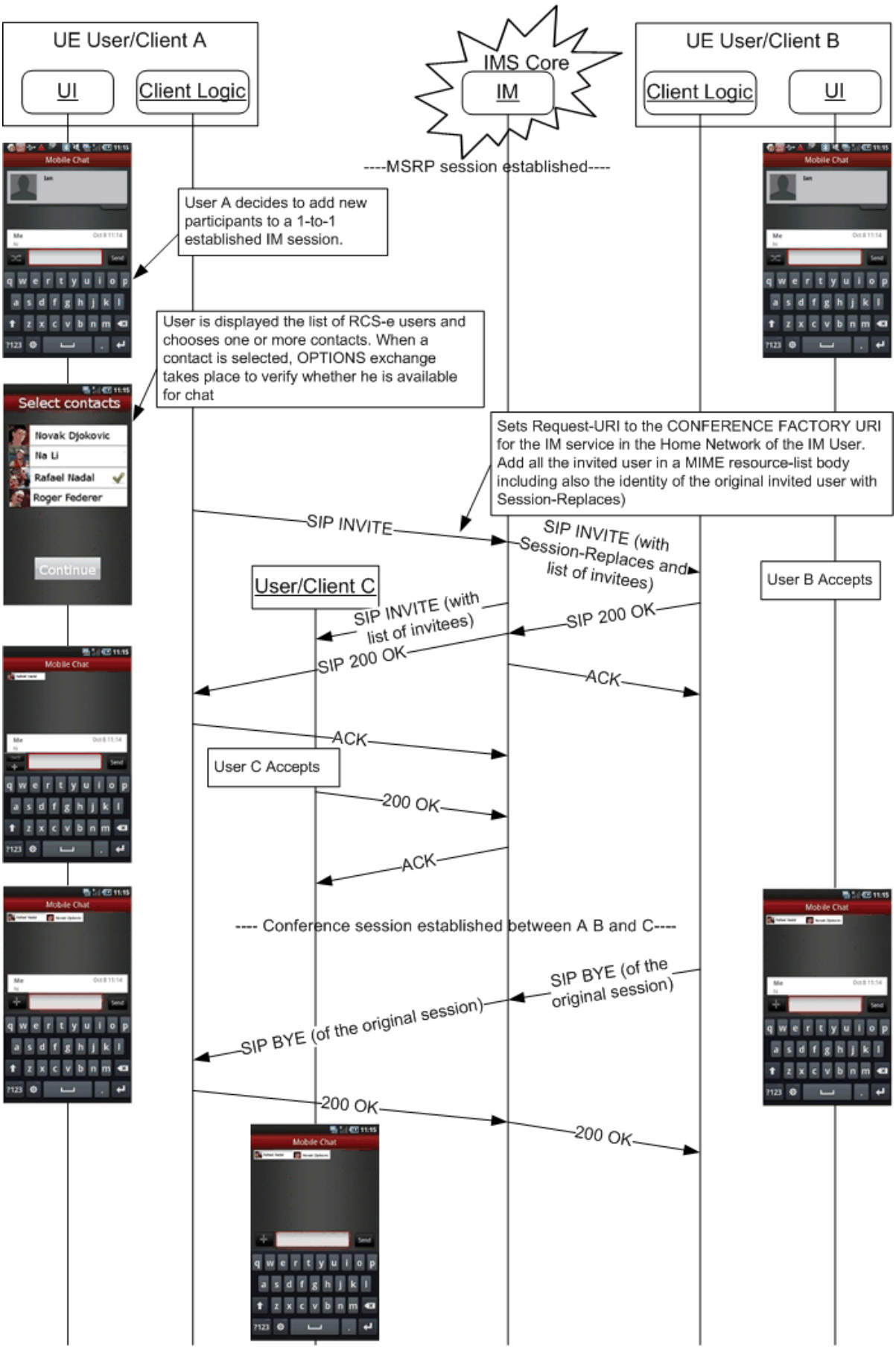

Figure 34: Group chat session initiation

3.2.5.5.2 *Get participants of Group chat IM session*

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

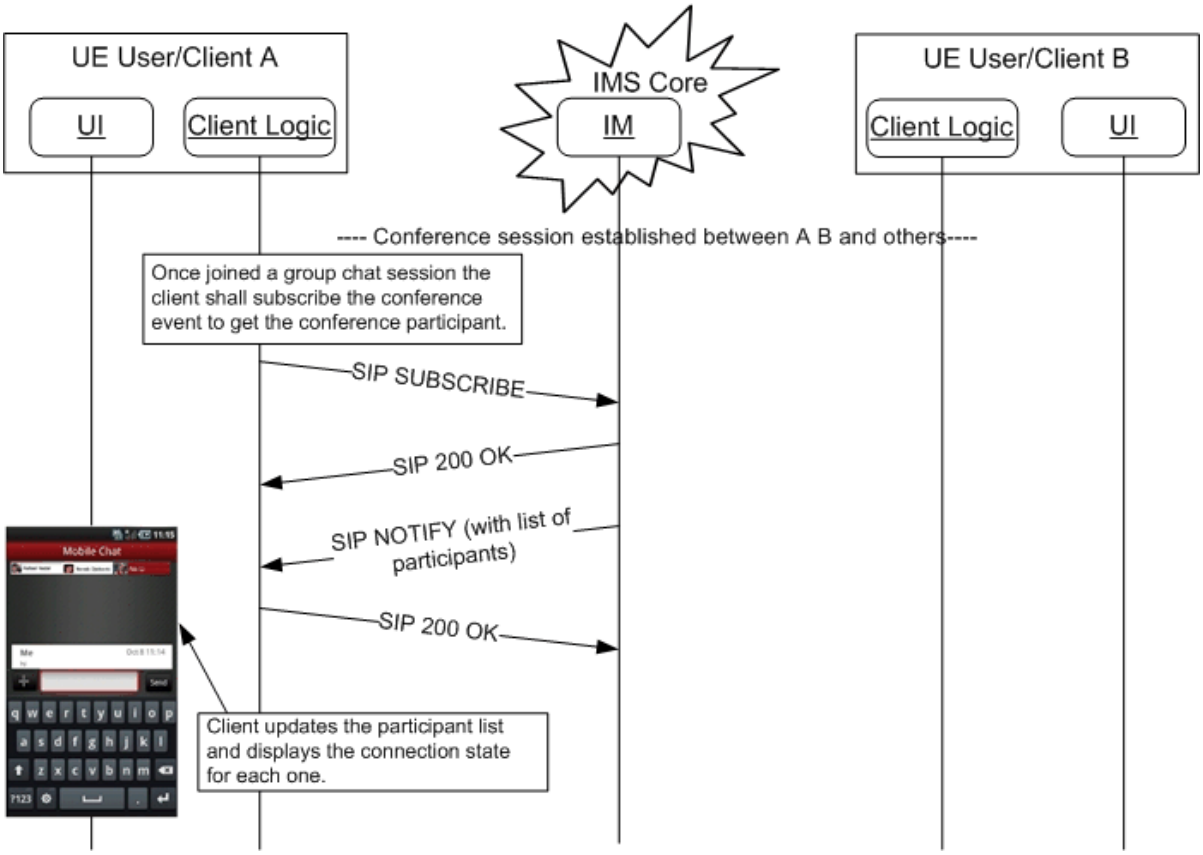

Figure 35: Group chat session initiation (II): Get participants

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

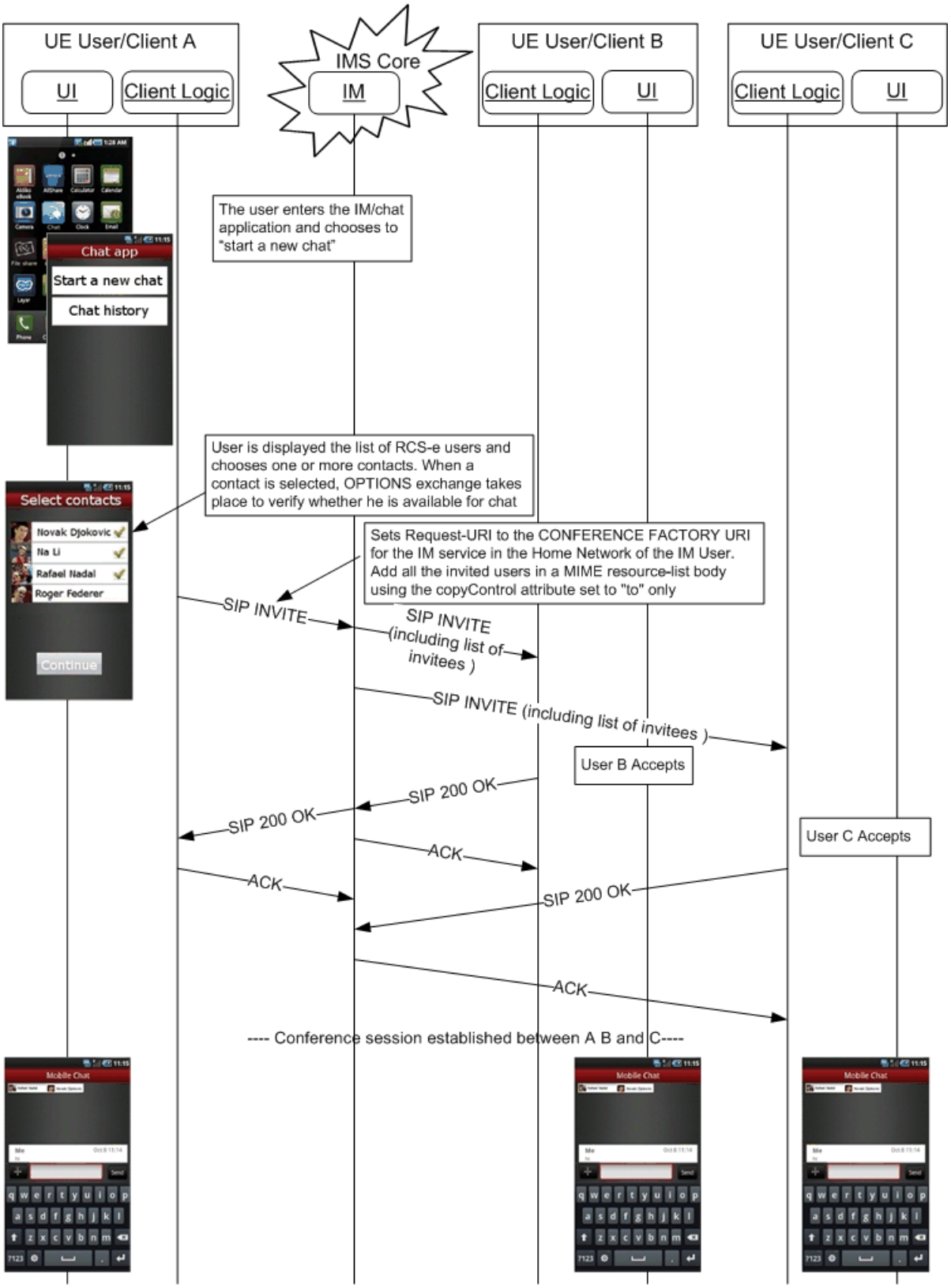

Figure 36: Start a group chat from the IM/chat application

3.2.5.5.4 *Add a participant to an already established group chat session*

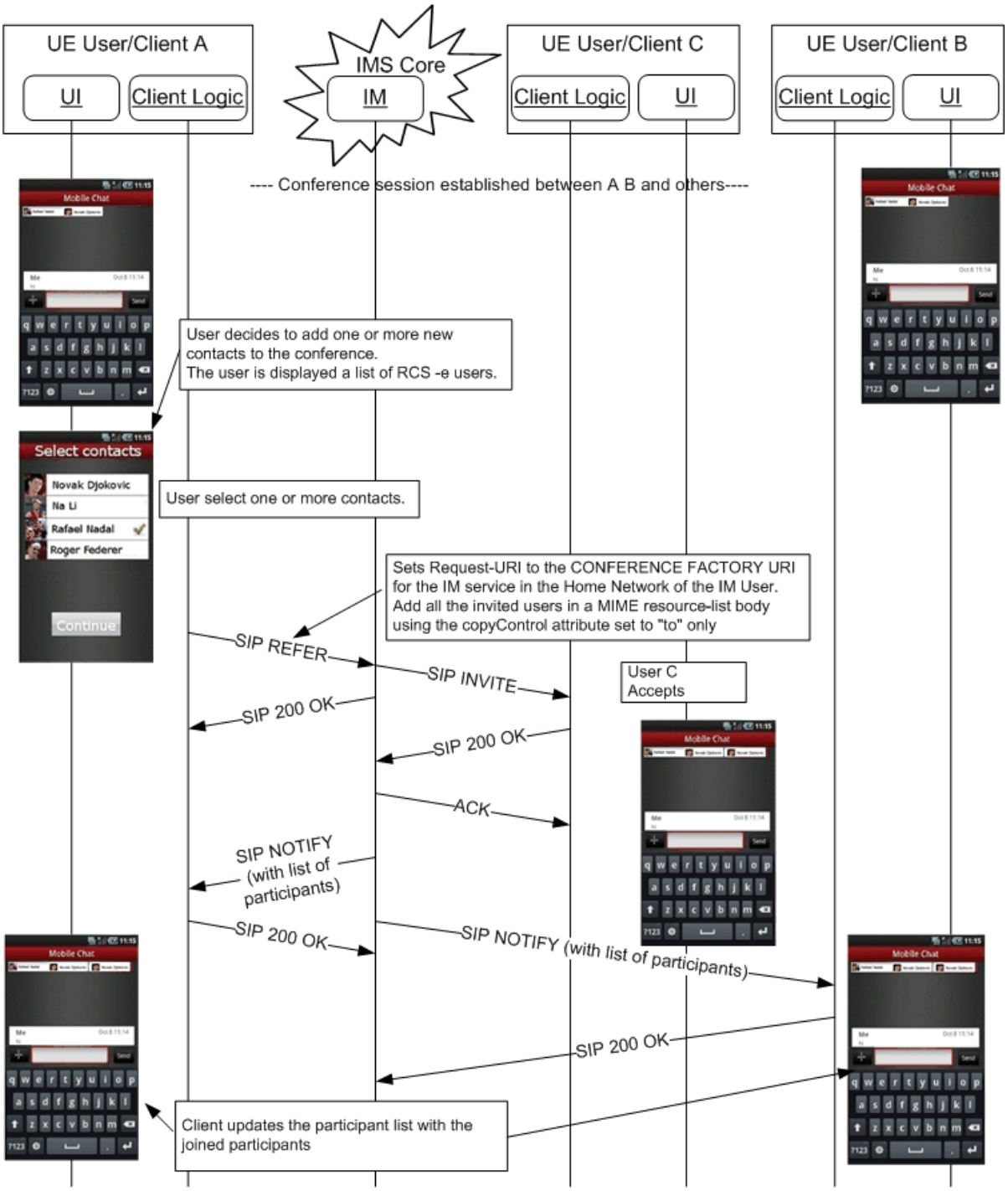

Figure 37: Adding new users to a multi-chat session

3.2.5.5.5 *Sending a IM message from the IM multiple session window*

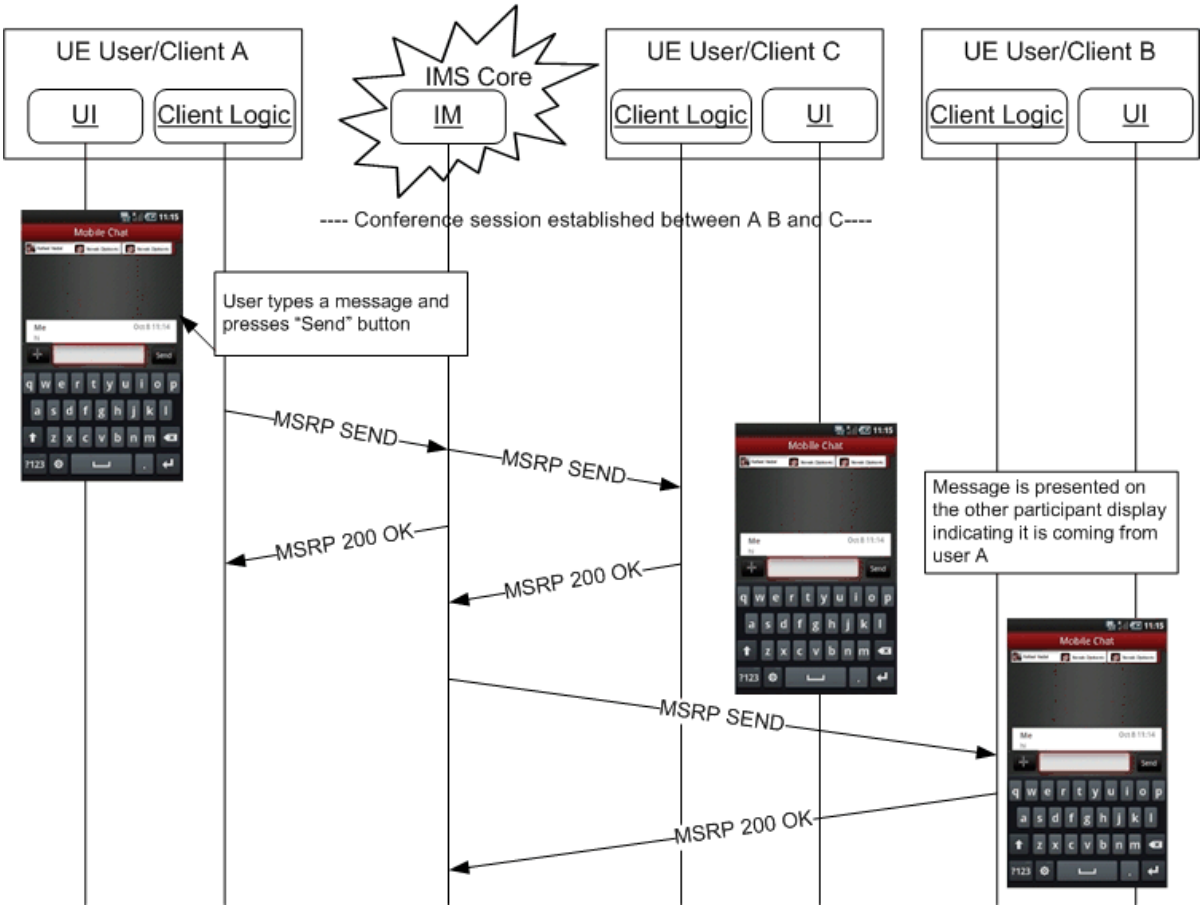

Figure 38: Chat message sequence on a multi-chat session

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 (group chat); suddenly User B goes offline (due to the loss of the connection to the network for example):

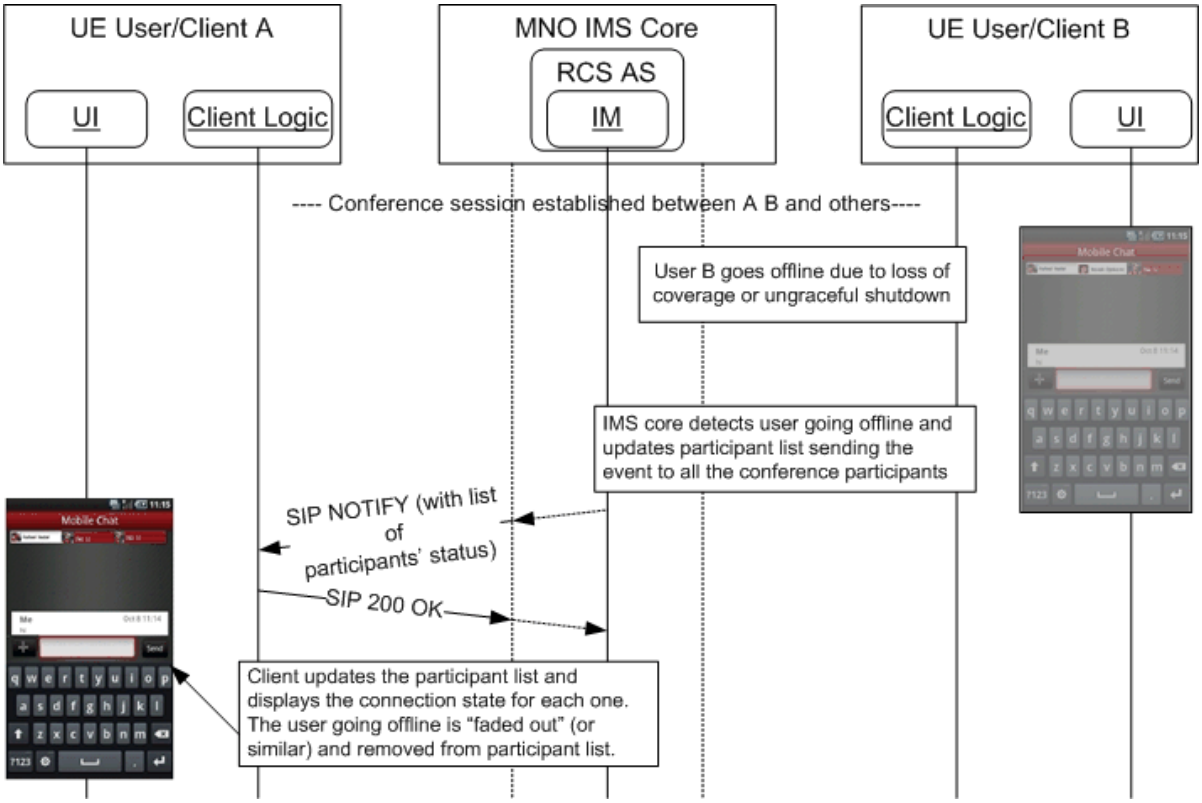

Figure 39: Forced chat termination in a multi-chat session

3.2.5.5.7 *Leaving a IM multiple session*

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

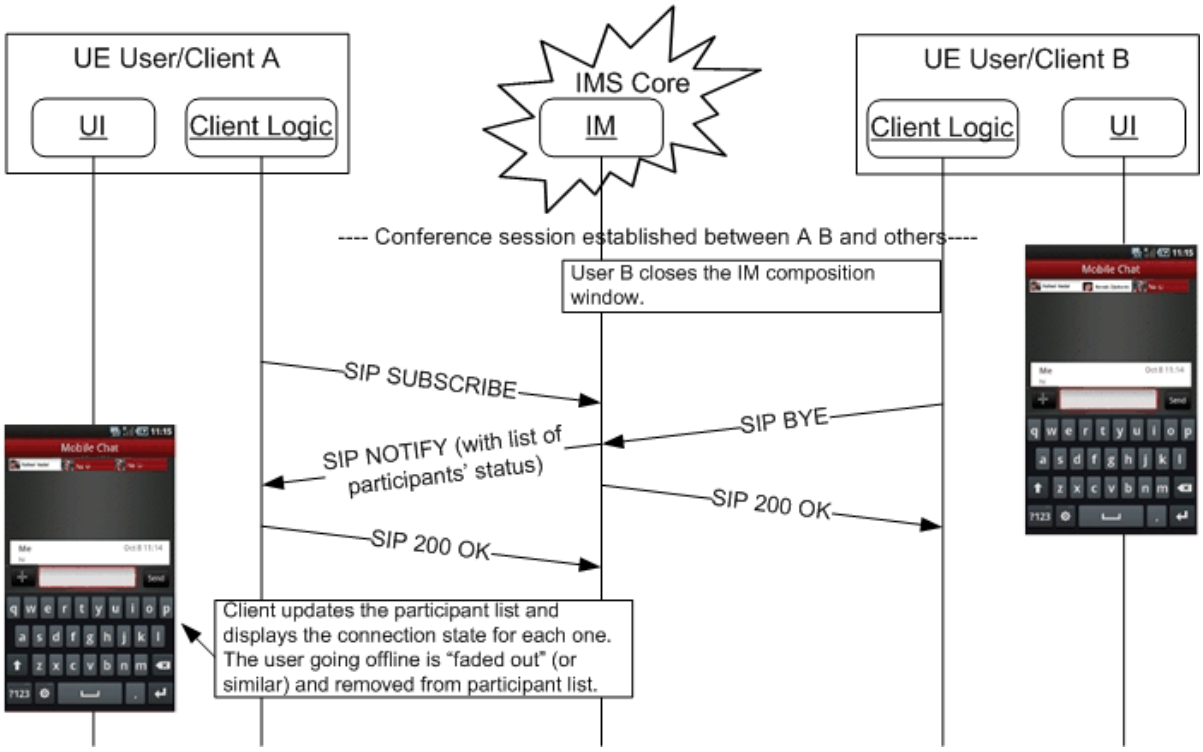

Figure 40: Leaving a multi-chat session

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 (this is video share with identical behaviour and version as the one defined in the RCS Release 2 specifications and thus being fully compatible with [PRD-IR.74]): The video can be originated from:
  - The front camera (“me”)
  - The rear camera (“what I see”)
  - A file (“video streaming”)
- Share a picture (this is image share with identical behaviour and version as the one defined in the RCS Release 2 specifications and thus being fully compatible with [PRD-IR.79]): 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 on the respective capabilities of the other end to avoid showing a service as available when this is no longer the case.

Both video and image share are unidirectional. It is possible however 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, , user B can also start to share video with A simultaneously, provided the right coverage conditions are in place. In this case each video share session is independent and should be handled separately. The same example would also apply to image share or even to a combination of video share ine one direction and image share in the other.

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 show 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 shown in the following sections.
- The terminal supports 2G DTM mode and it is therefore always possible to gracefully terminate the transaction providing the terminal remains switched on. If 2G DTM is not supported, the case where on one of the ends a handover occurs to 2G would be result in a behaviour towards the other end and the network that is equivalent to the one described for the case of a client error.
- The terminal comes with a front and rear camera. If one or both are missing, the user should be notified only with the available options.
- Prior to the call, the user accessed the client’s address book, call log or dial-pad to make the call. As described, while these actions are performed an OPTIONS message is sent to double-check on the available capabilities. As video and image share services are only available in a call, another OPTIONS exchange is required once the call is established. This exchange can be initiated by either the sender or the receiver. In the following diagrams we are assuming that this initial exchange (OPTIONS and response) has already take place, and therefore, both ends are aware of the capabilities and the available RCS-e services.

- In the diagrams we have assumed for simplicity that MSRP chunking is enabled. This is for representation purposes and it is up to the OEM to decide 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 on a call. The capabilities of one of the users change (due to a hand-over to a different data carrier for instance). Therefore the other end has to be informed using the OPTIONS message[3132] .

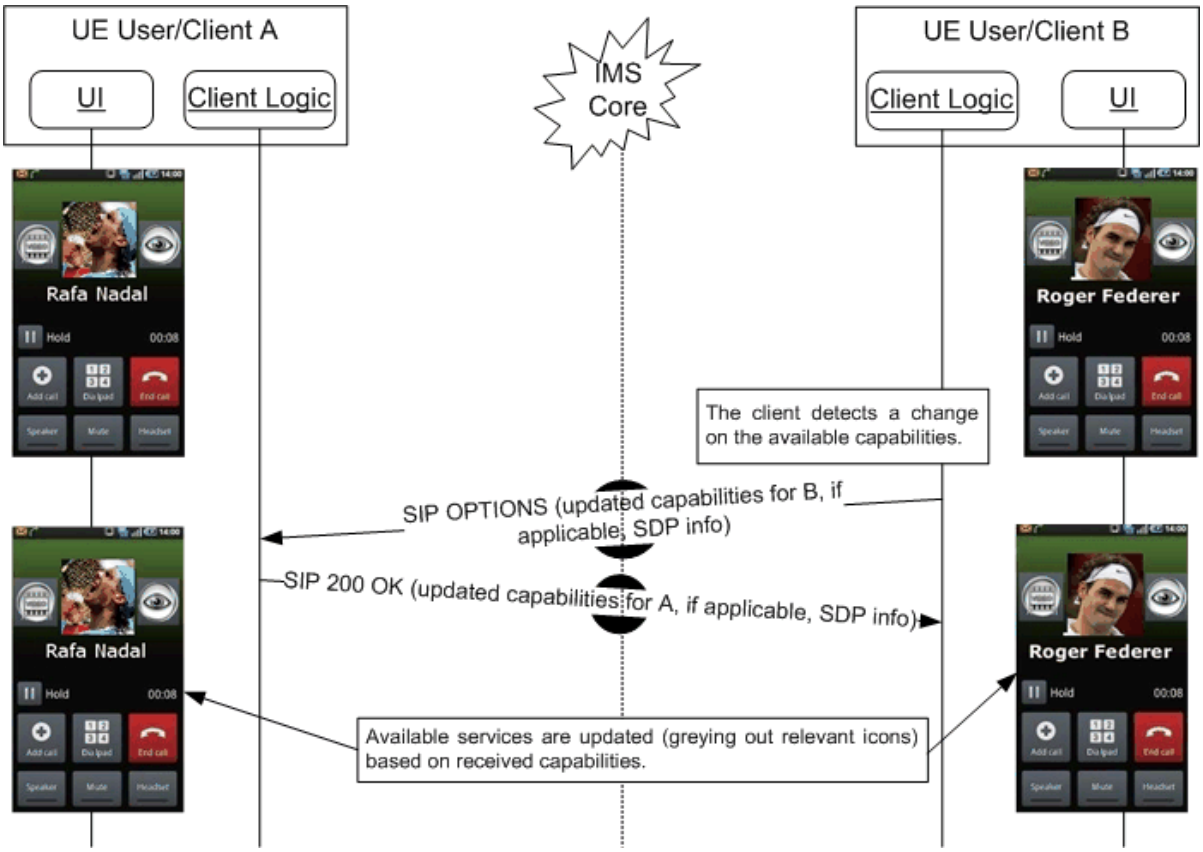

Figure 41: Capabilities exchange during a call

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.

---

[31] The SDP information included in the response to the OPTIONS request is required due to the compliancy to [PRD-IR.74]. This will only be used during OPTIONS exchanges related to a call. The video share service shall only be considered to be available if at least one codec in the received SDP is supported by the client.

[32] As in RCS Release 2 (see [RCS2-TEC-REAL]), when there is no call a broadband access client shall respond to an OPTIONS request indicating that it supports video share and image share during a call. This may allow the user to see the shared content on a larger screen when in a call through the mobile device.

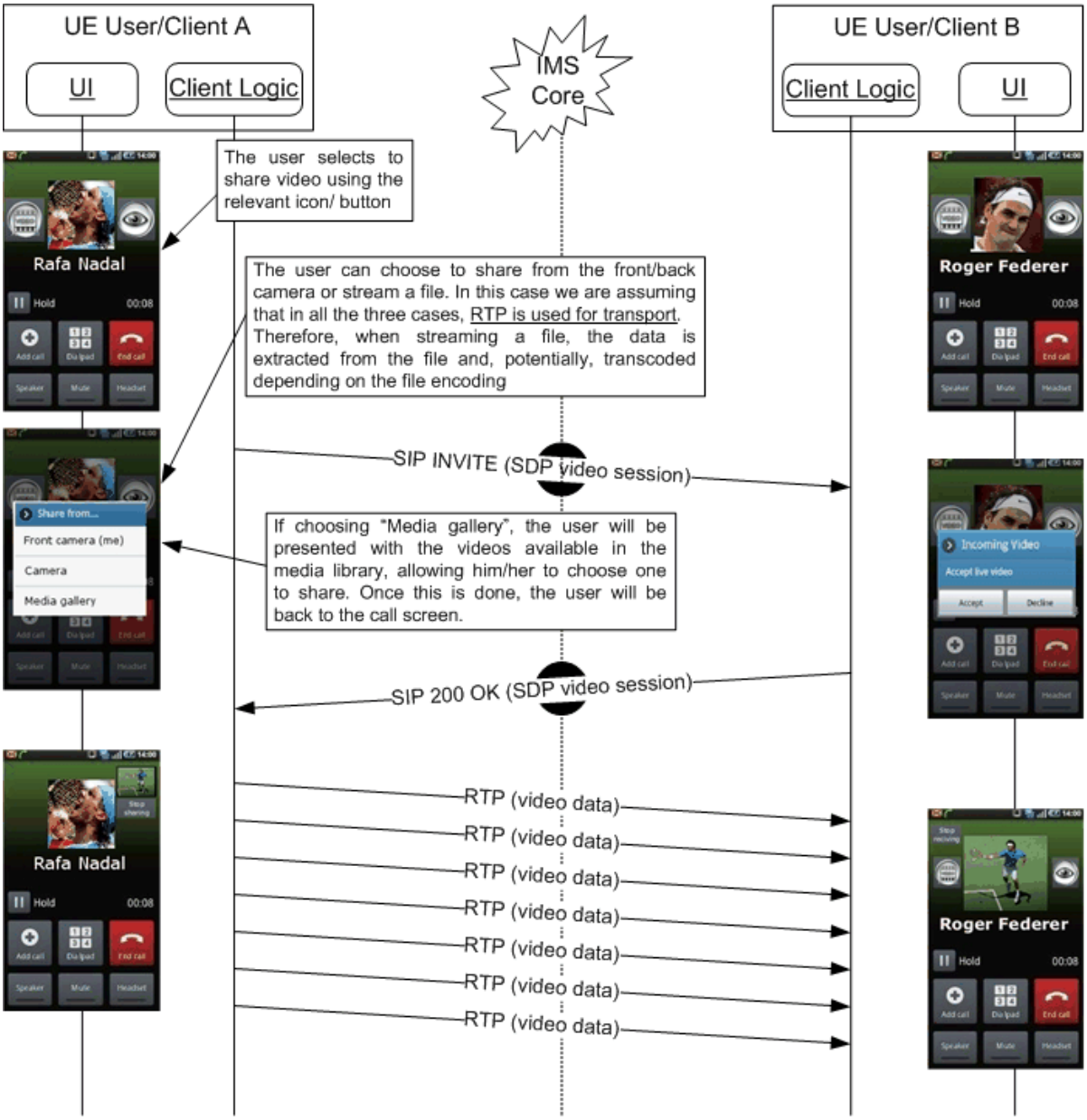

Figure 42: Share video during a call

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

The assumptions in this case are that user A is sharing a video (through RTP) with user B, however user A no longer wants to keep sharing it.

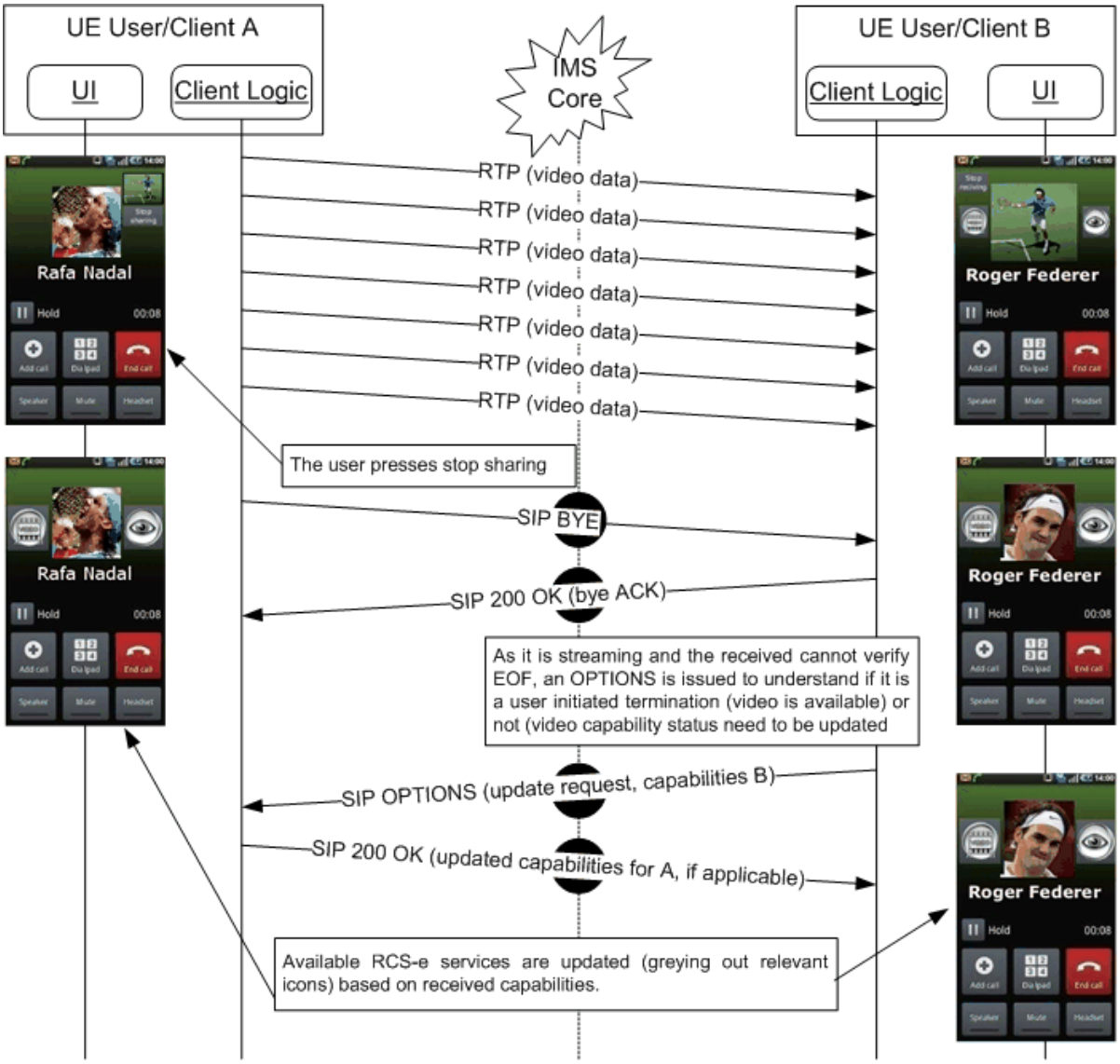

Figure 43: Sender stops sharing video during a call

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 want to keep receiving the video.

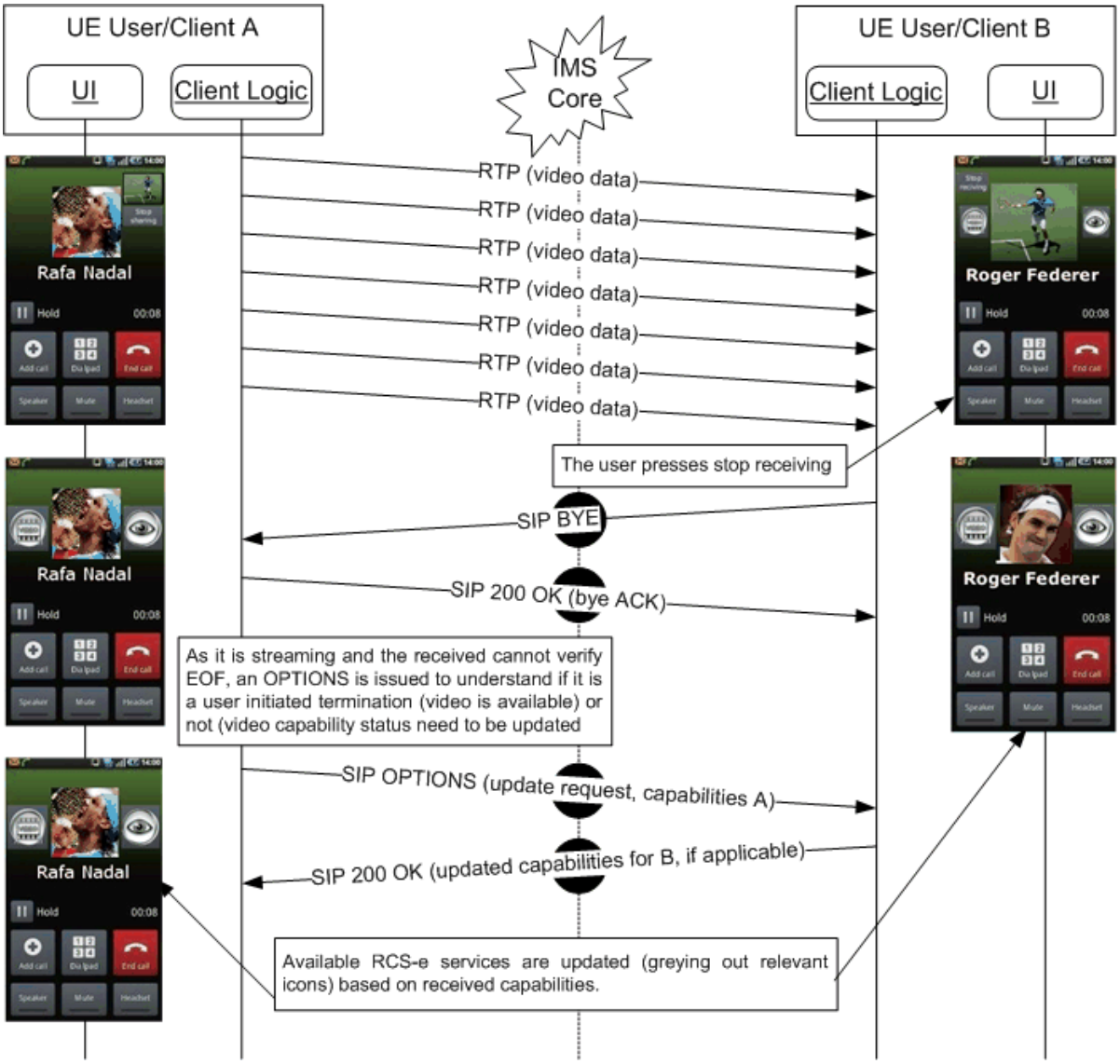

Figure 44: Receiver wants no longer to receive video during a call

3.3.6 Stop sharing video (RTP) during a call as 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 user A or user B is no longer capable (for instance because the terminal is busy, suddenly has no 3G+ or Wi-Fi coverage available without triggering an IP reconfiguration or loss of connection) of sending or receiving a video. Please note that in the example, we have assumed that the sender (user A) is the one losing the capability. This sequence will be equivalent in case:

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

By losing the capability to send video, we are excluding the case in which there is an IP reconfiguration. Please note that this particular case is covered under the “Client Error” section later in this chapter (see 3.3.12 and 3.3.13)

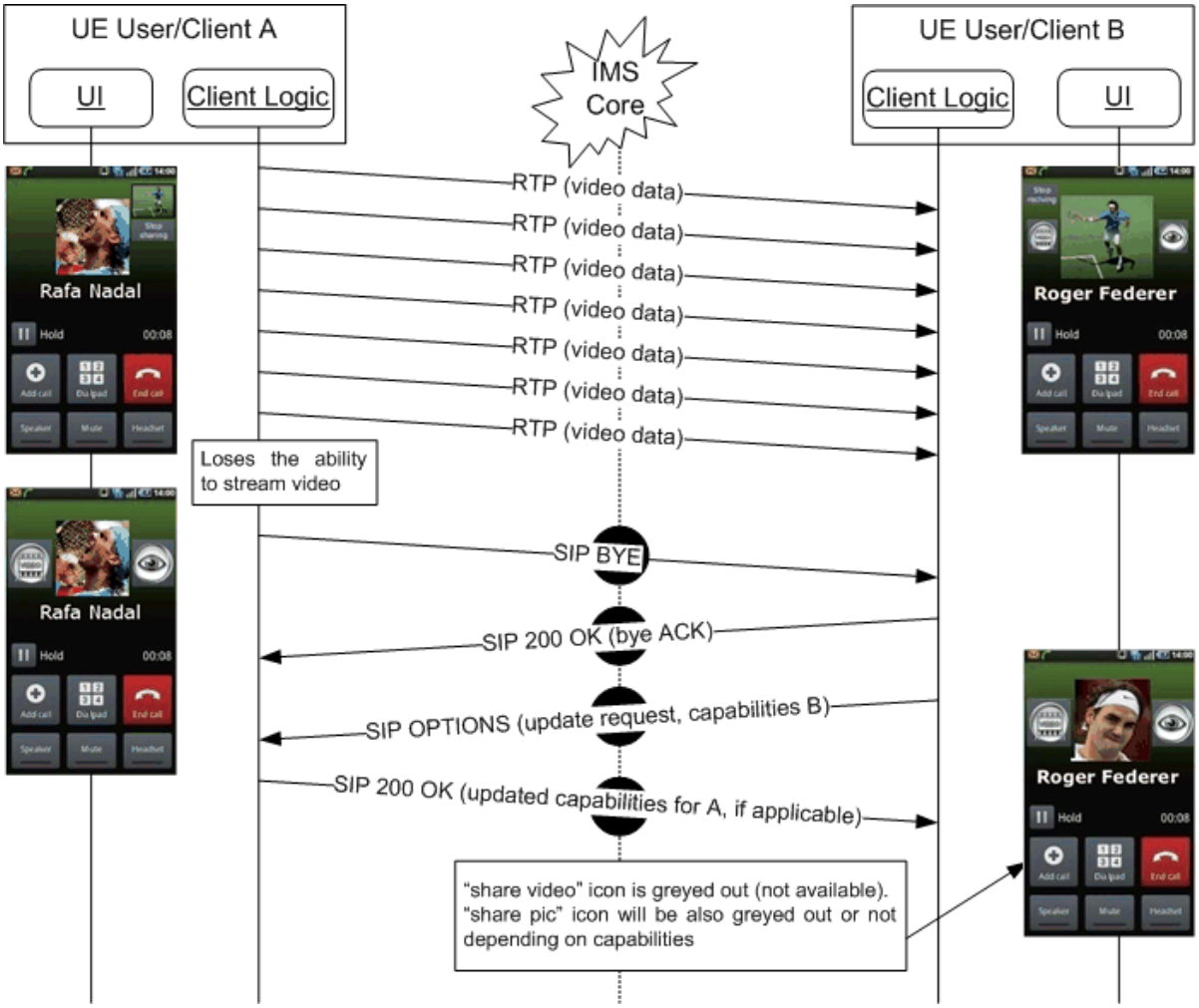

Figure 45: Video can no longer be shared during a call (capability not available)

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 messages. Therefore both clients are aware that image sharing is possible (that is both UEs are on a 3G+ or Wi-Fi network).

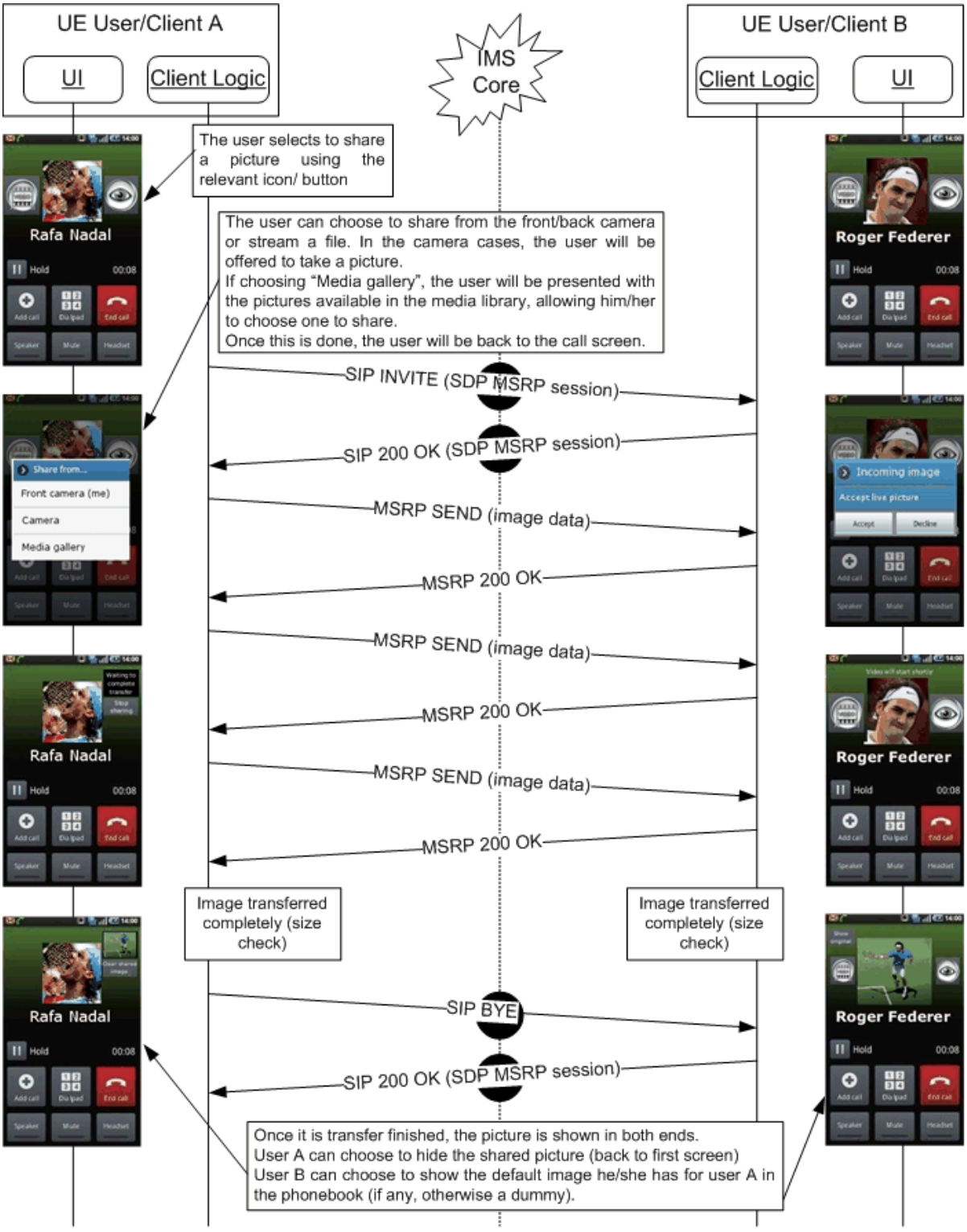

Figure 46: Sharing a picture during a call

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, but user A no longer wants to keep sharing the picture.

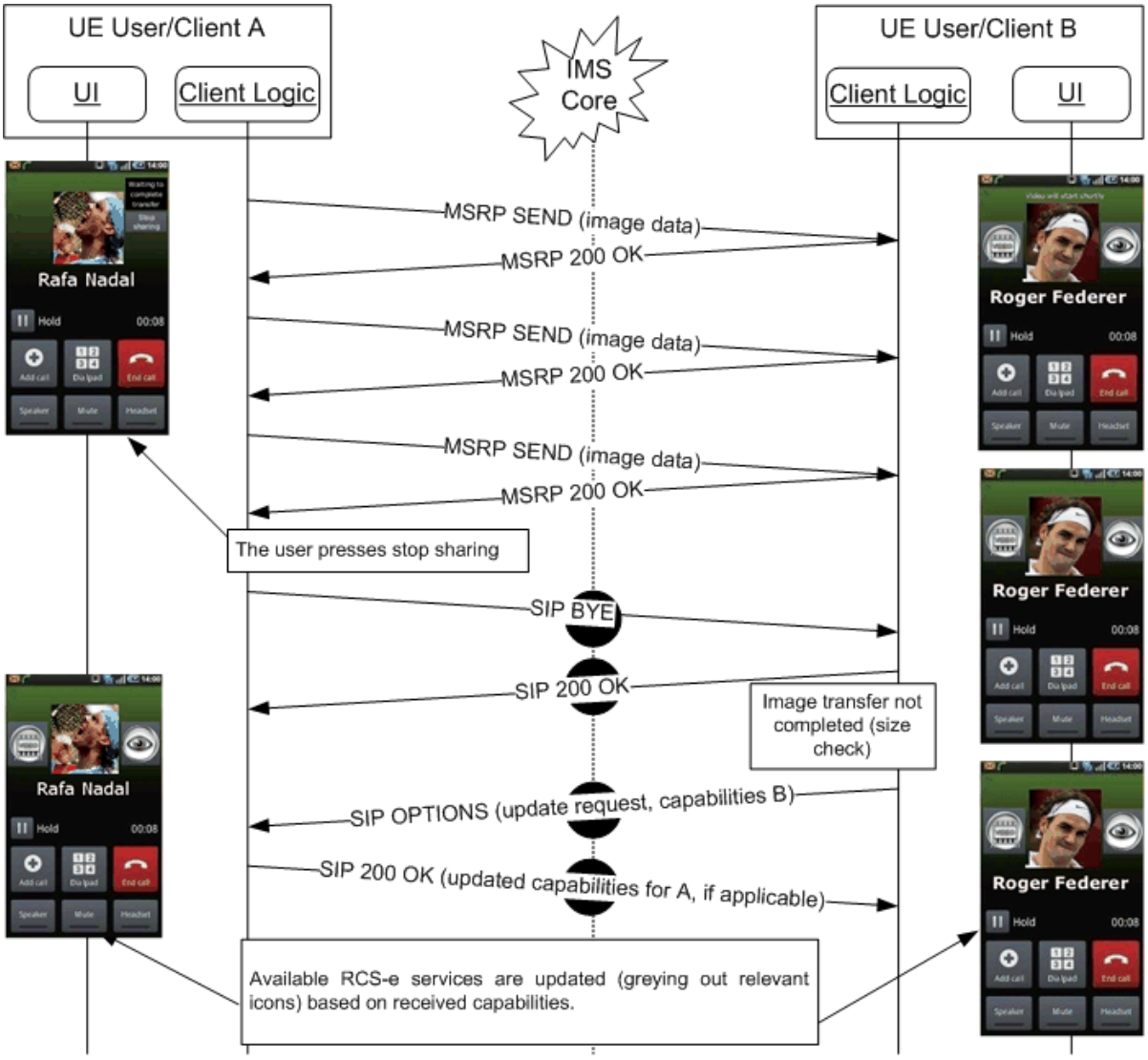

Figure 47: Sender stops sharing a picture during a call

3.3.9 Stop sharing a picture during a call: Receiver initiated

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

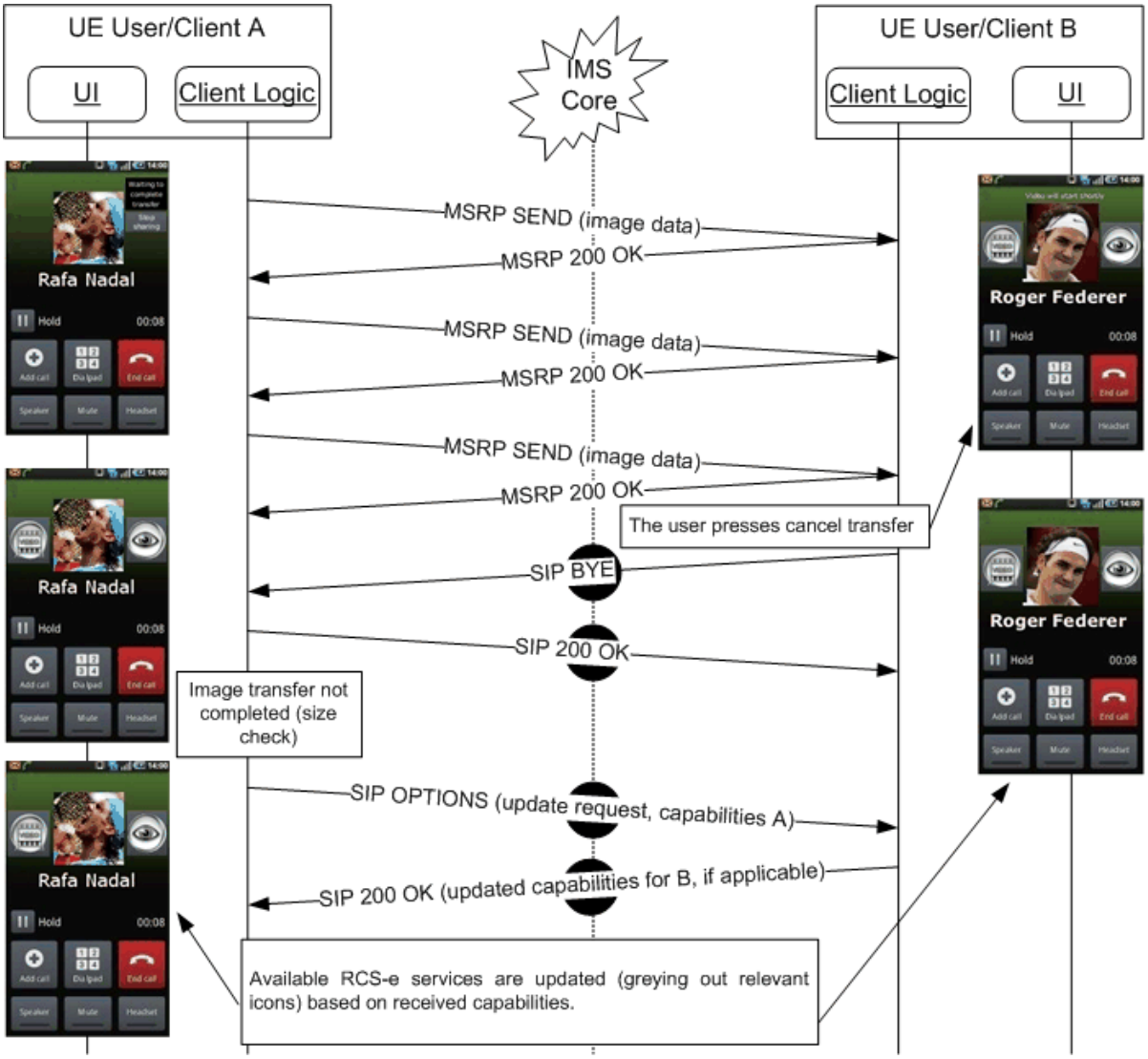

Figure 48: Receiver stops picture sharing

3.3.10 Stop sharing a picture during a call as 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 user A or user B are no longer capable (for instance because the terminal is busy) to sharing or receiving the image respectively. Please note that in the example we have assumed that the sender (user A) is the client losing the capability. The sequence will be equivalent however for:

- The Receiver (user B) losing the capability to receive pictures: The BYE and OPTIONS exchange would be initiated by the receiving client (user B) in this case.
- Both lose the capability to share pictures: The BYE and OPTIONS exchange would be initiated by the first client to lose the capability in this case.

Please note that there is an exception to stop a file transfer due to capabilities. If one of the users is left with 2G coverage (on a DTM terminal) once a transfer has started, the transfer may continue until completed, provided the handover did not trigger an IP bearer

reconfiguration. Once the transfer is completed however, picture sharing will no longer be available as a service during the call.

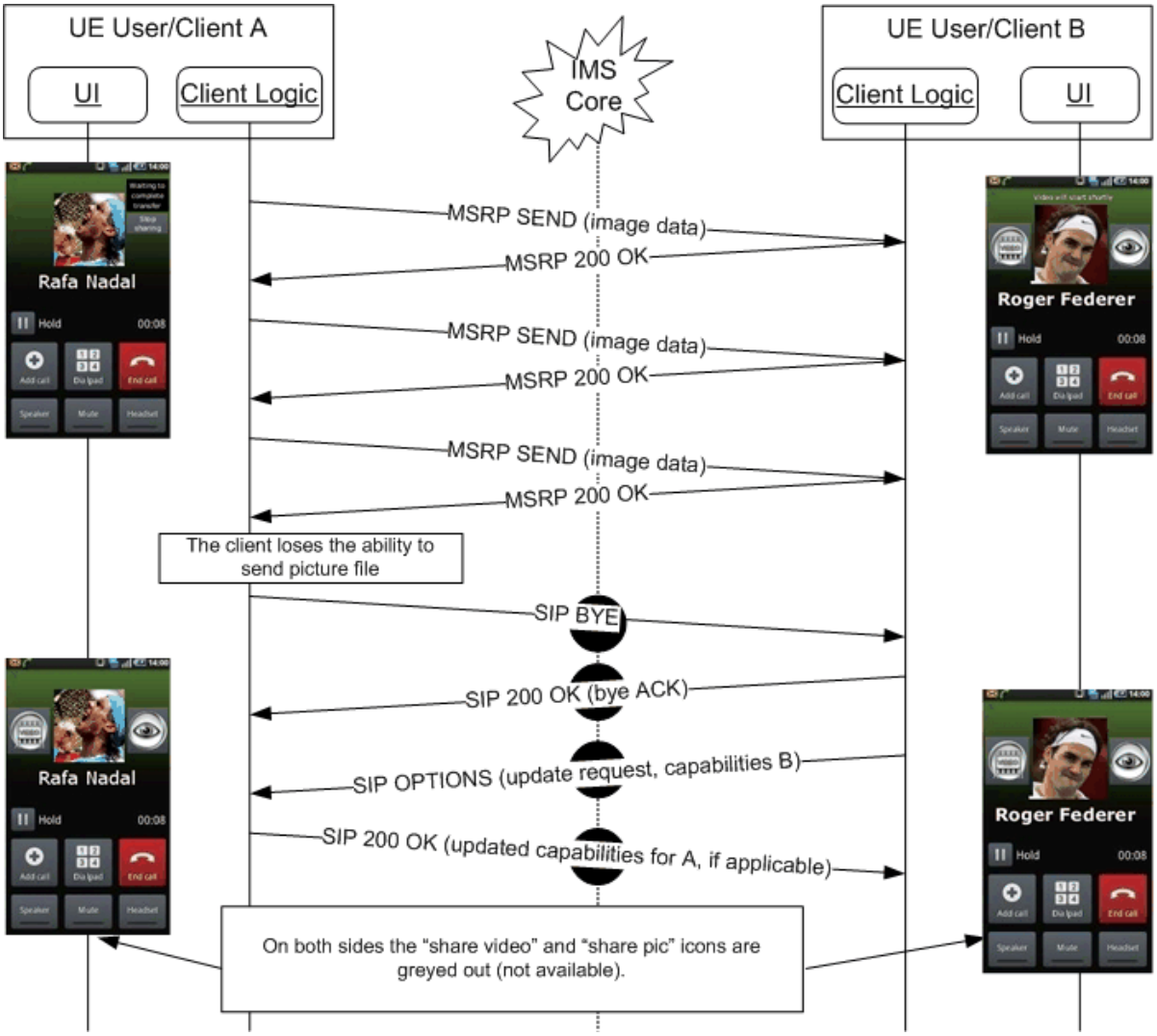

Figure 49: A picture can no longer be shared during a call (capability not available)

3.3.11 Decline share video or picture during a call

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

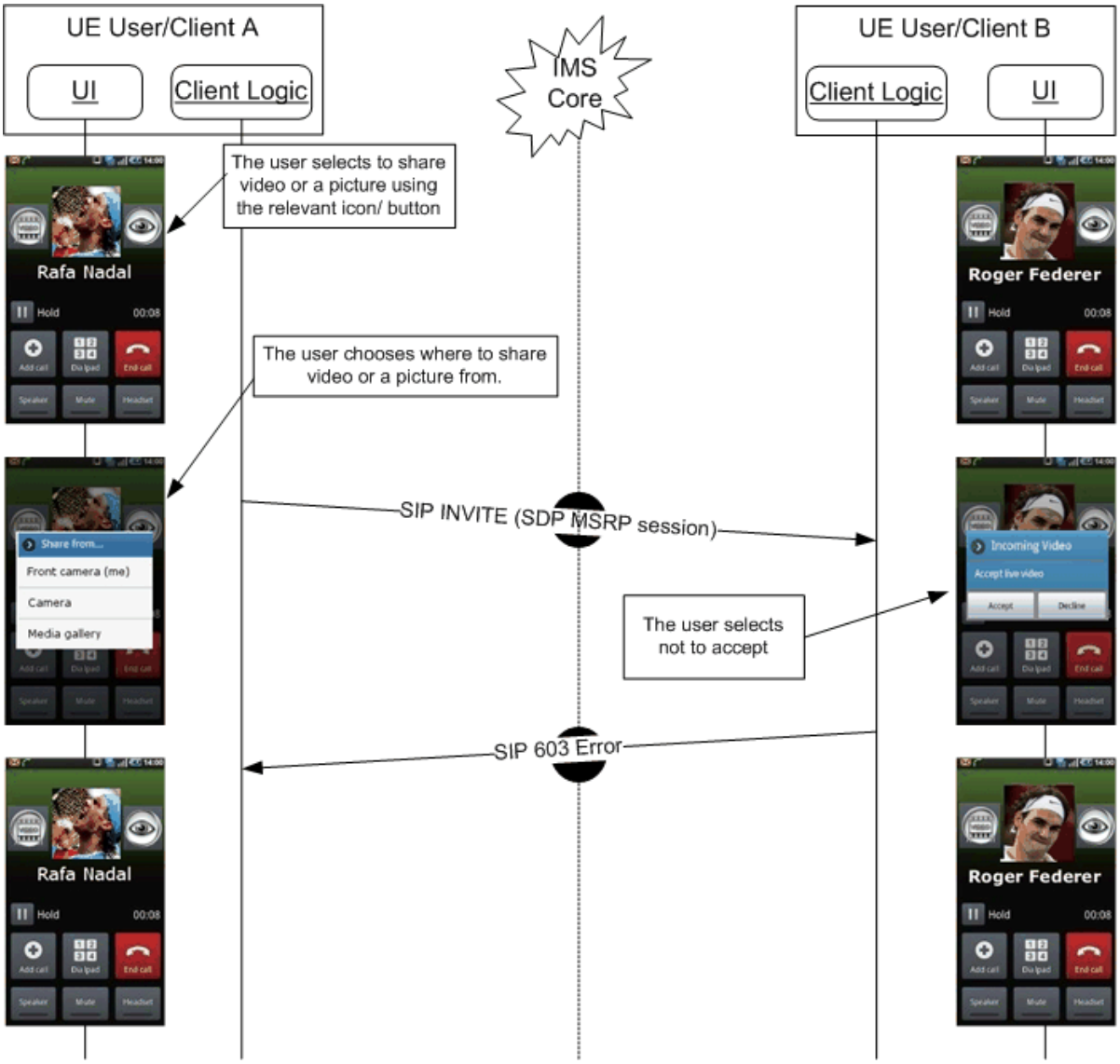

Figure 50: User declines sharing a picture during a call

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

In this case, User A is sharing video or a picture with user B. Suddenly, user A's connection to the network fails (This may for instance be due to a client error, a reboot of the phone, the loss of the data bearer, a switch in data carrier [like for instance 3G+ to 3G] causes an IP layer reconfiguration and so on).

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

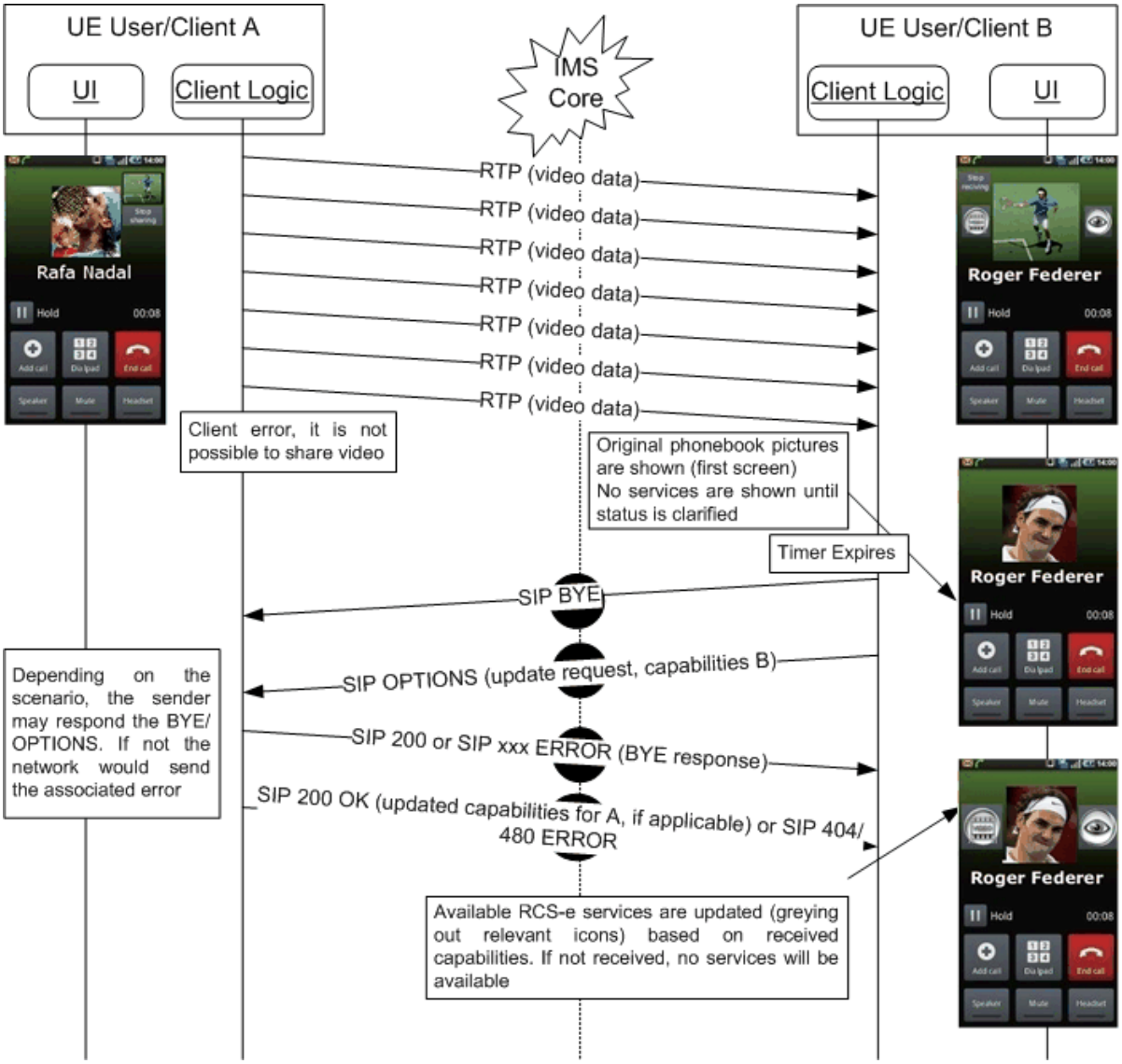

Figure 51: Non-graceful termination (sender) for video

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

To protect the IMS Core 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] in a similar way to the one mandated in [RCS2-OMA-SIMPLE-ENDORS], that is 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 use case, except that in this case User B (receiver) loses the ability to receive/process MSRP messages (this can for instance be due to a client error, a reboot of the phone, a loss of the data bearer and so on).

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

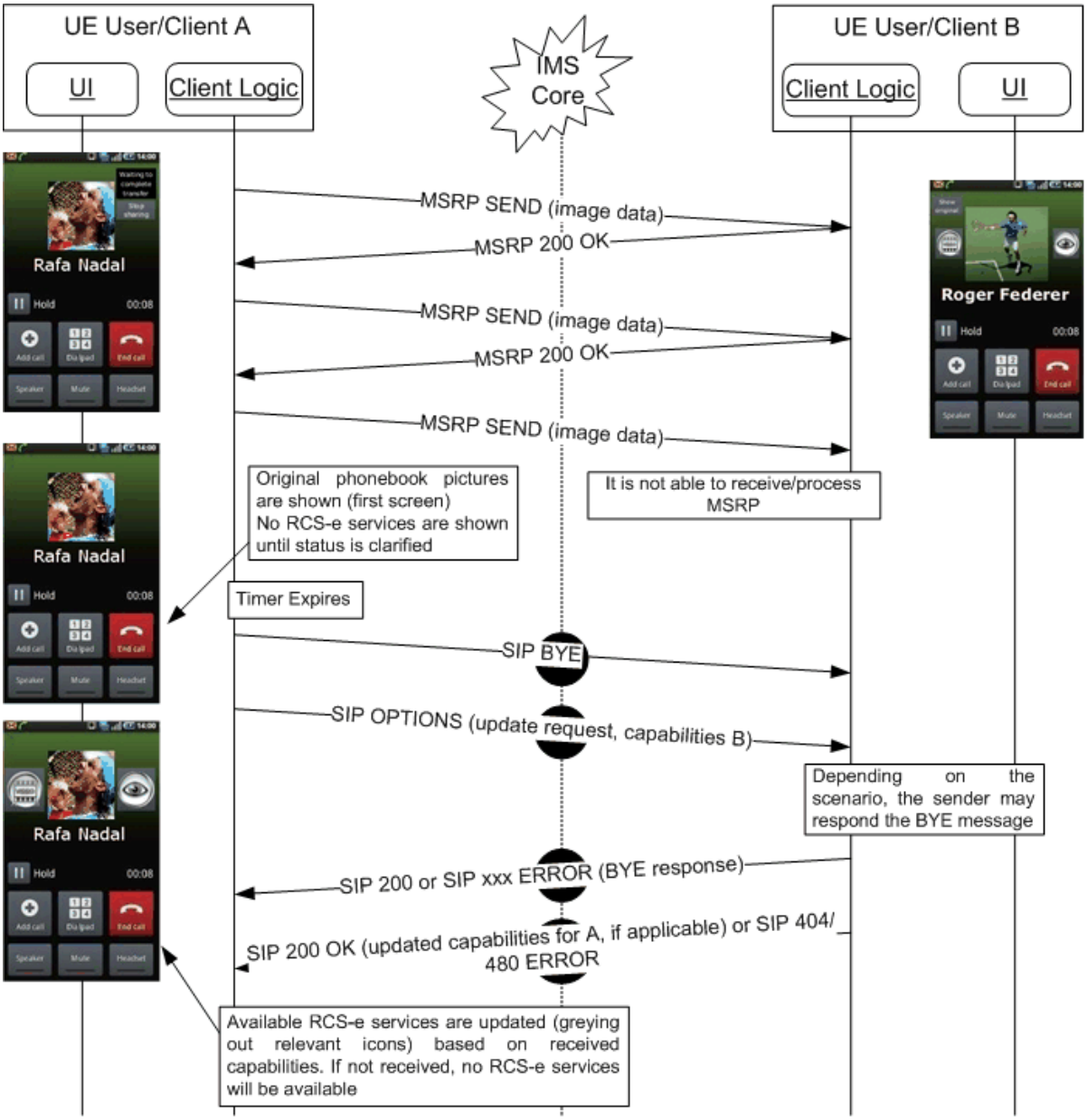

Figure 52: Non-graceful termination of video or picture sharing during a call

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

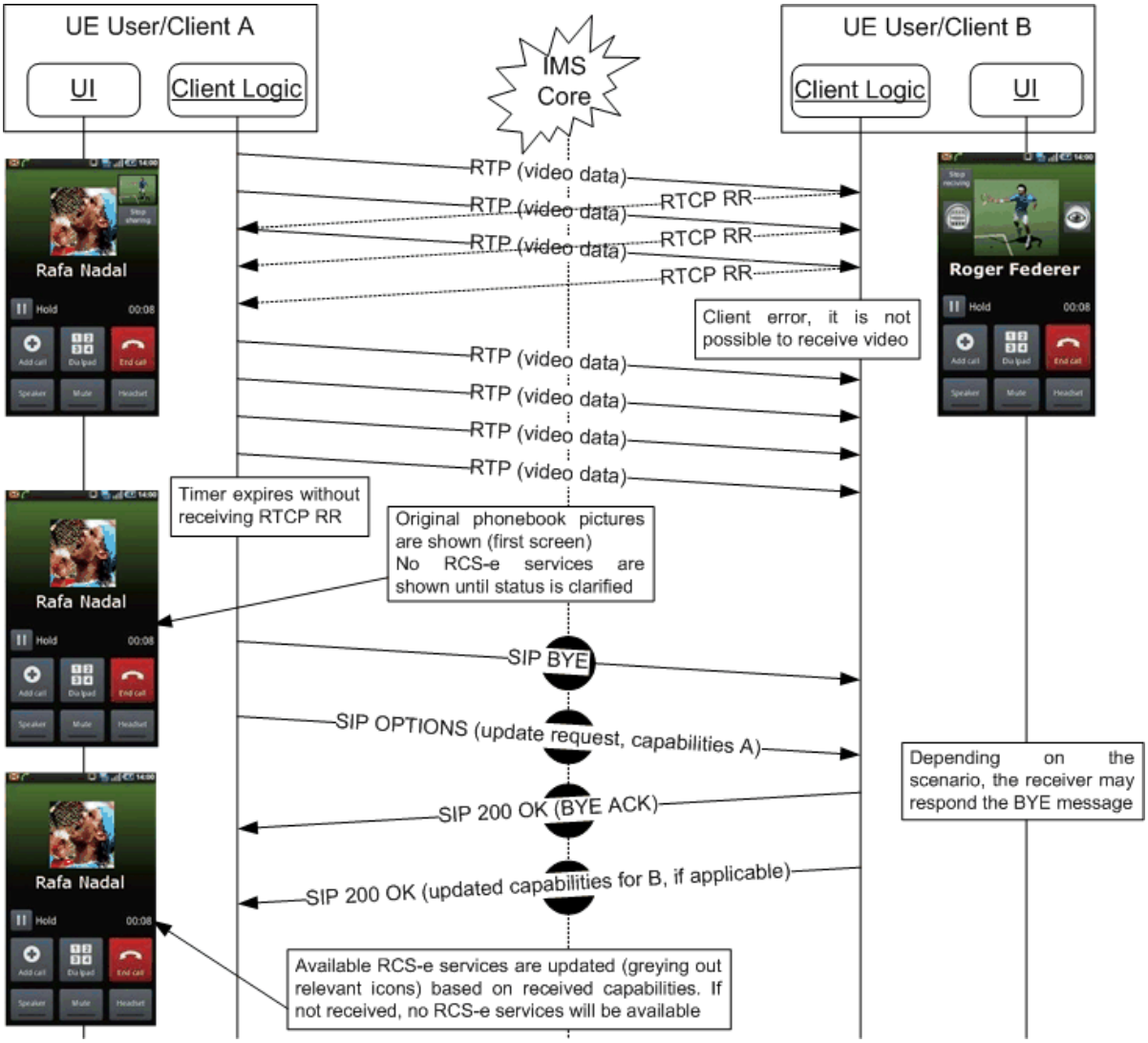

Figure 53: Non-graceful termination of video sharing during a call

3.3.14 Multiparty call and image/video share

Once a CS call is established between two users, it is possible for any one of them to add another party to the call, and consequently, initiate a multiparty call. From RCS services perspective 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, when switching to a multiparty call the client starting the process has to send a SIP OPTIONS request with a capability update (as described in section 3.3.2) indicating that the image and video share services are no longer available. The on-screen icons/layout should be 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. This can be either sender or receiver terminated, depending upon the 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 client initiating the multiparty call should report that the image

and video share services/capabilities are no longer available. The on-screen icons/layout should be updated accordingly.

- The users were in a CS call using image share with the transfer not being complete yet: In this case, switching to a multiparty call means ending the image share service. This can either be sender or receiver terminated, depending upon the 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 client initiating the multiparty call should report that the image and video share services/capabilities are no longer available. The on-screen icons/layout should be updated accordingly.
- The users were in a CS call using image share after the transfer has completed: In this case, switching to a multiparty call means that the picture is no longer shown in the call screen and that the client starting the process has to send a SIP OPTIONS message with a capability update (as described in section 3.3.2) indicating that the image and video share services are no longer available. The on-screen icons/layout should be 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 call is converted into a standard call (That is it becomes 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-e services perspective 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 on a CS call without using the image or video share services: In this case, when putting the call on hold the client starting the process has to send an SIP OPTIONS request with a capability update (as described in section 3.3.2) indicating that the image and video share services are no longer available. The on-screen icons/layout should be 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. This can either be sender or receiver terminated, depending upon the 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 client putting the call on hold should report that the image and video share services/capabilities are no longer available. The on-screen icons/layout should be updated accordingly.
- The users were in a CS call using image share with the transfer not having completed: In this case, putting the call on hold putting the call on hold means ending the image share service. This can either be sender or receiver terminated, depending upon the 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 client putting the call on hold should report that the image and video share services/capabilities are no longer available. The on-screen icons/layout should be updated accordingly.
- The users were on a CS call using image share after the transfer has completed: In this case, putting the call on hold means that the picture is no longer shown in the call screen and that the client starting the process has to send a SIP OPTIONS message with a capability update (as described in section 3.3.2) indicating that the image and

video share services are no longer available. The on-screen icons/layout should be updated accordingly.

It should be also noted that from the moment the call is put on hold (that is the call is not 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 the image and video share services (that is both for the capability exchange and the services itself) should not be affected by the fact that another call is on hold.

Finally, if the call is 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 (that is both for the 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 (because a hidden number is used for instance), it should not be possible to access the image and video share services between the caller and receiver.

3.3.18 Call divert/forwarding

If the receiver has call divert/forwarding active (the calls are for instance forwarded to another number or to voicemail), it is not possible to access the image and video share services from the caller to the receiver.

3.4 File transfer

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

From the UX experience perspective, there are five possible entry points to this service:

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

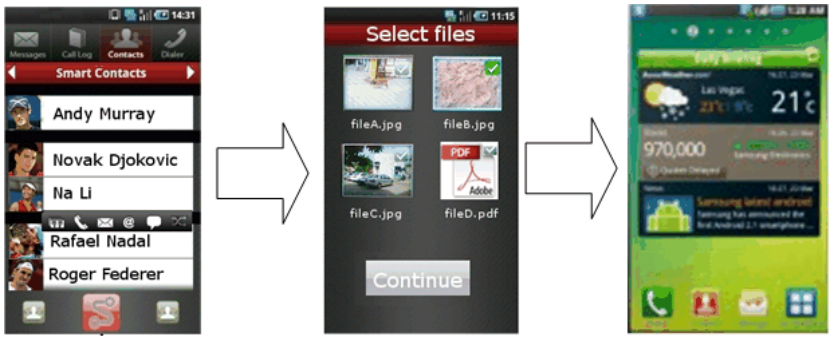

Figure 54: Reference UX for accessing file share from address book/call-log

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

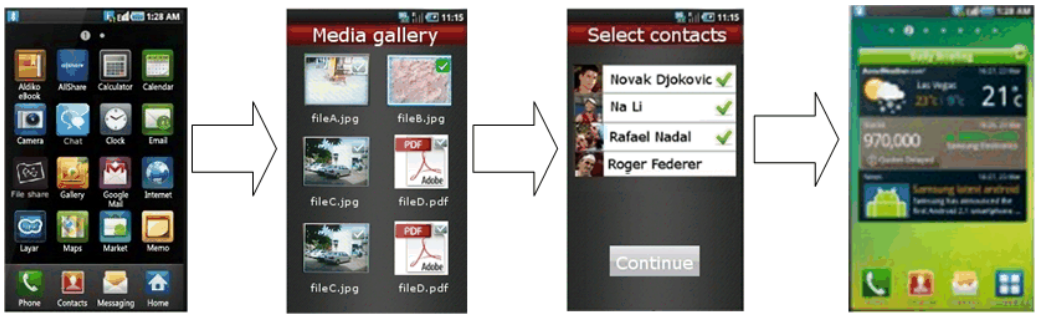

Figure 55: Reference UX for accessing file share from media gallery or file browser

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.

3. Camera application: The experience is similar to the media gallery/file browser experience with the difference being that the user is able to select only the last picture or video (and, in some cases, a picture or video from the camera gallery) to be shared.
4. IM/chat window: From the IM (only in one-to-one chat) 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 the user can choose a file which, is then shared with the conversation partner.

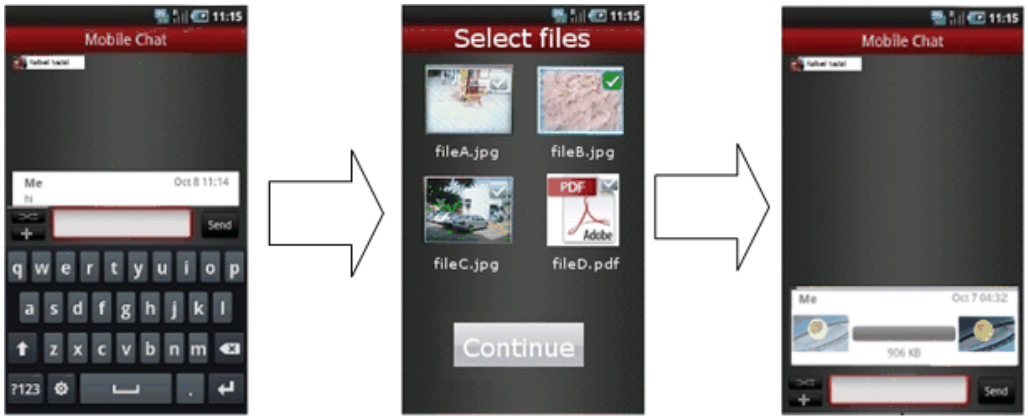

Figure 56: Reference UX for accessing file share from an IM window

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

When transferring a file whilst not in an existing session (that is when not in a call or IM with the contact with whom the file is shared) and after the transfer has started (that is 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 57: Reference UX for file transfer on the receiver side

3.4.1 General assumptions

In the following sections the relevant message flows and reference user experiences (UX) will be shown. These are based upon the following assumptions:

- For simplicity, the internal mobile network interactions are omitted in the diagrams that are shown.
- It is assumed that by the time the file transfer begins, both the sender and the recipient have exchanged their capabilities using the OPTIONS exchange. Please note that if there is a UI flow which invalidates this assumption, OPTIONS requests should be exchanged between the sender and the receiver (bidirectional) prior to starting these flows.
- All the file transfer service exchanges presented in this document comply with the GSMA RCS[33] and OMA-SIMPLE IM specification[34] 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 with whom the file will be shared. Please note that the list that is presented initially 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 (that is that user should be registered and the right capabilities should be in place)

[33] By this reference we include both the technical and functional references contained in the RCS Release 2 specifications ([RCS2-TEC-REAL], [RCS2-SD] and [RCS2-FUN-DESC])

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

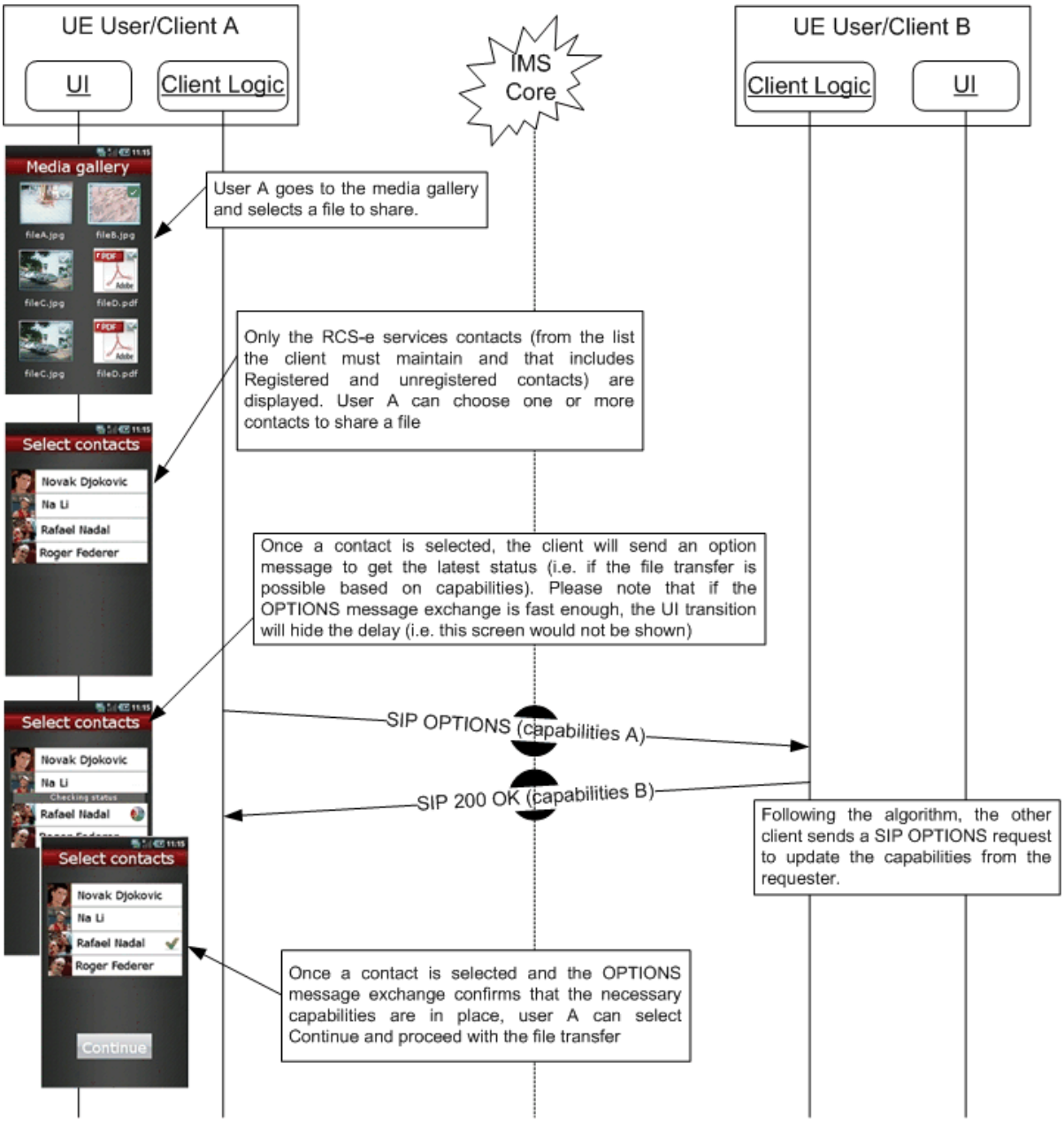

Figure 58: Selecting users when sharing a file from the media gallery/file browser

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, the individual file transfers (in each transfer only a single file is shared with one user only) are serialised. This means that it is not supported to have simultaneous file sharing sessions running in parallel.

In the following diagram, it is assumed the receiver accepts the transfer.

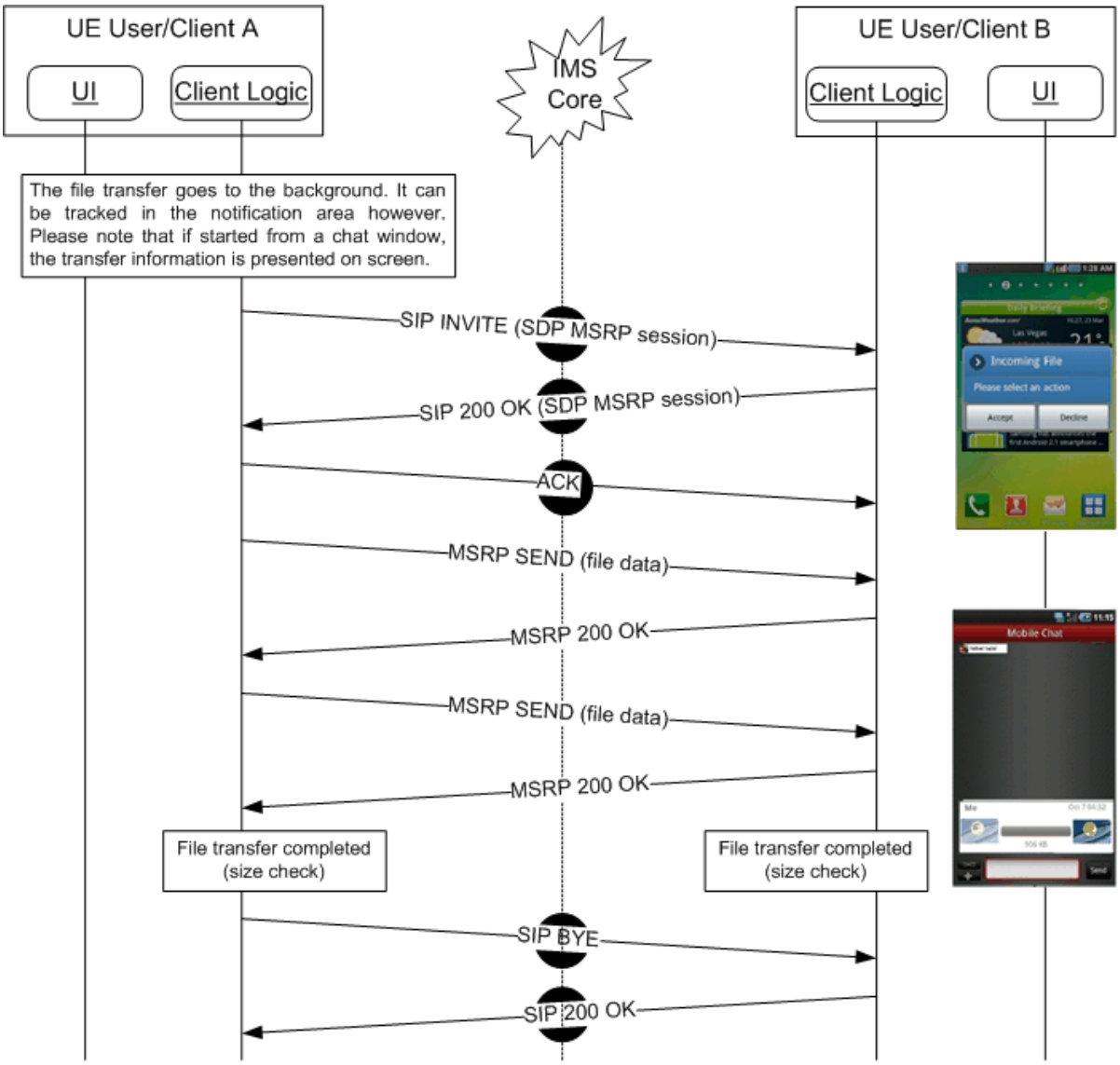

Figure 59: Standard file transfer sequence diagram – Successful transfer

In the following diagram, User B rejects the transfer.

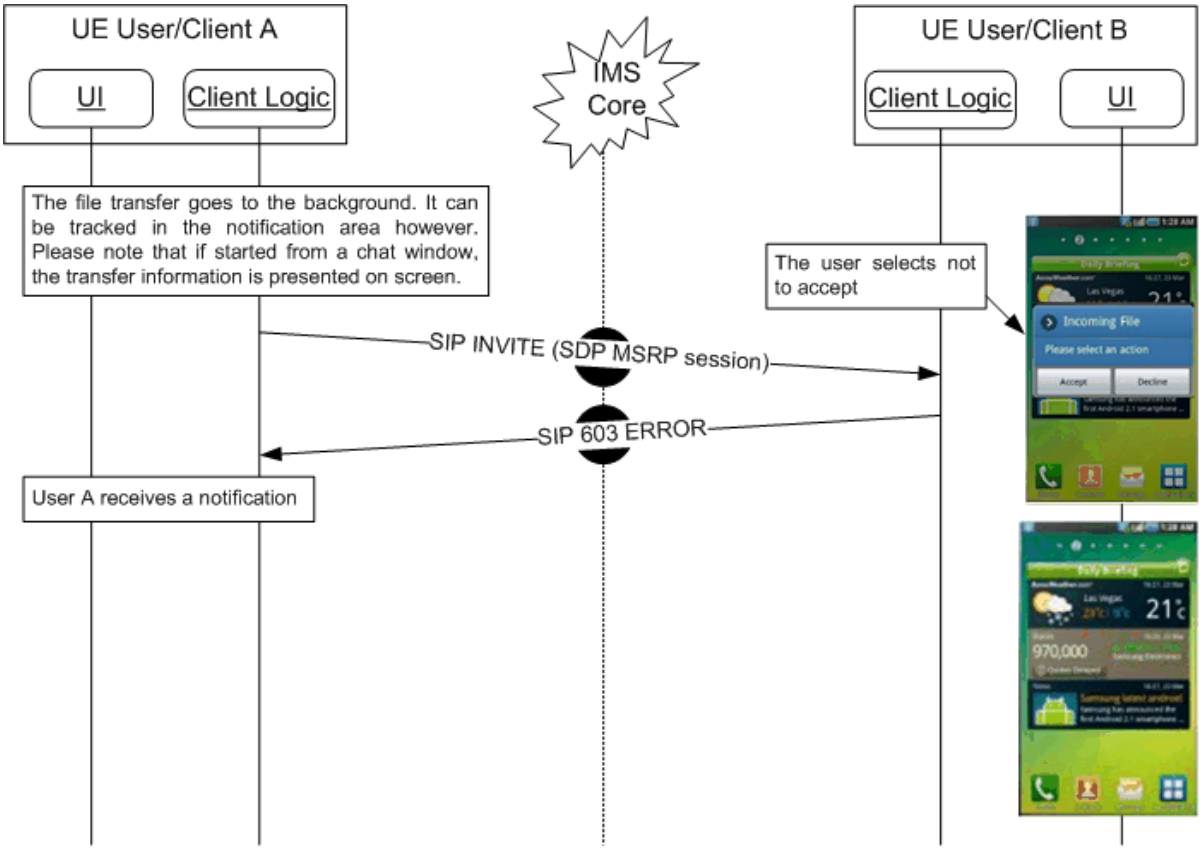

Figure 60: Standard file transfer sequence diagram – Receiver rejects the transfer

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 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 image 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 image 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 change, 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 on one of the ends a handover into 2G (2G GPRS data coverage) occurs 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. This means that any kind of file can be transferred using this service. Taking this into account and with the aim of providing all the necessary facts to the receiver allowing to make an informed decision on whether to accept or to 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 their handset cannot process that document, 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 user making the decision on accepting or rejecting the file transfer.

Finally note that each individual MNO may introduce restrictions taking into account different considerations such as security, intellectual property and so on.

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 2 for reference) may be enabled.

From the user experience perspective and assuming that 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 (that is at protocol level, the SIP INVITE will never be sent or an automatic rejection response will be sent to the other end depending on the scenario).

ANNEX A Extensions to the data model

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

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

A.1 Management objects parameter additions

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

A.1.1 Presence related configuration

The 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] apply.	Mandatory parameter

Table 23: RCS-e additional presence related configuration parameters

A.1.2 XDM related configuration

The RCS-e specification does not include any additional XDM related parameters apart from those mentioned in [RCS2-MO]. 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

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

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 (such as Group Chat) will not be available to 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 by 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 purposes only. If the 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 circumstances (by showing a message on the screen for instance). 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 confirming that the MSRP session can be established: 0 (RCS-e default): The 200 OK is sent when the receiver consumes the notification by opening the chat window. 1 (RCS default): The 200 OK is sent when the receiver starts to type a message to be sent back in the chat window. 2: The 200 OK is sent when the receiver presses the button to send a message (that is the message will be buffered in the client until the MSRP session is established). Note: as described in section 3.2, the parameter only affects the behaviour for a 1-to-1 session in case no session between the parties has been established yet.	Mandatory parameter

Table 24: 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]. Again, if set to 0, this limitation does not apply.

A.1.4 File transfer related configuration

The 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 Kilobyte (KB). If a file is bigger than FT MAX SIZE, the transfer will be cancelled automatically. Please note that if it is 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 it is set to 0, the user will not be warned.	Mandatory parameter

Table 25: 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]. Again, if set to 0, this limitation does not apply.

A.1.5 IMS Core /SIP related configuration

The RCS-e specification includes the following additional IMS Core/SIP related configuration parameters:

Configuration parameter	Description	RCS-e usage
DEVICE ID	This controls the identity provided in the sip.instance parameter during registration (see chapter 2.15). It is only relevant in case the client has access to the device's IMEI. Then handling will be as follows: 1: a UUID or hashed value of the IMEI is provided 0: the value is set to the device's IMEI Please note that if not provided the device should use the IMEI. The value of 0 is thus the default.	Optional parameter

Table 26: RCS-e additional IMS Core/SIP related configuration parameters

Also, it should be noted that:

- The USER and PASSWD parameters described in section 2.1 Table 2 map to the UserName and UserPwd parameters described in [RCS2-MO].
- The TEL-URI and SIP-URI parameters map to the Public_User_Identity parameters defined in [3GPP TS 24.167][35] and endorsed in [RCS2-MO].
- The SIP PROXY parameter maps to the parameters hosted by the LBO_P-CSCF_Address sub-tree defined in [3GPP TS 24.167] and endorsed in the Managed Object document (version 1.1) that is part of the GSMA RCS Release 2 specifications. When the P-CSCF address has an "FQDN" type (Fully Qualified Domain Name), the SIP transport protocol can be selected by the RCS-e client thanks to Domain Name System (DNS) Server (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

The 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

The 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, the RCS-e specification includes the following additional capability discovery configuration parameters:

[35] 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 considers them writable during the autoconfiguration process (OMA-DM, OMA-CP or the alternative HTTP mechanism).

Configuration parameter	Description	RCS-e usage
POLLING PERIOD	This is the frequency in seconds at which to run a periodic capabilities update for all the contacts in the phone's address book whose capabilities are not available (such as non-RCS-e users) or are expired (see CAPABILITY INFO EXPIRY parameter). Please note that if set to 0, this periodic update is not/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 SIP OPTIONS. When performing a whole address book 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 tag associated 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 tag associated 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 27: RCS-e additional capability discovery related configuration parameters

A.1.9 APN configuration

Although not covered in RCS Release 2, the 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 of 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 (MNO decision) only be shown during roaming.	Mandatory parameter

Table 28: RCS-e roaming configuration parameters

A.1.10 End user confirmation parameters

Although not covered in RCS Release 2, the RCS-e specification includes the following additional configuration parameters targeting the End user confirmation configuration (see section 2.14):

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

Table 29: RCS-e end user confirmation parameters

A.2 RCS Management trees additions

Please note that the information contained in this section is aimed to complement section 4 of [RCS2-MO]. 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 (that is the /<X> root nodes) is *urn:gsma:mo:rcs:rcse* instead of *urn:gsma:mo:rcs:2.0*. All RCS-e specific MOs shall be placed in RCS-e subtree

A.2.1 IMS sub tree additions

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

As the RCS Release 2 specifications do not cover OMA-CP based configuration of RCS clients, the OMA-CP configuration XML structure associated to the parameters defined in the RCS Release 2 specification is presented in the table below.

```
<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”/>
        <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 30: IMS sub tree associated OMA-CP configuration XML structure

A.2.2 Presence sub tree additions

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

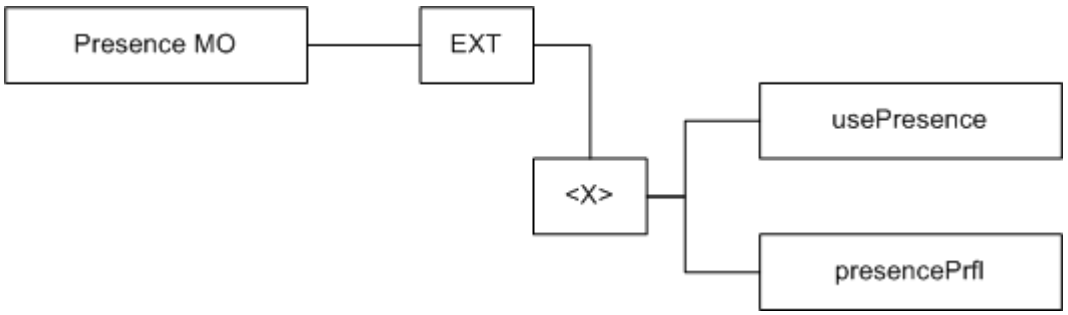

Figure 61: RCS-e additions to the presence MO sub tree

The associated OMA-CP configuration XML structure is presented in the table below. Please note that as RCS Release 2 specification does not cover the OMA-CP based configuration of RCS clients, both RCS (marked in blue) and RCS-e parameters are shown in this case (and thus not only additions as is the case 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="PublishTimer" value="X"/>
        <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 31: Presence sub tree associated OMA-CP configuration XML structure

Node: /<X>

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

Status	Occurrence	Format	Min. Access Types
Required	One	node	Get

Table 32: 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 33: 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 or not the social presence functionality is supported.

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

Table 34: 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 [RCS2-MO].

As the RCS Release 2 specifications do not cover the OMA-CP based configuration of RCS clients, the OMA-CP configuration XML structure associated to the parameters defined in the RCS Release 2 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 35: XDMS sub tree associated OMA-CP configuration XML structure

A.2.4 IM MO sub tree addition

The RCS-e specification includes the following additions to the IM MO sub tree:

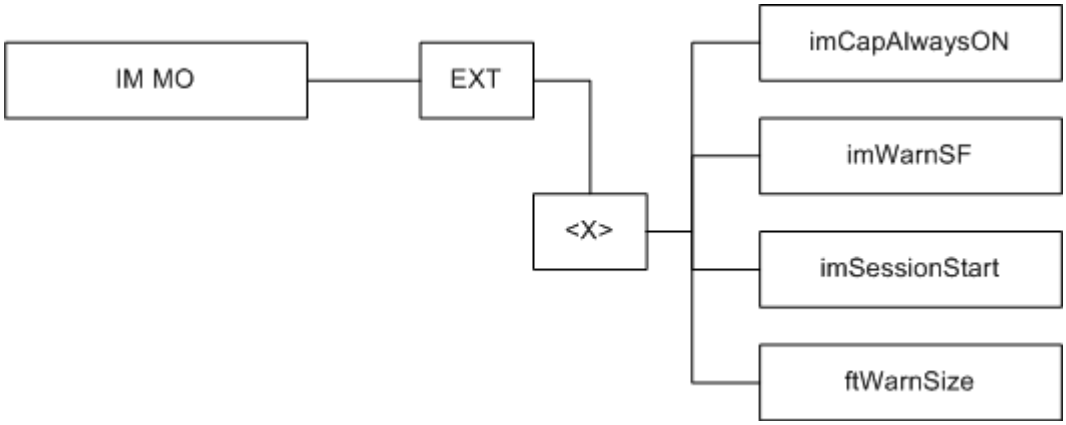

Figure 62 : RCS-e additions to the IM MO sub tree

The associated OMA-CP configuration XML structure is presented in the table below. Please note that as the RCS Release 2 specifications do not cover OMA-CP configuration of RCS clients, both RCS (marked in blue) and RCS-e parameters are shown in this case (and thus not only additions as is the case 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 36: IM sub tree associated OMA-CP configuration XML structure

Node: /<X>

Under this interior node the RCS parameters related to the IM configuration are placed.

Status	Occurrence	Format	Min. Access Types
Required	One	node	Get

Table 37: 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 of whether or not 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 38: IM MO sub tree addition parameters (IMCAPAlwaysOn)

- Values: 1, RCS IM/chat server based store and forward is enabled; 0, it 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 ID: “imCapAlwaysOn”

Node: /<X>/imWarnSF

Leaf node that describes whether the UX should alert the user that messages are handled differently when the store and forward functionality is involved.

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

Table 39: IM MO sub tree addition parameters (imWarnSF)

- Values: 1, the user is made aware via the UX when the messages are deferred using S&F. 0, the user is not aware that messages are deferred.
- 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 ID: “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 40: 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 by opening the chat window.
    - 1 (RCS default):
      The 200 OK is sent when the receiver starts to type a message to be sent back in the chat window.
    - 2 (new option):
      The 200 OK is sent when the receiver presses the button to send a message (That is the message 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 ID: “imSessionStart”

Node: /<X>/ftWarnSize

Leaf node that describes the file transfer size threshold (in KB) 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 41: 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 ID: “ftWarnSize”

A.2.5 Capability discovery MO sub tree

The RCS-e specification includes the following additions as a new configuration sub tree, the capability discovery MO sub tree. Please note this sub tree is not included in the RCS Release 2 specifications. So no other nodes from those specifications need to be added:

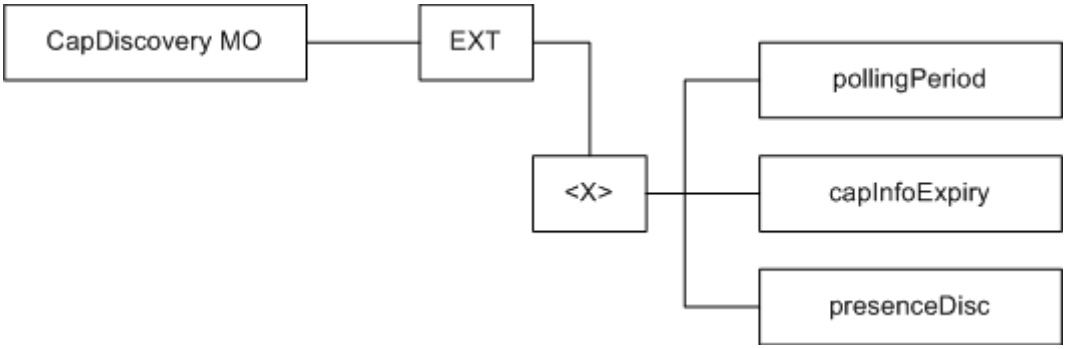

Figure 63 : RCS-e additions, capability sub tree

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 42: Capability sub tree associated OMA-CP configuration XML structure

Node: /<X>

Under this interior node the RCS-e parameters related to capability discovery are placed.

Status	Occurrence	Format	Min. Access Types
Required	One	node	Get

Table 43: 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 44: Capability MO sub tree addition parameters (pollingPeriod)

- Values: The time in seconds. If it is 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 ID: “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 45: 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 ID: “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 46: Capability MO sub tree addition parameters (presenceDisc)

- Values: If it is set to 1, it is supported. If it is 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 ID: “presenceDisc”

A.2.6 APN configuration MO sub tree

The RCS-e specification includes the following additions as a new configuration sub tree, the roaming MO sub tree. Please note this sub tree is not included in the RCS Release 2 specifications. So no other nodes from those specifications need to be added:

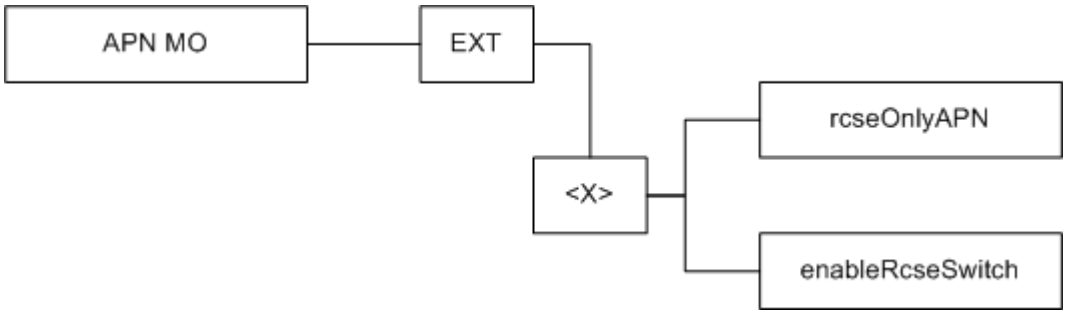

Figure 64: RCS-e additions, roaming sub tree

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 47: APN sub tree associated OMA-CP configuration XML structure

Node: /<X>

Under this interior node the RCS parameters related to roaming are placed.

Status	Occurrence	Format	Min. Access Types
Required	One	node	Get

Table 48: 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 49: 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 ID: “rcseOnlyAPN”

Node: /<X>/enableRcseSwitch

Leaf node that describes whether or not to show the RCS-e enabled/disabled switch permanently as described in section 2.10.

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

Table 50: Roaming MO sub tree addition parameters (enableRcseSwitch)

- Values: If it is set 1, the setting is shown permanently. Otherwise it may (MNO decision) only be 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 ID: “enableRcseSwitch”

A.2.7 Other RCS-e configuration sub tree

The RCS-e specification includes the following additions as a new configuration sub tree, containing the remaining RCS-e configuration parameters. Please note this sub tree is not included in the RCS Release 2 specifications. So no other nodes from those specifications need to be added:

Figure 65: 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"/>
        <parm name="deviceID" 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 51: Other sub tree associated OMA-CP configuration XML structure

Node: /<X>

Under this interior node the RCS-e parameters which do not fit in the other categories are placed.

Status	Occurrence	Format	Min. Access Types
Required	One	node	Get

Table 52: 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-Identity) used for sending the end user confirmation request.

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

Table 53: Other MO sub tree addition parameters (endUserConfReqId)

- Values: The identity (P-Asserted-Identity) 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 ID: “endUserConfReqId”

Node: /<X>/deviceID

Leaf node that describes how a client that supports GRUU and has access to the device’s IMEI must generate the deviceID that is used in the sip.instance parameter in the REGISTER request

Status	Occurrence	Format	Min. Access Types
Optional	One	Int	Get/Put

Table 54: Other MO sub tree addition parameters (deviceID)

- Values:
    - 0, the device’s IMEI is used as value for the sip.instance parameter (default if parameter is not provided)
    - 1, either a hashed version of the IMEI is used or a generated UUID.
- 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: “deviceID”

Node: /<X>/transportProto

Under this interior node the RCS-e parameters related to the transport protocols which are employed to carry the signalling and media data required for RCS-e, are placed.

Status	Occurrence	Format	Min. Access Types
Required	One	node	Get

Table 55: 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 the signalling when connecting over PS cellular access.

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

Table 56: 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 the media (e.g. IM, file transfer and image share services) when connecting over PS cellular access.

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

Table 57: 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 the real time media (e.g. video share) when connecting over PS cellular access.

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

Table 58: 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 the signalling when connecting over Wi-Fi.

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

Table 59: 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 the media (e.g. IM, file transfer and image share services) when connecting over Wi-Fi___33 access.

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

Table 60: 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 the real time media (e.g. video share) when connecting over Wi-Fi___33 access.

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: “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[36]:

```
<?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 62: Complete RCS-e OMA-CP configuration XML structure

[36] Please note the application Id’s used in the example are provided for reference only 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
                <parm name=”title” value=”Example”/>
                <parm name=”message” value=”Hello world”/>
                <parm name=”Accept_btn” value=”X”/>
                <parm 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”/>

                -- Continues in the next table --
```

Table 63: Complete RCS-e autoconfiguration XML structure (1/3)

```
        -- Follows from previous table –

        <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>
    <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”>
                <parm name=”AutMa” value=”X”/>
            </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=”PublishTimer” value=”X”/>
            <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>

        -- Continues in the next table --
```

Table 64: Complete RCS-e autoconfiguration XML structure (2/3)

```
        -- Follows from previous table –

        <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>
        <characteristic type=”OTHER”>
            <parm name=”endUserConfReqId” value=”X”/>
            <parm name=”deviceID” 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 65: Complete RCS-e autoconfiguration XML structure (3/3)

ANNEX B IM and store and forward diagrams

B.1 IM without store and forward

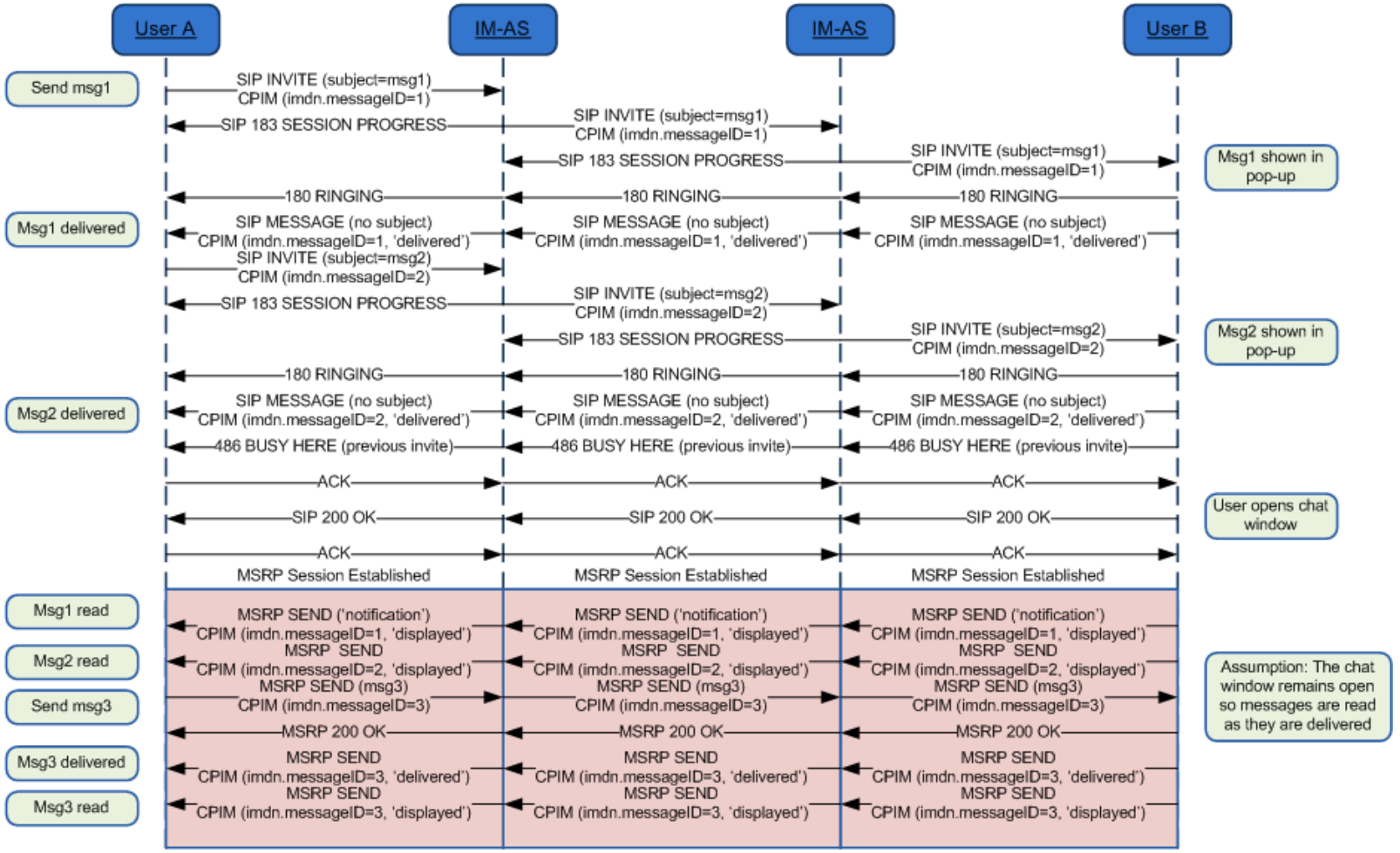

Figure 66: IM flow without store and forward *

*: Check NOTE 1 in section B.12

B.2 Store and forward: Receiver offline

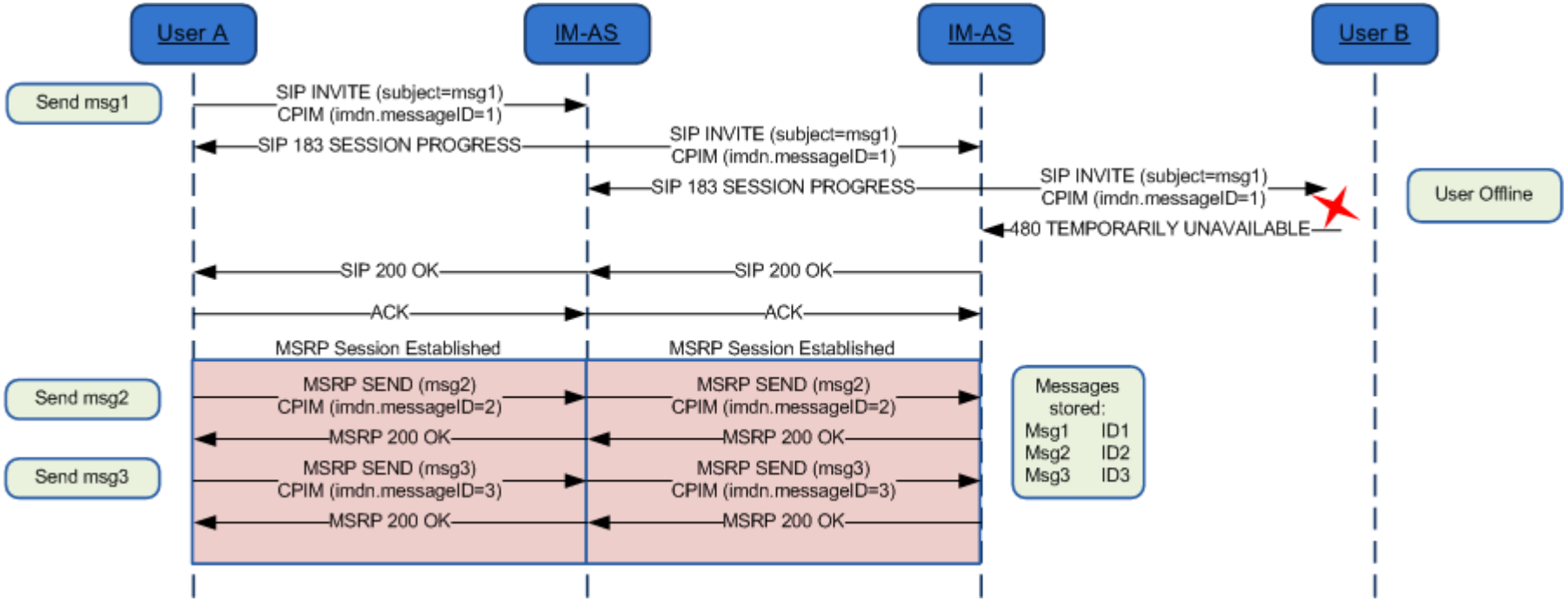

Figure 67: Store and forward: Receiver offline*

*: 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

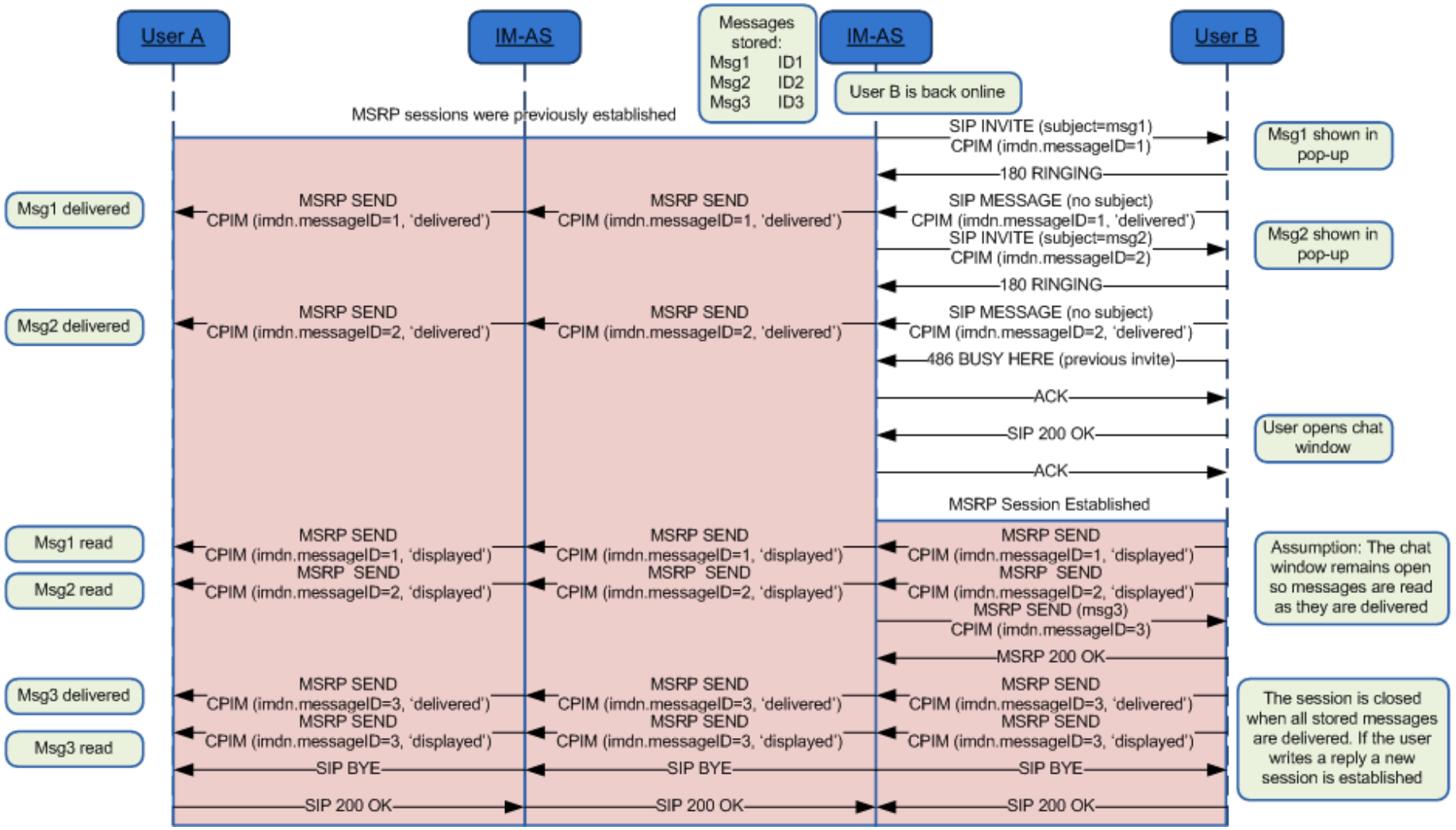

Figure 68: Store and forward: Message(s) deferred delivery with a sender still on an MSRP session*

*: Check NOTES 1, 2, 3, 4, 7, 11 and 12 in section B.12

B.4 Store and forward: Message deferred delivery with sender online

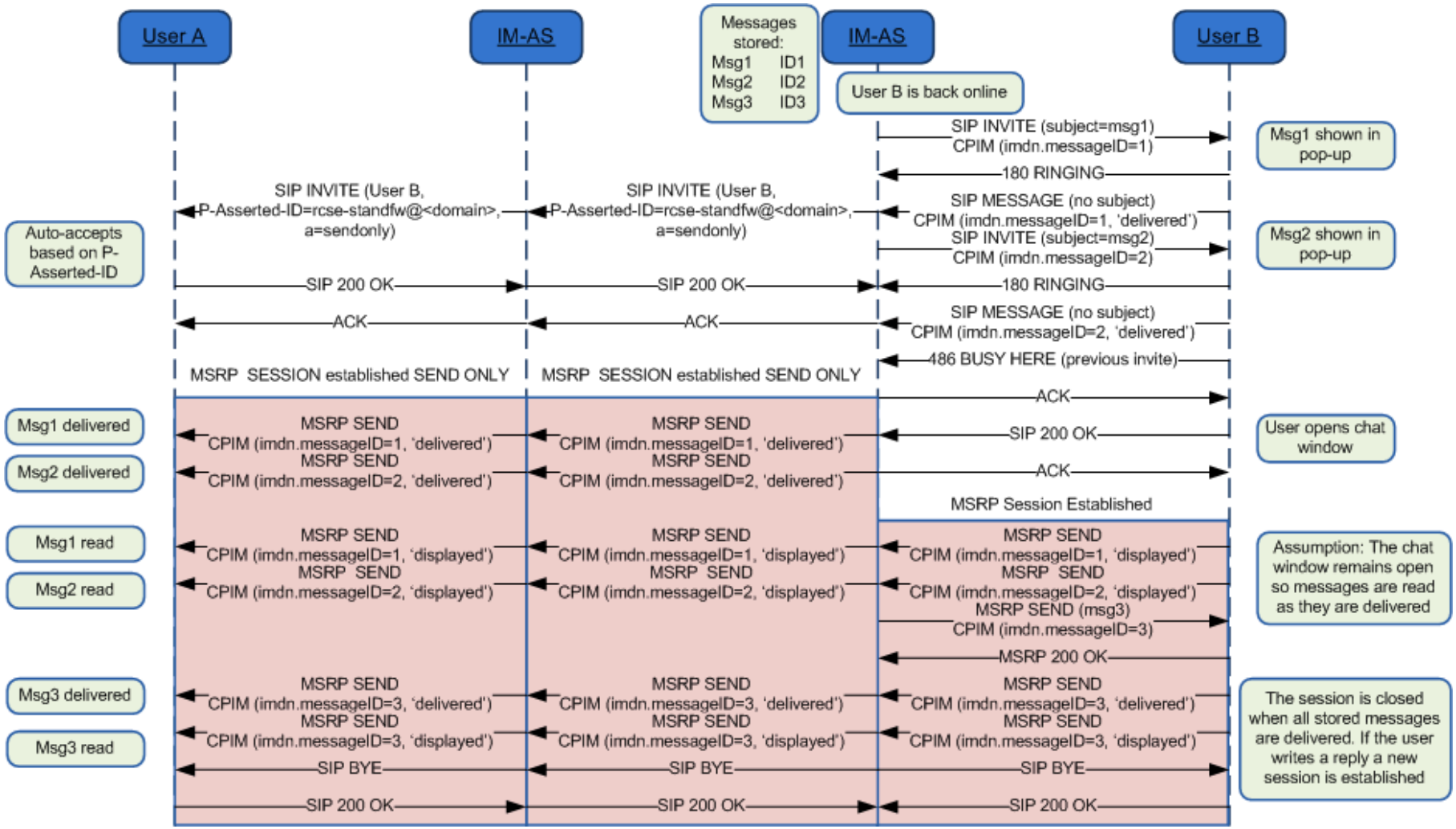

Figure 69: Store and forward: Message deferred delivery with sender online *

*: Check NOTES 1, 3, 4, 5, 7, 11 and 12 in section B.12

B.5 Store and forward: Message deferred delivery with sender offline (delivery notifications)

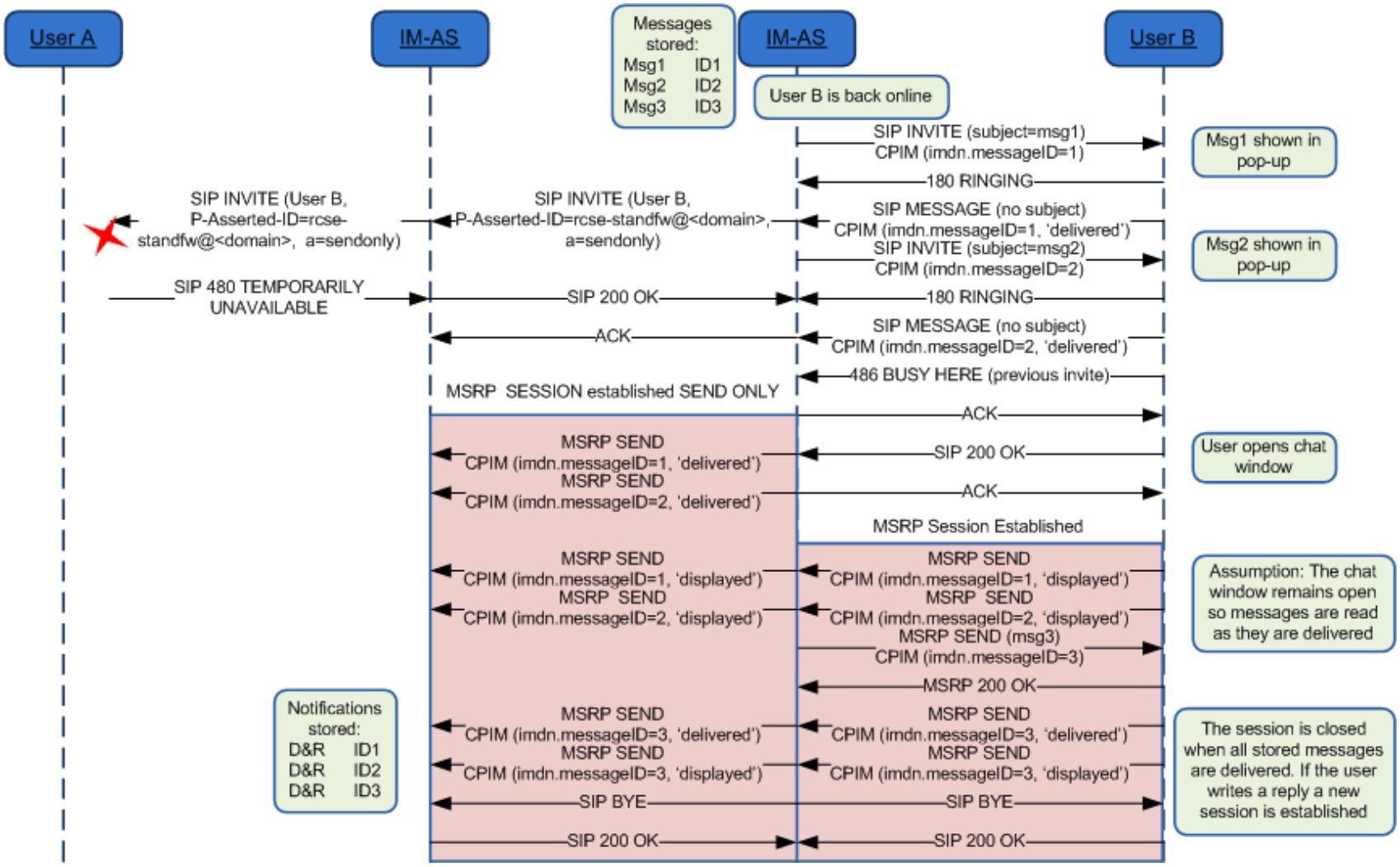

Figure 70: Store and forward: Message(s) deferred delivery with a sender offline (delivery notifications)*

*: Check NOTE 1, 5, 7, 11 and 12 in section B.12

B.6 Store and forward: Notifications deferred delivery

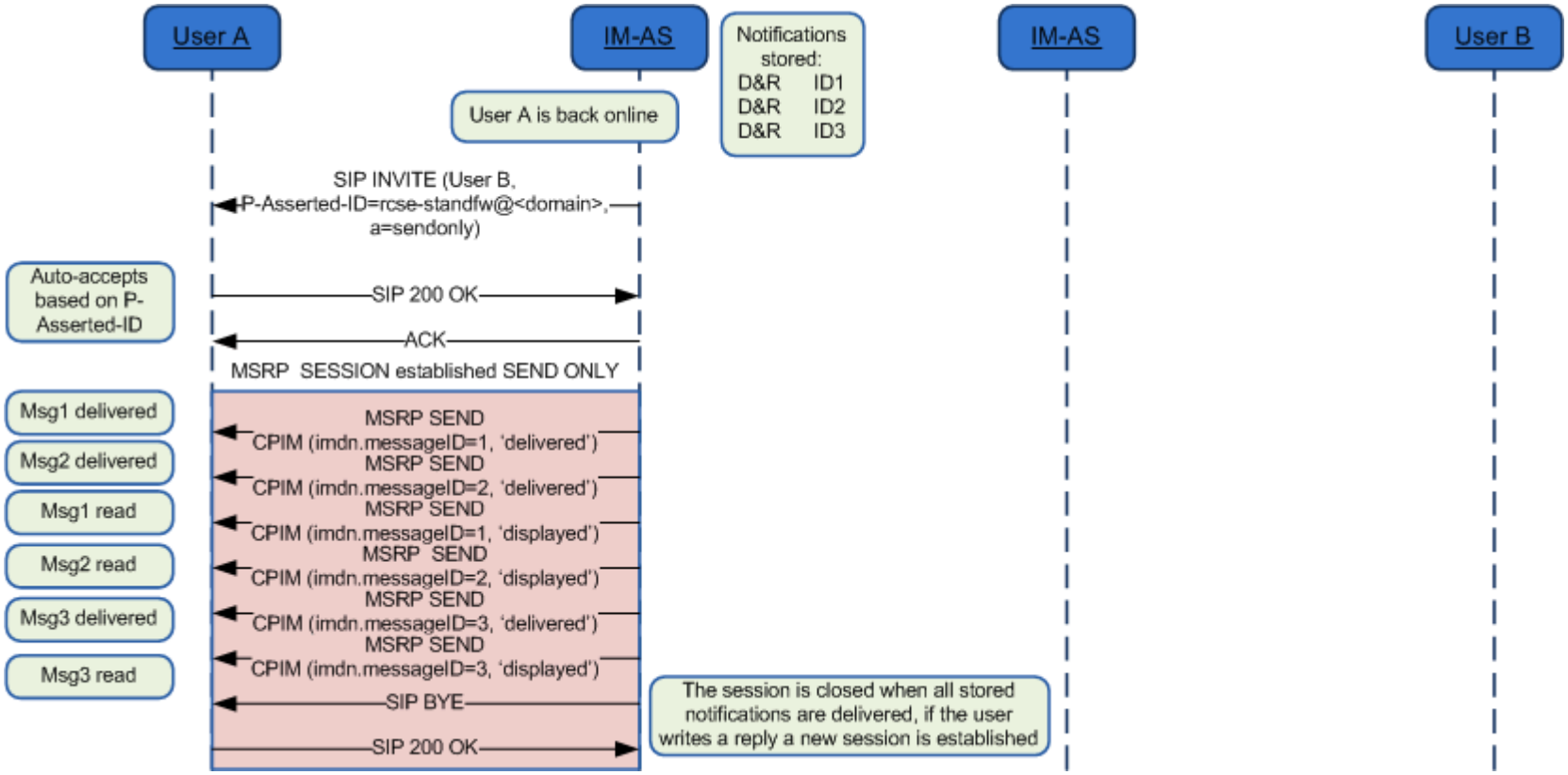

Figure 71: Store and forward: Notification(s) deferred delivery*

*: Check NOTES 1, 4, 5, 11 and 12 in section B.12

B.7 Delivery of displayed notifications in an unanswered chat (without store and forward)

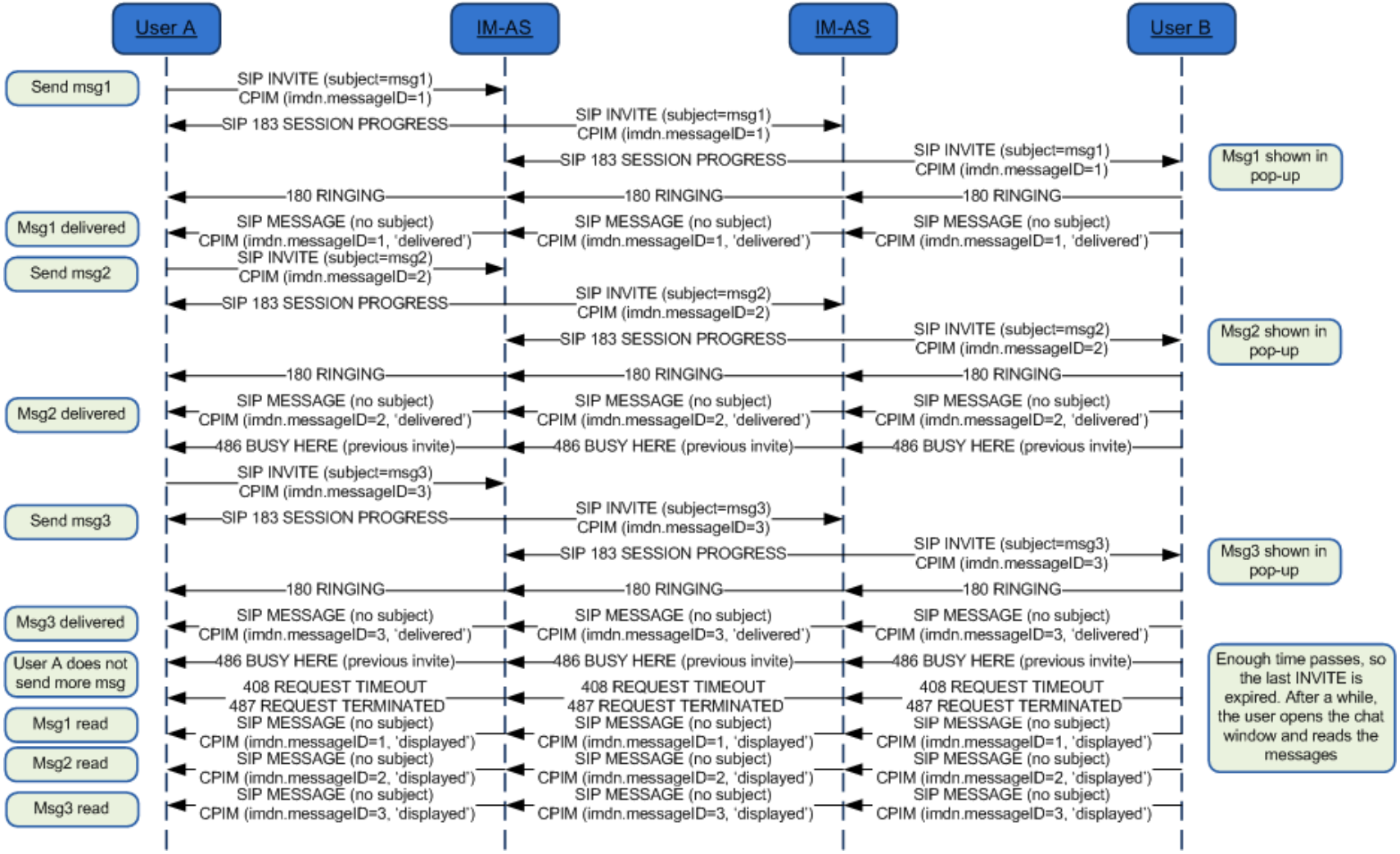

Figure 72: Delivery of displayed notifications in an unanswered chat (without store and forward)*

*: Check NOTE 1 and 10 in section B.12

B.8 Store and forward: Handling errors in the receiver's side

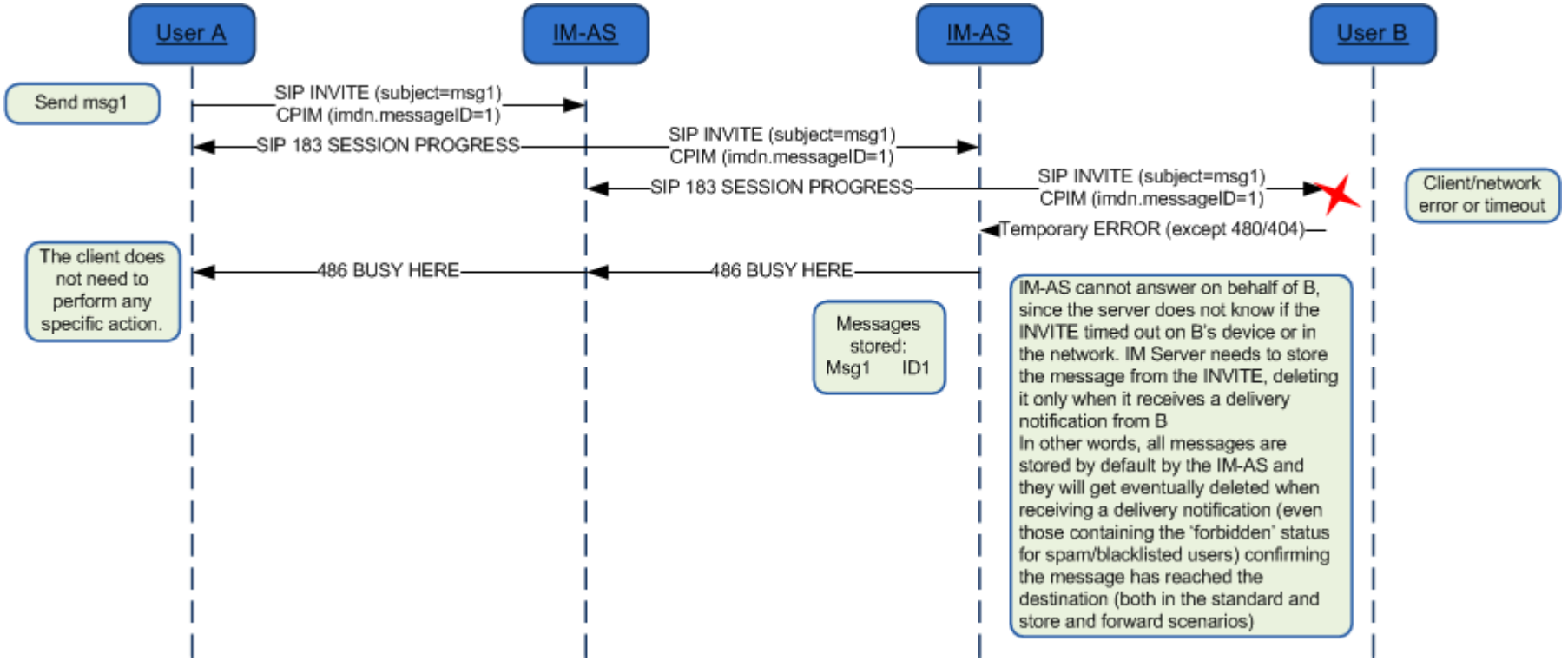

Figure 73: Store and forward: Handling errors in the receiver's side

Note: The error messages that are mapped to 486 Busy Here are listed in Table 22.

Also on the path between the IM-ASs similar errors could occur. In that case if the originating IM-AS supports Store and Forward, it will behave in the same way and store the message.

B.9 Race conditions: Simultaneous INVITEs

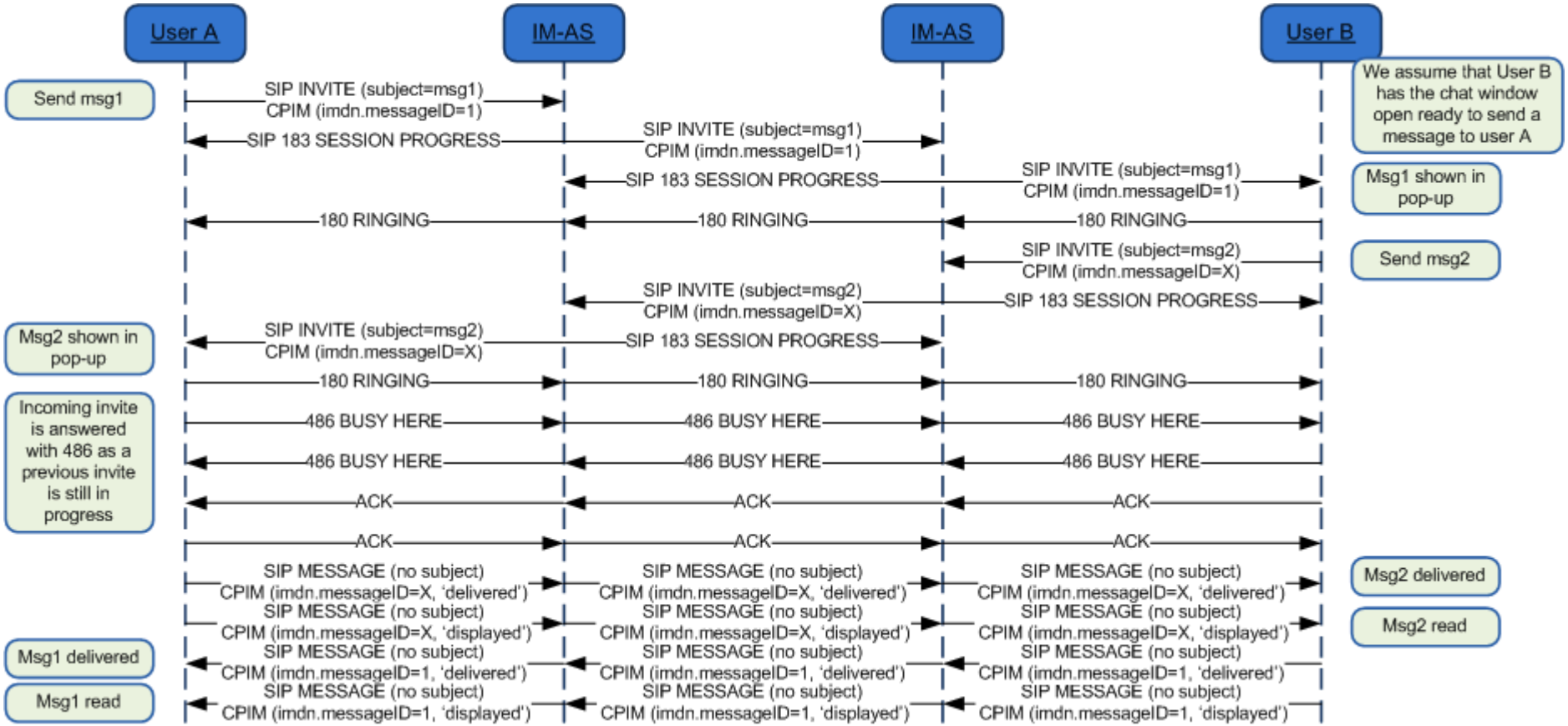

Figure 74: Store and forward race conditions: Simultaneous INVITEs*

*: Check NOTE 1 in section B.12

B.10 Race conditions: New INVITE after a session is accepted

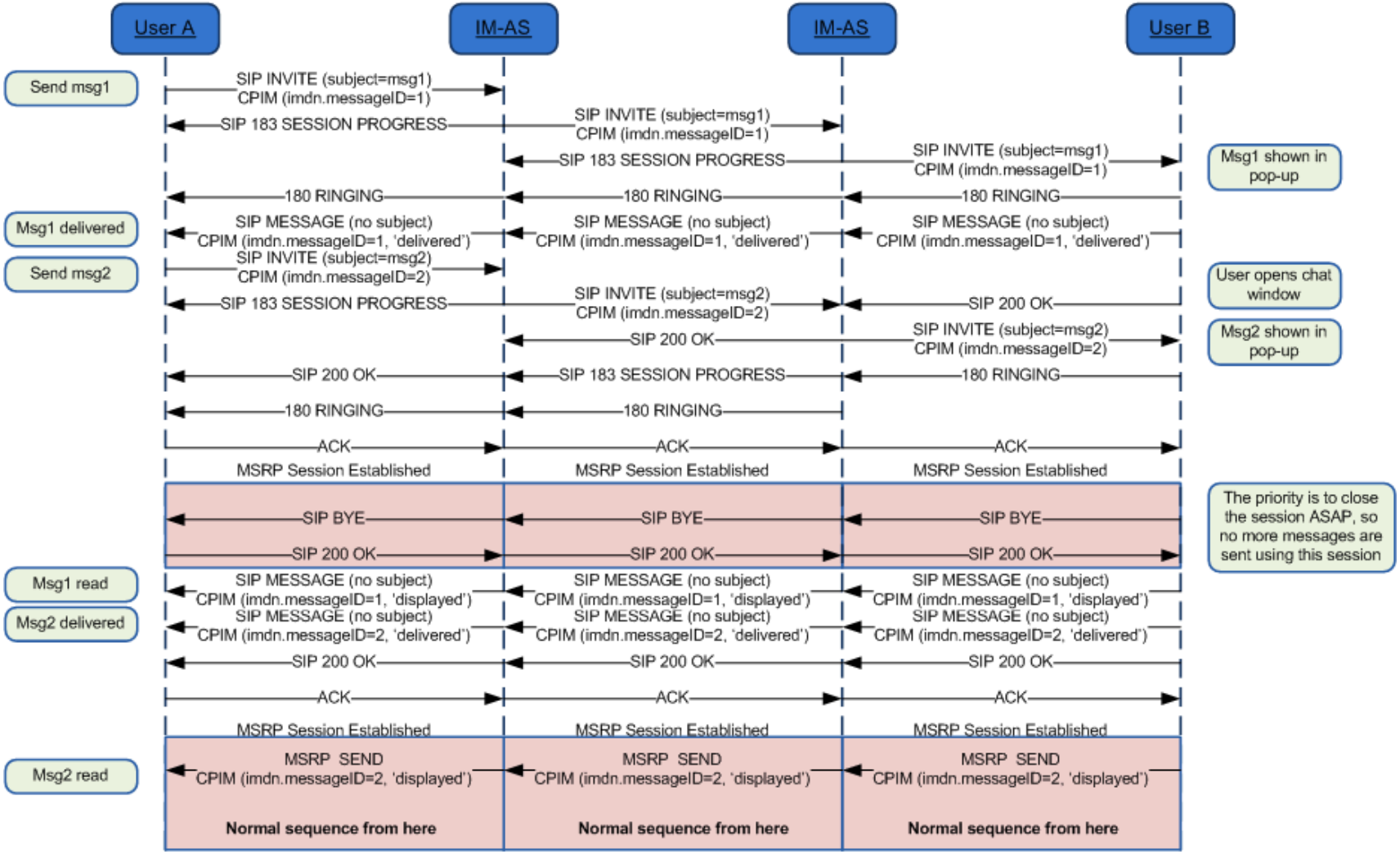

Figure 75: Store and forward race conditions: New INVITE after a session is accepted*

*: Check NOTE 1 in section B.12

B.11 Store and forward: Message(s) displayed notifications via SIP MESSAGE with sender offline

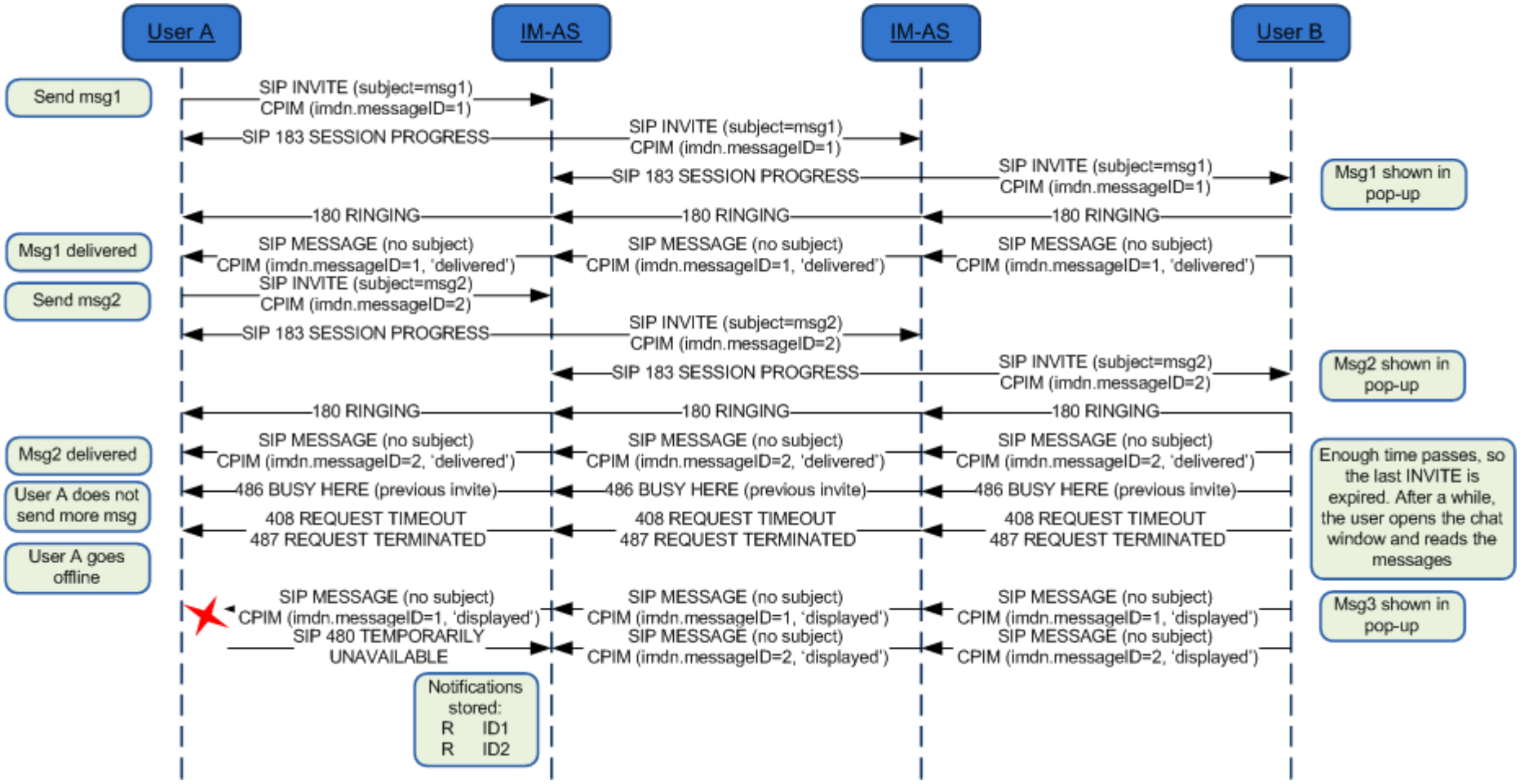

Figure 76: Store and forward: Message(s) displayed notifications via SIP MESSAGE with sender offline*

*: 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 rcse-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 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 in which the order in which the INVITEs arrive is reversed.
  The INVITE from the IM server on behalf of A to deliver the stored messages can be differentiated from an INVITE request for a standard session as it would have Referred-By header set to A and the Contact header would not include an "isfocus" tag indicating that this is not an invitation for a group chat.
- NOTE 5 (B.3, B.4, B.5 and B.6): The session established by the IM-AS to deliver deferred messages to the destination only allows the receiver (client/phone) to send back notifications (that is 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 (That is if user B (the receiver) 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 where the MSRP socket is closed between the IM-AS and the Terminating client (B) in a deferred message delivery (due for instance to a small connectivity loss with the PDP context remaining active) and no re-registration takes place, if there are notifications pending (delivery or displayed) and all the deferred messages have been sent to B already (no need to open a new MSRP session), SIP MESSAGE can be used to confirm the pending delivery/display notifications that could not be sent over MSRP.
- NOTE 8 (B.11): Note that the deferred delivery of the display 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 (neither in the sender's nor in the receiver's domain) and in the case the display notification fail to be delivered because the sender is offline, these notifications will be discarded and the receiver's client 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, neither in the sender's nor in the receiver's network, there is a chance that display notifications carried via SIP MESSAGE may be lost if the original sending client is offline when the receiver sends those display notifications (that is the 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 receiving user.
- NOTE 11 (B.3, B.4, B.5 and B.6): As a general rule the session established by the IM-AS server to deliver deferred messages or notifications should be terminated once the all the messages and notifications have been delivered. In more details:
    - When delivering deferred messages, the session should be terminated (by sending a BYE) either (whatever is shorter) when the display notification corresponding to the last deferred 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 defined by the MNO.
- NOTE 12 (B.4, B.5 and B.6): Whether an IM Server sets up a session for the delivery of notifications or sends them using SIP MESSAGE requests as specified in section 3.2.2.3 or 3.2.2.4 is up to its local policy. This could depend on factors such as the number of notifications that were stored or the number of messages for which notifications can be expected (during delivery of stored messages for instance).

ANNEX C RCS-e IM/Chat and multidevice

C.1 Delivery prior to acceptance

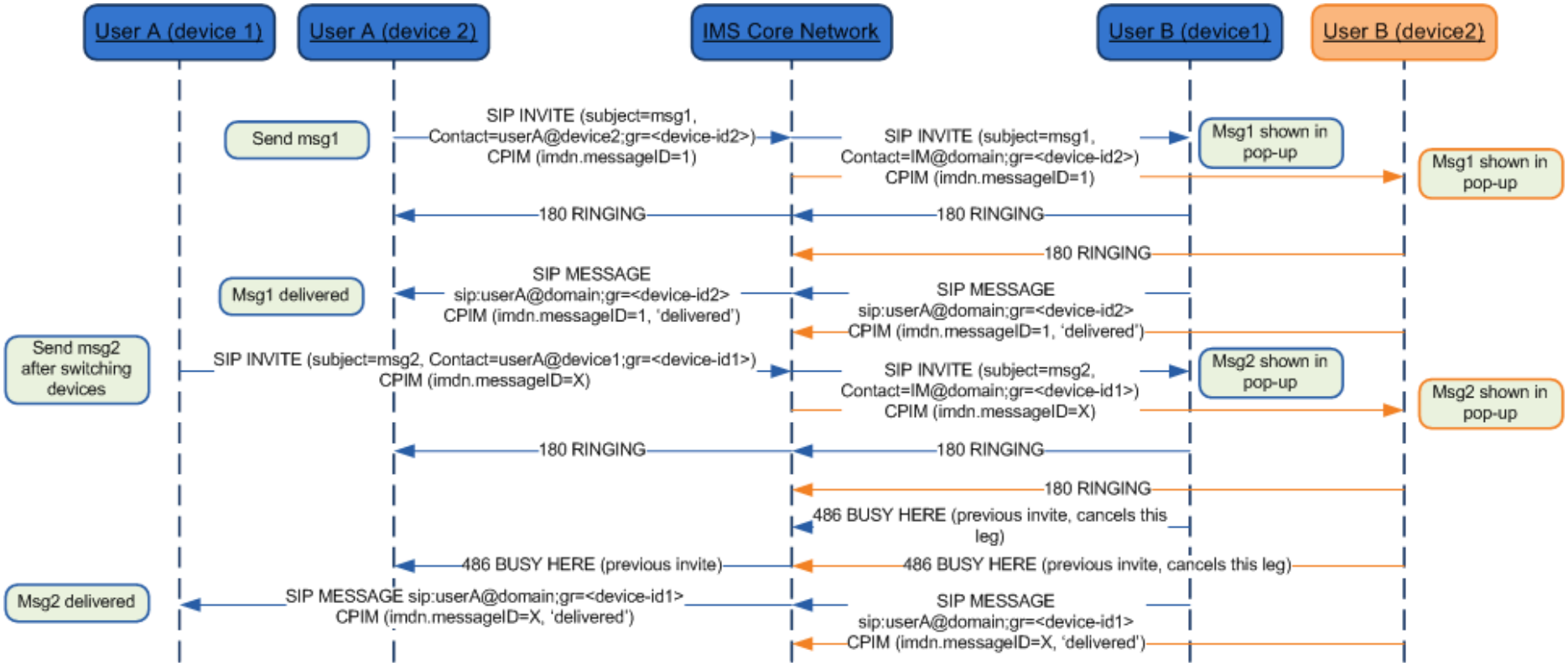

Figure 77: IM and multidevice: Delivery prior to acceptance*

*: Check NOTES 1, 2, 3 and 4 in section C.3

C.2 Post-acceptance behaviour

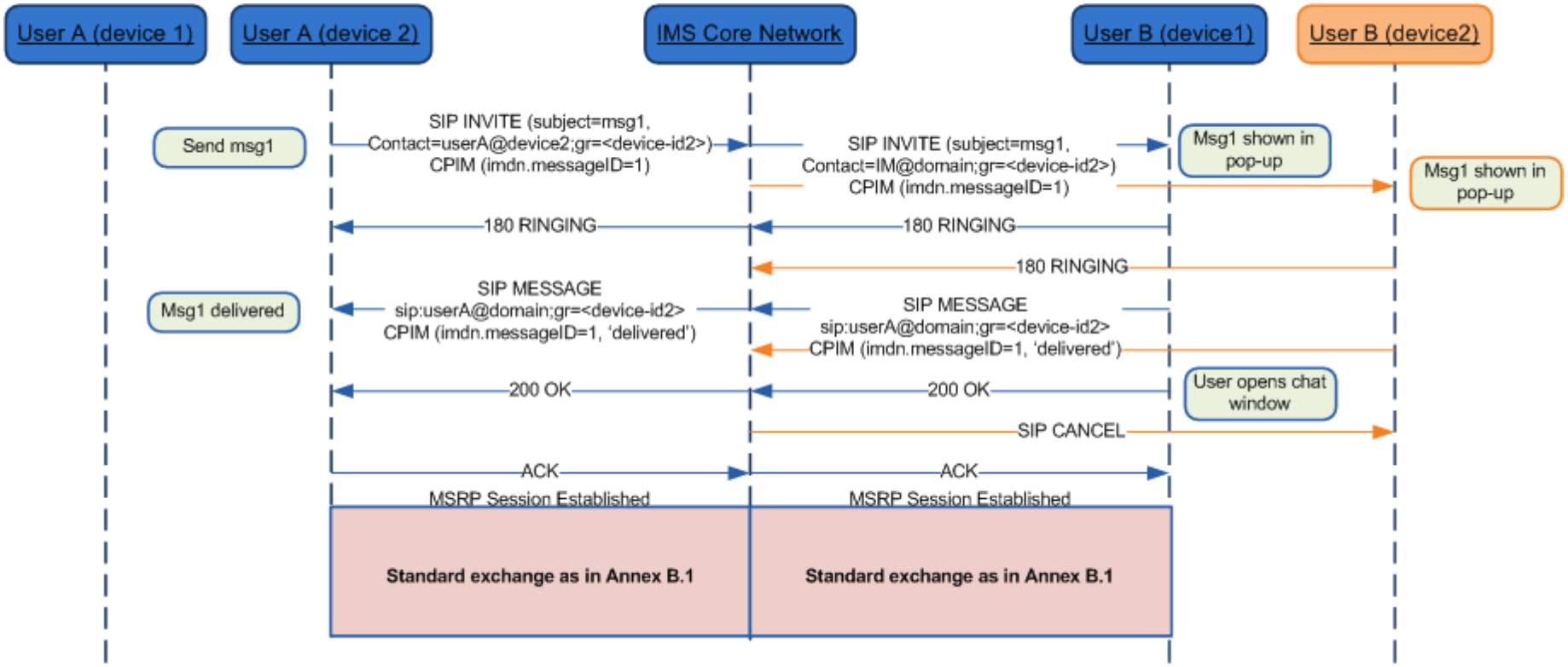

Figure 78: IM and multidevice: Post-acceptance behaviour*

*: Check NOTES 1, 2, 3 and 4 in section C.3

C.3 RCS-e IM/Chat and multidevice: Notes

Please note the following notes apply to diagrams in ANNEX C:

- NOTE 1 (C.1 and C.2): 200 OK responses to SIP MESSAGE and MSRP SEND messages are omitted for clarity.
- NOTE 2 (C.1 and C.2): As mentioned in section 2.15, the diagrams display the solution in a network supporting the pub-gruu generation. For a network supporting the sip.instance tag only, they would be equivalent with only a change of the mechanism to carry the device ID (sip.instance instead pub-gruu).

- NOTE 3 (C.1 and C.2): The diagrams show that “delivered” notifications for messages for which such a notification was sent already, are suppressed by the network. As this cannot always be guaranteed, clients shall be prepared to receive such duplicate notifications and discard them silently. This holds also for display notifications and for notifications related to messages that were not sent by that client.
- NOTE 4 (C.1 and C.2): The SIP URIs in the diagrams (including those in the contact headers and Request URIs) are shown for illustrative purposes only. Any part of those URIs may thus differ in actual deployments. The details of the URIs are also dependent on the exact location in the network where the message is sent.

ANNEX D Scope and summary of changes with 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 occurring from October 2011 onwards should follow this version of the specification until a new version, superseding the present one, is published.

The main motivation behind publishing this version is, based on the feedback provided by vendors and the experience acquired during the initial interoperability tests, 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 delta between the RCS-e specification versions 1.1 and 1.2 is listed in the following table:

Section	Title	Change description
1	Introduction	• complete RCS-e positioning description and figure • Incorporated original sections VI (Definition of terms) and VII (Normative References) as respectively sections 1.3 and 1.4 to comply with the GSMA template. For that same reason sections 1.2 and 1.3 were demoted to subsections of chapter 1.2 scope
2.1	First time registration and client configuration provisioning	• IP:port and FQDN:port removed from configuration parameters for SIP proxy and XDM server • Configuration Parameter 'Device ID' introduced controlling value used in sip.instance • Configuration Parameter 'IM SESSION START' introduced to control the '200 OK' feedback message • Clarify behaviour with regards to the provisioning of both SIP and TEL URI parameters
2.2.2.1	First Time Registration	• Include support for Factory Bootstrap Procedure • Remove handling of XDM list
2.2.2.1.2	Autoconfiguration mechanisms	Requirements added for the configuration mechanism via OMA DM: • Multiple management authorities • Include support for Factory Bootstrap Procedure • 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 OPTIONS request defined • Clarified that during a call at least the 200 OK response to the OPTIONS request includes SDP information
2.3.2	Capability discovery via Presence	• Possibility to use XDM list for capability polling of RCS-e presence enabled contacts removed • Chapter “Enhancing ANONYMOUS SUBSCRIBE mechanism with XDMS lists” removed
2.4.1	Discovery via OPTIONS message	Presence based capability handling doesn’t depend on XDM list any longer
2.5	Capability Polling Mechanism	Capability polling using presence now bases on individual anonymous fetch requests rather than on polling a list.
2.6	Management of supplementary RCS functionality	References to the own XDM list removed
2.7	RCS-e and capabilities	Clarify capability handling during a call
2.7.3	Video interoperability	• specified how H.264 support should be indicated in SDP • H.263-200 is recommended to be supported as a consequence of using IR.74 as the basis for video sharing
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 on the use of alias information
2.12	RCS-e and capability discovery	The section on LTE Capability discovery using LTE was removed
2.13	Other Access Networks	New chapter clarifying that RCS R2 Broadband access is within the scope of RCS-e
2.14	End User Confirmation Requests	• Clarify that clients can be addressed using GRUU • Removed the possibility to send answers and acknowledgements in the body of 200 OK responses to SIP MESSAGE requests. Those have to be sent in dedicated MESSAGE requests • Corrections to the XML schema • Acknowledgement for responses to messages that are displayed result in the discarding of the message even if a response was not sent
2.15	GRUU and multidevice support	sip.instance value will be set based on DEVICE ID configuration parameter in case the device supports GRUU
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; transfer 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 • Handling of DateTime headers by the IM Server • Notifications are also sent using SIP MESSAGE requests in case the original session has timed out • Clarification on the extension of a 1-to-1 to a group chat session 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 • Clarification on the delivery of notifications in multi-device environments • Clarification on the way the Request-URI for sending notifications is composed • Description of the use case in which 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 on the way the Request-URI for sending of notifications is composed • Clarification on the delivery of notifications in multi-device environments • Clarification about the store and forward handling of display 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 SESSION START
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 for the case in which the message was not sent
3.2.4.10	Re-Opening an older chat	Clarification of sending outstanding display notifications
3.2.4.11	Store and Forward Mode	• Clarification regarding the duration of the storage • Clarified the handling of responses and their relation to storage
3.2.4.13	Switching to Group Chat	Clarification on the handling of the 1-to-1 session when receiving an invitation to switch to group chat
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 containing information about: • Details on SPAM transaction handling • Handling of emoticons • Recommendation for chat message size limit • Handling of simultaneous invites • Handling of late invites (when the previous one has already been accepted) • Handling of multiple notifications in short time

		periods Clarifications on the fact that the spam filter applies to both IM and file transfer
3.2.4.20.1	General One-to-One chat	Clarify handling of OPTIONS in case of fall-back to SMS
3.2.4.20.4	Leaving a One-to-One chat	• Clarify handling of notifications for messages received in the background • Clarification for relation between fall-back to SMS and OPTIONS requests
3.2.4.20.5	One-to-One chat forced termination	• Clarification for handling of messages send prior to detecting offline status • Clarification on timing of detection of offline status
3.2.5.1	Group Chat / Initiating a chat	• Added remarks on UX requirements regarding participants list • Clarification on acceptance of the session
3.2.5.2	Group Chat / General Behaviour	• Clarification on the acceptance of the session • Clarification on the signalling of the invitee list
3.2.5.4	New chapter: Chat message size limitations	Recommendation for chat message size limit
3.2.5.5.1	Start a multiple IM session from the IM composition window	• Clarification for OPTIONS handling • Clarification for handling of acceptance • Correct handling of the BYE request • Clarification for handling of invitee list
3.2.5.5.3	Start a group chat session from a IM/chat application	• Clarification for OPTIONS handling • Clarification for handling of acceptance • Clarification for handling of invitee list
3.2.5.5.4	Add a participant to an already established group chat session	Clarification for handling of acceptance
3.3	RCS-e services during a call	Clarification on the basis of content sharing: IR.74 and IR.79
3.3.1	RCS-e services during a call / General Assumptions	Clarification on OPTIONS handling
3.3.2	RCS-e services during a call / Exchange capabilities during a call	Clarification on handling of SDP in OPTIONS request and response
3.3.18	New chapter: Call divert/forwarding	Clarification about restrictions in case a user has call divert/forwarding activated
3.4.2	Selecting the file transfer recipient(s)	Clarification on handling of SDP in OPTIONS request and response
A.1.3	Management objects parameter additions / IM related configuration	IM SESSION START configuration parameter added
A.1.5	IMS Core / SIP related configuration	DEVICE ID configuration parameter added
A.2.2	Presence sub tree additions	“PublishTimer” added to OMA CP structure to be in line with RCS
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 • deviceID parameter added controlling the value used for sip.instance in the IMS registration
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
ANNEX D	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

Table 66: Document change log

Document Management

Document History

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
1.0	12/02/2011	Version 1.0 ready for release to GSMA	E5	Oscar Gallego / Vodafone
1.0.1	11/03/2011	1.1-final draft-1: 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.	E5	Oscar Gallego / Vodafone
1.0.2	23/03/2011	1.1-final draft-2: 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.	E5	Oscar Gallego / Vodafone
1.1	06/04/2011	Version 1.1: ready for release to GSMA	E5	Oscar Gallego / Vodafone
1.1.1	05/08/2011	1.2-preview-draft1: Version ready for release to GSMA incorporating those changes required for initial commercialization.	RCE	Tom Van Pelt / GSMA
1.1.2	23/09/2011	Final Draft for the first Release as GSMA document. Document approved by the RCE project: incorporating the comments received on the 1.2-Preview Subject to final approval of the GSMA	RCE	Tom Van Pelt / GSMA
1.1.3	14/10/2011	Editorial updates before DAG submission	RCE	Tom Van Pelt / GSMA
1.2	28 November 2011	Approved in DAG & EMC as GSMA PRD	EMC	Tom Van Pelt / GSMA

Other Information

Type	Description
Document Owner	RCE Project
Editor / Company	Tom Van Pelt / GSM Association

It is our intention to provide a quality product for your use. If you find any errors or omissions, please contact us with your comments. You may notify us at prd@gsm.org
Your comments or suggestions & questions are always welcome.