ETSI TS 103 269-2 V1.2.1 (2017-06)

TETRA and Critical Communications Evolution (TCCE);
Critical Communications Architecture;
Part 2: Critical Communications application mobile to network interface architecture

Reference
RTS/TCCE-04191

Keywords
broadband, radio, security, TETRA

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Contents

Figures

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Specification (TS) has been produced by ETSI Technical Committee TETRA and Critical Communications Evolution (TCCE).

The present document is part 2 of a multi-part deliverable covering TETRA and Critical Communications Evolution (TCCE); Critical Communications Architecture, as identified below:

ETSI TR 103 269-1: "Critical Communications Architecture Reference Model";

ETSI TS 103 269-2: "Critical Communications application mobile to network interface architecture";

ETSI TS 103 269-3: "Critical Communications application mobile to network interface specification".

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

1 Scope

The present document presents an overview of the architecture for a generic mission critical service for use by a Critical Communications Application in network and terminal over a broadband IP bearer, with specific focus for LTE. The architecture is part of the overall Critical Communications Architecture Reference Model, described in ETSI TR 103 269-1 [i.11]. The overall architecture and services are described and the implementation of services equivalent to the existing narrowband technologies, for example those in TETRA and Tetrapol systems. Off network services are for future study and so are outside the scope of the present document.

2 References

2.1 Normative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are necessary for the application of the present document.

[1] Void.

[2] IETF RFC 3261: "SIP: Session Initiation Protocol".

[3] IETF RFC 5389: "Session Traversal Utilities for NAT (STUN)".

[4] IETF RFC 6665: "SIP-Specific Event Notification".

[5] IETF RFC 3428: "Session Initiation Protocol (SIP) Extension for Instant Messaging".

[6] IETF RFC 3903: "Session Initiation Protocol (SIP) Extension for Event State Publication".

[7] IETF RFC 4566: "SDP: Session Description Protocol".

[8] Void.

[9] IETF RFC 791: "Internet Protocol (v4)".

[10] IETF RFC 2460: "Internet Protocol, Version 6 (IPv6) Specification".

[11] IETF RFC 793: "Transmission Control Protocol".

[12] IETF RFC 4960: "Stream Control Transmission Protocol".

[13] IETF RFC 5246: "The Transport Layer Security (TLS) Protocol Version 1.2".

[14] IETF RFC 6347: "Datagram Transport Layer Security Version 1.2".

[15] IETF RFC 768: "User Datagram Protocol".

[16] IETF RFC 3550: "RTP: A Transport Protocol for Real-Time Applications".

[17] IETF RFC 3711: "The Secure Real-time Transport Protocol (SRTP)".

[18] IETF RFC 5245 (04-2010): "Interactive Connectivity Establishment (ICE): A Protocol for Network Address Translator (NAT) Traversal for Offer/Answer Protocols".

[19] IETF RFC 5766: "Traversal Using Relays around NAT (TURN): Relay Extensions to Session Traversal Utilities for NAT (STUN)".

[20] ETSI TS 100 900 (V7.2.0): "Digital cellular telecommunications system (Phase 2+) (GSM); Alphabets and language-specific information (GSM 03.38 version 7.2.0 Release 1998)".

[21] IETF RFC 3629 (11-2003): "UTF-8, a transformation format of ISO 10646".

[22] IETF RFC 7230 (06-2014): "Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing".

[23] IETF RFC 2818 (05-2000): "HTTP Over TLS".

[24] IETF RFC 3986 (01-2005): "Uniform Resource Identifier (URI): Generic Syntax".

[25] ANSI INCITS 4-1986 (R2007) (formerly ANSI X3.4-1986 (R1997)): "Coded Character Sets - 7-Bit American National Standard Code for Information Interchange (7-Bit ASCII)".

[26] IETF RFC 4122 (07-2005): "A Universally Unique IDentifier (UUID) URN Namespace".

[27] IETF RFC 4825 (05-2007): "The Extensible Markup Language (XML) Configuration Access Protocol (XCAP)".

[28] W3C Recommendation (16 August 2006, edited in place 29 September 2006): "Extensible Markup Language (XML) 1.1 (Second Edition)".

NOTE: Available at http://www.w3.org/TR/xml11.

[29] IETF RFC 5626 (10-2009): "Managing Client-Initiated Connections in the Session Initiation Protocol (SIP)".

[30] IETF RFC 5627 (10-2009): "Obtaining and Using Globally Routable User Agent URIs (GRUUs) in the Session Initiation Protocol (SIP)".

[31] OpenID Connect 1.0: "OpenID Connect Core 1.0 incorporating errata set 1".

NOTE: Available at http://openid.net/specs/openid-connect-core-1_0.html.

[32] IETF RFC 3680 (03-2004): "A Session Initiation Protocol (SIP) Event Package for Registrations".

[33] ETSI TS 124 229: "Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3 (3GPP TS 24.229)".

[34] OMA (03-05-2016): "XML Document Management (XDM) Specification", Approved Version 2.2.

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] ETSI TR 102 022-2: "User Requirements Specification Mission Critical Broadband Communications; Part 2: Critical Communications Application".

[i.2] TETRA and Critical Communications Association; List of TIP features.

NOTE: Available at https://tandcca.com/fm_file/listoftipfeaturesv2-0-pdf/.

[i.3] ETSI EN 300 392-12: "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 12: Supplementary services stage 3".

[i.4] ETSI TS 122 179: "Universal Mobile Telecommunications System (UMTS); LTE; Mission Critical Push to Talk (MCPTT) over LTE; Stage 1 (3GPP TS 22.179)".

[i.5] IEEE 802.11™: "IEEE Standard for Information technology - Telecommunications and information exchange between systems local and metropolitan area networks - Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications".

[i.6] IEEE 802.16™: "IEEE Standard for Air Interface for Broadband Wireless Access Systems".

[i.7] IETF RFC 5359: "Session Initiation Protocol Service Examples".

[i.8] ETSI TS 123 003: "Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); Numbering, addressing and identification (3GPP TS 23.003)".

[i.9] ETSI TS 136 300: "LTE; Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Overall description; Stage 2 (3GPP TS 36.300)".

[i.10] IETF RFC 959 (10-1985): "File Transfer Protocol (FTP)".

[i.11] ETSI TR 103 269-1: "TETRA and Critical Communications Evolution (TCCE); Critical Communications Architecture; Part 1: Critical Communications Architecture Reference Model".

[i.12] ETSI TS 122 278: "LTE; Service requirements for the Evolved Packet System (EPS) (3GPP TS 22.278)".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

5-tuple: set of five values required to specify a TCP or UDP connection, comprising a protocol identifier (TCP or UDP), a source IP address, a source port number, a destination IP address and a destination port number

Access Point Name (APN): reference to a GGSN comprising an external network identifier and an optional PLMN operator identifier

NOTE: To support inter-PLMN roaming, the internal GPRS DNS functionality is used to translate the APN into the IP address of the GGSN (ETSI TS 123 003 [i.8]).

affiliation: process of negotiating access to communications with a group

NOTE 1: The TETRA term for affiliation is "Group Attachment".

NOTE 2: ETSI TS 122 179 [i.4] uses the term "Affiliation".

call: set of one or more transmissions of media between two or more parties

call hang time: period within a call during which no communications are sent or received, and following expiry of which, the call will be cleared

CCA client: entity that provides the CCA application functionality within an access network client terminal

NOTE: A CCA client may create multiple instances of its application functionality within a single access network client terminal.

CCA client identity: URI that identifies the CCA client in a specific device

CCA functional identity: SIP URI used when identifying and routing call related and call unrelated signalling sent to and from a CCA client application that has been associated with a user role

CCA group identity (CCA group ID): SIP URI used when identifying and routing call related and call unrelated signalling sent to a CCA group

CCA group reference: short reference to a CCA group identity that is used in media control protocol messages

CCA individual identity: SIP URI used when identifying and routing call related and call unrelated signalling sent to and from a CCA client instance that has been associated with a user

CCA server identity: name used to uniquely identify a critical communications application server

CCA user identity: name utilized for authentication of the user as an enabling step to gain access to CCA services

critical communications application: infrastructure based application which provides critical communications services to its CCA clients

full-duplex: method of communication in which participants can send and receive information at the same time

Fully Qualified Domain Name (FQDN): host name (including all subnames) and domain name, including the top level domain

NOTE: An FQDN is not the same as a URL (universal resource locator), but rather it is a part of it. This is because an FQDN lacks the TCP/IP protocol name (e.g. HTTP [23] or FTP [i.10]) that is always used at the start of a URL. Moreover, a URL may also include a directory path, a file name and a TCP port number.

Gateway GPRS Support Node (GGSN): component responsible for connecting a GPRS network or a GSM-based 3GPP network to an external packet switched network such as the Internet or an X.25 network

NOTE: A P-Gateway is the equivalent of the GGSN in the evolved packet core.

Globally Routable User agent URI (GRUU): SIP URI that routes to a specific UA instance and can be successfully used by any UA in the Internet, not just UAs in the same domain or IP network as the UA instance to which the URI points

half-duplex: method of communication in which only one participant can send information at one time

NOTE: In a half-duplex call, the call consists of a sequence of unidirectional transactions.

local breakout: optimized routing for a user with mobility within and across one operator-defined network region such that user plane traffic does not need to leave the current region

NOTE: An operator may define network regions e.g. according to administrative domains. Local breakout is applicable for user-to-user traffic and for 3GPP-operator provided services (including Internet access) [i.12]. The routing is per APN.

MBMS Service Area: area within which data of a specific MBMS session are sent

NOTE: Each individual MBMS session of an MBMS Bearer Service may be sent to a different MBMS Service Area.

MBSFN Area: group of cells within an MBSFN Synchronization Area of a network which are co-ordinated to achieve an MBSFN transmission

MBSFN Synchronization Area: area of the network where all eNodeBs can be synchronized and perform MBSFN transmissions

NOTE: MBSFN Synchronization Areas are capable of supporting one or more MBSFN Areas. MBSFN Synchronization Areas are independent from the definition of MBMS Service Areas.

media path transport parameters: set of parameters including at least a 5-tuple, direction (send-only, receive-only or send and receive), codec type and bandwidth

migration: obtaining Critical Communications service from a CCAS other than the home CCAS

Mobile Unit (MU): combination of access network client terminal and client application for critical communications which provides critical communications services to its user

participant type: functional category of a CCA user (e.g. first responder, second responder, dispatch, dispatch supervisor) typically defined by individuals authorized to control CCA service parameters and user profiles, etc.

registration: process of negotiating service from a CCAS

roaming: obtaining an IP connection to the home CCAS from a broadband IP network other than the home broadband IP network

NOTE: If a 3GPP LTE PLMN provides home service to a user, obtaining service from a different PLMN is an example of roaming.

session: period within a period of affiliation to a group within which transmissions may be sent and received to and from that group by using media control signalling only

session hang time: period following a call during which the CCAS may maintain a session before clearing it

Universal Resource Identifier (URI): compact sequence of characters that identifies an abstract or physical resource

Universal Resource Locator (URL): type of URI that identifies a resource via a representation of its primary access mechanism (e.g. its network "location"), rather than by some other attributes it may have

Universally Unique IDentifier (UUID): 128-bit identifier that is effectively unique across space and time

User Agent (UA): software that acts on behalf of a user

user instance: unique combination of a CCA individual identity, a user profile and a CCA client instance

XML Configuration Access Protocol (XCAP): set of conventions for mapping XML documents and document components into HTTP URIs, rules for how the modification of one resource affects another, data validation constraints and authorization policies associated with access to those resources

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

3GPP	3rd Generation Partnership Project
AGNSS	Assisted Global Navigation Satellite System
AL	Ambience Listening
APN	Access Point Name
ASCII	American Standard Code for Information Interchange
ASSI	Alias Short Subscriber Identity
AVL	Automatic Vehicle Location
BIC	Barring of Incoming Calls
BOC	Barring of Outgoing Calls
BS	Base Station
CAD	Call Authorized by Dispatcher
CCA	Critical Communications Application
CCAS	Critical Communications Application Server
CCS	Critical Communications System
CF	Call Forwarding

CFB	Call Forwarding on Busy
CFNRy	Call Forwarding No Reply
CFU	Call Forwarding Unconditional
CSCF	Call Session Control Function
CW	Call Waiting
DGNA	Dynamic Group Number Assignment
DHCP	Dynamic Host Control Protocol
DL	Discreet Listening
DMO	Direct Mode Operation
DNS	Domain Name Server
DOTAM	DMO Over The Air Management
DTLS	Datagram Transport Layer Security
DTMF	Dual Tone Multi Frequency
E-MBMS	Enhanced Multimedia Broadcast Multicast Service
EPC	Evolved Packet Core
EPS	Evolved Packet System
E-UTRAN	Evolved Universal Terrestrial Radio Access Network
FFS	For Further Study
FQDN	Fully Qualified Domain Name
GBR	Guaranteed Bit Rate
GGSN	Gateway GPRS Support Node
GPRS	General Packet Radio Service
GRUU	Globally Routable User agent URI
GSM	Global System for Mobile communications
HPLMN	Home Public Land Mobile Network
HTTP	HyperText Transfer Protocol
HTTPS	HTTP over TLS
ICE	Interactive Connectivity Establishment
IMS	IP Multimedia Subsystem
IMSI	International Mobile Subscriber Identity
IP	Internet Protocol
ISDN	Integrated Services for Digital Network
LIP	Location Information Protocol
LTE	Long Term Evolution
MBMS	Multimedia Broadcast Multicast Service
MBSFN	Multicast-Broadcast Single-Frequency Network
MCP	Media Control Protocol
ME	Mobile Equipment
MU	Mobile Unit
N/A	Not Applicable
NAT	Network Address Translation
OMA	Open Mobile Alliance
PABX	Private Automatic Branch Exchange
PDN	Packet Data Network
PIN	Personal Identification Number
PLMN	Public Land Mobile Network
PMR	Private/Professional Mobile Radio
ProSe	Proximity Services
PSTN	Public Switched Telephone Network
PTT	Press To Talk
RFC	Request For Comment
RTCP	Real-time Transport Control Protocol
RTP	Real-time Transport Protocol
RX	Receive
SC-PTM	Single-Cell Point-To-Multipoint
SCTP	Stream Control Transmission Protocol
SDP	Session Description Protocol
SDS	Short Data Service
SDS-TL	Short Data Service - Transport Layer
SIM	Subscriber Information Module
SIP	Session Initiation Protocol
SRTCP	Secure Real-time Transport Control Protocol

SRTP	Secure Real-time Transport Protocol
SS	Supplementary Service
STUN	Session Traversal Utilities for NAT
TBD	To Be Decided
TCCE	TETRA and Critical Communications Evolution
TCP	Transport Control Protocol
TETRA	Terrestrial Trunked Radio
TIP	TETRA Interoperability Process
TLS	Transport Layer Security
TMGI	Temporary Mobile Group Identity
TURN	Traversal Using Relays around NAT
TX	Transmitter
UA	User Agent
UDP	User Datagram Protocol
UE	User Equipment
URI	Universal Resource Identifier
URL	Universal Resource Locator
URS	User Requirements Specification
US	United States
UTF	Unicode Transformation Format
UUID	Universally Unique Identifier
VPLMN	Visited Public Land Mobile Network
WAP	Wireless Application Protocol
WCMP	Wireless Control Message Protocol
WLAN	Wireless Local Area Network
WMAN	Wireless Metropolitan Area Network
XCAP	XML Configuration Access Protocol
XDCP	XDM Command Protocol
XDM	XML Document Management
XDMS	XML Document Management System
XML	eXtensible Markup Language

4 Architecture overview

4.1 Architecture reference

The Critical Communications Architecture Reference model is detailed in ETSI TR 103 269-1 [i.11]. The architecture and interfaces are shown in figure 1.

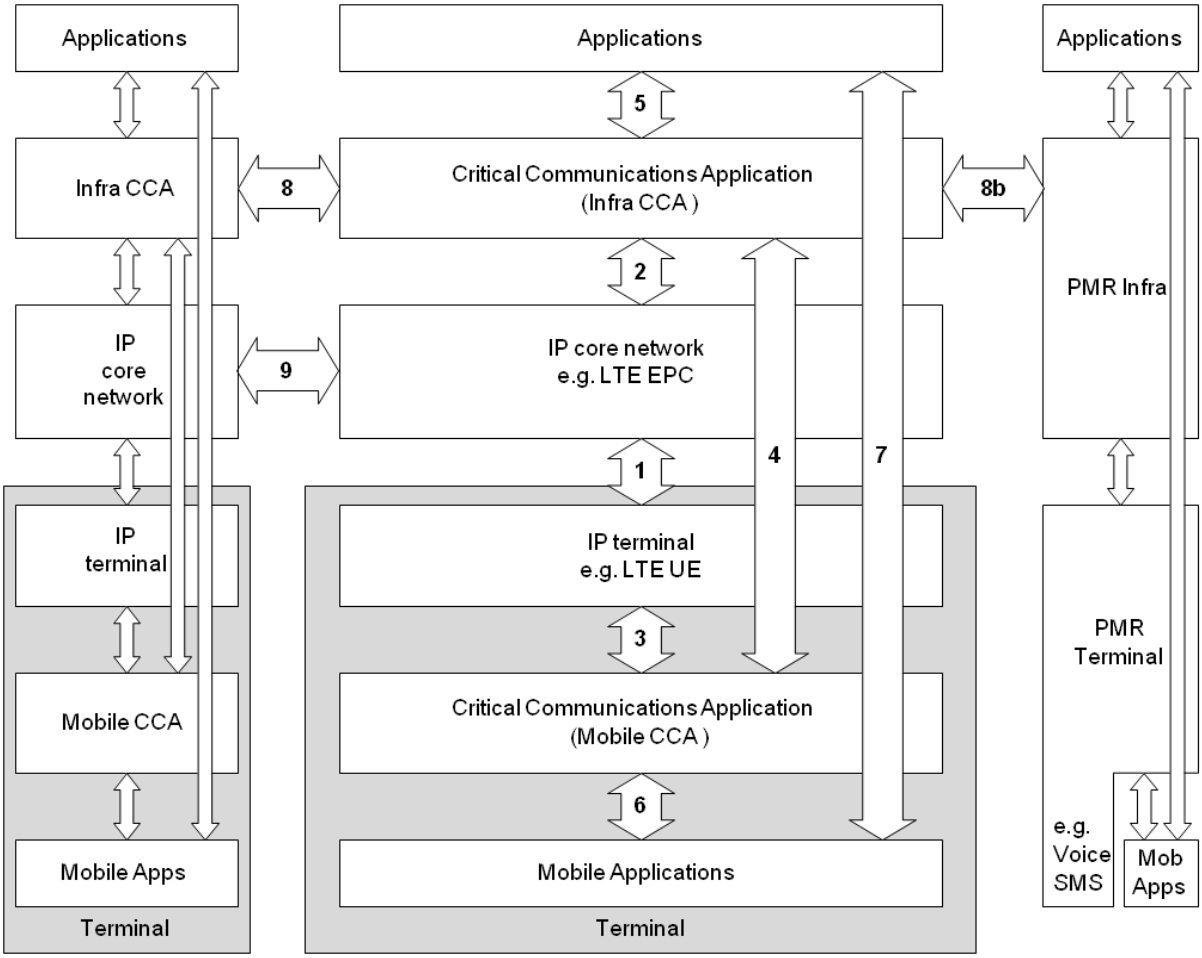


Figure 1: CCS Reference Model

The present document describes the architecture of interface 4 in the reference model shown in figure 1.

NOTE: ETSI TR 103 269-1 [i.11] contains the normative version of this figure.

4.2 Configurations

4.2.0 Functional Architecture

The functional architecture covered in the present document is presented in the following clauses.

4.2.1 Single CCA system

The functional architecture for a single CCA system according to the present document is presented in figure 2.

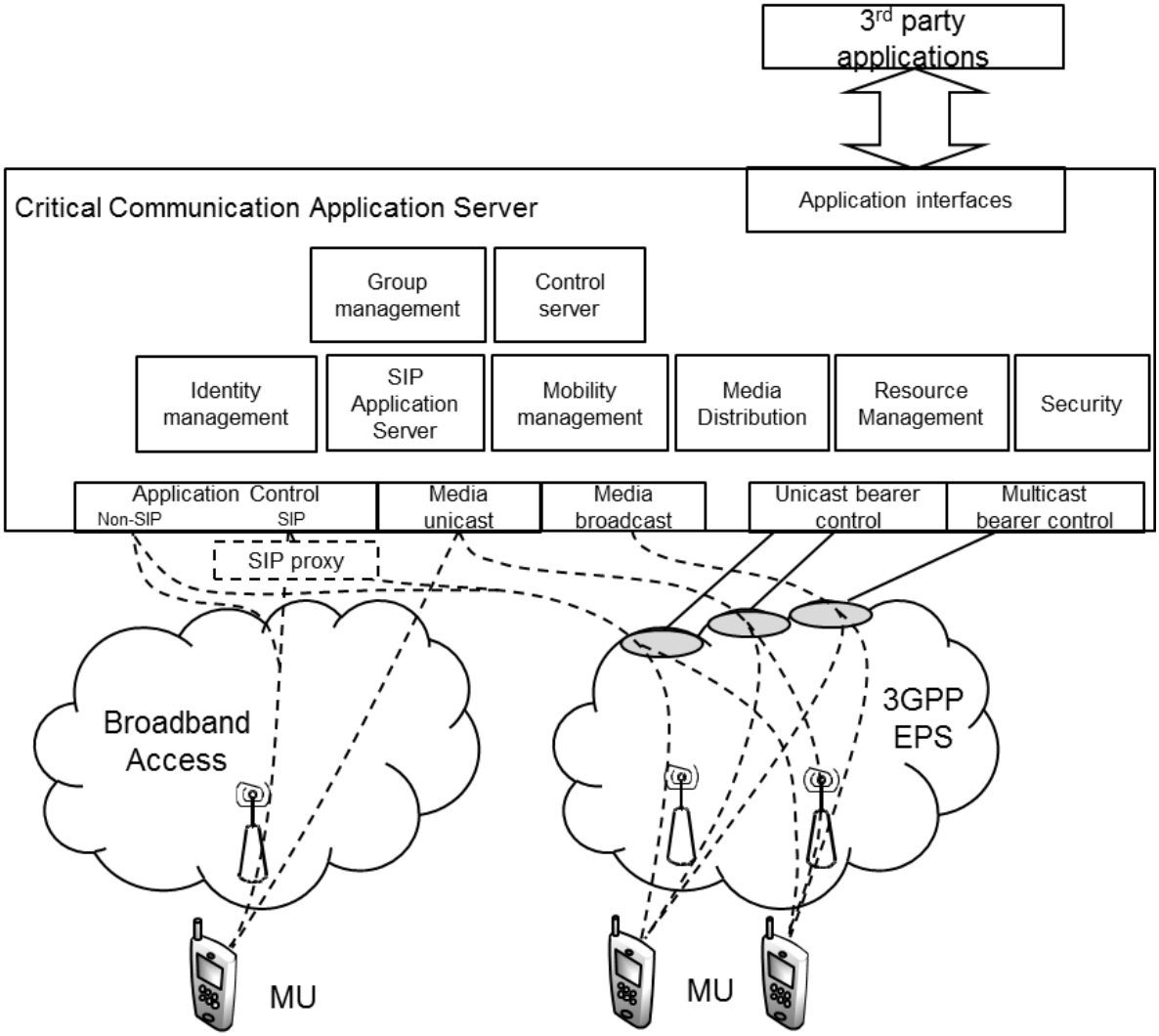


Figure 2: Functional architecture

NOTE 1: The SIP proxy function may be part of the "application control" interface or may be separate.

The Critical Communications Application Server (CCAS) has a number of entities responsible for establishing the service and for exchanging individual and group communications with Mobile Units. The various entities of the CCAS use the transport interfaces of the underlying broadband networks to exchange signalling and media with the mobile units. Depending on the nature of the broadband access and of its capabilities and available interfaces, the CCAS uses control interfaces of the broadband network to manage the transport bearers, i.e. to set up and release bearers and to request for specific Quality of Service. This is typically the case when the broadband access is an LTE Core Network, as illustrated by the "3GPP EPS" in figure 2. If those control interfaces do not exist, for instance in the case of WiFi access, or are not available, for instance in the case of an LTE network for which the control interface (Rx) is not made available to the CCAS (for example in a back up commercial operator network), then the CCAS uses transport on default bearers. (Note that in this case, a fully mission critical service may not be available.) This is illustrated by the "Broadband Access" network in figure 2.

NOTE 2: The term Critical Communications Application Server is used to denote the set of entities that provide the fixed end part of the CCA, which provide service to the client, or mobile, part of the application in the MUs. The term "server" does not imply any physical structure or number of physical devices that provide this service.

One CCAS may make use of more than one broadband network. The broadband networks may be of the same type, for example in the case where multiple 3GPP LTE networks are used to provide access to one CCAS. The broadband networks may also be of mixed network types, such as a mixture of 3GPP LTE and WiFi networks which provide service to the same CCAS. Multiple CCASs may also share the same broadband IP access network. Therefore there can be a many-to-many relationship of CCASs and broadband IP access networks.

The CCA provides services to additional third party applications, for example to provide group addressed services, or prioritized access services.

4.2.2 Multi-CCAS system

A multi-CCAS system is depicted in figure 3.

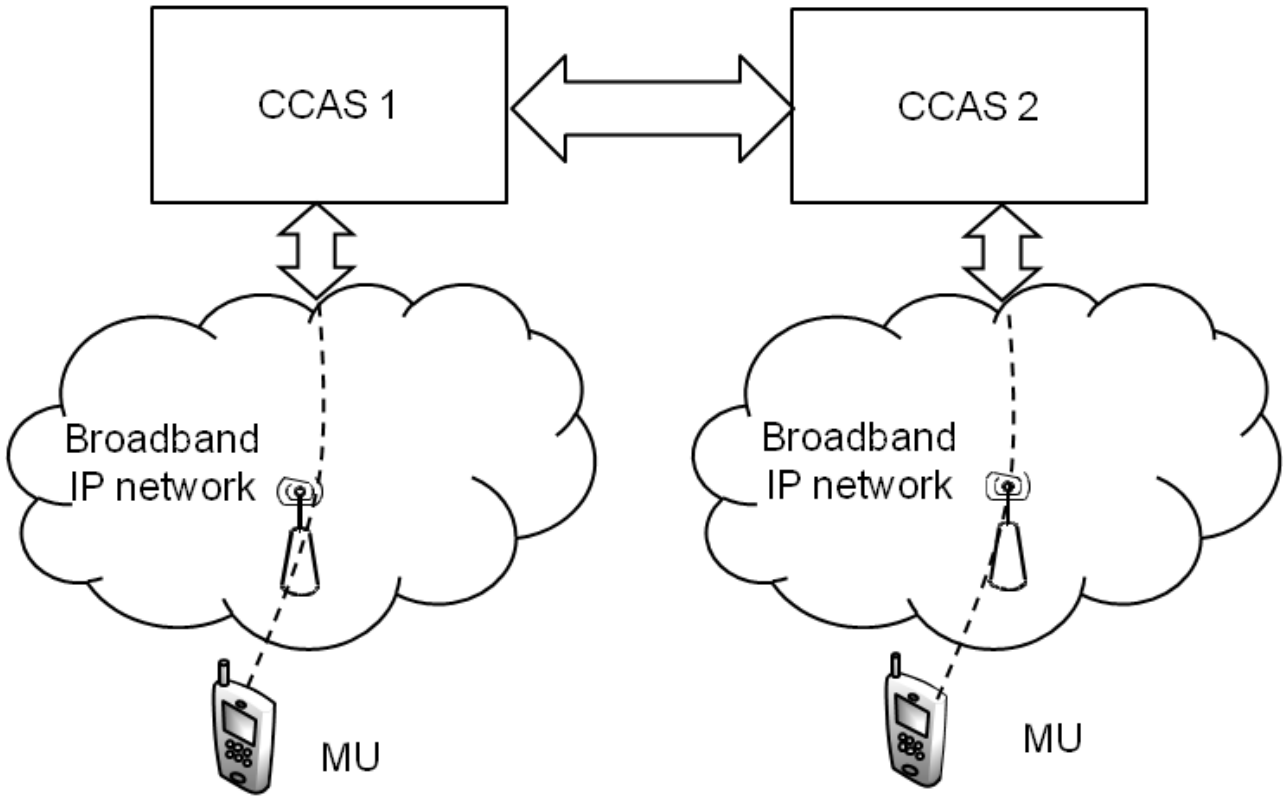


Figure 3: Multi-CCAS system

In the multi-CCAS system each CCAS may be in contact with "home" mobile units, but may also offer access to mobile units that have migrated to that CCAS as visitors. The visited CCAS allows routing of the signalling from a migrated mobile unit to its home CCAS. The same inter-CCAS connection may also support communications between two MUs, each at home in different CCASs.

NOTE 1: Each CCAS may use one or more broadband IP network for access by MUs.

NOTE 2: Multiple CCASs could be using one or more broadband IP networks in common for communication with their respective MUs, and still support the migration behaviour.

NOTE 3: The interface between CCASs is outside the scope of the present document.

4.2.3 Interconnection with legacy

Interconnection with legacy networks is outside the scope of the present document. It will be satisfied by interface 8b (8 bis) in figure 1, and its function is described in [i.11]. It may be realized by an existing interface from a legacy technology, for example an inter system interface from the appropriate technology.

An interconnection with a legacy network may put constraints on services within the CCA, where a call includes one or more parties connected over a legacy interface.

5 Components

5.0 Functional groups

The following clauses describe the functional groups involved in the implementation of the mission-critical PMR services over broadband.

5.1 Mobile unit

The Mobile Unit (MU) is the (mobile) sub-system used by the user to access the mission critical application. The MU contains the CCA client (the client part of the application) and one or several modems able to interface with the access sub-systems which provide IP connectivity for the client application.

The access device may be an LTE UE, but the MU may alternatively comprise further access devices such as a WLAN interface based on IEEE 802.11 standard [i.5] and/or various types of IP based wire-line interfaces.

5.2 Access sub-systems

The access sub-systems provide the link between the CCA client and the infrastructure based application. They are generally based on wireless technologies, particularly the 3GPP Long Term Evolution (LTE) technology, but access may also be based on other type of wireless technologies such as WLAN (IEEE 802.11 [i.5]) or WMAN (IEEE 802.16 [i.6]), or wire-line technologies.

It is assumed that the access sub-systems provide an IP based transport from the MU to the CCAS(s). It is also assumed that the corresponding sub-systems provide any ancillary functions required for proper use of IP, e.g. a DHCP function to give a dynamic IP address to the MU where required and a master DNS function to allow the MU to discover the addresses, ports and protocols, etc. of the available CCAS(s) where this is needed.

NOTE: No assumption is made on the use of a specific version of IP, i.e. IPv4 and/or IPv6.

5.3 Critical Communication Application

5.3.0 General

The CCA comprises a number of functional entities which when combined provide the application service to the MUs. The functional entities are not prescriptive, but illustrate the functionality required in offering the various aspects of the service.

The CCA contains both application related services, for example which provide registration of users, affiliation to groups, call services, etc. and control functionality, for example the ability to set up bearers with the required characteristics to communicate with the MUs and control the levels of priority of the various bearers in the access sub-system, where this control is available. The application level services are described further in the present document. The control functions make use of interfaces provided by the access sub-systems, and whereas aspects of their functionality are described in the present document, the interfaces will be specified by standards relating to the access sub-system, not the application standards.

5.3.1 Access interfaces

5.3.1.0 General

The CCA provides a number of access interfaces for both application purposes and for access network control, where available.

The interfaces described in this clause are logical and do not imply a specific physical implementation. For example, a CCAS may employ more than one interface of each type to distribute the load, or may use different physical interfaces for different types of media.

Each interface point will provide appropriate security protection for the packets flowing in and out of the interface (encryption, integrity protection, etc.).

5.3.1.1 Application control interface

The application control interface is the access point for signalling, both SIP and non-SIP (e.g. HTTP [22]) for the implementation of mission critical services over broadband. It is not used for the actual media flows. It provides facilities such as user authentication and registration with the CCAS, affiliation to groups and other such services. It also may provide a SIP [2] proxy function for the other entities of the CCA. The IP address of the application control interface is, in effect, the IP address of the application control entity of figure 2.

It is recommended that the CCA client accesses the CCAS via a single (logical) application control interface. The following cases are relevant:

- through a 3GPP access network:
  - from the home PLMN to a CCAS on the home PLMN:
    - the application control interface may be accessed at an IP address, fully qualified domain name (FQDN) or URI within a pre-provisioned Access Point Name (APN) provided by the access sub-system;
  - from a visited PLMN to a CCAS on the home PLMN using home-routing:
    - the application control interface may be accessed at an IP address, FQDN or URI within a pre-provisioned home-routed APN (an APN that contains the home PLMN operator identifier) - the visited PLMN needs a roaming agreement with the home PLMN;
  - from a visited PLMN to a CCAS on the home PLMN using local breakout:
    - the application control interface may be accessed at an IP address, FQDN or URI within a pre-provisioned local APN (an APN that does not contain the home PLMN operator identifier) - the visited PLMN needs a roaming agreement with the home PLMN and there needs to be routing means between the local breakout and the home CCAS;
  - to a CCAS on a non-home PLMN:
    - the application control interface may be accessed at an IP address within a pre-provisioned home-routed or local APN (the non-home PLMN does not require a roaming agreement with the home PLMN if the MU is using its home PLMN but the home PLMN may need to provide access to an APN that provides local breakout to the CCAS);

  The IP address, FQDN or URI of the application control interface may:
  - be pre-provisioned in the MU; or
  - may be discovered by DNS search of the pre-provisioned APN; or
  - may be obtained by using the Protocol Configuration Options information element when activating an EPS bearer context as described in the "EPS bearer context activation and P-CSCF discovery" procedure in ETSI TS 124 229 [33], clause L.2.2.1.

NOTE 1: The user may be given a choice of using a home routed or a local APN.

NOTE 2: The MU and the user can have different home CCASs. The method by which the CCA client discovers the identities of the home PLMN of the MU and the home CCAS of the user is outside the scope of the present document.

- through a non-3GPP access network:
  - the application control interface is accessed via its IP address. The IP address may be pre-provisioned or may be obtained by DNS search of a pre-provisioned fully qualified domain name (FQDN) or URI that is pre-provisioned in the MU.

More than one TCP or UDP IP port may be in use to support different protocols (e.g. SIP [2], HTTP [22], etc.). Different ports (pre-provisioned in the MU) may be used to access different entities within the application control interface. The physical nature of the interface and relationship between host name and physical interface is outside the scope of the present document; for example a DNS search by the MU or CCA client instance for a single DNS access name, FQDN or URI may be resolved by the DNS into different physical access points at different times for reasons such as for load sharing or redundancy. The access to the application control interface may be limited by Network Address Translators (NATs) and/or firewalls/security gateways. (The application control interface should be protected against denial of service attacks, etc.)

NOTE 3: Use of a DNS is optional for the CCA client, but DNS search will be necessary if a pre-provisioned IP address cannot be reached (e.g. when NAT is used, or when obtaining service on a foreign IP network).

The CCA client establishes relevant interface information (IP address, port numbers) for the unicast and multicast media interfaces subsequent to the authentication process, using the access procedure of clause 7.2.3.2. The application control interface may also be used by other applications to provide a single point of access to services.

5.3.1.2 Media unicast interface

The media interface is the access point for media and media control signalling sent to and from the MU in unicast mode. The discovery of its transport address(es) is derived from service initiation dialogue with the application control interface.

Information sent via this interface includes the media which is the content of calls (e.g. speech flow), and also media related signalling (e.g. PTT signalling in a speech call). The interface is bi-directional. It is always used for uplink communications sent from the MU and may be used for downlink communications sent from the CCAS.

5.3.1.3 Media multicast interface

The media multicast interface is used by the CCA to transmit media to a group of MUs simultaneously using only a single resource from the underlying access sub-system. An example of a means of transport is the Enhanced Multimedia Broadcast Multicast Service (E-MBMS) offered by 3GPP LTE (see ETSI TS 136 300 [i.9]. The interface may also carry control signalling related to calls.

5.3.1.4 Unicast bearer control interface

The unicast bearer control interface is used by the CCA to set up unicast bearers with the relevant characteristics for control signalling and media exchange. More than one bearer may be established between CCAS and MU at any time, as the quality of service and priority characteristics required for control and various types of media are likely to be different.

5.3.1.5 Multicast bearer control interface

The multicast bearer control interface is used by the CCA to set up multicast bearers for carrying control and media information to groups of users using the broadcast service of the underlying access sub-system. Note that, depending on the characteristics of the access sub-system, more than one application layer group may be multiplexed over the same broadcast bearer.

5.4 CCAS functional entities

5.4.0 General

The notional functional entities of the CCAS which, when combined, provide the application service to the MUs that are described in the following clauses. The functional entities are not prescriptive, but illustrate the functionality required in offering the various aspects of the service.

5.4.1 SIP application server

The SIP application server provides functionality for terminal registration, and additionally provides registration functions for naming, group affiliation and individual call processes. Once the MU has established an IP connection with the application control interface, it performs a registration with the SIP application server. The SIP application server is then responsible for routing calls and group affiliations to and from the MU.

5.4.2 Mobility management

The mobility management entity tracks the location of both individual MUs and the various communication groups of MUs that will participate in the various services. The mobility management entity tracks the following with respect to individuals and affiliated group members:

- To the current CCAS which is providing service to an MU or a group.
- To the current broadband IP network which is providing service between the CCAS and an MU or a group.
- The current IP addresses (and relevant subnets, etc.) of individual subscribers.
- In a multicellular environment which offers multicast services, to the current multicast operating area (e.g. an LTE Multicast-Broadcast Single-Frequency Network (MBSFN) area).

When a call is to be placed to a target individual or group, the mobility management entity is responsible for indicating the available paths to that target individual or group. This information is used by the resource management entity.

5.4.3 Group management

The group management entity is responsible for the definitions and memberships of communication groups within the CCA. For migrating MUs, the visited CCAS co-operates with the home CCAS. Each group has a defined set of parameters, such as priority level, permitted media types and so on, and also the defined membership list. When an MU makes a request for affiliation to a group to the SIP server, the SIP server checks with the group manager that the MU is a member of the group.

The group management entity is responsible for the disabling and enabling of existing groups. The CCAS does not permit the MU to use or be affiliated to a disabled group (see clause 7.4.4). When the CCAS disables a group, the CCAS terminates any existing calls and SIP sessions for the group (see clause 7.5.6) and cancels any pending call setup requests to the group (see clause 7.4.5).

5.4.4 Resource management

The resource management entity is responsible for interaction with the access networks for setting up and maintaining the appropriate bearers to and from MUs and groups of MUs in order to carry signalling and media information related to calls.

It makes use of the information provided by the mobility management entity in order to determine the optimum path to transport call related control information and media between participants in a call. If participants can be reached by multiple paths, e.g. unicast and multicast, the resource management entity determines the most efficient means of distributing the information. The resource management entity also determines the available and required quality of service for each of the connections comprising the call, and reports to the application control function if there are insufficient resources of adequate quality to carry some parts or all parts of the call.

5.4.5 Control server

The control server entity is responsible for managing call related information. When a call is to be placed, the control server receives the call request from the initiator; determines whether the called party or group is available; requests resources from the resource management entity and determines whether the call should go ahead based on the available resources, and sends appropriate signalling to the parties in the call to initiate the call using the resources provided by the resource management entity.

The control server also provides priority management within calls based on the priority of the users within the groups, the priority associated with the groups, priority dependencies on the hours of operation and duty hours, the priority associated with each MU's present location and on the call priority requested by each user.

The quality of service and priority may vary according to a number of factors such as media type, individual role, location, etc. and the control server makes its decisions according to these various factors.

5.4.6 Media distribution

The media distribution entity distributes the media within calls from current sourcing party to target party/parties within a call, making use of the various unicast and multicast paths provided by the resource management entity.

5.4.7 Security

The security entity is responsible for maintaining all elements of application related security, to ensure that CCA signalling and media is protected even when carried over otherwise unprotected bearers. Its functions include:

- Control of encryption of signalling and media flows.
- Control of integrity protection for signalling and media flows.
- Key management for the authentication, encryption and integrity functions.
- Support for end to end encryption between users at appropriate security levels, with appropriate algorithm negotiation and clear override where needed.

5.4.8 Identity management

The identity management entity is responsible for authenticating the CCA user and providing the CCA client instance with the information the CCA client requires to obtain service from the CCAS. This information includes:

- an access token;
- an identity token;
- a CCA individual identity;
- agreed user profile identities;
- a limited-access token.

6 Reference points, identities and protocols

6.0 Reference points

The reference points are defined with reference to figure 4 where an LTE EPS provides the broadband IP connection between MU and CCAS.

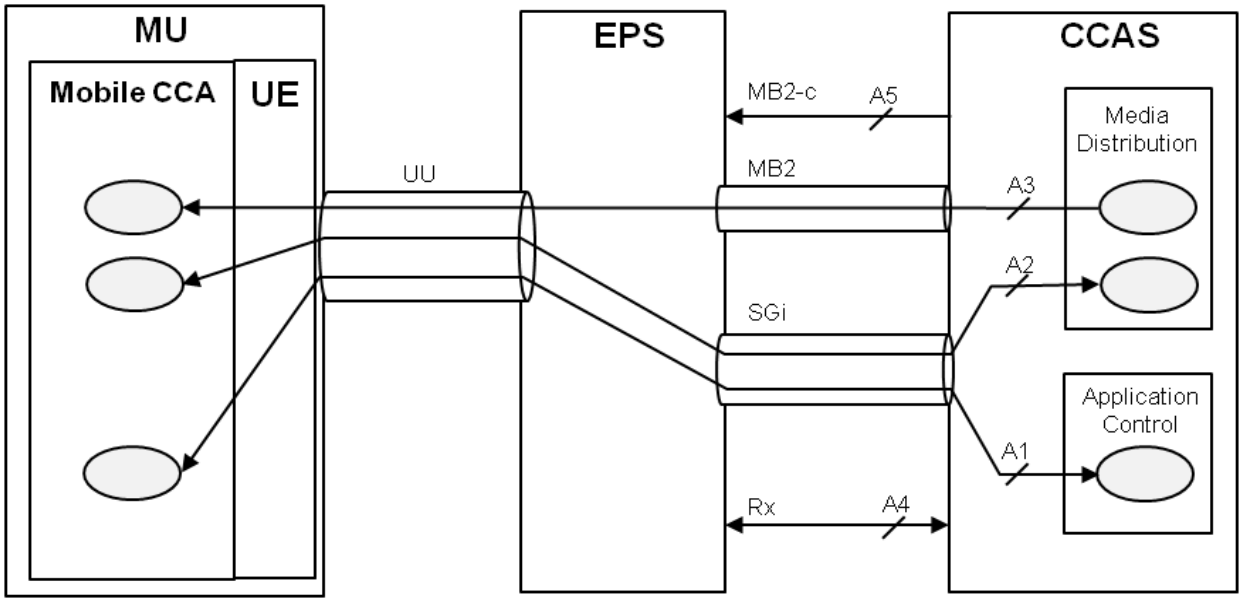


Figure 4: Reference points

A1: is the channel used for communication between the Mobile CCA (which is part of the Mobile Unit) and the Application Control entity of the CCA Server. The protocol over this reference point carries all individual signalling except for the media associated signalling, and may include location information.

A2: carries media and associated signalling flows carried over unicast transport bearers, between the mobile CCA (which is part of the Mobile Unit) and the media distribution entity of the CCAS.

A3: carries media and associated signalling flows carried over broadcast transport bearers, from the media distribution entity of the CCAS to the mobile CCA (which is part of the Mobile Unit).

A4: provides control of unicast bearers for application signalling and media flows.

A5: provides control of multicast bearers for application signalling and media flows.

The set of reference points A1, A2 and A3 corresponds to interface 4, and the set of A4 and A5 corresponds to interface 2 described in [i.11].

NOTE 1: A future interface, or an extension of an existing interface, may allow flow of location information from the EPS (or alternative broadband IP network) to the CCAS.

NOTE 2: A broadband IP network other than an LTE EPS may not offer equivalents of reference points A3, A4 and A5.

6.1 Identities and protocols

6.1.0 CCA User identities

The CCA user identity is specific to an individual user and a CCAS. The CCA user identity is used only for human user log-on and mutual authentication with the user's home CCAS. The CCA user identity is hidden from other users.

The format of the CCA user identity is outside the scope of the present document. A user identifies himself to the identity management entity of the CCAS by means of his CCA user identity, and supplies some form of security credential for authentication purposes in order to be given access to the CCAS. Following successful authentication of the CCA user identity, the identity management entity provides the MU with the CCA individual identity for that user, which allows that user identity to be bound to the MU during the step of registration with the CCAS.

When performing user authentication, the user may select from one or more profiles which allow the user's current role to be taken into account. A user may select different profiles at the same time on different devices.

6.1.1 CCA application identities

CCA application identities take the form of SIP Universal Resource Identifiers (URIs - see IETF RFC 3261 [2]) which have a format of user@application_domain.org (where the "user@" portion is optional and is called "userinfo"). These SIP URIs are globally usable and identify the user's home CCAS. If the network design permits, external calling to and from a user will be possible.

Percent-encoded octets (see IETF RFC 3986 [24], section 2.1) may be used within the URIs to represent characters outside the range of the US-ASCII coded character set [25]. The UTF-8 character set (IETF RFC 3629 [21]) shall be used to map characters outside the range of the US ASCII characters set to octets prior to being percent-encoded for the URI.

A displayable name may be associated with a SIP URI (see clause 9). Displayable names shall use either the 7-bit GSM default alphabet (see ETSI TS 100 900 [20]) or the UTF-8 character set (IETF RFC 3629 [21]).

The following application identities are defined:

- CCA server identity - the CCA server identity is a name used to uniquely identify a particular CCAS;
- CCA individual identity - the CCA individual identity is a SIP URI specific to an individual user. It has a one-to-one relationship with the CCA user identity;
- CCA functional identity - the CCA functional identity is a SIP URI that represents a role rather than an individual so may be used by different individuals at different times. Depending on the user profile of the CCA functional identity (see clause 9.2) the CCA functional identity may be used by only one user or may be shared by more than one user at the same time;
- CCA group identity - the CCA group identity is a SIP URI identifying a particular group;
- CCA group reference - the CCA group reference is a short-form group reference created by the CCAS for each group. It is used as the "target group identity" in uplink media control protocol (MCP) messages (see annex B): the CCA group reference is not a SIP URI; it may be based on part of the CCA group identity plus a media-type identifier;
- CCA client identity - the CCA client identity is a SIP URI that identifies the CCA client. It includes a field containing a unique hardware identifier of the MU in which the CCA client is installed. The CCA client identifier is also used as the "OAuth 2.0 Client Identifier" required by OpenID Connect for identity management transactions (see clause 7.2.0.2).

NOTE: The CCA client identity may include a field containing a hash of the rest of the CCA client identity and the unique hardware identity to prevent cloning of the CCA client identity.

A CCA individual identity or CCA functional identity may be reached via more than one device. MUs should present users with displayable names.

There may be extra "layers" of addresses if the terminal or its subscription has its own address; e.g. a SIP URI related to the SIM which is used for IMS in a 3GPP LTE system. This is however distinct from the address used for the terminal's user (and distinct from addressing structures used for groups), and is not used as a mechanism by which the user is addressed. The user identities may need to be secured or hidden from the underlying broadband network.

Functional addressing may be supported by allocating suitable addresses to user functional roles. The CCAS may translate calls sent to or from these addresses to user addresses, as described in clause 7.6. A call to a functional identity may result in more than one actual user being called, for example in a control room.

The addressing structure uses a SIP URI, which allows an almost infinite number of addresses to be formulated.

A user may be reached by more than one address, e.g. a SIP URI and a routable (e.g. telephone) number.

6.1.2 Transport protocols

6.1.2.0 Protocol layers

All transport protocols utilized by the CCA make use of IP (IPv4 [9] or IPv6 [10]), to allow operation over any broadband IP network.

The main signalling channel (SIP) is carried over a reliable transport protocol, such as TCP [11] or SCTP [12]. This enables early re-transmission of signalling messages without forcing short application layer timers. Appropriate higher layer signalling such as TLS [13] and/or DTLS [14] are used to encapsulate signalling flows, as illustrated in figure 5.

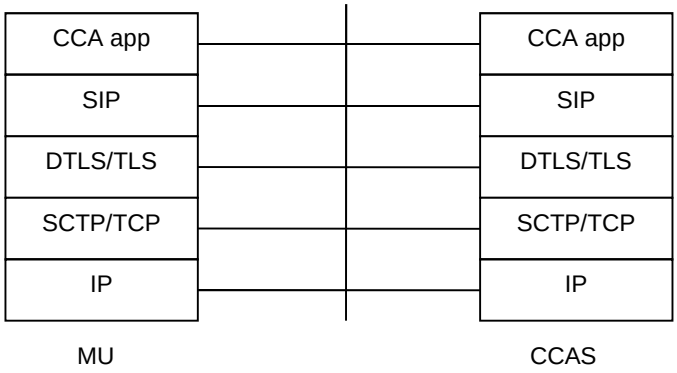


Figure 5: MU to CCAS interface, control plane part

NOTE: SCTP may be run over UDP where NAT traversal is required.

Media and media related signalling are carried over UDP [15] to allow unidirectional flows and to avoid latency issues using TCP. Where protection against lost packets is required, the application provides the appropriate resilience, e.g. by application level retransmissions. Call related signalling and media make use of protocols such as (S)RTP (S)RTCP [16], [17] and carried over UDP/IP, as illustrated in figure 6.

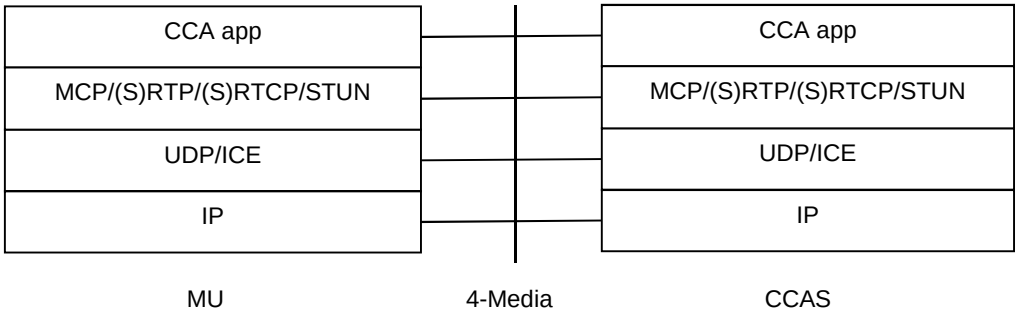


Figure 6: MU to CCAS interface, media plane unicast part

Further protocols such as ICE [18] will be utilized where the path between the MU and CCAS requires NAT traversal. The ICE protocol uses STUN [3] and TURN [19] for NAT traversal setup and NAT maintenance.

An MU may have several transport sessions to the CCAS active at any one time, differentiated by UDP port number. It is possible that more than one IP address will be used at the CCA. The IP address(es) and port numbers will be determined at session establishment.

Media and media-related signalling can alternatively be transported over a transparent broadcast bearer. In this case, the unicast transport is partly replaced by a simple multiplexing layer, as illustrated in figure 7.

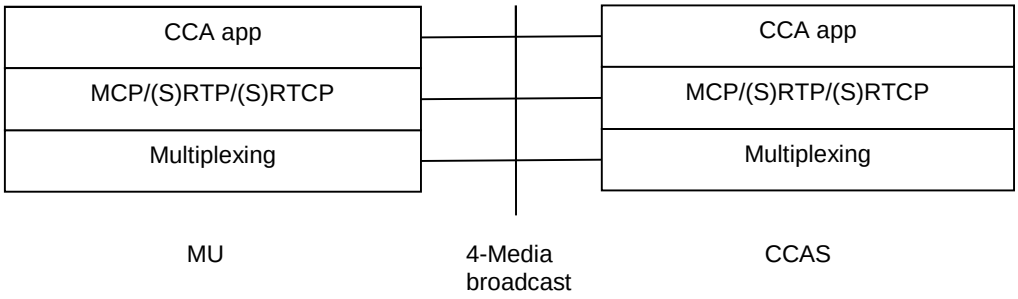


Figure 7: MU to CCAS interface, media plane multicast part

6.1.2.1 Unicast transport

Unicast transport will be provided by all types of underlying broadband IP network. Where an LTE EPS is the underlying network, the CCA makes use of the SGi interface for signalling and media. The characteristics of the bearer may be different for different application flows; for example an application signalling flow will use a non guaranteed bit rate bearer, but a real time media stream (e.g. containing speech) will require a guaranteed bit rate. The characteristics of bearer for different media flows (e.g. speech, video) may be different. The parameters with which the bearers are established is a matter for the application and outside the scope of the present document.

A unicast bearer will always be used to carry information from the MU to the CCAS. A unicast bearer may be used to carry information relating to either individual services or group services from the CCAS to the MU.

The bearers needed for the support of mission critical voice may be set up by the CCAS after registration and authentication as required, to join any ongoing calls or to take part in new calls. The strategy adopted by the CCAS when setting up such bearers is outside the scope of the present document.

6.1.2.2 Multicast transport

For group addressed media and signalling, unicast bearers may be complemented by a broadcast bearer if the access sub-system provides this. Inbound traffic for media and associated signalling related to group addressed media (from MU to CCAS) is always provided by a unicast bearer, while outbound traffic may be provided by transmission in a multiplex of several channels over a broadcast bearer.

NOTE 1: While the addressing of the unicast channel is specific for a given mobile unit, the addressing of the broadcast channel (TMGI in the case of LTE) is defined on a per group basis. There may be more than one group making use of the same TMGI.

NOTE 2: Although several media flows may be multiplexed on a single broadband bearer, the actual multiplexing policy is left to the implementation.

6.1.2.3 Control of unicast/broadcast transport over LTE

When an MU which is receiving media over a unicast bearer or set of unicast bearers moves into an area where the corresponding media stream(s) are broadcast over a set of broadcast bearers, transmission of this same information over the unicast bearers may be suspended. The CCAS may interact with the LTE EPC to release the bearers.

Conversely, when an MU which is receiving one or more media streams over broadcast bearers loses the required level of quality (or anticipates this loss), or moves outside the area where media broadcast is available, it may request that the infrastructure resumes transmission of the corresponding media over unicast bearers. The CCAS may need to interact with the LTE infrastructure to establish appropriate unicast bearers if none are presently active between CCAS and MU.

To achieve this successfully, the CCAS will need to understand the relationships between the areas where media broadcast is available and where it is not available. This may require having knowledge of cell by cell allocation of the multicast broadcast service. The CCAS may be provided with this as a static configuration, or may be able to access this information dynamically. The MU may assist by reporting the availability of multicast channels in its serving cells. The CCAS will also need to be aware of any provisioning restrictions concerning which MUs are permitted to use any configured multicast service.

The CCAS may also decide to move communications between unicast and multicast at any time on the grounds of efficiency.

6.1.3 Network layer protocols

The CCA makes use of SIP [2] for network layer protocols. SIP is used for:

- Application level registration and deregistration.
- Affiliation to groups for group calls.
- Session initiation (individual and group calls).
- Messaging and other such services.

The parameters of each service such as service type, codec type and bit rate are proposed and negotiated using SDP [7] parameters contained in the SIP messages. A separate SIP setup with appropriate SDP is required for each separate session, whether the different sessions carry the same or different media types.

6.1.4 Application layer protocols

6.1.4.0 Keep alive

Application layer protocols will be based on existing protocols where appropriate and carried over IP.

The application layer protocols may include a periodic "keep alive" message which firstly ensures continuous information about the status of the MU to the CCAS, and secondly may be used to maintain lower layer transport paths, especially where NAT traversal is used.

NOTE: The MU may not be aware that a NAT is in use unless specifically configured to know this.

6.1.4.1 Pseudo-broadcast protocol

The purpose of this protocol is to provide an information transmission function of background information from CCAS to its served MUs. Two main types of information may be transmitted using this method:

- Service related information: this is information is related to the services provided by the infrastructure, including relevant network status information if it is impacting the provision of some service (for example isolated system).
- Geographically related information: for example, information about neighbouring systems or list of border cells for the current MBSFN area in LTE.

To provide accurate geographically related information, the application using this protocol shall be aware of the geographic location of the MU.

Neither type of information requires fast real time updates.

6.1.4.2 Group information exchange

A protocol within HTTP (see IETF RFC 7230 [22]) is used by the MU to request and receive information about groups, including lists of affiliated users.

6.1.4.3 Priority information requests

Priority information requests from the MU to the CCAS uses a protocol within HTTP (see IETF RFC 7230 [22]).

6.1.4.4 Profile and CCA service parameter management

A protocol within HTTP [22] is used by MUs registered to suitably authorized users to read and modify user, device and group profiles and CCA service parameters, and is used by the CCAS to synchronize MUs with modified profiles and service parameters.

6.2 Standardized application codecs

6.2.1 Voice Codec

For voice, two categories of vocoder should be considered:

- a CCA code: the choice of this codec is outside the scope of the present document;
- interoperability codecs: TETRA, Tetrapol, P25 Full Rate, P25 Half Rate.

Any CCA codec shall have good intelligibility in noisy conditions.

6.2.2 Video Codec

The selection of a CCA video codec is outside the scope of the present document.

7 Overview of services

7.0 Introduction

The following clauses provide an overview of the services provided and a brief generic description of the signalling involved when applicable.

7.1 CCA system access

Before user access to a CCAS is possible, the MU has to attach to an access network and the CCA client has to perform SIP registration of the MU (i.e. the device) with a CCAS (see note) to permit an unauthenticated user to gain access to limited services, e.g. emergency calls. Then the CCA client can attempt to connect its users to their chosen CCASs.

NOTE: The choice of CCAS for SIP registration of the MU is outside the scope of the present document. The MU's choice of CCAS is limited to CCASs where the MU's limited access token can be used (see clause 7.2.0.2).

When the access to the CCAS is performed through a 3GPP E-UTRAN (LTE) access network, access implies the attachment of the mobile (UE) to E-UTRAN, the activation of a default bearer of appropriate QoS in the PDN offering the access to the CCAS, the allocation of an IP address, and the determination of a serving DNS address.

Following connection to the access network, the CCA client establishes an IP connection to the selected CCAS's application control interface (see clause 5.3.1.1) secured by an appropriate protocol (e.g. TLS, using, if available, the CCA client's pre-provisioned CCAS certificate for the selected CCAS to derive information for creation of the secure connection and to authenticate the CCAS). The CCA client shall then create a CCA client instance (i.e. an instance of the CCA client's application functionality) particular to the MU and shall create a UUID unique to the MU's CCA client instance (e.g. by using the timestamp method of IETF RFC 4122 [26]). The CCA client may then attempt SIP registration of the MU's CCA client instance with the CCAS (see clause 7.2.3). This allows a user to access the limited services that are available to the MU (e.g. emergency calls) for unregistered users.

The CCA client may now attempt to connect its users to their chosen CCASs by conducting user authentication (if required) of its users with their home CCAS identity management entities, validating the authentications with the users' selected CCASs (if not the user's home CCASs) and then SIP registering and establishing relevant interface information (IP address, port numbers) for the media interfaces for each user so that IP access is possible to the application control interface of the user's selected CCAS.

The CCA client uses ICE protocols to establish a connection with the CCAS through a NAT (see clause 7.2.3.2). If a NAT is in use, the CCA client may also use STUN protocols [3] to provide periodic keep-alive messages between the CCA client and the CCAS to keep the NAT address translation process alive.

7.2 Service registration

7.2.0 Initial authentication procedure

7.2.0.1 General

The normal sequence of events following power-on is illustrated in figure 8 (figure 8 does not consider the possibility of authentication or SIP registration failures).

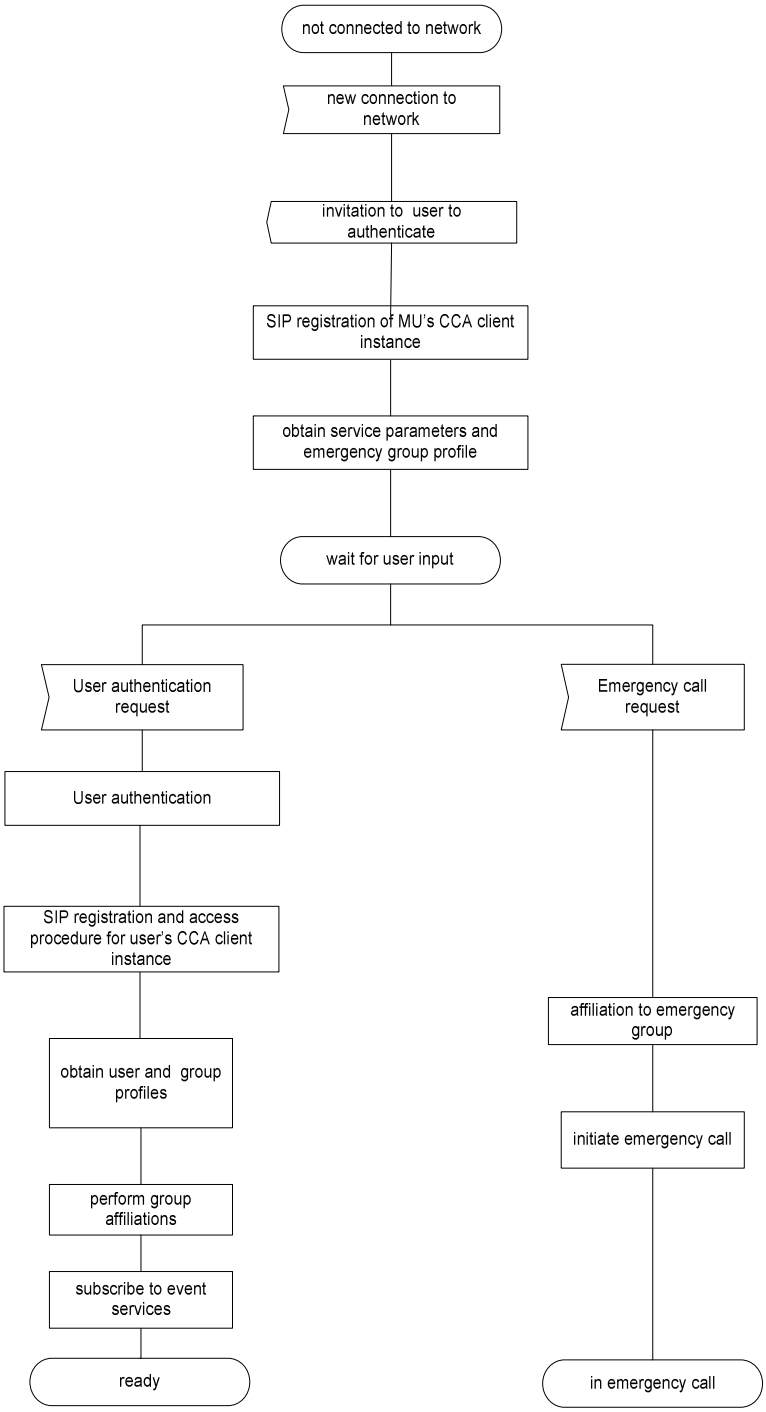


Figure 8: Sequence of events in the MU following power up

NOTE: Figure 8 shows how emergency calls are made available to an unauthenticated user. Other services may also be provided to unauthenticated users.

7.2.0.2 Authentication

Before the CCA client's users can be granted access to full services, the CCA client has to create a CCA client instance particular to each user and has to create a UUID unique to each user's CCA client instance (e.g. by using the timestamp method of IETF RFC 4122 [26]) The CCA client is then required to register each user's CCA client instance with a CCAS using SIP (see IETF RFC 3261 [2]) as specified in clause 7.2.3. Depending on pre-provisioned information in the CCA client, each user may first be required to authenticate to the user's home identity management entity. The user authentication process makes use of the non-SIP interface to the user's home CCAS application control interface (see clause 4.2.1). The CCA client needs to be configured with access details for the user's home CCAS and the CCA client needs to be informed of the user's home CCA server identity.

If authentication is required the user's CCA client instance provides the user's CCA user identity to the user's home CCAS identity management entity together with an appropriate security credential and the CCA client identity. The credential may take the form of a password, a biometric credential (fingerprint, etc.), proof of possession of a physical token, or some other form of credential.

"OpenID connect" [31] may be used for the authentication process.

If a certificate installed on the CCA client is used to verify the CCAS, then the identity management entity can be considered to be authenticated to the client. However this is not considered to be a mutual authentication between identity management entity and user, as the verification of the identity management entity takes place at a different layer to the authentication of the user. Mutual authentication of the user can be provided if the identity management entity can present some information that can be verified by the user or can be verified by some physical token in the possession of the user during the process within which the user authenticates to the identity management entity. However, a certificate installed on the CCA client can be used to prove the authenticity of the MU and its CCA client.

The identity management entity now generates a cryptographically-signed identity token, a cryptographically signed access token and a cryptographically signed limited-access token. The access and limited-access tokens are incomprehensible to the CCA client so the identity management entity provides metadata with each access and limited-access token that allows the CCA client to determine the scope and expiration time of each token.

The identity token identifies the authenticated user to the CCA client instance and any non-home CCAS. It contains, *inter alia*, the user's CCA individual identity, the identity token's time of issue, the identity token's expiry time and a URI for the issuing CCAS.

The access token contains the user's CCA individual identity, the MU's CCA client identity, a scope parameter (a list of services for which the token is applicable) and an expiration time. The metadata provided with the access token contains the scope parameter and the expiration time. The access token is presented during SIP registration to demonstrate that the user's CCA client instance has permission to use the CCAS services listed in the scope parameter. The access token provided during user authentication is only valid for use on the user's home CCAS.

The limited-access token contains the MU's CCA client identity, the scope parameter and an expiration time, which may be later than the expiration time of the access tokens. The metadata provided with the limited-access token includes the scope parameter (possibly indicating limited services), the expiration time, and a list of one or more CCASs where the limited-access token can be used. The limited-access token is presented by the MU to obtain access to limited services when the MU's CCA client instance performs SIP registration on this CCAS. The CCA client should store the limited-access token for use during future SIP registrations of the MU on this CCAS, replacing any previously-received limited-access token.

When multiple users wish to use a single MU at the same time and the pre-provisioned information in the CCA client requires its users to be authenticated, the CCA client is required to go through the above processes of authentication and obtaining of identity and access tokens for each user.

If the authentication fails, the SIP registration of the MU using the limited-access token provides the means for the user to access limited services that may be available through an authenticated CCA client (e.g. emergency calls), as defined in the device profile (see clause 9.5.2). Depending on the reason for the authentication failure, a timer controlled retry may be permitted or a permanent barring of access means may be invoked.

If a user wishes to use a non-home CCAS and the non-home CCAS requires user authentication, the user's CCA client instance uses pre-provisioned information about the non-home CCAS to make a secure HTTP connection with the non-home CCAS's identity management entity, sends the user's identity token to the non-home CCAS's identity management entity as proof of authentication and requests an access token for the non-home CCAS. If the non-home identity management entity finds the identity token to be valid, the non-home identity management entity may send the CCA client an access token valid for that user on the non-home CCAS.

NOTE 1: Different user CCA client instances can use different CCASs at the same time if they are accessible through the same PLMN.

Before SIP registration of the user, the CCA client selects a user profile for the user.

NOTE 2: The method by which the CCA client selects a user profile for the user is outside the scope of the present document.

7.2.1 Home network registration

Authentication and SIP registration with the user's home CCAS is possible as soon as the network used to access the Critical Communication Application provides connectivity. This may be achieved when the MU is in its home 3GPP network (e.g. when its LTE modem is attached to its HPLMN) or when the MU is using a non-home access network (e.g. when its LTE modem is attaching to a VPLMN, from another country/organization, from another Mobile Network Operator or from a non-3GPP network). See figure 9.

In the latter case, the MU activities and the usage of network resources are controlled by the CCA client's home application, based on service agreements with the visited network. A charging agreement may be in force.

NOTE: If the access network (e.g. VPLMN) hosts a CCAS that is not the CCA client's home CCAS or the user's home CCAS the CCA client instance does not obtain service from that CCAS unless the CCA client instance migrates to that CCAS (see clause 7.2.2). An un-migrated CCA client instance therefore does not have access to groups hosted by the non-home CCAS, unless those groups are available through an inter-CCAS connection from theuser's home CCAS.

If user authentication is required by the CCAS (the CCA client is pre-provisioned with this information), the CCA client attempts to perform user authentication with the user's home CCAS's identity management entity via an HTTPS connection (see IETF RFC 2818 [23]) as described in clause 7.2.0.2. When any required user authentication has completed, the CCA client conducts SIP registration of the user's CCA client instance with the user's home CCAS as described in clause 7.2.3. Immediately following a successful SIP registration, the CCAS service parameters, the user's user profile and the relevant group profiles are installed in the CCA client if not already present (see clause 7.2.3.8). Finally, the CCAS may affiliate the user's CCA client instance to some groups and the user's CCA client instance may request affiliation to other groups in the user profile's group membership list (see clause 9.2).

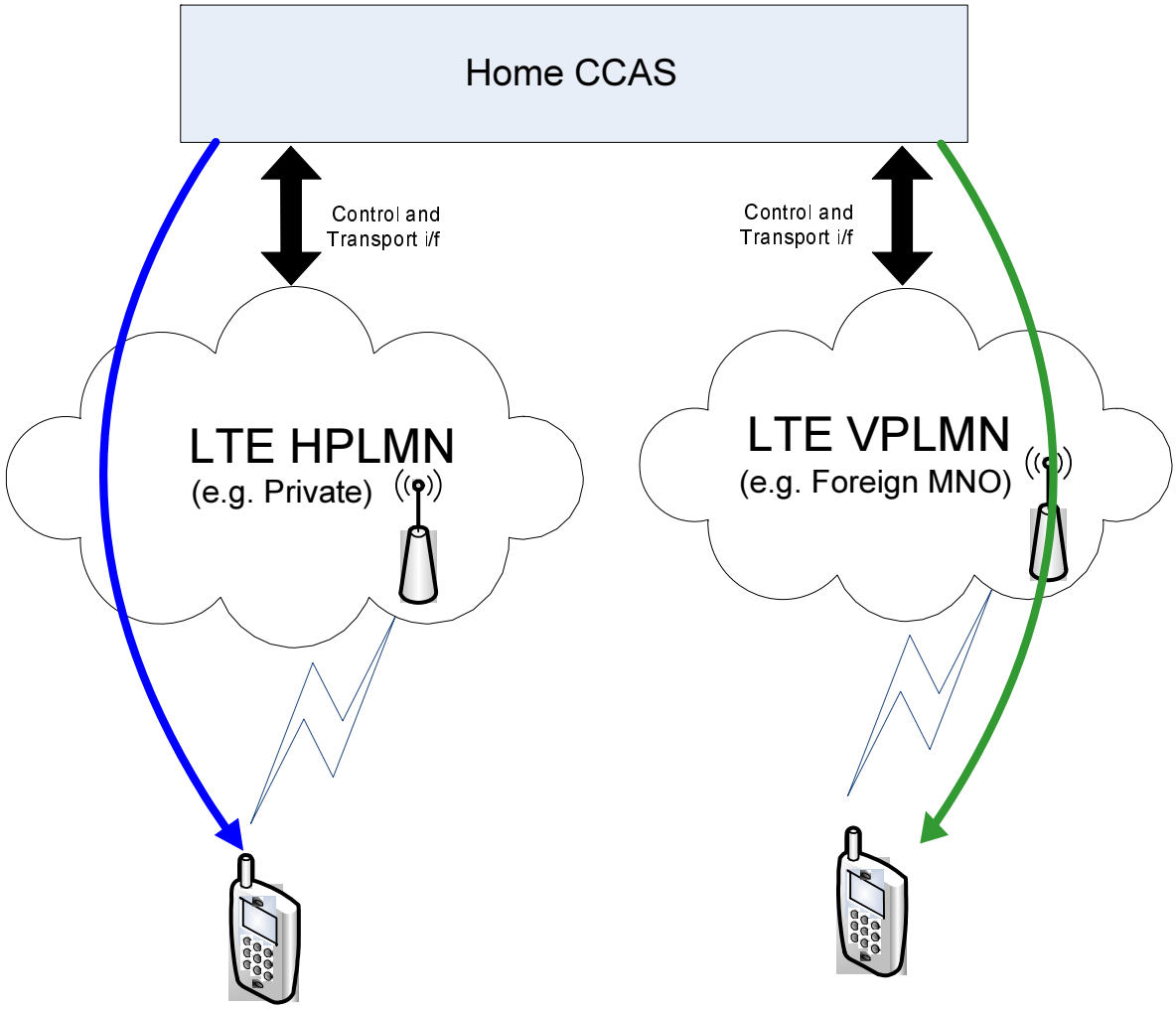


Figure 9: Home registration

7.2.2 Migration registration

When connected to an access network which provides connectivity to a CCAS that is not the home CCAS of the CCA client, the CCA client may elect to visit that CCAS by performing SIP registration with the non-home CCAS (see figure 10). This decision may be the result of manual selection by the user or may be configured in the CCA client. Use of a visited CCAS is only possible if the CCA client has been pre-provisioned with an APN (in the case of 3GPP access) and an IP address, FQDN or URI for the CCAS to be visited. The CCA client also needs to be pre-provisioned with the user authentication requirements of the non-home CCAS. Depending on security policies, the CCA client may need to be pre-provisioned with a certificate for the non-home CCAS.

The user's CCA client instance then attempts SIP registration with the visited CCAS, presenting the local access token (see clause 7.2.0.2) to the visited CCAS with the SIP registration. The user and the CCA client may be provisioned with access rights locally, but, more typically, the visited CCAS communicates with the user's home CCAS in order to retrieve access rights, service information and the user, group and device profiles. If SIP registration with the visited CCAS is successful, the CCA client and the user are marked as migrated in the home CCAS location registers and the user's previous group affiliations are cancelled. At the completion of the registration process, the user's CCA client instance may be sent a SIP NOTIFY message from the visited CCAS that contains a URI for supplementary configuration information specific to the visited CCAS (see clause 9.3).

NOTE: If a user attempts to set up an emergency call before that user's CCA client instance completes SIP registration, the emergency call will be sent to the CCAS with which the CCA client SIP registered the MU.

A CCA client instance that has performed a migration registration does not have a new identity, but may be a member both of groups managed by the non-home (visited) CCAS and groups managed by the home CCAS, under control of the visited CCAS. QoS for all the services remains under the final control of the visited CCAS.

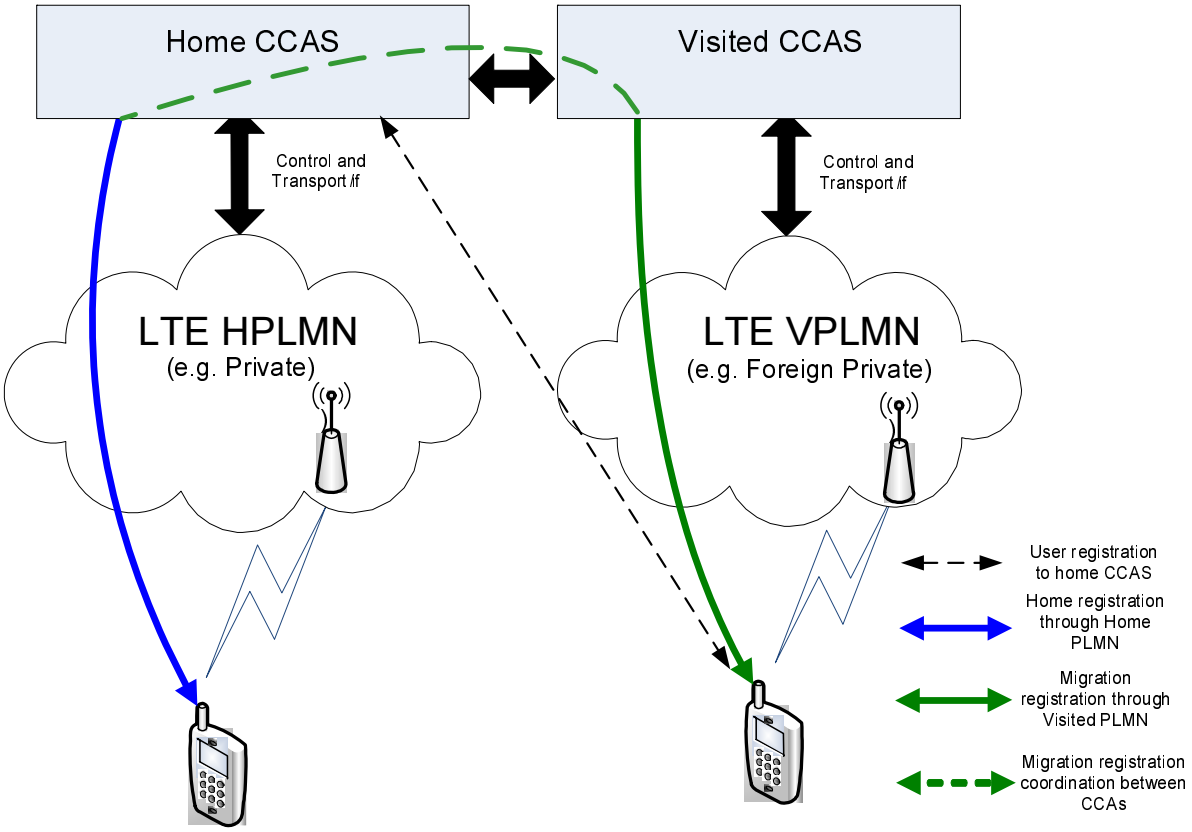


Figure 10: Migration registration

7.2.3 SIP registration and access procedure

7.2.3.1 General

The CCA client needs to register the MU and its users with the CCAS's SIP application server when it powers-up, joins a CCAS after having previously been registered with a different CCAS, changes its access network (e.g. from 3GPP to a non-3GPP network or from one WiFi network to another WiFi network), or after any other event that causes the MU's IP addresses to change.

The registration process uses the registration function of SIP [2]. The SIP registration may be performed with a CCAS SIP application server that is connected to the home network or may be performed with a CCAS SIP application server that is connected to a visited network.

SIP registration shall be periodically refreshed.

7.2.3.2 Preparation for SIP registration - the access procedure

The CCA client may be required to present a limited-access token for the MU and access tokens for each of its users during the SIP registrations. These are obtained during initial authentication. The CCA client is required to create and SIP register a separate CCA client instance for the MU and each of its users. The CCA client shall SIP register the MU CCA client instance before the CCA client SIP registers its user CCA client instances as illustrated in clause 7.2.0.1.

When the CCA client is ready to register with the CCAS's SIP application server the CCA client shall first establish a secure connection (e.g. with TLS using, if available, the CCA client's pre-provisioned CCAS certificate to derive information for creation of the secure connection and authentication of the CCAS) with the CCAS's SIP proxy or with the CCAS's SIP application server (if there is no SIP proxy). This may be a separate secure connection (optionally using a separate certificate).

During the establishment of the connection to the SIP proxy or SIP application server, each user's CCA client instance sends a set of STUN binding requests to the STUN server that has the same IP address as the SIP proxy or SIP application server using the well-known STUN port number '3478'. A STUN binding request is sent from each of the addresses and ports that the CCA client instance is intending to use for RTP/RTCP traffic (the host candidates). This action initiates the "access procedure" which subsequently makes use of the SIP registration process.

The purpose of the access procedure is to establish for each of the CCA client's users a set of 5-tuples for unicast media flow that can traverse multiple NATs. The access procedure enables NAT traversal without allocating GBR resources which would be detrimental to overall resource management. STUN and SIP are used for the required exchange of information between a CCA client instance and the CCAS server on the two different sides of a potential NAT; the eventually-translated address information may then be used to setup sessions without requiring using different procedures for the case where a NAT is present and the case where a NAT is not present.

The stage 2 description of the required steps is presented in figure 11.

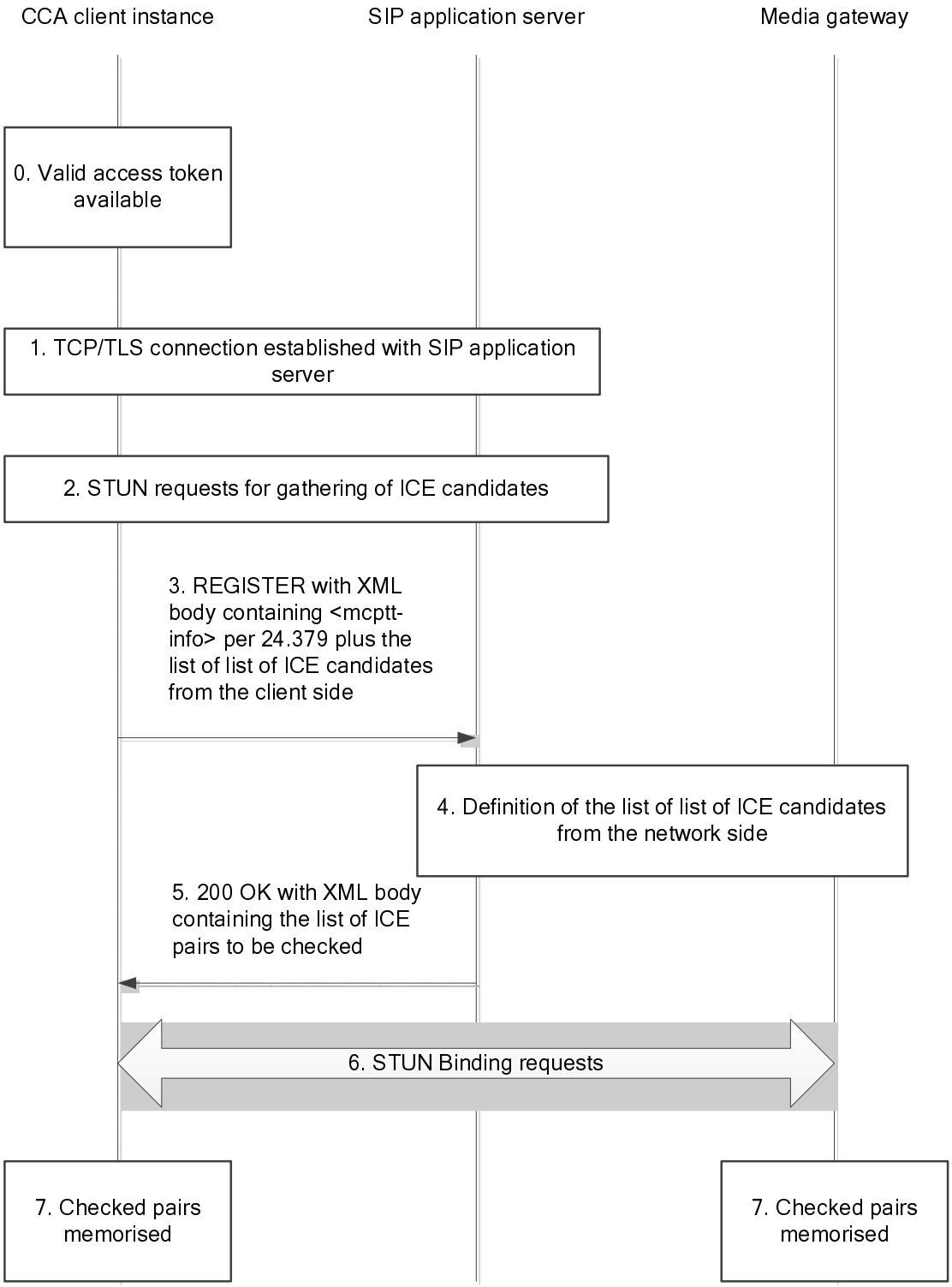


Figure 11: Access procedure

0. The CCA client instance has obtained from a previous transaction with its home identity management server a valid identity token and an access token with appropriate temporal and geographical validity. (Methods by which the CCA client instance can obtain the IP address of the CCAS's application control interface are described in clause 5.3.1.1.) If required, the CCA client instance can use its identity token to obtain a valid local access token.

1. The CCA client instance establishes a secure connection with the SIP application server.

NOTE 1: The connection between the CCA client and the SIP application server may be via a SIP proxy.

2. During the establishment of the connection to the SIP application server the CCA client instance sends from each of the addresses and ports that it is intending to use for RTP/RTCP traffic (the host candidates) a STUN binding request to the STUN server which has the same IP address as the SIP application server and the well-known STUN port number, i.e. 3478.

3. Based on the information gathered in step 2, the CCA client instance sends to the SIP application server a SIP REGISTER request with an XML body containing an <mcptt-info> body and an additional element providing the list of ICE candidates and their intended use.

4. The SIP application server and the media gateway determine a matching list of ICE candidates from the network side.

5. The SIP application server's 200 OK response to the SIP REGISTER request contains an XML body with the information about the list of IP addresses and ports (of a media gateway) to be paired with the candidates gathered by the client in the previous step.

6. Based on the information from steps 3 and 4, the client and the media gateway construct for each element of the external list a list of candidate pairs for connectivity checks according to IETF RFC 5245 [18].

NOTE 2: During the process of check according to IETF RFC 5245 [18], additional candidates, i.e. peer reflexive candidates may be discovered and are added in the connectivity checking process.

7. The client and the media gateway memorize the checked pairs and their intended use and will use the information to populate the SDP bodies. Periodic checks will be performed to maintain connectivity.

7.2.3.3 SIP registration of the CCA client

When performing SIP registration of the CCA client, the CCA client instance shall place its CCA client identity in the From header field of the SIP REGISTER message. If the CCA client has a limited-access token obtained during a previous user authentication, as described in clause 7.2.0.2, the MU should present the limited-access token with its request to SIP register the CCA client; otherwise the MU does not include a limited-access token in its SIP registration request. The CCAS may use the presence or absence of the limited-access token and its expiration time to determine the level of the limited services the CCAS will provide to the unauthenticated user. For example, the presence of a limited-access token may prove that the CCA client has previously been authorized for use with the CCAS but the limited-access token's expiration time may indicate that the limited-access token is "stale".

7.2.3.4 SIP registration of users

When performing SIP registration of a user, the CCA client instance shall place the user's CCA individual identity in the From header field of the SIP REGISTER message. In order to register a user with a CCAS's SIP application server the CCA client requires a CCA client instance specific to the CCA user and may require an access token. The CCA client instance may already exist or the CCA client may need to create it (see clause 7.1). The access token is derived from user authentication, as described in clause 7.2.0.2. If an access token is required, it shall be included in the SIP REGISTER message.

The CCA client may provide concurrent service to multiple CCA client instances. These may represent different CCA individual identities, each with its own user profile, or may represent one CCA individual identity with different user profiles, or a combination of both. If user authentication is required, each CCA individual identity requires its own identity token and access token.

NOTE 1: The method by which the CCA client selects the user's user profile is outside the scope of the present document.

NOTE 2: Where a user possesses more than one MU that may be registered with the CCAS at the same time, the user may specify a preferred CCA client identity for reception of individual voice calls. This may be specified by a parameter in the control field of the SIP registration message that overrides similar information in previous SIP registrations and device profiles.

7.2.3.5 Identities used for SIP registration

The CCA client instance shall place its CCA client identity in the Contact header field of the SIP REGISTER message and shall request a GRUU (see IETF RFC 5627 [30]) by including an "instance ID" in the "+sip.instance" Contact header field parameter defined in IETF RFC 5626 [29]. The instance ID shall contain the CCA client instance's UUID (see clause 7.1).

Before responding to the SIP REGISTER request the SIP application server tests the validity of the limited-access token or access token and the CCA client instance (e.g. by checking the validity of the signature and expiration time and by comparing the information in the From and Contact header fields of the SIP REGISTER message with information in the access token).

If the SIP registration is rejected the rejection is reported to the CCA client instance. Depending on the rejection reason, a timer controlled retry may be permitted or a permanent barring of access means may be invoked. The behaviour when rejected from a visited CCAS may be different to the behaviour when rejected from the home CCAS.

If the SIP registration is accepted, the SIP application proxy (or the SIP application server if no SIP application proxy exists) shall include a temporary GRUU and a public GRUU in its response. The MU shall include either the public GRUU or a temporary GRUU as the contents of the Contact header field in non-REGISTER SIP requests and responses that it emits. The SIP application server shall provide the MU with the TMGI and any other necessary information about any broadcast announcement MBMS in its response to the SIP registration.

If a further user wishes to use the MU, the MU shall create a separate CCA client instance for each further user. If user authentication is required, the further user shall perform the user authentication process with the identity management entity, thereby obtaining an access token to use in the SIP registration process. The further user's CCA client instance shall place the further user's CCA individual identity in the From header field of the SIP REGISTER message and shall request a GRUU by including the CCA client instance's UUID in the "+sip.instance" Contact header field parameter of the SIP REGISTER message.

NOTE: The SIP application server maintains the mapping between the CCA individual identity, the CCA functional identities (if any), the CCA client identity and the GRUUs. The CCAS decides which user instances to contact (see clauses 8.3 and 8.4) if more than one matches the URI in the "To" header field. Normally the calling CCA user would call any or all suitable user instances of the called user by placing the called party's CCA individual identity or CCA functional identity in the "To" header field of the SIP message. However, if a CCA user has previously received SIP signalling containing another party's GRUU, he may attempt to call that specific CCA client instance by placing the GRUU in the "To" header field of the SIP message. GRUUs are invalidated when the registered contact expires (either due to timeout or explicit de-registration) or if the SIP Call-id value of the registered contact is changed.

Following a successful SIP registration, the newly-registered CCA client instance shall issue a SIP SUBSCRIBE to its own status (i.e. to the "reg" event package - see IETF RFC 3680 [32]). If the CCA individual identity is already registered with another CCA client instance, the CCAS shall send the CCA client instance a SIP NOTIFY message informing the CCA client instance that the CCA individual identity is already registered with another CCA client instance. The CCA client instance should then notify the user.

7.2.3.6 Device class and device capabilities

The MU is pre-provisioned with the MU's device class and device capabilities (see clause 9.1). If either of these has changed since they were last sent to the CCAS, they should be sent to the CCAS now in a SIP PUBLISH message.

7.2.3.7 Subscription to event services

On completion of the registration and publication process, the CCA client instance shall subscribe to event services relevant to the CCA using the SIP Specific Event Notification process [4] (SIP SUBSCRIBE) and subscribing to the "reg" event package, and may subscribe to other relevant event packages using further SIP SUBSCRIBEs. Following the subscription(s), the CCAS may notify the CCA client instance of relevant events using SIP NOTIFY messages.

The case for direct registration is shown in figure 12. The access token obtained by user authentication to the identity management entity of the CCAS is provided in the first SIP REGISTER. An optional rejection and re-registration process is also shown whereby authentication is carried out to the CCAS at the SIP level, as the challenge from the CCAS is returned in the 401 Unauthorized message.

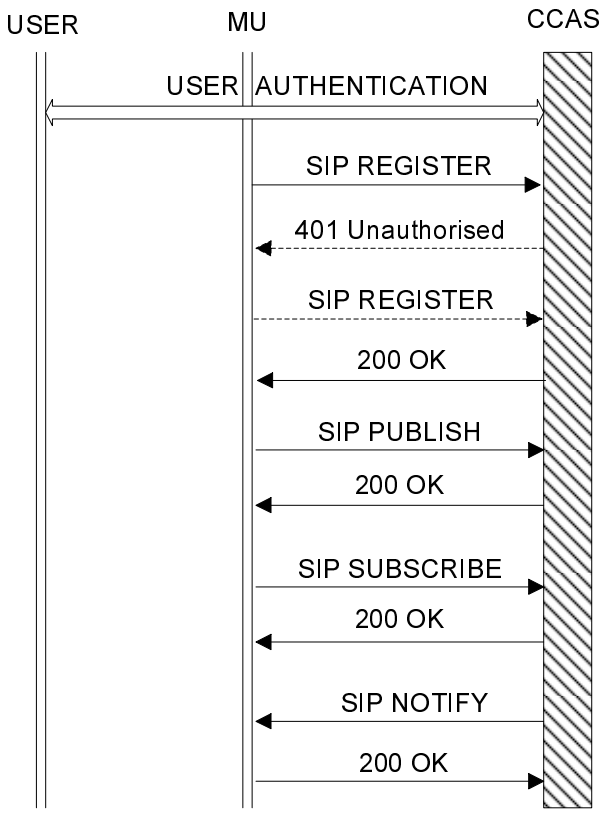


Figure 12: Message sequence chart for registration process

7.2.3.8 Service parameters, profiles and security parameters

Following registration, the CCA client instance obtains the CCAS service parameters and the device, user and group profiles that the CCAS has associated with the CCA client instance. Specifically, the CCA client instance sends a request for a particular profile in a SIP SUBSCRIBE message containing the CCA client identity and the CCA individual identity and receives a notification in a SIP NOTIFY message that contains a URI for the requested profile. The CCA client instance then retrieves the profile using HTTPS (see IETF RFC 2818 [23]).

The CCA client instance should request the CCAS service parameters and the device, user and group profiles using the following order:

- CCAS service parameters;
- device profile;
- user profile;
- group profiles.

Group security keys may be provided with the group profiles. Alternatively, the group security keys may be provided during affiliation.

If the MU already possesses a set of CCAS service parameters or a profile, the MU should not download the CCAS service parameters or profile unless the CCAS has a more recent version. Clause 9.1 provides a method for the MU to obtain the latest version of a profile and provides a method for obtaining the differences between the MU's version of a profile and the version of the profile stored by the CCAS.

NOTE 1: The SIP server uses the CCA client identity and the CCA individual identity (some device capabilities might be available only to certain users) provided by the CCA client instance in the SIP SUBSCRIBE message to choose a suitable device profile. The SIP server provides a URI for that device profile in its SIP NOTIFY response to the CCA client instance.

NOTE 2: The MU may need to download new CCA service parameters when it registers on a different CCA server. The method by which different CCASs agree on common parameter values is out of scope of the present document.

NOTE 3: The user profile lists groups to which the CCA client instance is required to affiliate at initial registration and other groups to which the MU may affiliate at any time.

The CCA client needs to obtain the device profile and an emergency group profiles before it can make an emergency group call if the user failed to register.

7.2.3.9 Group affiliations and media paths

Once the MU and the CCA client instance(s) have completed their SIP registrations, exchanged device class, device capabilities, service parameters and profiles, and subscribed to event services, the secure connection is used by the signalling protocols to set up group affiliations and calls as needed. The SIP message exchange which establishes the group affiliations and sets up calls will also be used to establish a secure communications path to allow the exchange of media and media related signalling. The security parameters for the secure path which will carry media and media related signalling may be exchanged using the signalling path.

Sets of unicast media path 5-tuples should have been established earlier by the access procedure (see clause 7.2.3.2). The 5-tuples are used to set up media paths which allow paths through a NAT to be set up and maintained. This will expedite call set up procedures when group sessions are not joined until calls are set up.

Unicast media path transport parameters for group communications are assigned to the CCA client instance at session setup (or possibly at affiliation). The 5-tuples may be assigned to the CCA client instance by the originator of the SIP INVITE from the set of pairs memorized by the CCA client instance during the access procedure (see clause 7.2.3.2). If there is no pre-assigned media path ready to be assigned when a session is started, the media path establishment and NAT traversal needs to be done when the session is established.

Unicast media path transport parameters for individual communications are assigned during call set up. If there are NATs in the path from the CCA client to the CCAS, it is preferable to choose the 5-tuples for individual communications from those established by the access procedure; otherwise the 5-tuples for individual communications could be established at call setup time.

Security keys for group communications may be provided earlier together with group profile delivery or may be provided during group affiliation. The method by which the encryption keys are provided is outside the scope of the present document.

If the CCA client instance's registration expires or is cancelled, it will receive a SIP NOTIFY from the "reg" event package telling the CCA client instance that its registration is terminated. The CCA client instance may then attempt to re-register.

7.2.4 Periodic update

A periodic registration update procedure allows the maintenance of accurate registration records in the CCAS and purging the database of records corresponding to units which have silently disappeared due to link failures. Timing of the periodic update is determined by a combination of the home and serving CCASs. On initial registration, the MU and serving CCAS agree an expiry time by negotiating the "expires" time interval in the contact header of the REGISTER message according to [2]. Subsequent REGISTER messages are used to extend the registration period.

The MU may periodically include location information as part of the procedure.

NOTE: The loss of connectivity through one network or one type of network (for example LTE) may not be deemed as an application level loss of connectivity as the mobile unit may re-establish connectivity through a different network or a different type of network.

Additionally, a periodic "heartbeat" may be required to keep IP paths including NAT alive (see clause 7.1). Application layer location information may also be used for this purpose (but note that if the NAT requires a frequent update, location information may add unnecessary load).

7.2.5 Deregistration

When the MU no longer requires service from the CCAS (for example as the result of a user action such as switching off the MU) the MU deregisters from the CCAS. A SIP REGISTER message is sent, with the "expires" header set to zero (i.e. reducing the lifetime of the current registration to zero).

The MU may send information during the deregistration process to indicate a change to a different state, for example entering into Direct Mode (direct MU to MU communication outside of an infrastructure).

If the CCAS wishes to deregister the MU from the CCAS, a SIP NOTIFY is sent to inform the MU that its registration has been terminated.

7.2.6 Remote deregistration

If a user is registered to the CCAS with two or more MUs, the user may use one MU to transmit a request to the CCAS to cancel his user registration on other MUs by using HTTPS (see IETF RFC 2818 [23]) to query the CCAS's identity management entity to obtain references to the relevant authentication instances and then sending a SIP REGISTER message specifying a list of references to the registration instances to be deregistered, with the "expires" header set to zero (i.e. reducing the lifetime of the current registration of the specified device to zero),

An authorized user may request the CCAS to cancel the registration of another user from one or more specified MUs or from all MUs by querying the CCAS's identity management entity to obtain references to the relevant registration instances and then sending a SIP REGISTER message specifying a list of references to the registration instances to be deregistered with the "expires" header set to zero (i.e. reducing the lifetime of the current registration of the specified registration instances to zero).

Such queries and requests will be rejected by the identity management server unless accompanied by a valid access token.

7.3 Individual streaming communication

7.3.0 General

7.3.0.1 The individual communication process

Individual communications may be established between two MUs or an MU and a fixed unit or external telephony subscriber, both in incoming or outgoing call mode. The individual calls that do not include an external telephony subscriber may use on/off hook signalling with explicit alerting of the call recipient, or may use direct signalling for automatic call setup. Calls may use a full-duplex or a half-duplex media flow. The call setup request from the originating MU indicates whether the recipient shall answer automatically or whether on/off hook signalling is required. The call setup request also indicates whether a full-duplex or half-duplex call is requested. The overall call control protocol is derived from IP based digital call control protocol used for IP telephony and is based on SIP [2].

For individual calls, resources are allocated at setup time.

NOTE 1: The originating user's profile (see clause 9.2) may indicate which types of call the user is permitted to request and for which set or sets of destination users the originating user may request an individual call. The called user's profile may permit the called user to restrict providing the caller with the reason for any failure of an incoming call. An authorized CCA user may query and modify users' profiles (see clause 7.11.13).

When a user attempts to setup an individual full-duplex voice call to another MU, the calling user's MU shall check that its user's profile authorizes the calling user to setup an individual full-duplex voice call to the destination user. When the CCAS receives a request to setup an individual full-duplex voice call and the destination user is currently associated with more than one registered MU, the CCAS shall send the call setup request to the MUs as indicated by the user's profile.

NOTE 2: The user's profile may be configured to specify that incoming call setup signalling is be sent to each of the CCA individual identity's registered MUs in order of device preference until the call is answered, or sent only to the CCA individual identity's most preferred MU or device, or sent simultaneously to all the CCA individual identity's registered MUs of a device class (see clause 9.7) that can handle incoming calls of this type, such that when one MU answers the call, the other MUs stop alerting and are excluded from the call (see clause 9.2).

A CCA user is only permitted to participate in one individual full-duplex voice call at one time, even if he possesses multiple registered MUs. An ongoing call that does not have emergency priority may be replaced by an incoming emergency priority voice call sent to a group with which the user is affiliated.

The CCAS normally (see note 3) provides the calling MU's CCA individual identity and/or associated displayable names and, if available, the calling user's CCAS server identity to the receiving MU. The receiving MU may display this information to its user. The CCAS may send location information about the calling MU to the called MU, subject to privacy restrictions, and may send location information about the called MU to the calling MU. The sending of location information can be activated and deactivated by an authorized user (see clause 7.10).

NOTE 3: Except in the case of talking party identity restriction, see clause 7.11.2.

The receiving user should experience no lost audio at the start and end of a voice burst.

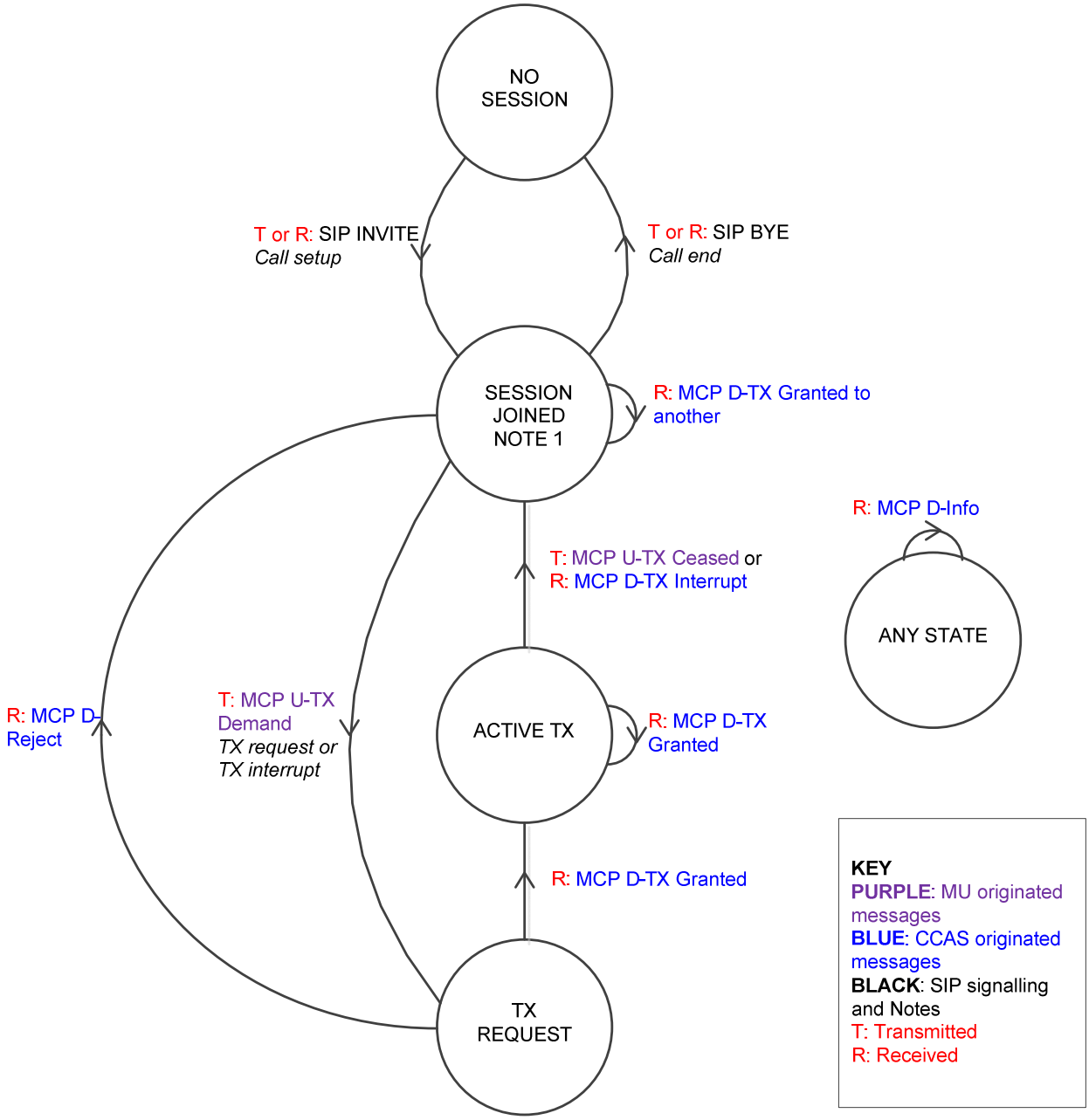
NOTE 4: The messages that are shown in the following clauses use SIP protocols and terminology.

7.3.0.2 Media control protocol for individual calls

The Media Control Protocol (MCP) - see annex B - shall be used to control the flow of media during a half-duplex call. Different calls and media types are distinguished by different flow identifications. The first MU to request permission to transmit in a call with a particular media type chooses a flow identification and the CCAS may either confirm the proposed flow identification or replace it in the MCP D-TX Granted message that gives the MU permission to transmit. The MU should continue to use the agreed flow identification for further transmissions and MCP messages in the same call unless the CCAS provides a replacement flow identification in an MCP D-TX Granted message. However the two MUs should choose different flow identifiers.

7.3.0.3 Individual call states

A simplified state-event diagram for individual call is shown in figure 13.



NOTE 1: The CCA client instance may be idle or receiving in a call in the "Session joined" state.
NOTE 2: The CCA client instance may receive media in "Active TX" state (full duplex call) and "TX Request" states (half and full duplex calls).
NOTE 3: State changes in the CCA client occur in response to a received message, or in response to the received acknowledgement to a transmitted message.
NOTE 4: The CCA client may be kept waiting in the TX REQUEST state until bearers become available.

Figure 13: State-event diagram for individual call

Figure 13 shows the states from the perspective of the CCA client instance. The description of the states follows.

- No session: The CCA client instance is not participating in an individual call.
- Session joined: The CCA client instance may be idle and not receiving media, or may be receiving media from the other party in the call. The CCA client instance may initiate transmission requests using floor control signalling. All reception of media and floor control takes place using unicast bearers.

- TX Request: The CCA client instance moves to the "TX Request" state following reception of an acknowledgement to a transmitted "MCP U-TX Demand". The CCA client instance may continue to receive media if the other party is still transmitting.

- Active TX: The CCA client instance is transmitting media within the call. The CCA client instance may be unable to receive media in this state in a half-duplex individual call, but is able to receive media in a duplex individual call.

7.3.1 Individual unit to unit call with on/off hook signalling

This service is analogous to the normal fixed telephony or cellular telephony service. After dialling by the calling party, the calling MU sends a SIP INVITE containing a parameter indicating that call setup is being requested to initiate call set up signalling to the CCAS and also containing parameters indicating that on/off hook signalling is required and whether a half-duplex or, if permitted by the calling user's profile (see clause 9.2), a full-duplex call is requested. The CCAS both acknowledges the set up signalling by returning a SIP TRYING message containing a parameter indicating that the call setup is proceeding, and forwards the call request as a SIP INVITE to the called MU.

The called MU acknowledges the setup using a SIP RINGING message, and a corresponding SIP RINGING message is passed to the calling party. The called MU alerts its user.

The called user may accept or reject the incoming call. The acceptance of the call by the called user causes the transmission of a SIP OK connection message, and the SIP OK is forwarded by the CCAS to the calling MU. At this point, media paths are made available by the CCAS to carry the call. The media interface transport parameters include the destination IP address and port number (see clause 7.2.3.2) and the codec type. The SIP ACK acknowledgement message from the calling MU is forwarded to the called party, and this completes the call setup. Media exchange can then be performed in full-duplex or half-duplex mode depending on setup information.

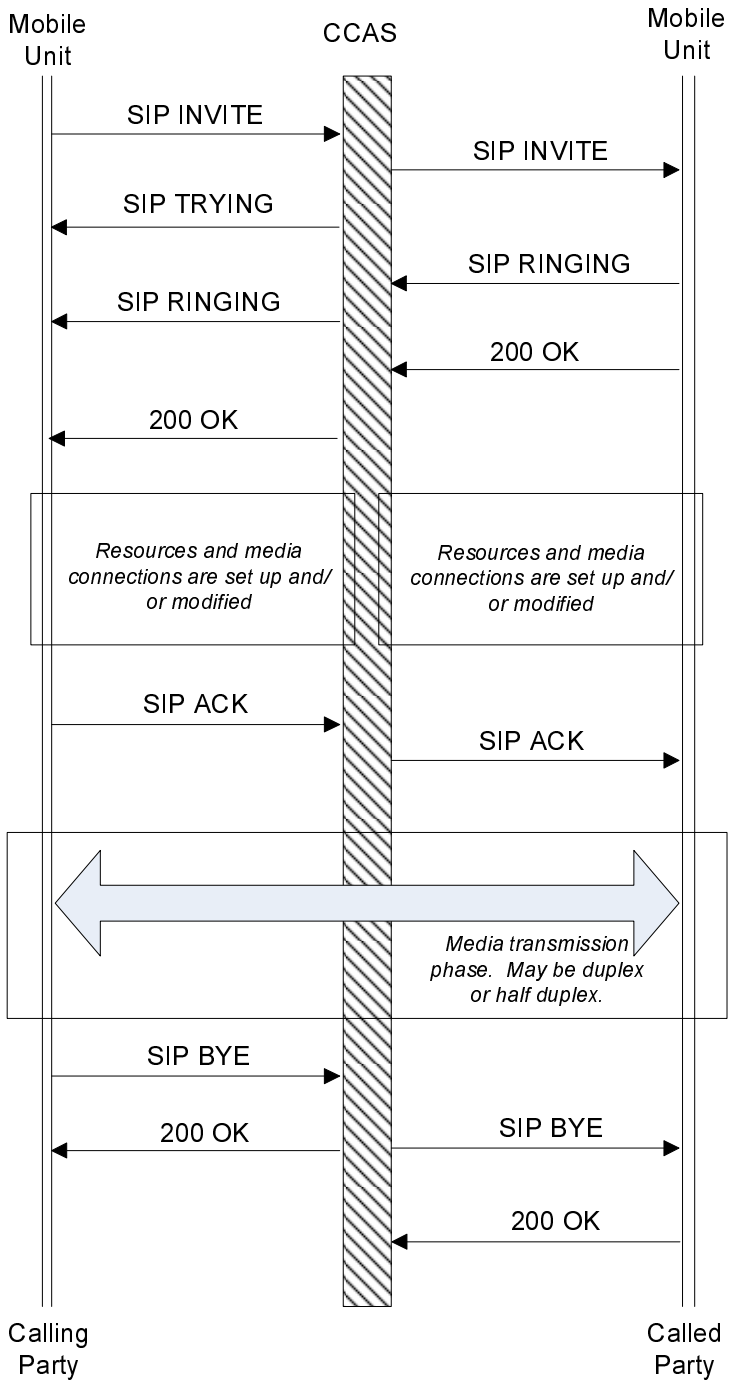
Additional information may be exchanged during the setup procedure through the exchange of SIP 183 SESSION PROGRESS messages, but the transmission or reception of these messages does not lead to any state transition in the call setup state machines. SIP INFO messages may also be used if needed following the set up completion (200 OK).

The call may be queued, for example whilst waiting for a bearer to become available for either party; in this case, the CCAS will send 182 QUEUED messages, and may send 183 SESSION PROGRESS messages whilst waiting for the bearer to be available. Such messages may be sent to both parties prior to the 200 OK which connects the call.

The calling and called MUs are kept informed by the CCAS of the status of the call (e.g. queued, ringing, accepted, rejected, active). However, an authorized user may cause the CCAS to suppress sending to a calling user the reason for any failure of an incoming call.

The calling user may attempt to cancel the call setup request before it completes. Both units may request call release by sending a SIP BYE call disconnection message, or the CCAS may terminate the call (for example following expiry of an inactivity timer) by itself sending a SIP BYE message.

The sequence of messages is outlined in figure 14.



NOTE: Either party may end the call; calling party ending the call is shown in the figure.

Figure 14: Message sequence chart for a successful individual unit-to-unit call setup

7.3.2 Individual unit to unit call with direct signalling

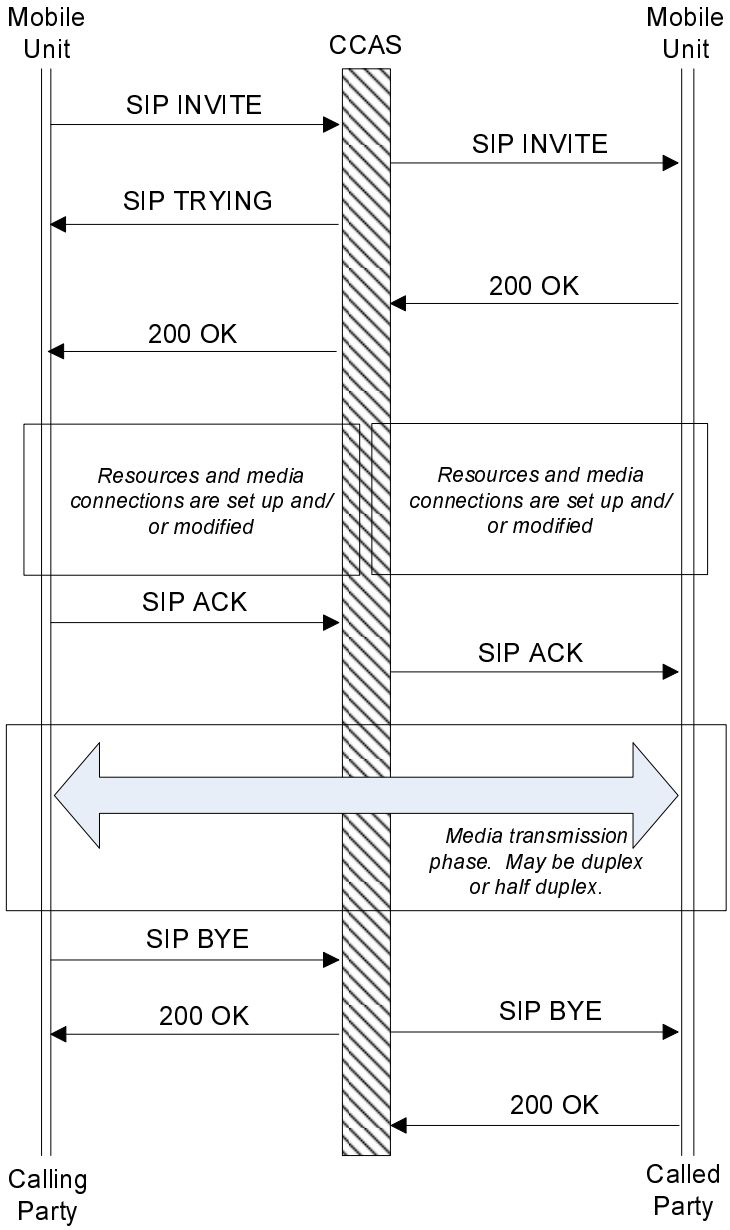
It is possible to shorten the call setup time for individual call by bypassing the alerting step and connecting directly as soon as the called unit is reachable. This also allows the user experience to be more similar to normal (unacknowledged or unconfirmed) group call.

In this case, the alerting step of sending SIP RINGING is omitted leading to the shorter message sequence outlined in figure 15. However, the 200 OK connection messages are retained in order to make sure that media capabilities of the calling and called parties (for example codecs) are properly matched before the setup is completed.

Call queuing and call release are similar to the previous case.

The calling and called MUs are kept informed by the CCAS of the status of the call (e.g. queued, accepted, active). However, an authorized called user may cause the CCAS to suppress sending to a calling user the reason for any failure of the requested call. The calling user may attempt to cancel the call setup request before it completes.

The sequence of messages is outlined in figure 15.



NOTE: Either party may end the call; calling party ending the call is shown in the figure.

Figure 15: Message sequence chart for a successful individual unit-to-unit call setup with direct signalling

7.3.3 Individual unit to telephony call (outgoing call)

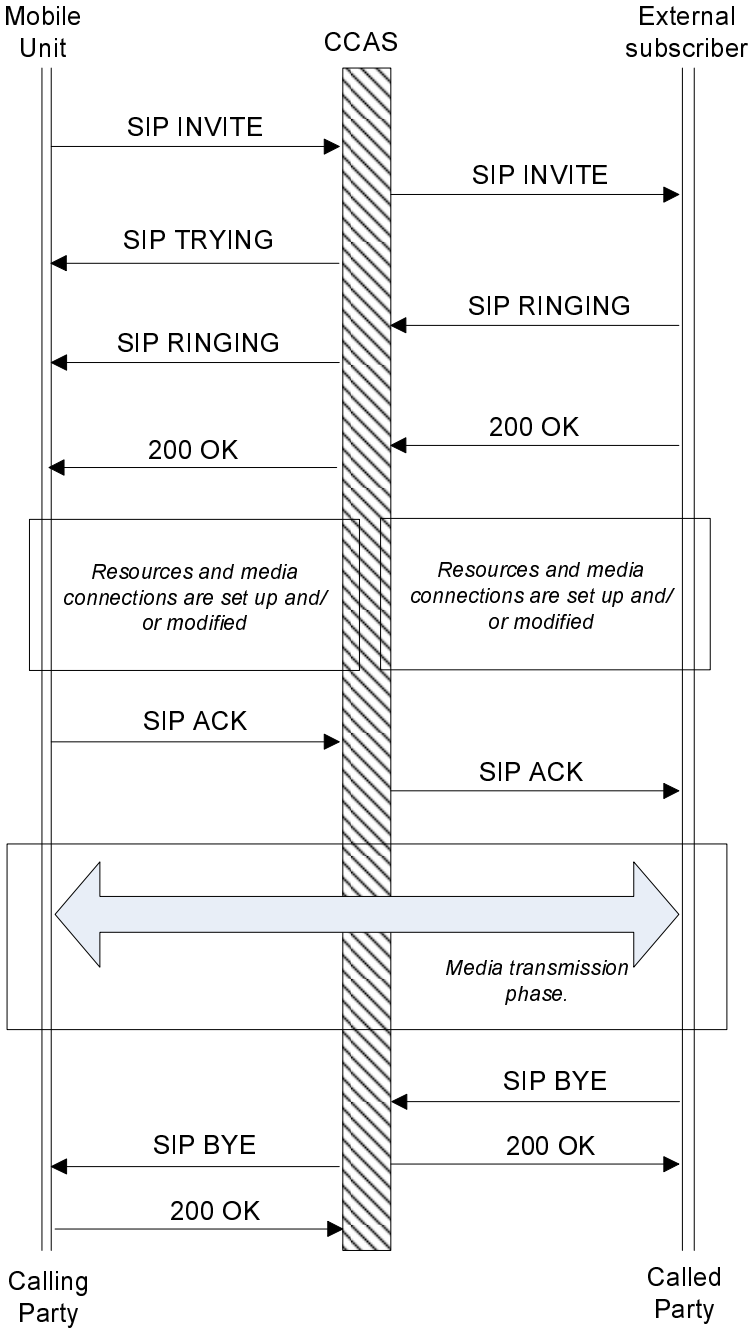
Mobile units may perform calls to external subscribers (including emergency addresses) using fixed telephony interface. Only the message flows for a SIP based interface are standardized, but legacy ISDN interfaces may be supported through additional (non-standardized) gateways.

The calling MU is kept informed by the CCAS of the status of the call (e.g. queued, ringing, accepted, rejected, active). The calling user may attempt to cancel the call setup request before it completes.

Figure 16 presents an example of the sequence of messages exchange for outgoing call setup and release with an external telephone subscriber.

NOTE 1: Support of call to an external subscriber may be subject to restrictions. These restrictions may be general or a per subscriber basis. Dispatcher controlled bypass of these restrictions may be performed using call forwarding and call transfer supplementary services, which can replicate a Call Authorized by Dispatcher supplementary service, as used in some narrowband technologies.

NOTE 2: Media transmission to an external subscriber may imply several transformations of the media, including encryption/decryption of end-to-end encrypted media and vocoder adaptation as required.



NOTE: Either party may end the call; called party ending the call is shown in the figure.

Figure 16: Message sequence chart for outgoing call to an external subscriber

DTMF signalling may be carried in SIP INFO messages during the call.

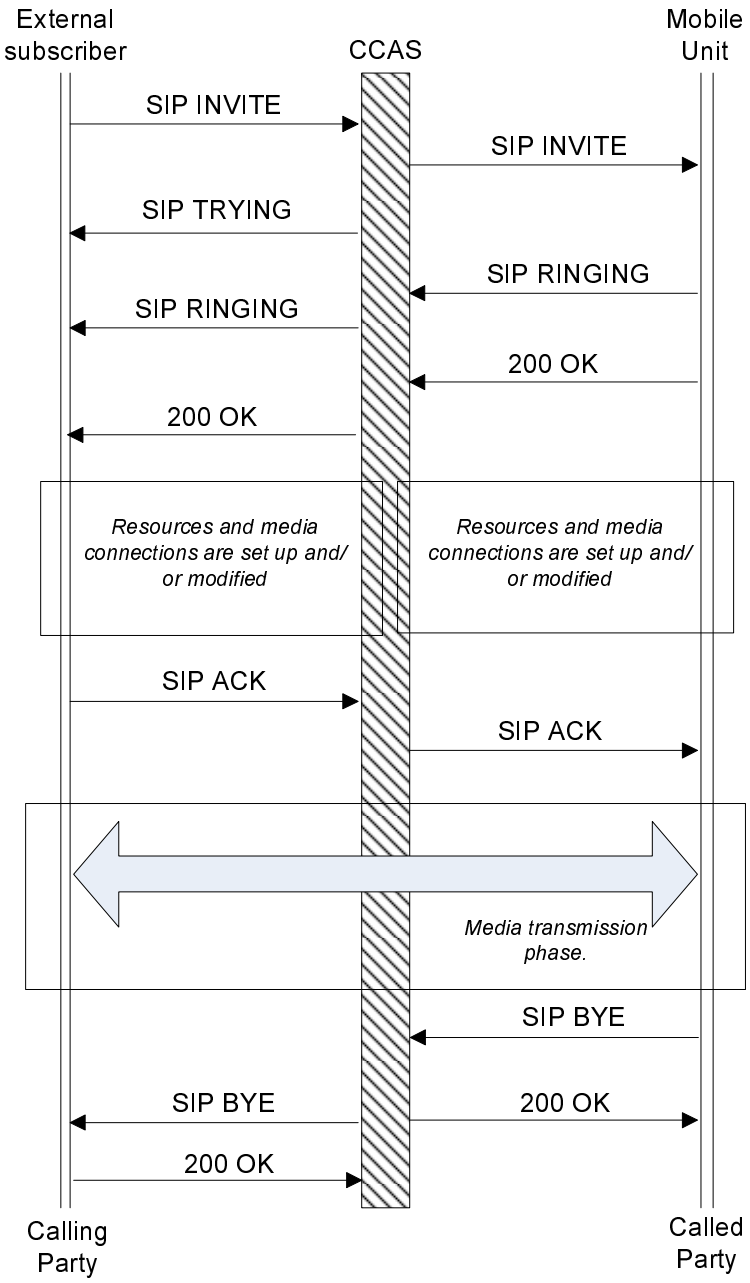
7.3.4 Individual unit to telephony call (incoming call)

Mobile units may receive calls from external subscribers using a fixed telephony interface. As indicated above, only SIP based message flows are standardized, but legacy ISDN interfaces may be supported through additional (non-standardized) gateways. The receiving user may reject the call. An authorized user may cause the CCAS to suppress sending to the external subscriber the reason for any failure of an incoming call.

Figure 17 presents an example of the sequence of messages exchange for incoming call setup and release with an external telephone subscriber.

NOTE 1: Support of call from an external subscriber may be subject to restrictions under infrastructure control. These restrictions may be general or a per subscriber basis. External calls may be diverted to a dispatcher, who may permit a call to be forwarded to the MU using the call transfer service (see clauses 7.11.5 and 7.11.9). This provides an equivalent of a "Call Authorized by Dispatcher" function as provided in narrowband technologies.

NOTE 2: Media transmission to an external subscriber may imply several transformations of the media, including encryption/decryption of end-to-end encrypted media and vocoder adaptation as required.



NOTE: Either party may end the call; called party ending the call is shown in the figure.

Figure 17: Message sequence chart for incoming call from an external subscriber

DTMF signalling may be carried in SIP INFO messages during the call.

7.4 Group streaming communication

7.4.0 General

7.4.0.1 The Group communication process

The group call service is a point to multipoint service, where one MU transmits to a group of MUs who receive the transmitted information almost simultaneously (subject to small variations in delay of the media transport service). In the normal case, group members affiliate to the group before placing calls. This allows the CCAS to prepare to manage resources for the group in real time, even whilst calls are not taking place, and ensures the best possible response time for the group call service. It allows permissions to take part in the group to be determined at affiliation time to avoid any delays due to security procedures at call set up time, and allows parameters for the call (e.g. codec types) to be agreed in advance.

There are four steps to consider in a group communication process:

- Provisioning.
- Affiliation.
- Session join.
- Call start.

The timing of these steps allows slight variations in the service to be offered. The process for each is described in the following clauses of the present document.

Group calls may take the form of open session or discrete calls:

- in open session calls, resources are allocated under control of the floor control automaton when required, when uplink is used after floor grant or when unicast downlink is required;
- in discrete calls, unicast bearer resources are allocated at setup time for the required participants under control of the floor control automaton as above for the other participants.

The open session call service should normally be used for group calls except as described below for discrete calls.

Discrete calls shall be used for CCAS users who are required to be present in a group call and who will be given unicast downlinks and uplinks so that the participants can observe when the required CCAS users leave the call. In the case of an emergency call the required users will be given unicast downlinks and uplinks with increased priority.

An MU may participate in more than one group call at the same time.

Within the same group, different media types may be exchanged in different calls at the same time as each other. Under some circumstances more than one instance of the same media type may be sent to the group (e.g. a partial pre-emption scenario where both the originator and pre-emptor are allowed to transmit, or when multiple group members are sharing video for situational awareness purposes within the same group). The MU may also be a participant in more than one call of the same media type within different groups. Likewise, the MU may be in a different call of a different call type (e.g. in an individual call) at the same time as in a group call. Depending on the capabilities of the MU and the configuration of the CCAS, the second and further calls may be offered to the MU by the CCAS for the MU to respond before receiving media, or media streams may be directly set up. The CCAS may decide to present or withhold lower priority calls than the current call when the MU is sending or receiving information during a call, or in between transmissions during a call. The MU may present the call media from the second and further calls to the user depending on its capabilities and configuration. The MU's decision on whether to indicate that the additional calls are taking place, or to present the media to the user, may depend on whether the MU considers itself to be within a current call (which may include being within the call hang time between transmissions or at the end of a call).

An MU may request to leave a call in progress by sending appropriate signalling to the CCAS. An authorized MU may be able to clear a call in progress for all group members.

The various procedures for taking part in mission critical group streaming communications are described below, together with some closely related services.

Group calls may be unacknowledged, where the calling user does not receive specific feedback about receiving participants in the call, or acknowledged, where feedback from some or all recipients may be used by the CCAS in setting up the call, and where some or all of this feedback may be relayed to the calling party.

A group communication may be setup by an external subscriber (or including an external subscriber) using SIP signalling. The signalling to the called parties is identical to the signalling used for a normal call setup. Acknowledged group call is not supported in this case.

The CCAS shall create a CCA group reference (see clause 6.1.1) for each group. The CCA group reference is provided to MUs when they affiliate to the group. The CCA group reference is used in MCP messages (see annex B).

At any moment in time in a call only one participant type shall be used per group call participant.

The receiving user shall experience no lost audio at the start and end of a voice burst.

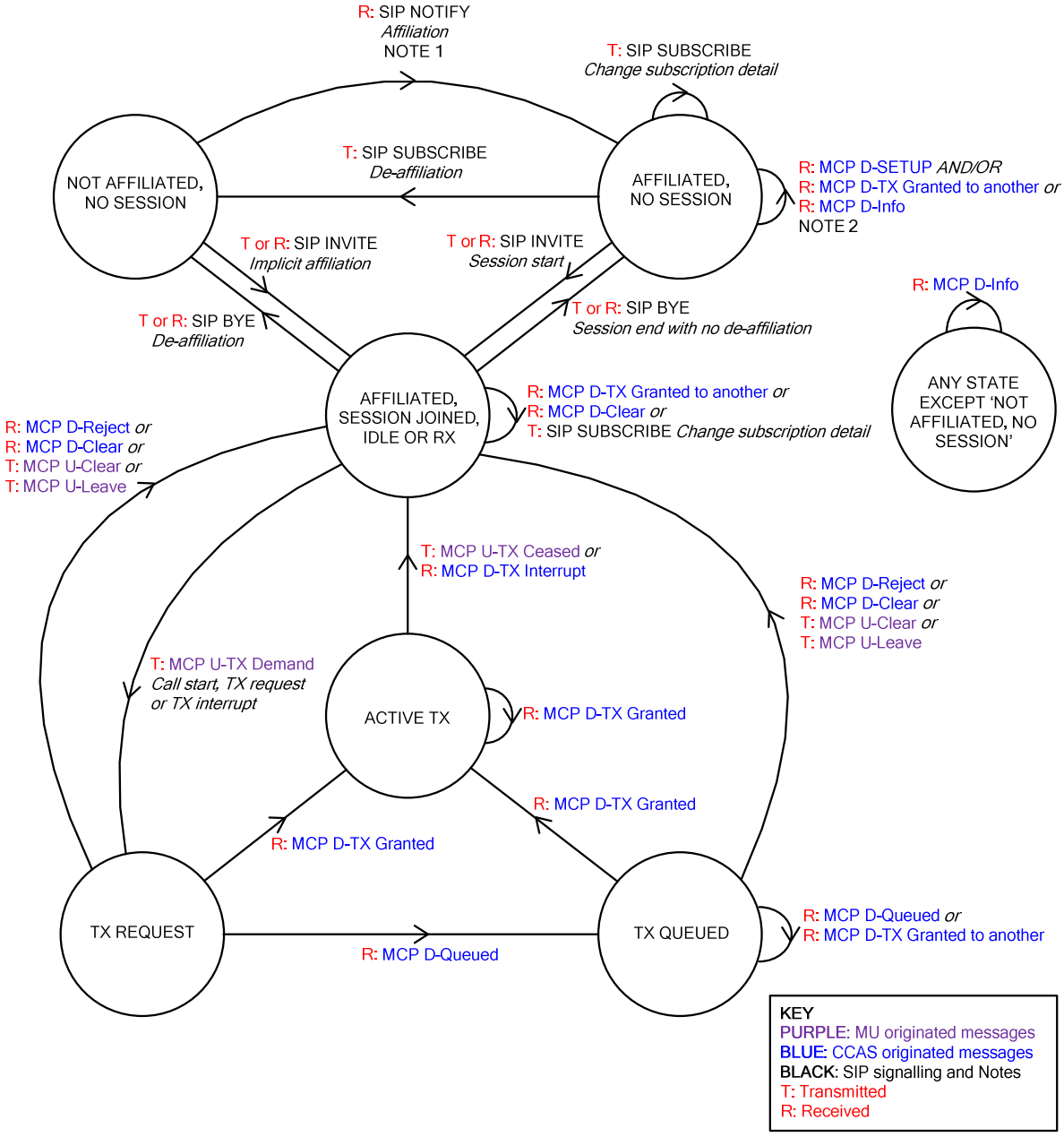
7.4.0.2 Media control protocol for group calls

The Media Control Protocol (MCP - see annex B) shall be used to control the flow of media during the call. Different calls and different media types can be distinguished by different flow identifications. The first MU to request permission to transmit in a call with a particular media type chooses a flow identification and the CCAS may either confirm the proposed flow identification or replace it in the MCP D-TX Granted message that gives the MU permission to transmit. The MU should continue to use the agreed flow identification for further transmissions and MCP messages in the same call unless the CCAS provides a replacement flow identification in an MCP D-TX Granted message. However each MU that transmits in the call should choose a different flow identifier.

An MU taking part in a group call may use the MCP U-Stop and MCP U-Resume messages to control the flow of downlink media e.g. when switching between a unicast and a multicast bearer.

7.4.0.3 Group call states

A simplified state-event diagram for group call is shown in figure 18.



NOTE 1: Prior to receiving a SIP NOTIFY, the CCA client instance subscribes to its affiliation document.
NOTE 2: Floor control signalling in the "Affiliated, no session joined" state is received over a multicast channel.
NOTE 3: State changes in the CCA client occur in response to a received message or in response to the received acknowledgement to a transmitted message.

Figure 18: State event diagram for group call

The figure shows the states from the perspective of the CCA client instance. The description of the states follows.

- Not affiliated, no session: The CCA client instance has not declared an interest in participating in the group, and is not affiliated. The CCA client instance does not receive floor control signalling or media related to the group.
- Affiliated, no session: The CCA client instance has affiliated to the group but has not joined a session. The CCA client instance may receive group calls by receiving floor control signalling and media over multicast bearers. The CCA client instance shall not transmit floor control signalling.

- Affiliated, session joined, idle or RX: The CCA client instance is affiliated to the group and has joined a session. The CCA client instance may receive media following reception of an "MCP D-TX Granted to another" where this floor control signalling and the media may each be received over either unicast or multicast bearers. The CCA client instance may initiate a transmission request from this state either to initiate a new call if idle, or to request to interrupt a currently talking party.

- TX Request: The CCA client instance moves to the "TX Request" state following reception of an acknowledgement to a transmitted "MCP U-TX Demand". The CCA client instance may continue to receive media in an already active call. The CCA client instance will return to the "Affiliated, session joined, idle or RX" state if the request is subsequently rejected, on reception of an "MCP D-Reject" message.

- TX Queued: The CCA client instance has been accepted into the call queue for transmission. The CCA client instance may continue to receive media in a call. The CCA client instance will remain in the "TX queued" state if there is a repetition of or change to the talking party in the call, signalled by reception of a "MCP D-TX Granted to another". The CCA client instance will return to the "Affiliated, session joined, idle or RX" state if the transmission request is subsequently rejected and the CCA client instance removed from the queue on reception of an "MCP D-Reject" message.

- Active TX: The CCA client instance is transmitting media within the call. The CCA client instance may be unable to receive media in this state. Repetitions of "MCP D-TX Granted" do not change the state of the CCA client instance. The CCA client instance will return to the "Affiliated, session joined, idle or RX" if it ends its transmission and receives an acknowledgement to the transmitted "MCP U-TX Ceased", or if transmission is interrupted by reception of an "MCP D-TX Interrupt".

The CCA client instance will return to the "Affiliated, session joined, idle or RX" state from either the "TX Request" or the "TX Queued" states if either the user decides to leave the call or attempts to clear the call following reception of an acknowledgement to a transmitted "MCP U-Clear" or "MCP U-Leave" respectively, or if the call is cleared and the MU receives an "MCP D-Clear". In each case, the outstanding transmission request is cleared, and the user may be informed.

7.4.0.4 E-MBMS use

A group call downlink from a 3GPP network may be broadcast using the Enhanced Multimedia Broadcast Multicast Service (E-MBMS) in some areas. The E-MBMS may use a multicast-broadcast single-frequency network (MBSFN) or single-cell point-to-multipoint (SC-PTM). In those areas the 3GPP network may broadcast announcements on an MBSFN or SC-PTM bearer that informs MUs of the MBSFN or SC-PTM bearer frequency and the temporary mobile group identity (TMGI) corresponding to each CCA group identity using the E-MBMS. The MU is sent the bearer frequency and TMGI of relevant announcement broadcasts in a SIP MESSAGE. When the MU changes to a new MBSFN area, it reports its new MBSFN area to the CCAS and may then receive a SIP MESSAGE replacing the MBSFN bearer frequency and TMGI. When the MU moves out of MBSFN coverage, it informs the CCAS that it has left MBSFN coverage.

The CCAS determines when and where it is appropriate to use the E-MBMS for a group call downlink and when to switch a group call participant between unicast and the E-MBMS. The switching should be arranged to minimize any loss of downlink audio in the MU.

The MU's configuration data (clause 9.7) contains information about the MU's support for E-MBMS, and the CCAS maintains a copy of this information in the device profile (see clause 9.5.3).

7.4.1 Broadcast and system call

A broadcast call is a group communication to a given group where the receiving parties are not allowed to request transmission. Thus, the authorization to request transmission shall be indicated in an information element of the call setup or TX Granted message. The CCAS may merge multiple groups (see clause 7.11.3) to create a temporary group for reception of broadcast group calls. A broadcast group call transmitted on a merged group should have priority over calls to its constituent groups. Broadcast calls should normally be given higher priority than non-broadcast group calls.

A system call is a communication that shall reach a larger subset of mobile units than a single group, whilst being of a broadcast nature. The group identity used for a system call is generally provided to the corresponding mobile units at group affiliation time and may be related to the organization the user is belonging to and/or the groups to which it has affiliated.

An imminent peril or emergency call may be automatically linked to a broadcast or system call within an area.

7.4.2 Group communication coverage

The coverage of a group communication may be potentially unlimited, i.e. extended to the location of every affiliated group member, including affiliated members migrating in all or part of any visited networks, or potentially unlimited but only inside the home network, or limited inside a given geographic area defined by a subset of the access sub-networks. A group member may only make and receive group communications if that group member is inside the permitted coverage.

There is an exception to this. When the mobile unit setting up the call is in an imminent peril or emergency condition, but is not within the nominal permitted coverage area, the call can be setup over an area which contains at least the nominal permitted coverage area and the (normally non-permitted) cell where the mobile unit is located. As a matter of policy, the infrastructure may decide to further extend the coverage to some cells neighbouring the one where the mobile unit is located, or to other cells pre-defined for inclusion in the imminent peril or emergency call.

NOTE: The purpose of the coverage restriction is to save network resources (by not using network resources where unnecessary) and human resources (by not disturbing users which are far from an event and unable to provide any help). However, the implementation of coverage restriction should be smart enough to avoid a bad user experience with ping-pong behaviour at the edge of the communication coverage.

An MU may also request that a group call is placed within a local area only by inclusion of an appropriate parameter in the call setup request. The CCAS configuration will determine the actual coverage when such a request is received. The definition of this local coverage is outside the scope of the present document.

7.4.3 Group provisioning

The group(s) to which an MU may request affiliation are expected to be provisioned in the database of the terminal. The configuration may be programmed statically or may be updated using the individually addressed Dynamic Group Number Assignment supplementary service (DGNA). The CCAS may accept or deny the affiliation(s). The affiliation to some group(s) may trigger further affiliation(s) initiated by the CCAS to group(s) to be used for announcement or system calls or for imminent peril or emergency related group communications.

NOTE 1: The CCAS may also direct the MU to affiliate to certain groups which are not provisioned in the database of the MU (either statically or by DGNA). It is possible that CCAS directed affiliation would only be used in some instances, with no MU requested affiliations.

NOTE 2: The CCAS may limit the total number of group members.

It is possible that in a simple system, a group could be joined by the user simply entering the group name or identifier in the terminal and performing an affiliation to the group by this means, but permission for access to the group will be determined by the CCAS.

Groups may be provisioned in the MU with certain parameters which determine how the MU will behave in those groups. In particular, for the purposes of scanning or reception of broadcast calls, groups may be provisioned as receive-only. A receive-only group may be allowed to operate without a specific group affiliation process, as described in clause 7.4.4 (for example, a default broadcast group for an organization), or may still require affiliation (for example a scanned supervisory group related to the MUs current role).

The CCAS may also support MUs who are provisioned with no groups. In this case the CCAS may determine which group or groups that the MU should use, and may affiliate the MU to those groups.

7.4.4 Group affiliation, mobility and selection

7.4.4.0 Group affiliation

The group service affiliation procedure allows the CCA client instance and the CCAS to negotiate permission for the CCA client instance to participate in calls to a group of which the CCA client instance's user is a member. The affiliation process supports both CCA client-requested group affiliations and CCAS-directed affiliations. In any situation either CCA client-requested, or CCAS-directed, or a combination of both affiliation processes may be supported. The group affiliation process is performed by one or more SIP procedures described in clause 7.4.7. Group membership is achieved by configuration of the group profile by an authorized administrator. Affiliation is necessary before a CCA client is able to communicate with a group. If a CCA client instance needs to urgently send information to a group to which it is not affiliated, it shall carry out the affiliation procedure before attempting to send information. The CCAS shall reject requests to transmit information to a group if the CCA client instance has not previously affiliated. The CCAS may also reject a request by the CCA client instance to be affiliated to one or more groups.

The CCAS shall not permit a CCA client instance to affiliate to a group of which the CCA client instance's user is not a member. The CCAS shall not permit a CCA client instance to affiliate to a disabled group. If the CCAS group manager entity (see clause 5.4.3) disables a group to which CCA client instances are affiliated, those CCA client instances shall be deaffiliated from the group and shall be notified that they are no longer affiliated to the group.

An authorized user (e.g. a dispatcher) may ask the CCAS to request a CCA client instance to change its affiliations. However, the CCA client instance may reject a CCAS request to change the CCA client instance's affiliations. The CCAS shall notify the requesting authorized user as to whether the CCA client instance accepted or rejected the proposed change. An authorized user may ask the CCAS to make a mandatory change to the CCA client instance's affiliations.

Group affiliation may be managed as a combined procedure with the service registration or as a separate procedure.

Certain groups may be provisioned as receive-only groups for an MU. The MU may not need to carry out an explicit affiliation procedure in order to affiliate to those groups. If the MU does carry out an explicit affiliation process, the response from the CCAS will indicate that the group is receive-only, and that the MU is not allowed to transmit to the group. Such groups may be used for such purposes as organization wide broadcast calls, area related broadcast calls and suchlike.

The CCAS may allow an MU to transmit an imminent peril or emergency call to a specific address to which it has not explicitly affiliated. This address will be known to the MU by configuration.

There shall be a default address (a system wide address), and all MUs shall be capable of receiving transmissions to this address.

The MU shall be provided with the CCA group reference (see clause 6.1.1) when it affiliates to the group. The preferred codec type for calls to the group is specified in the group profile. When the MU becomes affiliated to a group it is subscribed to receive SIP MESSAGEs informing the MU of the bearer frequencies and TMGIs of relevant E-MBMS announcement broadcasts available to the MU (see clause 7.4.0.4).

Encryption keys for group communications may be provided during group affiliation. The method by which the encryption keys are provided is outside the scope of the present document.

The CCAS may change the group affiliations of an MU by the CCAS initiated procedure, both to affiliate the MU to further groups and to de-affiliate the MU from any previously affiliated groups. The CCAS may make the changes in response to movement of the MU to different geographic areas.

NOTE 1: There is no theoretical limitation to the number of groups to which a MU may simultaneously belong and thus no limitation of the number of simultaneous group calls that a MU may simultaneously be part of. Therefore, scanning is provided natively and does not require any specific protocol (although the CCAS may prioritize the media flows and restrict the number of media flows sent simultaneously to the same MU). Any such restriction may be made with knowledge of the capabilities of the terminal.

NOTE 2: The capabilities of the MU may be changed by configuration, either locally (including by the addition or removal of accessories) or by over-the-air provision of configuration parameters stored in the CCAS. See clause 7.11.13. The means for locally changing the configuration of the MU are outside the scope of the present document (but see clause 9.7).

NOTE 3: The MU may affiliate to, or be affiliated to, groups owned by non-home CCASs or groups owned by CCASs to which the MU is not currently registered. The affiliation is conducted via the CCAS to which the MU is currently registered. However, the CCAS to CCAS interface is not part of the present document.

When the MU wishes to not participate in further communications within a group, it shall perform a de-affiliation procedure. This is achieved by a SIP procedure.

The codec type is communicated to the CCA client during group affiliation.

7.4.4.1 Relation between group affiliation and mobility

When the geographic location (reported, for example, by the signalling channel heartbeats) indicates that the MU has moved outside a designated coverage area for a group (see clause 7.4.2), for example due to a change of jurisdiction, the network may modify or suspend the group affiliations of the mobile unit. This may be considered as a special case of CCAS initiated group affiliation triggered by MU location reporting.

When the MU migrates to a visited CCAS (see clause 7.2.2), it may be provided with a supplementary configuration providing membership of groups that are locally defined in that visited CCAS in order to be able to interwork with other local MUs. Registering with the visited CCAS causes all the MUs existing group affiliations to be cancelled, so the MU has to affiliate to all its groups on the new CCAS. An MU may also be permitted to affiliate to a group that is home in a different CCAS, even while the MU is registered in its home CCAS.

7.4.4a Group selection

The selected group is the group to which the MU will request a call if the user attempts to transmit when the MU is not in a call. The action of "selecting" a group will cause a change in state at the MU, as the MU will know that pressing the PTT switch when the MU is not in a call should result in a request to transmit to the selected group in a new call. An MU may affiliate to multiple groups, but shall only have one selected group for each media type (e.g. voice, video, data) at one time. A user may select different groups on different MUs.

The MU is not necessarily permitted to select all groups to which it is affiliated. Each group profile specifies which group members are permitted to select the group. In addition, the MU is not permitted to select a disabled group. The MU may be required to notify the CCAS when the MU changes the selected group.

An authorized user (e.g. a dispatcher) may ask the CCAS's control server to send an MU a request to change its selected group. The control server then sends a SIP notification message to request the MU to change its selected group. The MU may accept or reject the requested change. The MU shall inform the control server as to whether or not the MU accepted the proposed change and the control server shall then inform the authorized user about the result of the request.

7.4.5 Session join and call start

A group session is joined by an exchange of SIP signalling between MU and CCAS. Once an MU has joined a session, only media control protocol signalling (see annex B) is required to perform call transactions.

An MU may join more than one session within the same group in order to send or receive different media types within that group. Separate media control state machines are used for each session, such that transmission control is independent for different media types.

If a session join is combined with the affiliation process, calls may be started using media control protocol signalling, providing an "open session" (or "chat model") call service. In this case the session remains open until explicitly cleared by further SIP signalling. Alternatively, the session join may be combined with the call setup process, and ended at the end of call, providing more of a "discrete call" service where a call and a session are coincident. A parameter in the SIP/SDP signalling which joins the session may indicate whether an MU is requesting to set up a call at the same time as joining a session.

The open session call service should normally be used for group calls. However, the discrete call service shall be used for acknowledged group calls and emergency calls except as described in clause 7.4.8.

A call set up request may be rejected by the CCAS, either when made with a request to join a session, or when a session is already joined. If a request is rejected together with a session join, a SIP 4xx rejection response may be sent. If the session is already joined, an "MCP D-Reject" may be sent. The reason codes may include "not authorized" if the MU is not authorized to send calls to the group (or the group is receive-only) and "no other group members" if the MU is the only participant currently affiliated to the group. The rejection may also indicate reasons such as capacity limitations. A call set up request shall be rejected by the CCAS with the reason "disabled group" if the requested group has been disabled (see clause 5.4.3) by the CCAS.

A call setup request using either SIP signalling or media control signalling may include parameters with which the calling party wishes to determine the characteristics of the call, such as call priority (see clause 7.7) or selected area (e.g. local/wide area - see clause 7.11.10).

The CCAS may provide the transmitting MU's CCA individual identity and/or associated displayable names and, if available, the transmitting user's CCA server identity to all receiving MUs, so that the receiving MUs may display this information to their users.

When the MU receives a group call it may generate an audible or visible notification to the user. However the user's profile (see clause 9.2) may contain information that causes the MU to enable or disable the generation of user notifications for incoming group calls that are not imminent peril or emergency calls.

At the end of a call, the CCAS may decide whether to continue or end the session. The CCAS may decide to maintain a session for a period, considered to be a "session hang time" following completion of a call, but may then decide to end the session if no further calls take place by the end of the session hang time.

NOTE: The CCAS determines the lifetime of a session and when the session starts and ends. A new session may be started when a new call is set up, or the CCAS may decide to maintain one session permanently for one group (or for one media type within one group, etc.) and simply join MUs to that session either at affiliation time or at the start of a call.

7.4.6 Late entry

The late entry function allows the setup of a group call to a called party when the initial setup message has been missed, for various reasons such as radio conditions, mobility or late affiliation to the corresponding group.

The late entry function is implemented through appropriate repetition of the corresponding call set up message, triggered by the relevant events. The location of the current talking party may be sent to late entrants (depending on privacy requirements).

7.4.7 Message exchanges related to group call

7.4.7.1 Group subscription and affiliation

Group subscription and affiliation are achieved by exchange of SIP messages. The MU achieves subscription by sending a SIP SUBSCRIBE in order to express an interest in a group and to receive relevant events relating to the group's operating state, according to a defined event package. The MU may subscribe to an individual group, or send separate SUBSCRIBEs to several groups individually. The MU may also send a SUBSCRIBE containing a list of groups in order to be subscribed to several groups at the same time.

The SUBSCRIBE message will indicate whether the subscription is also a request for affiliation, i.e. whether the MU is requesting to join sessions automatically when calls are set up and to receive or send media in those calls, or to simply receive events related to the group without joining sessions and receiving media streams.

The CCAS will respond to the SUBSCRIBE with a NOTIFY response, which is used to inform the MU about relevant parameters for the group, and may include parameters such as media characteristics. If the MU subscribes to a list of groups, the NOTIFY response from the CCAS may indicate the list of groups to which the MU is affiliated; this list may omit groups requested by the MU if the affiliation is refused, and may include additional groups if the CCAS wishes to affiliate the MU to further groups that were not requested by the MU.

The MU may change its subscriptions to groups at any time by sending new SUBSCRIBE message(s). If a list of groups is used, the MU shall send the complete list of groups to which it now wishes to subscribe, and will receive a complete list back from the CCAS which indicates to which groups it has successfully subscribed.

The SUBSCRIBE may be omitted if the MU also joins a session at affiliation time. However in this case, the MU will not be notified of events relating to the group, unless it also sends a SUBSCRIBE to the CCAS.

The subscription to the group allows the MU to receive notification of relevant events within the group which are both non-call related (e.g. relating to affiliations of other users) or call related (e.g. relating to current affiliation to a group within a call). An authorized user may request and receive information about the affiliations of other users using either an HTTP GET request (see IETF RFC 7230 [22]) or a SIP SUBSCRIBE message.

Subscription and affiliation is shown in figure 19.

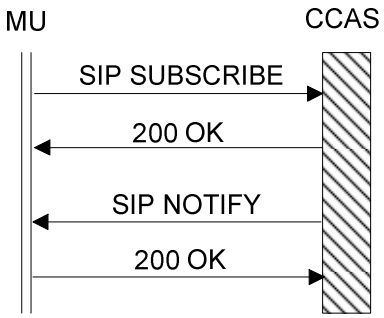


Figure 19: Message sequence chart for subscription and affiliation

7.4.7.2 Joining a session

To join a session, a SIP INVITE is sent. This may be subsequent to the subscription described in clause 7.4.7.1. The INVITE may be sent by MU or CCAS depending on the scenario.

If the MU has not affiliated by use of a SIP SUBSCRIBE, the SIP INVITE will cause the CCAS to affiliate the MU to the group for the duration of this session. The MU shall send a SUBSCRIBE if it also wishes to be notified about events in the group.

The sequence of messages for session join following affiliation using the SUBSCRIBE process is shown in figure 20.

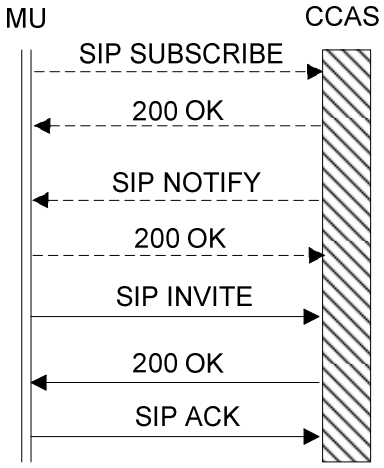


Figure 20: Message sequence chart for joining a session

Note that the optional SUSCRIBE and corresponding NOTIFY may also be sent following the INVITE, instead of prior to it as illustrated here.

The CCAS may also join the MU to the session, for example if the MU has already performed a SUBSCRIBE to the group in order to affiliate. This may be done at the start of the call, or in advance of the start of a call. If the MU has not previously used the SUBSCRIBE mechanism to affiliate to the group, the CCAS initiated session join shall also make the MU consider itself to be affiliated to the group for the duration of the session. Note that in this latter case, the MU will not receive events related to the group unless it also subscribes to the group.

The sequence of messages is shown in figure 21.

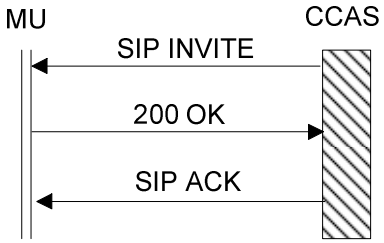


Figure 21: Message sequence chart for infrastructure initiated session join

Session join requires two way signalling. A unicast bearer (previously established at registration) is used between the CCAS and the MU in order to carry this signalling. However if the CCAS has directed the MU to a multicast bearer with the objective of receiving calls and call related signalling, the CCAS may start a call and include MUs receiving on this bearer without explicitly joining the MU to the session. In this case, the MU may consider itself to be temporarily attached to the session. Note that each MU still has a separate non-GBR bearer for mobility and other individual signalling functions, and therefore a path does exist for any further signalling that the MU needs to send outside the call.

7.4.7.3 Non-acknowledged group communication

7.4.7.3.0 Call setup sequence for group communication

The call setup sequence for normal group communication is similar to unit to unit call with direct signalling as the called parties do not answer to the call setup message but proceed immediately to a reception state.

NOTE: As the called parties belong to the same group as the caller, it is assumed that they have negotiated compatible capabilities at group affiliation time, so that there is no need for any negotiation that could impair setup time due potentially unlimited number of affiliated group members.

7.4.7.3.1 Group call combined with session join

If the affiliated group members are not currently included in a session for that group, the calling party sends a SIP INVITE to join a session for the group, which includes a parameter indicating that the SIP INVITE also is a request to set up a call, and to request transmit permission. Where the CCAS uses unicast downlinks, the CCAS will send corresponding SIP INVITEs to called group members to join them to the session to allow reception of the call. The final SIP 200 OK from the CCAS to the MU may give the calling MU transmit permission. A following explicit Media Control Protocol message (MCP D-TX Granted) shall be sent to the MU if the transmit permission is not included in the final 200 OK from the CCAS to the MU. Once the calling MU has received transmit permission, it starts to send media. Reception of this media causes receiving parties to unmute and play the media stream to their users.

The message exchange where receiving parties use unicast bearers is shown in figure 22.

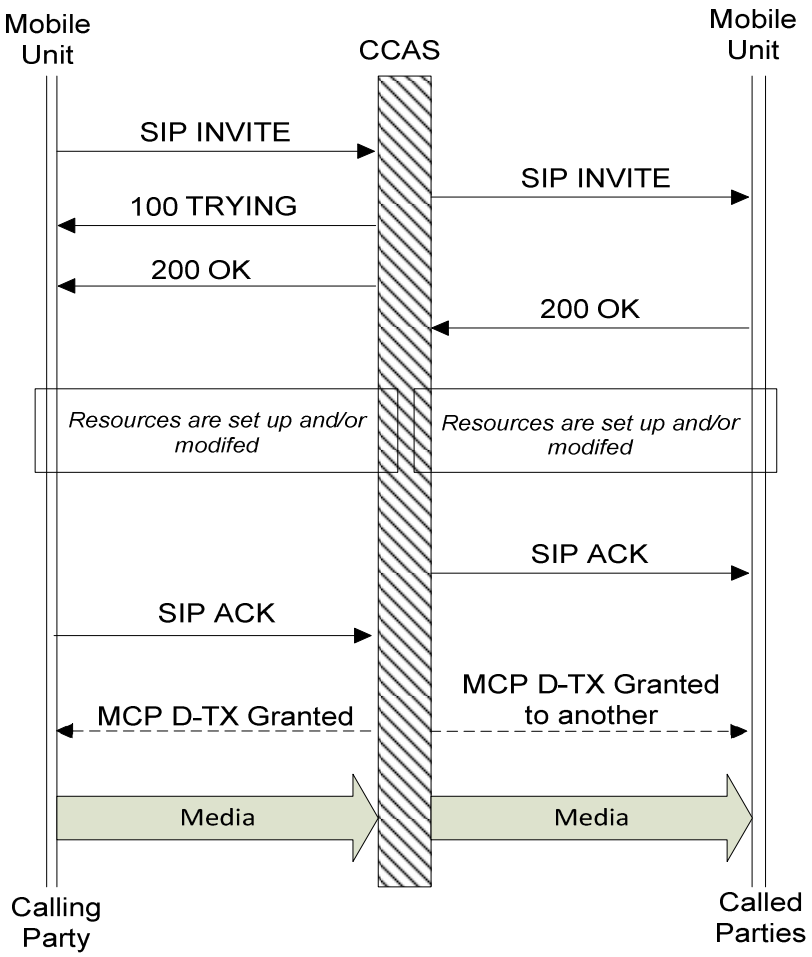


Figure 22: Non-acknowledged group call setup including session join, using unicast bearers

The message exchange where receiving parties use multicast bearers is shown in figure 23. The "MCP D-TX Granted to another" message will contain the parameters relating to the media type (e.g. codec type and rate, etc.). An MU that receives the start of the call on a multicast bearer will not join the session at this time, but will join the session if it moves from the multicast to a unicast bearer (e.g. due to movement outside the coverage area of a multicast bearer).

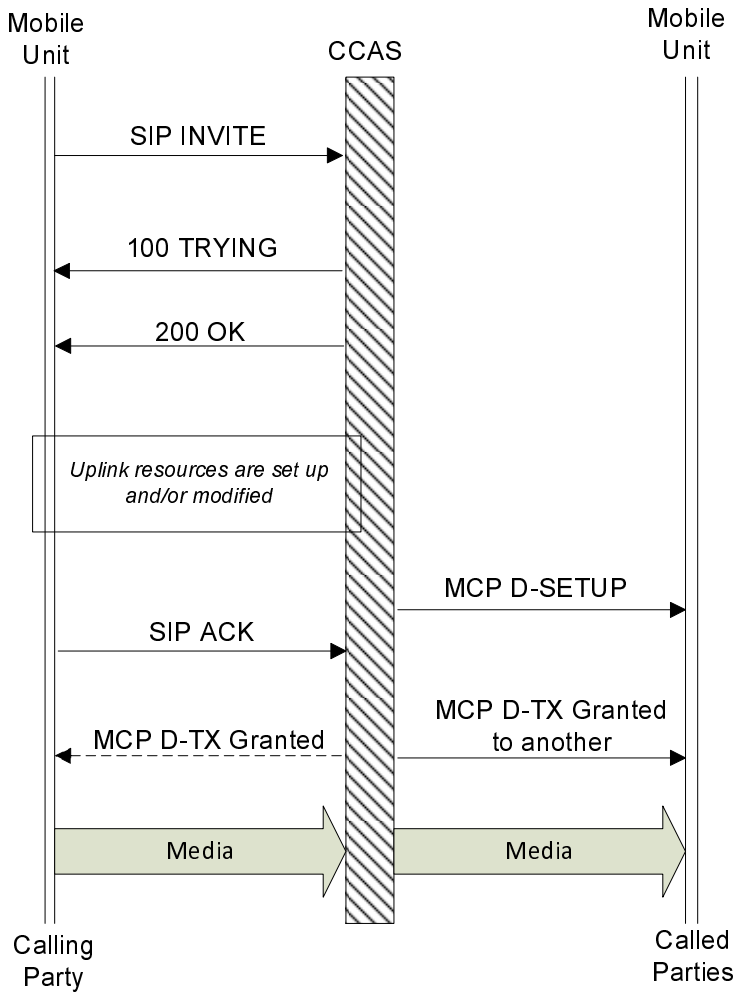


Figure 23: Non-acknowledged group call setup with multicast bearer for receiving parties

If the calling party's request to place the call is rejected, the CCAS will send a 4xx (client error) message to the calling party instead of the 200 OK message; alternatively if the call is rejected or cleared by the CCAS following the 200 OK, but before the optional "MCP D-TX Granted" message has been sent, a SIP BYE can be sent by the CCAS to clear the call. If the "MCP D-TX Granted" has been sent, but the CCAS then requires to terminate the call, an MCP message removing transmit permission shall be sent prior to sending the SIP BYE.

If the MU moves from a multicast to a unicast bearer whilst the call is continuing, for example due to a change in location that causes the MU to move outside the coverage area of the multicast bearer, the MU shall send a SIP INVITE to the CCAS to join the session and to restore the call. If the CCAS decides to withdraw the multicast bearer serving the MU, the CCAS may initiate the move to a unicast bearer, and to join the MU to the session by sending a SIP INVITE to the MU. If the MU moves from a unicast bearer to a multicast bearer during the call, the MU will consider itself to be still attached to the session; however the MU shall send a re-INVITE or UPDATE which removes the unicast media stream. If the MU should move back to a unicast bearer (having previous established a unicast bearer and then moved to a multicast bearer), the MU shall send a re-INVITE or UPDATE to re-establish the media session, or if the move was due to the CCAS withdrawing a multicast bearer, the CCAS shall send the re-INVITE or UPDATE to re-establish the media session. At the end of the session, the CCAS will release any sessions from MUs that have transferred from unicast to multicast bearers by sending a SIP BYE (individually) to those MUs.

If the CCAS is unable to start (or join MUs to) the session immediately, for example because of resource limitations, or because a critical group member is occupied in another call, and so needs to delay the call start, the CCAS may queue the call. In this case, the CCAS will complete the SIP signalling to set up the media paths, but will not provide the calling party with transmit permission in the 200 OK message. The CCAS may immediately send an "MCP D-Queued" message to the calling party to allow the user to be informed of the queued condition. Further "MCP D-Queued" messages may be sent to update the calling party of the status of the queue. When the queuing condition clears, "MCP D-TX Granted" signalling is sent to the calling party to allow the call to commence.

The CCAS may adopt various strategies in deciding whether to queue a call: it may decide to queue until one or more specific users is able to hear the call, and then proceed even if other users do not have available resources; it may decide to queue until all users can receive the call, or it may even decide not to queue a call and simply start the call with whichever MUs are able to receive the call.

The case for a queued call where called parties receive the call using unicast bearers is shown in figure 24.

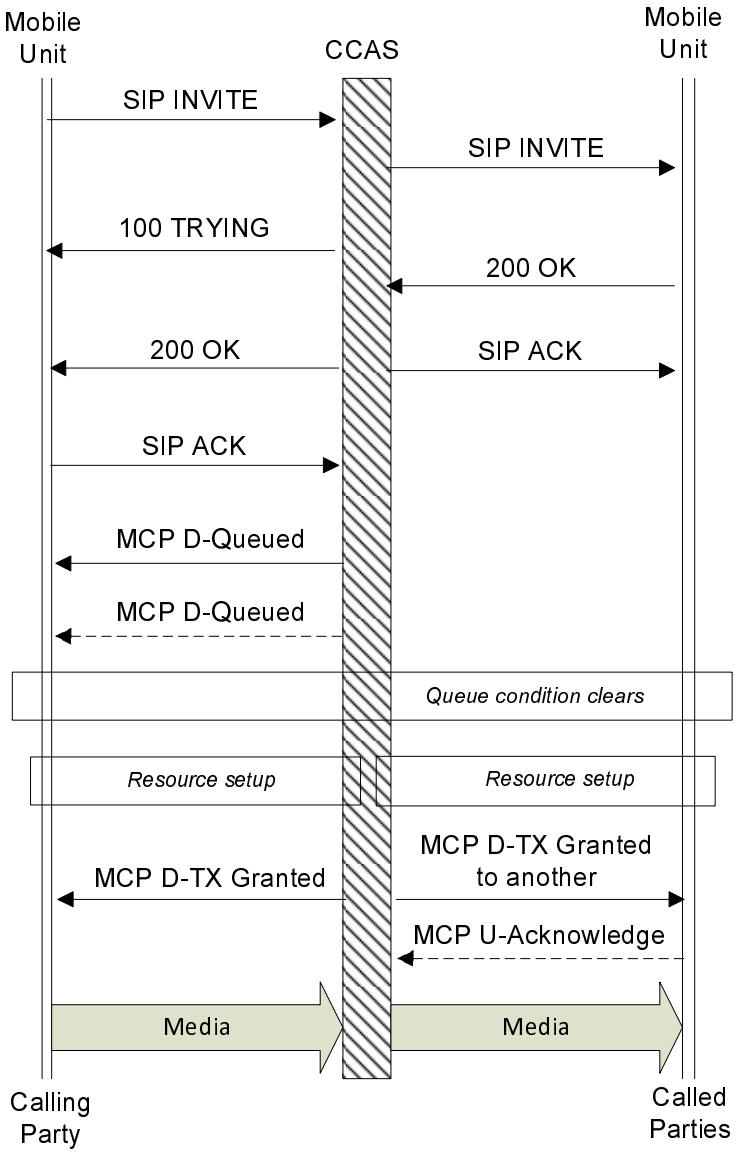


Figure 24: Non-acknowledged group call at session join time with call queuing

The case where called parties make use of a multicast bearer is similar, i.e. the called parties are signalled with the appropriate MCP signalling at the start of the call once the queue condition has cleared.

If a second party attempts to set up a call whilst the calling party is queued, the CCAS will reject the second caller, unless it is of a higher priority. In that case, the original calling party may be rejected, and the new calling party placed in a queue instead (depending on the relative priority to other ongoing communications).

In the event of a collision between two parties, i.e. both parties attempt to set up a call at the same time, the CCAS will arbitrate and decide which call to grant. The unsuccessful party may receive a 4xx rejection message, which will be followed by the INVITE which brings that party as a receiving party into the call; alternatively the CCAS may still complete the session setup for the unsuccessful party, but will indicate that transmit permission has been granted to another user.

7.4.7.3.2 Group call in pre-joined session

If the MU has already joined the session at group affiliation time, the SIP signalling has completed with the session establishment phase. Media Control Protocol is used by the calling party to request resources for transmission, to grant transmission to the calling party and to inform the called parties of the commencement of the call. The calling party sends an "MCP U-TX Demand", which identifies the target group; the CCAS responds with an "MCP D-TX granted" message to grant the call and provide transmit permission. The called parties receive an "MCP D-TX granted to another" message which informs them of the start of the call, and the identifier of the transmitting party; receiving parties may send an application level response if requested within the "TX granted to another" message. The CCAS may delay the transmission of the "MCP D-TX Granted" message to the calling party until after one or more acknowledgements have been received, in order to generate a simple acknowledged group call service, but a service which does not provide information to the calling party concerning which parties have responded.

If the talking party is denied permission to transmit, an "MCP D-Reject" message is sent. In the event of a collision, this may be followed by an "MCP D-Granted to another" message indicating the granted talking user.

At the end of transmission, the talking party sends an "MCP U-Release" message. The CCAS will send "MCP D-TX ceased" messages to receiving parties.

The MCP signalling is the same whether the receiving MU receives the call on a unicast or multicast bearer. If the MU moves between bearer types (where the move may be either initiated by the MU or the CCAS) there is no change to the SIP session.

The message sequence is shown in figure 25.

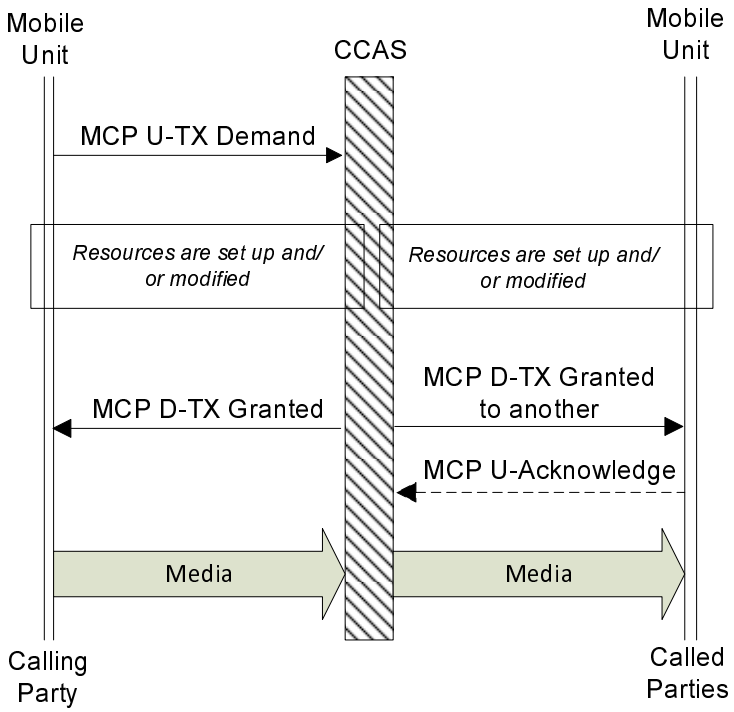


Figure 25: Non-acknowledged group call setup with pre-joined session

In the event of a call queued situation, for example because of resource limitations, or because a critical group member is occupied in another call, media control protocol is used to indicate the queued state to the calling party. One or more "MCP D-Queued" messages may be sent, to provide an updated status of the call queue. The CCAS strategy in deciding when to queue a call may depend on the availability of certain specific users as described in clause 7.4.7.3.1. The process is shown in figure 26.

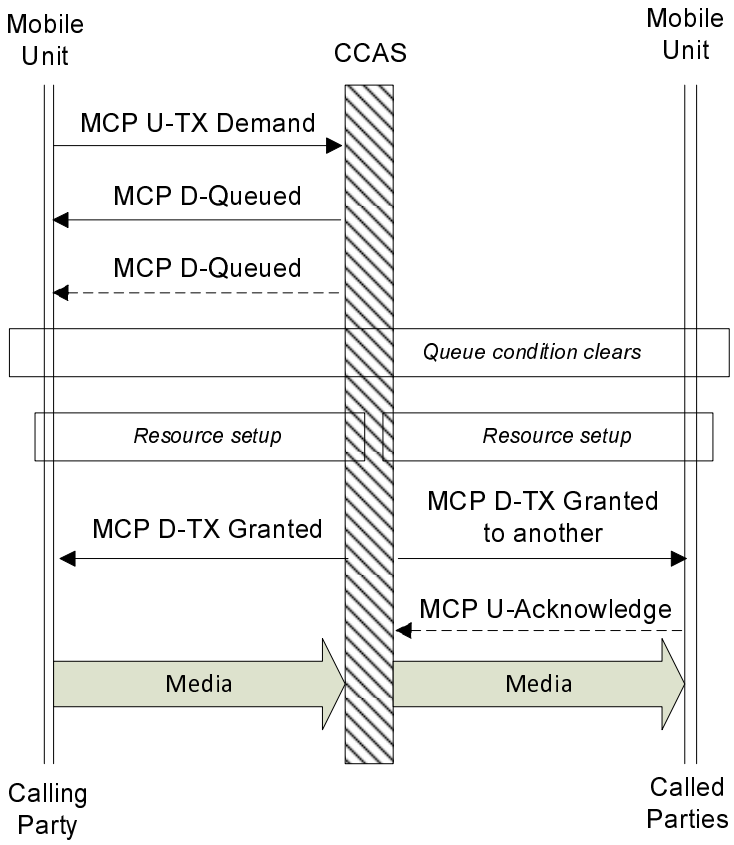


Figure 26: Non-acknowledged queued group call setup pre-joined session

A second party attempting to set up a call whilst the calling party is queued may be rejected by the CCAS using media control signalling, unless the call request is of a higher priority. In that case, the original calling party may be rejected, and the new calling party placed in a queue instead (depending on the relative priority to other ongoing communications). Alternatively, the unsuccessful party may simply be sent into the call using media control signalling, with the other party's identity given in the "MCP D-TX Granted" message.

7.4.7.4 Acknowledged or ringing group communication

The purpose of the acknowledged or confirmed group call is to provide to the calling party information that a number of called parties or specific called parties will be available to receive the call. Several options may be offered depending on network operator requirements.

There can be different strategies for confirmation, which may be based on the number of mobile units which have affiliated to the group and are still reachable, or on the number of mobile units which have explicitly acknowledged the call, or the acknowledgement of a predefined subset of mobile units. In this later case, the message sequence for the set up of the group call is a mix of the acknowledged group call set up (see figure 27) for the mobile units whose acknowledgement is required, and of the non-acknowledged group call set up (see figure 22) for the other mobile units participating in the group call.

Optionally, the acknowledgement may be triggered by a ringing and on/off hook signalling for the mobile units whose acknowledgements are required, to ensure that the users are consciously alerted and are required to respond before joining the call. Confirmation may not be provided to the calling party until this response has been sent.

Acknowledged or ringing group calls may also be imminent peril or emergency calls, i.e. such calls set up with an imminent peril or emergency priority requested.

The acknowledged call service where information on called parties' responses is sent to the calling party can only be achieved where session join takes place at the same time as the call is started. Note however that a simple acknowledged service is possible, where feedback on users' responses is not provided to the calling party, if the session is joined at affiliation time.

The message sequence chart shows the addition of information messages to the calling party to provide information on the progress and/or final result of the polling. The 183 SESSION PROGRESS message is used until the CCAS decides that the responses have been sufficient to allow the call to proceed. Further SIP INFO messages may be sent following the grant of the call.

The message sequence for calling party and for parties who are requested to acknowledge is given in figure 27. The message exchange requesting and providing acknowledgement will be carried over a unicast bearer. However the final "MCP D-TX Granted to another" message and the following media may still be sent over a multicast bearer to acknowledging MUs who have a multicast bearer available.

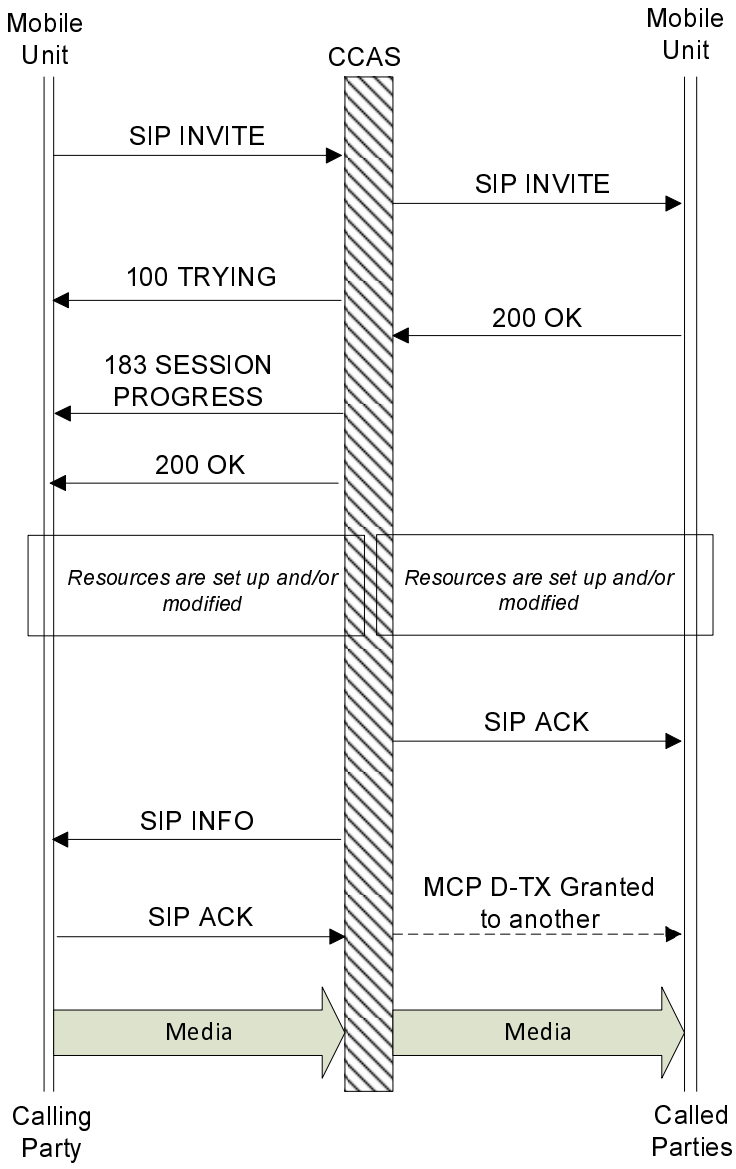


Figure 27: Acknowledged group call setup with session join

NOTE 1: The actual timing between the 200 OK from the called MUs messages and the 200 OK sent from the CCAS to the calling MU is flexible to accommodate with the different confirmation modes (all, some, pre-defined subset of mobile units) and the case illustrated in figure 27 is purely illustrative. Moreover, nothing precludes the sending of several information messages to the calling party for size and/or incremental update reasons.

The message sequence for a receiving MU that takes part in a call where the calling party requires acknowledgement, but where that particular receiving MU is not one of those from whom acknowledgement is demanded follows that for the unacknowledged case. An MU who is required to acknowledge may therefore receive both an MCP "Setup" message over a multicast bearer, addressed to the group, and an individually addressed SIP INVITE message on a unicast bearer.

NOTE 2: To avoid an uplink load caused by unnecessary acknowledgements from MUs whose acknowledgements is not required by the CCAS, the "MCP D-TX-Granted-to-another" message should not include an acknowledgement request when sent over a multicast bearer.

In the event of a need to queue the call before its completion, the process follows that for the unacknowledged group call. The calling party is informed of the queue, and the called parties are not informed about the call until the queue condition clears.

The MU may move to a multicast bearer when the media flow starts, or during the call. If so, the SIP session shall be modified to remove media by following the processes for unacknowledged group call with session join described in clause 7.4.7.3.1. The procedures described in clause 7.4.7.3.1 shall also be followed if the MU moves between multicast and unicast bearers during the call.

7.4.7.5 Bearer control

In all types of call, the CCAS will assign appropriate bearers (unicast and/or multicast) to carry the media and media related signalling within the call as part of the call setup process. The process is outside the scope of the present document. Note that the CCAS may have a little more time available when acknowledgement is required due to the additional time needed to poll and receive responses from affiliated group members.

NOTE: If a 3GPP specified IMS is in use, there still may be practical limitations in the speed of bearer set up particularly if the group has a large number of members making use of unicast bearers. In any case, the CCAS may need to delay the "TX granted" messages until bearers are in place.

7.4.8 Conversion of an ongoing group call into an emergency group call

If the CCAS receives an emergency-level call request from a call participant during an ongoing open session group call, the CCAS may decide to provide discrete call sessions and emergency priority only to the talking party and specific nominated parties who may be required to acknowledge. These selected users may need to have their bearers changed, possibly to unicast bearers.

NOTE: This is to minimize the load on resources.

7.5 Push-to-talk management procedures

7.5.0 General

The infrastructure controls the management of the transmission rights and implements PTT management procedures as detailed in the following clauses.

NOTE: The following clauses apply both to individual and group streaming communications.

7.5.1 Initial allocation of right to transmit

The initial allocation of the right to transmit is defined by default behaviour according to the type of communication. However this behaviour may be overridden by the CCAS if it needs to modify the service.

In a half-duplex call by default, the called party of an individual call with on/off hook signalling should be given transmit permission when the call is completed. However, the right to transmit is given by default to the calling party in the cases of group call or individual call with direct signalling. In a full-duplex call, both parties are able to transmit as soon as the call set up phase has been completed.

7.5.2 Releasing the right to transmit

When a MU which has been granted transmission wants to release the floor, it shall send an indication of this release (MCP U-TX Ceased) and immediately stop the transmission of any media traffic, including buffered media whenever possible.

The CCAS should inform all MUs involved in the call that the floor control has been released by sending outbound floor release messages (MCP D-TX Ceased). Further MUs may then request the right to transmit, and may be granted transmit permission by the CCAS (MCP D-TX Granted). In event of contention, the CCAS may decide which MU to allow transmit rights according to priority, or in accordance with the first request received. The "MCP D-Granted to another" message informs MUs who have not been granted transmit permission of which MU has been granted transmission rights.

If requests to transmit have been previously made and queued, the CCAS shall send a message to the designated MU (MCP D-TX Granted) indicating that it has been granted the right to transmit and shall send a message to the other MUs (MCP D-TX Granted to another) indicating that the right to transmit has been granted to another MU.

7.5.3 Requesting the right to transmit

The right to request the right to transmit may be denied to all MUs at call setup time for broadcast calls.

Otherwise, a MU in the call hang time, or in a receiving state of a streaming communication may at any time request the right to transmit (MCP U-TX demand) and shall indicate a priority level for the processing of the request. The CCAS shall respond to the MU by accepting or rejecting the MU's request to transmit, or by indicating to the MU the place of its request to transmit in a queue of requests. The MU may send subsequent messages to the CCAS requesting the present position of its transmit request in the queue. The MU may send the CCAS a request to remove the MU's transmission request from the queue and the CCAS shall acknowledge the request. The CCAS may also remove the MU's transmit request (e.g. on expiration of a timer) and should notify the MU when this happens. It shall be configurable within the CCAS as to for how many transmission grants to other MUs an MU's transmit request may remain in the queue, with a minimum value of 0.

7.5.4 Interrupting a granted transmission

If an MU requests transmit permission whilst receiving media sourced from another user, but the priority level does not lead to an immediate allocation (pre-emption) and when the currently granted party has not released the floor, the request may be rejected or queued and the requesting party shall be notified of the status of its request.

If the requesting MU is rejected, figure 28 shows the sequence of messages.

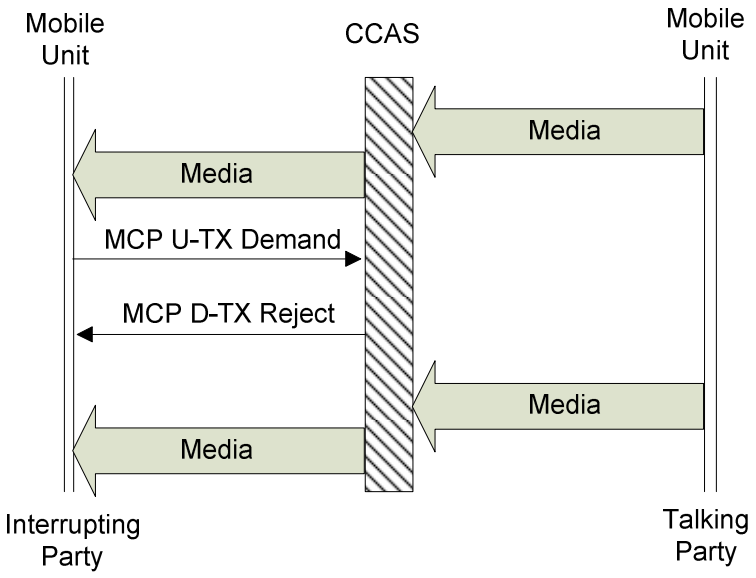


Figure 28: Rejection of talking party interruption

If a pre-emption request is made but the request is queued by the CCAS without interrupting the currently transmitting MU, when the floor is released the granted party receives a positive acknowledgement of its request with the right to transmit and the other parties are notified of the fact that another party has been granted the right to transmit (MCP D-TX granted). See figure 29.

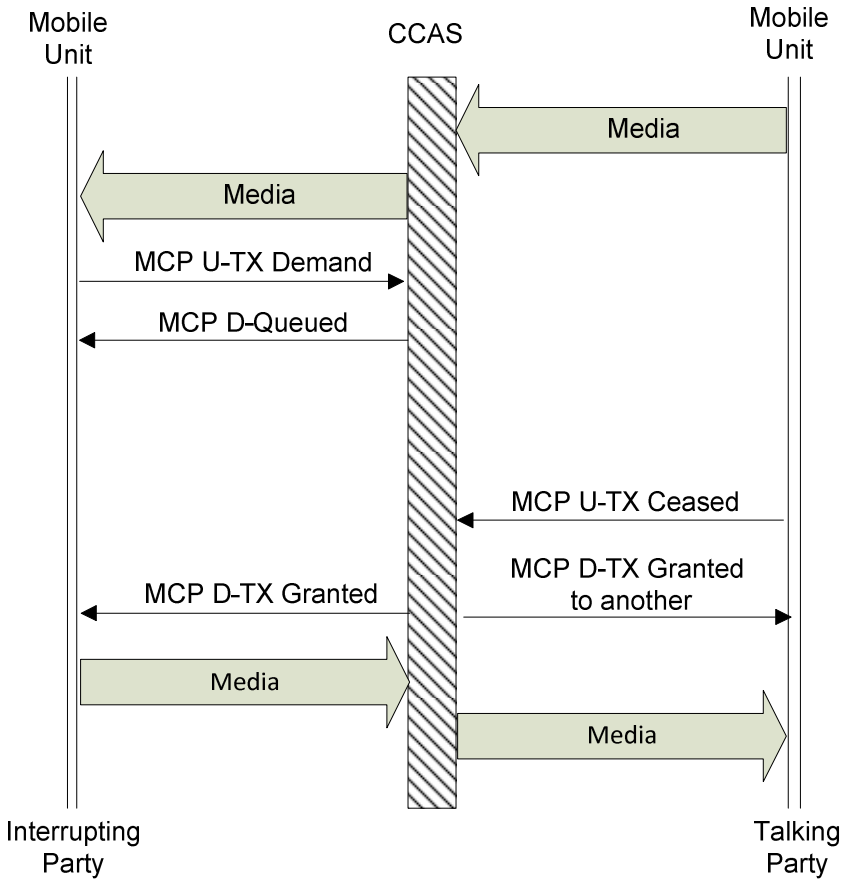


Figure 29: Processing of a request to transmit without pre-emption

If a request to transmit is made which is considered having a higher priority than the currently granted transmission, the CCAS should stop the transmission of the currently granted MU and grant the right to transmit to the requesting MU. This is accomplished by sending a message to the transmitting MU to stop transmission (MCP D-TX Interrupt). The infrastructure may then send a message (MCP D-TX Ceased) to the interested parties to inform them about the interruption before sending a further message indication the granting of the right to transmit to the interrupting party (MCP D-TX Granted). Note that due to latency in the system, the interrupting party may still receive media sourced from the currently transmitting party even after the interrupting "MCP D-TX Demand" has been sent. See figure 30.

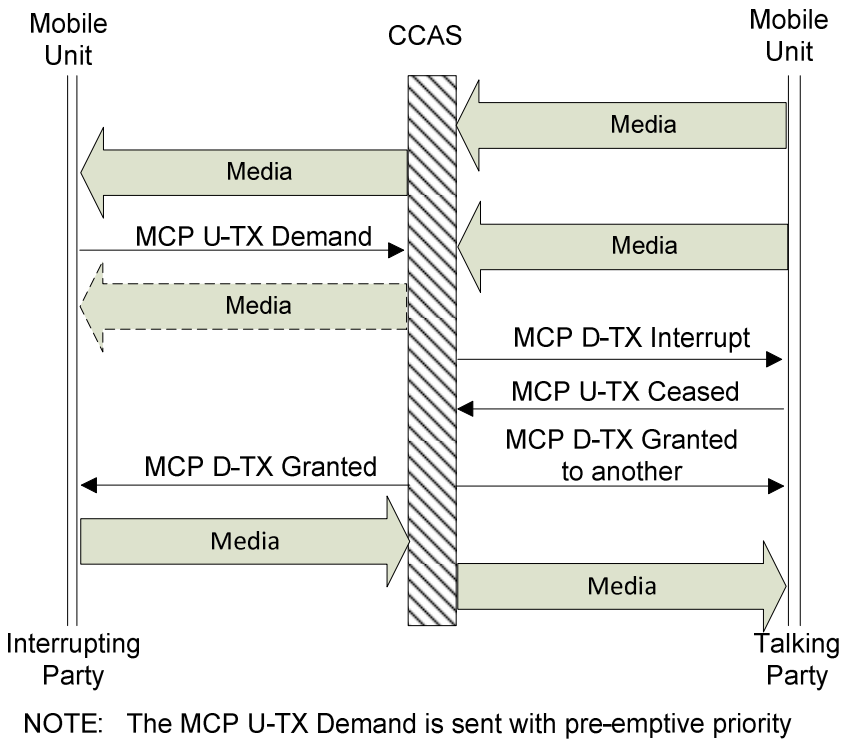


Figure 30: Stopping a granted transmission

However, in some specific cases, the pre-emption of the media flow shall apply only to the outbound media and the inbound media shall continue to be transmitted, for example, to be recorded in emergency situations. In that case, the interruption message shall indicate to the currently granted MU that the interruption does not apply to its current inbound transmission and that it may continue transmission over an independent call leg until transmission right is released using the corresponding release message (MCP D-TX Ceased).

7.5.5 Suspending a transmission

The CCAS may decide to temporarily suspend the call by removing transmit permission from the talking party using the "MCP D-TX Interrupt" message without granting transmission rights to another user. This may be adopted if some critical resource or user (e.g. a dispatcher) becomes unavailable, or if the talking party is served by a cell which exceeds its capacity limit.

Similarly, the media flow to a receiving user may be suspended if the user is served by a cell which exceeds its capacity limit. If the user was defined as critical for that call (or the call was an individual call), the transmitting party may have transmit permission withdrawn until the critical user is able to receive media once more.

The maximum time for which an MU is permitted to transmit may be configured in the CCAS service parameters (see clause 9.6.1) by an authorized administrator. An advanced warning time limit may be configured in the user's profile (see clause 9.2) by an authorized administrator. These items need to be copied into the MU. When the advanced warning time (if any) is reached, the MU may issue a warning message to its user. When the transmission time limit (if any) is reached the MU shall cease transmission. If the MU does not cease transmission at that time, the CCAS shall send the MU an "MCP D-TX Interrupt" message.

7.5.6 End of call

Following the last transmission, after the end of an appropriate timer, the call will be ended. The call may also be ended by the CCAS if the overall call time exceeds maximum permitted group call duration (see clause 9.4.3) or the CCAS's maximum permitted individual call or emergency call duration (see clause 9.6.2). The CCAS shall end the call and the session immediately if the CCAS disables the group (see clause 5.4.3) and should notify the MU when this happens. Provisioned values of timers for call ending (whether following the last transmission or because of call length considerations) may be different for different call priority types. The CCAS may provide an indication to the call participants when the call is within a configurable time of the call limit timer. The CCAS may end the call if the last or second-to-last participating MU removes itself from the call or if less than a minimum number of group members is present in the call.

NOTE 1: Where a call spans multiple CCASs with different maximum permitted call durations, the call may be ended when the first call timer expires.

If the session is to be ended at the end of the call, a SIP BYE is sent by the CCAS to return the MUs to the idle state. If an authorized MU (or dispatcher) wishes to end the call and session prior to expiry of a timer, it may transmit a SIP BYE to the CCAS which includes a parameter requesting the end of the call.

If the session is not to be ended at the end of the call, MUs may return to an idle state following expiry of a timer within the MU following the last "MCP D-TX ceased" message received. Alternatively, an "MCP D-Clear" message may be sent by a CCAS to explicitly end the call. An authorized MU may send an "MCP U-Clear" message to the CCAS if it wishes to end the call prior to expiry of the timer. If the MU wishes to leave the call without ending the call for other users, the MU should send an "MCP U-Leave" message to the CCAS (this could still cause the call to end if the MU's departure results in less than the minimum number of group members remaining in the call).

If the group was in an imminent peril or emergency state, the MU (or dispatcher) may make a request to clear the imminent peril or emergency state of the group, and further calls within the group are returned to being normal calls. The CCAS may reject such a request if the MU does not have authority to request this.

An MU may withdraw itself from a call whilst the call continues. If the MU also wants to end its session, a SIP BYE is sent to the CCAS. If the MU does not want to end its session, an "MCP U-Clear" message can be sent. In both cases, a parameter in the message is used to indicate that the MU intends only to withdraw itself, and not end the call for other users.

NOTE 2: The definition of an authorized user who is able to end the call and/or session is outside the scope of the present document. It could be a user with specific privileges, or could be related to users participating in the call, for example only the user that initiates the call could be authorized, or any user participating in the call could be authorized.

NOTE 3: In some narrowband PMR/LMR technologies, one or more "call owners" who are authorized to end the call can be defined, and may also the person who initiates the call. The present document does not consider a group call initiator to be a call "owner" but the call initiator may be one of those authorized to end a call.

In certain circumstances, for example emergency conditions, the CCAS may suspend the end of a call (e.g. set the timer to infinity).

7.6 Call modification

A call may be modified at setup or whilst it is continuing. Call modifications include:

- Half-duplex to full-duplex and vice versa (individual calls only).
- Direct to hook signalling and vice versa (individual calls only).
- Group to individual (e.g. call diversion when out of area).
- Change in the priority of the call.

Where the media characteristics of an individual call are to be modified (e.g. a call changing from half-duplex to full-duplex or vice versa), a re-INVITE may be used, conveying the new characteristics in the SDP descriptors.

Where the type of call is modified, the CCAS may reject a call setup request, and instead set up the required type of call (either using SIP signalling or MCP signalling as required) with transmit permission granted to the appropriate party. Alternatively the CCAS may simply complete the call, but modify the parameters of the call in the call completion signalling; or may modify parameters in the session related signalling if the session is joined at the same time as the call is started.

The target address of a call may also be translated to another address by the CCAS according to a local policy. In this case, the calling party may request a call to a generic address; the CCAS will determine the actual address (URI) of the target of the call according to some rules concerning the condition of the calling party, for example its location. This allows services to be provided such as ensuring that an emergency call can always be sent to a local dispatcher, and functional addressing, where a caller places a call to an address associated to a role, and the CCAS transfers the call to the user(s) responsible for that role at that time.

7.7 Management of priority and pre-emption

7.7.0 General

The management of priority and pre-emption covers several aspects listed below. There are at least 8 possible priority levels for each type of priority.

7.7.1 Provisioned priority

Individual MUs and groups may each be provisioned with a relative priority level. The CCAS uses this provisioned priority to decide which calls to grant first and which calls to queue in the event of resource limitations. It may also be used to decide whether to pre-empt a user or a group when another user wishes to place a call of pre-emptive priority which includes a particular user or set of affiliated group members.

The CCAS may change the priority of an individual or group dynamically to react to user operational needs (e.g. during an imminent peril or emergency call). An authorized user may request the CCAS to change another user's priority for requesting calls.

If an MU is active in a call, and receives a setup indication for a call of pre-emptive priority, the MU shall release the ongoing call and join the pre-emptive priority call instead.

7.7.2 Setup priority

Each call set up request may include a priority value which can be determined either by the user or the application in the MU. This shall distinguish between at least:

- Normal calls.
- Broadcast calls (should have a higher priority than normal calls).
- Urgent calls.
- Imminent peril calls.
- Emergency calls.

Additionally, the setup request may indicate whether the call request is for a pre-emptive call or not.

Priority of setup request applies to both individually and group addressed calls.

The priority of a call in progress may be modified by the CCAS, for example to convert a normal call into an emergency call. This may be as a result of an action by a dispatcher.

If an imminent peril or emergency call is requested, the CCAS shall establish and maintain an imminent peril or emergency status until the imminent peril or emergency status is cancelled. While the imminent peril or emergency status is maintained, the CCAS shall record the identity of the call initiator and shall provide the identity and location of the call initiator to existing and late-entering call participants.

An MU receiving an imminent peril or emergency call setup may alert its user and present the media, even if the group was being scanned at a lower priority than the currently selected group. The CCAS may also include designated MUs and dispatchers in the call, affiliating them to the group if necessary. The CCAS may continue to give the group imminent peril or emergency priority even if following transmissions do not request imminent peril or emergency priority, until a specific action is taken by a dispatcher or administrator.

7.7.3 Push-to-talk priority

Each request for transmission using MCP includes a priority indication (with the same possibilities as the call setup priority). An authorized user may request the CCAS to change another user's priority for requesting permission to transmit. An imminent peril transmission request shall convert a non-emergency call into an imminent peril call. An emergency priority transmission request shall convert the call into an emergency call.

When prioritizing the transmit queue, the CCAS may assign higher priority to groups and users during hours of operation or while on duty if known.

During a (half-duplex) call, an authorized user may pre-empt the floor allocation of another user by setting the priority indication to "pre-emptive". The mechanism for interruption is described in clause 7.5.4.

7.7.4 Scanning priority

A MU may receive several calls simultaneously and shall be able to select the calls to be presented to the user application based on a predefined set of priorities. The affiliation messages will include a parameter which indicates the relative priority of a group (the class of usage) to the CCAS. An authorized user may change the order in which multiple simultaneous incoming group calls are presented to the user.

Calls with the emergency status shall have a pre-emptive priority over the other type of calls. Calls with the imminent peril status shall have a pre-emptive priority over calls other than emergency calls and system calls.

7.7.5 Resource allocation priority and resource retention

When queuing for resources, several queues may be organized for the different priorities and resources will be allocated based on relative priorities. However, a call with a non pre-emptive priority shall not lead to tear down of resources already allocated to another ongoing call.

Pre-emptive communication shall be able to tear down other communications in order to get access to the required resources.

If some affiliated group members become excluded from a call in progress due to loss of capacity, the CCAS may inform the calling/talking party and/or other affiliated group members by SIP NOTIFY or "MCP D-Info" signalling. Parties excluded from a call in progress for capacity reasons may also be notified of this. MUs that suffer call termination due to pre-emption may be given an appropriate reason code in call termination signalling.

7.7.6 Priority attributes requests

The CCA user may send the CCAS an HTTP request (see IETF RFC 7230 [22]) for information about the attributes being used by the control server to determine the priority of the user's call requests and transmissions. The CCAS may then send the user an HTTP response listing the user's priorities relevant to call requests and transmissions.

7.8 Status and messaging

7.8.0 Supported status and messaging types

The CCAS shall support both pre-defined status transmission and free format messaging. Both functions shall use the SIP MESSAGE facility [5], which will include an application dependent message body header within the message to identify status, pre-defined messages and free format messages, as well as other applications of messages (e.g. simple terminal control and management facilities).

Status is used to transmit a pre-defined message with a limited size to an MU, to a group of MUs or to a system address. There shall be status values whose meaning is predefined in the standard, and freely chosen values which can be defined by the application.

The transport of the status to the recipients is acknowledged by the recipient using a 200 OK message. However this merely indicates that the status has reached its destination, not that the receiving application has interpreted it (or presented it to a user). It is up to the application using the status(es) to create higher layer acknowledgement statuses as required.

7.8.1 Standard defined status

7.8.1.0 Pre-defined status

Some statuses have a predefined meaning and a mandatory processing as defined in the following clauses. Further definitions are possible.

7.8.1.1 Emergency status

The emergency status is sent to the CCAS by a MU upon action of the user to signal an emergency condition or upon action of the user to request emergency PTT priority. The emergency status is then sent by the CCAS to a pre-programmed set or group of MUs which usually includes one or several wire-line connected units for dispatchers. The sending user shall be notified when the emergency status message has been received by the CCAS. If an MU affiliates with a group that is already in an emergency condition, the CCAS shall send the MU an emergency status message.

When an MU receives an incoming emergency status message it shall generate an alert to its user. The type of alert (e.g. visible, audible, vibration) shall be defined in the user's profile (clause 9.2) and may also be defined in the device profile (clause 9.5.2). The user's profile also determines if the user is permitted to change the type of emergency alert on his MUs, and each MU's device profile determines if a user is permitted to change the MU's emergency alert type.

When the emergency status has been sent, the sending MU is considered in emergency and all communications that are setup by this MU or directed to this MU and the requests to transmit of this MU will be managed with an emergency priority.

The emergency status of the MU can be cleared by its own initiator and may be cleared by a designated authorized user.

7.8.1.2 Call alert

The call alert (or call back or request to speak) function allows the indication of a willingness to be called back at a later time without the need of trying a call which may fail. The call alerting message is routed to the "alerted" party and contains the address of the altering party in order to allow a simple call-back. No resource allocation is needed at any step of the processing of this feature. The alerted party shall record the time at which the call back request was received. Both the calling party and the called party may cancel the call back request. If the request is cancelled, both parties shall be notified.

7.8.1.3 Urgent call back

The urgent call back status provides the same facility as the call alert status, i.e. a desire to enter into a communication, but with an increased degree of urgency. The urgent call back status message shall indicate the level of urgency ("urgent" or "most urgent"). The alerted party shall record the time at which the call back request was received. Both the calling party and the called party may cancel the call back request.

7.8.1.4 Ambience listening call request

The ambience listening call request provides a similar function to the call alert request; except that the user desires the recipient (usually a dispatcher) to activate ambience listening on the user's terminal. The called party shall record the time at which the ambience listening call request was received. Both the calling party and the called party may cancel the call back request.

7.8.1.5 Ambience listening urgent call request

The ambience listening call request is similar to the ambience listening call request, but indicates an increase degree of urgency. The ambience listening urgent call request message shall indicate the level of urgency ("urgent" or "most urgent"). The alerted party shall record the time at which the request was received. Both the calling party and the called party may cancel the ambience listening urgent call request.

7.8.1.6 Scanning on and off

Scanning on and off status values may be used to indicate to the CCAS whether the MU wishes to be presented with calls from its list of scanned groups or no.

7.8.1.7 Transmit inhibit on and off

A user may select a transmit inhibit mode which restricts the transmissions made by an MU. The status indicates the current state of this function.

NOTE: It is for further study whether a transmit inhibit mode can prevent UE/terminal transmissions, or can only suppress CCA level messages.

7.8.1.8 Imminent peril status

The imminent peril status is sent by a MU upon action of the user to signal an imminent peril condition. The imminent peril status (including the identity of the initiator) is then sent to a pre-programmed set or group of MUs which usually includes one or several wire-line connected units for dispatchers. The sending user shall be notified when the imminent peril status message has been received by the CCAS. If an MU affiliates with a group that is already in an imminent peril condition, the CCAS shall send the MU the imminent peril status message.

When an MU receives an incoming imminent peril status message it shall generate an alert to its user. The type of alert (e.g. visible, audible, vibration) shall be defined in the user's profile (clause 9.2) and may also be defined in the device profile (clause 9.5.2). The user's profile also determines if the user is permitted to change the type of imminent peril alert on his MUs, and each MU's device profile determines if a user is permitted to change the MU's imminent peril alert type.

When the imminent peril status has been sent, the sending MU is considered in imminent peril and all communications that are setup by this MU or directed to this MU and the requests to transmit of this MU will be managed with an imminent peril priority.

The imminent peril status of the MU may be cleared by its own initiator or may be cleared by a designated authorized user.

7.8.2 Messaging

7.8.2.0 Message service

Messaging is a service that supports transfer of messages that are usually, but not required to be, short. Messages shall use either the 7-bit GSM default alphabet (see ETSI TS 100 900 [20]) or the UTF-8 character set (IETF RFC 3629 [21]). The messaging service is also known as the Short Data Service (SDS). The maximum size of a single message is defined by [5] as 1 300 bytes or less, and may be defined by system specific parameters. The CCA may employ application level chaining of several messages to achieve a greater overall message length.

The Messaging service supports transfer of messages between users, from a user to a group or from/to a user to/from a system functional entity such as e.g. a chat room.

Messages can be either acknowledged or non-acknowledged, the acknowledgement being end to end.

The Messaging service relies on SIP method MESSAGE described in [5]. The SIP MESSAGE method allows for two types of acknowledgement: one, SIP 200 OK, is end to end and means that the message has been delivered to the target user or entity; the other, SIP 202 Accepted, is a partial acknowledgment, in case the message goes through a message relay such as a Store & Forward server, and it confirms that the message has been correctly transmitted e.g. from a Mobile Unit to the infrastructure. In this later case, if end to end acknowledgement is required, it will be managed by the application on top of SIP. Status or other messaging functions may be used to create such an end to end acknowledged service. Parameters may be included in messages to indicate their eligibility for storing and forwarding, and any validity time for the storage.

NOTE 1: Presence (clause 7.9) and Messaging are building blocks that can be combined and used at the application level to provide further application features.

NOTE 2: One example of an application feature is "Callout", where a message is sent to one or more MUs which requires an acceptance or rejection response, and where the response may be sent in the form of a simple status or message. On acceptance, further messages may be sent, or group calls may be set up that include the accepting MU, in order to provide details of an incident to which the user is being called.

Messages may be linked to other services, for example may contain a hyperlink to a location where stored media can be retrieved.

7.8.2.1 Message broadcast

Messages may be sent to specific broadcast addresses, both defined organizationally and system wide. Broadcast messages may be intended for user consumption (i.e. may be human readable text), but also may be used for functions usable by the mobile application. When the CCAS receives a request for a message to be sent to a broadcast address, it shall send individual messages to the intended recipients.

7.9 Presence

Presence is a service that provides information about user availability (presence) to authorized users.

A Mobile Unit may publish the Presence status of its user(s) to the CCAS. Presence status includes an availability status and may include other metadata such as e.g. the group(s) the mobile unit is monitoring or a system functional entity the user is part of or interested in, like a chat room or an adhoc group.

Mobile Units can subscribe to the presence status of users of other Mobile Units, subject to adequate authorization controlled by the CCAS. Authorized subscribers are notified of the presence status of a target MU following successful subscription when a new status is published by that target MU.

The presence service relies on SIP methods SUBSCRIBE and NOTIFY described in [4] and on SIP method PUBLISH described in IETF RFC 3903 [6].

The CCA client instance's user profile determines whether the CCA client instance is permitted to view which CCA individual and function identities are registered on the CCAS and whether other users are permitted to view the state of this CCA client instance's registration.

7.10 Localization and geographic information

7.10.0 General

The MU shall be able to provide its geographic location when it is able to discover it, for example when in an outdoor location. The user and device profiles may permit the user or another authorized user to enforce or prevent transmission of location information.

The location information should be sent using encryption between the MU and the CCAS. The MU may be configured to send no location information unless such encryption is available. The CCAS's record of MU locations should be protected against unauthorized access.

7.10.1 Mode of transmission

The system shall support different modes of transmission of the geographic location information as listed below:

- Spontaneous transmission mode: in this mode, the MU spontaneously transmits its location information to the infrastructure. The transmission may be one-shot, periodic with a programmable period or may be dependant of a change of location.
- Status triggered transmission mode: when the status of the MU is modified by an external event, especially when triggering to an imminent peril or emergency status, the MU shall be able to send its location information.
- Queried transmission mode: in this mode, the MU shall transmit its location information when explicitly queried by the infrastructure.
- Delivery to the CCAS of location information from an MU engaged in an individual call (if the user's profile permits this - see clause 9.2).
- Delivery from the CCAS to an MU engaged in an individual call of location information about the other party in the call (if the other party's user's profile permits this - see clause 9.2).
- Delivery to the CCAS of location information from an MU transmitting in a group call (if the transmitting user's profile permits this - see clause 9.2).
- Delivery from the CCAS of location information about the MU that is transmitting in a group call to the parties in the call (if the transmitting user's profile permits this - see clause 9.2). (If permitted by privacy considerations, the location information may be included in the MCP D-TX Granted to another message.)

Depending on security policy, the transmitting party may send its location to the CCAS in the MCP U-TX DEMAND message. If security policy allows, the location of the transmitting party can be broadcast to all group members in the "MCP D-TX Granted to another" message or may be sent individually to each group member in a SIP INFO message so that it can be acknowledged and logged (for non-repudiation reasons). An MU can also send its location to the CCAS at any time in an MCP U-Info message.

The MU may make a spontaneous transmission of its location information:

- when registering;
- with each call setup and speech request;
- when sending imminent peril or emergency call or status (this may be enabled when location transmissions are otherwise disabled);
- on switch-off;
- arrival and/or departure from locations specified by an authorized user;
- timer expiry;
- when distance from previous location report exceeds a distance specified by an authorized user;
- direction change (as specified by an authorized user);
- geographical areas outside which location updates shall not be sent.

There may be additional triggers such as power on, power off (could be sent at next power on), emergency condition detected, PTT press, status entered, loss of service, regain of service, change of serving cell, low battery, connected to car kit, disconnected from car kit, arrival at destination, arrival at point, approaching point, lost ability to determine location, ambience listening call.

The location information shall contain the MU's CCA client identity (see clause 6.1.1), location information protocol type (extensible to future protocol types) and a timestamp and may contain in addition to the coordinates, the direction of mode and velocity, estimates of resolution, error ellipse, triggering conditions and suchlike.

NOTE 1: The location message content should allow location applications to provide a compatible service with applications build on legacy narrowband standard protocols.

NOTE 2: Where the MU contains more than one registered CCA client instance, it is not necessary for the MU to send a separate location update for each CCA client instance.

An authorized user can set and remove triggers for spontaneous location reporting in another MU. The authorized user can also temporarily suspend and re-enable all location reporting in a single MU or, by group-addressed signalling, in multiple MUs.

An authorized user can ask MU to start and stop store location reports at defined intervals and can subsequently request delivery of the MU's recorded location reports (each recorded location report shall contain a time stamp). The authorized user can also cause the MU to delete its recorded location reports, i.e. the authorized user can control and obtain tracking information. If the MU overfills its store of location records it should overwrite previous records with new records (preferably by "thinning out" the density of older records).

An authorized user uses HTTPS to store in the CCAS an XML document that defines the location information triggers to be used by an MU. The CCAS then sets the triggers in the MU by sending to the MU a SIP message containing the XML document.

7.10.2 Assisted location

The system shall support assisted location for improved accuracy. Assistance may be broadcast in a suitable manner, see clause 6.1.4.1.

7.11 Supplementary services

7.11.0 Introduction

The supplementary services described in the following clauses complement the services described in the previous clauses.

7.11.1 Ambience Listening

Ambience Listening (AL) is a service available to authorized units (such as dispatchers) allowing them to silently trigger transmission of a mobile unit. This may be required when the actual user of the mobile unit has been in some way incapacitated to allow the dispatcher to listen at the environment to assess the situation without the help of the user. This may also be required in the case of stolen terminal to allow assessing the situation around the terminal.

This service shall be unnoticeable at the terminal and should have minimal interaction with other services, in particular with location services. In particular, there shall be no ringing and no display of the calling party (dispatcher invoking the service). If there is an attempt to switch off an MU that is in the ambience listening state, the MU may appear to switch off but the MU shall remain in the ambience listening state. If the user attempts to setup a call or accept an incoming call while in the ambience listening state, the MU may suspend the ambience listening call until the end of the transmission and then return into the ambience listening call. Alternatively the MU is permitted to maintain the ambience call concurrently with the new call.

If the ambience listening state is remotely triggered by an authorized user, the ambience listening state may be terminated only by a message from a remote authorized user. If the ambience listening state is locally triggered, the ambience listening state may be terminated locally, or may be terminated by a message from a remote authorized user.

The service is similar to the individual call procedure, sent without alerting, and with transmit permission granted to the target unit. The target unit may request that an AL call is set up by use of a status function (see clause 7.8.1).

7.11.2 Talking party and calling party identity

Talking party identity (PTT calls) and calling party identity (full-duplex/telephone calls) are transmitted for display by the receiving parties in a call at the beginning of a media transmission sequence. The identity may be the CCA individual identity of the user of the MU or an identifier of the connected telephone subscriber or it may be a displayable name. These shall be application level as described in clause 6.1.1.

This service may be subject to restrictions (i.e. able to provide anonymous transmissions) which may be overridden by authorized users. Restrictions shall be configurable in the CCAS with potential dispatcher control. They are not intended to be configured by the MUs themselves.

7.11.3 Dynamic group number allocation and group merging

The dynamic group number allocation allows the dynamic provision of additional group identities to the MU. These identities may immediately be used for group communications when the allocation uses simultaneous affiliation or they may be kept inside the MU memory for later use under user control. In this later case, selection of the dynamically programmed group will be lead to a MU initiated affiliation. One use of group merging is to create a temporary group for reception of a broadcast group call. Depending on CCAS configuration, the CCAS may automatically affiliate the relevant MUs to groups created by group merging.

The allocation messages may be either individually addressed for one-by-one programming of the MUs or group addressed (with appropriate repetitions) for on the fly group merging, eventually with additional individual additions to the merged group. Where groups are merged, the merged group may be given the higher priority of the constituent groups, for example may give the merged group emergency priority if one of the constituent groups was in an emergency condition.

De-allocation may be performed by explicit de-allocation message or by use of a temporary allocation for a duration ranging from one call to a full mission.

The facility may be provided by a document management service or other alternative means.

Group merging may be initiated by a suitably-authorized user. The group merging request may specify the security level required for the merged group, including the use of encryption. Where the group merging request does not specify the security level, the security level shall be set to the level of the lowest of the groups comprising the merged group. Users of a merged group shall be notified if the merging operation causes the security level of the merged group to be lower than the security level of the users' original group.

The group merging request may include conditional parameters such as geographic areas and participant types, such that an MU receiving the group merging instructions only participates in the merged group when the conditional parameters match the MU's present circumstances. To facilitate frequent identical merging into a temporary group, a set of group merging request parameters may be preconfigured in the CCAS so that an authorized user may activate the request and communicate with the merged group with minimal delay.

7.11.4 Disabling and enabling

The MU application may be disabled and re-enabled under control of the infrastructure to manage stolen MU or rogue user cases. The disabling process shall be appropriately secured to avoid misuse of this feature. The MU application may be temporarily disabled or permanently disabled. A temporarily-disabled MU application may be re-enabled by a signalling message. A permanently disabled MU cannot be enabled by the CCAS or the user. When an MU is permanently disabled its stored user and device profiles and its security information shall be erased. A permanently-disabled MU shall have no access to CCA services. This disabling and enabling applies only to the client part of the MU and not to the LTE UE.

When the MU is involved in a communication at the time of the reception of the disabling message, it shall immediately leave the communication and not re-enter until it has been re-enabled.

However, the mobility update function of the MU remains activated when the MU is disabled to allow tracing of the unit and the ambience listening supplementary service may be activated. All keys except the ones required to allow these two functions shall be erased. Re-enablement of the MU requires a full refresh of the non-permanent cryptographic elements contained in the MU.

Disabling and enabling may be carried out by the NOTIFY procedure (related to the REGISTRATION). The message shall be authenticated cryptographically.

NOTE: It is for further study whether the enable/disable supplementary service can provide further disabling of the UE or terminal, e.g. to prevent transmission.

7.11.5 Call forwarding

7.11.5.0 Call redirection

Call forwarding (or call diversion) reroutes a call for a given MU to another one when some conditions are fulfilled. This service only applies to individual streaming calls.

As the MU which is the target of the call redirection may itself be subject to call forwarding, a redirection counter is maintained during the redirection process to check that the total number of redirections remains lower than a system defined limit, preventing the risk of looping.

In all cases, the MU receiving the redirected call shall be indicated that the call is redirected and should receive the identity of the initially called party.

7.11.5.1 Call forwarding unconditional

The unconditional call forwarding service (CFU) redirects to another MU every individual call to a given MU. This may apply for all type of calls or only for some specific types. The other MU may be statically designated at the time of the definition of the forwarding or may belong to a list address, allowing the redirection of the call to an available party among a predefined set of MUs.

This service may only be activated by authorized parties and is configured in the CCAS (not configured by the MU) and may apply to call to external parties (PSTN) or from external parties to given MUs. The service is achieved by the CCAS on receiving an INVITE from the calling party, first sending a 100 TRYING message back to the calling party, and then sending a 181 "Call is being forwarded" message back to the calling party, and sending an INVITE to the party who is the target of the diversion.

The use of CFU combined with call transfer provides a simple management of the call authorized by dispatcher feature. The dispatcher may decide whether to allow the call to be transferred or not; the decision process is outside the scope of the present document.

7.11.5.2 Call forwarding on busy subscriber and on no reply

The main use of this type of call forwarding is the implementation of voice messaging services. When the service is activated and when an individual call cannot be completed for one of the above reasons (the subscriber is already involved in a call and not willing to respond or the subscriber does not reply, including for MU which are not reachable), then the call is directed to another party.

In the case of a busy subscriber, the CCAS may know that the called party is engaged in another call immediately and then follows the message sequence used for unconditional call forwarding without attempting to complete the call to the originally called party. However the situation can also arise where the CCAS is not aware that the called MU is not able to accept the call: in this case an INVITE is first sent by the CCAS to the intended called party; the called party responds with a 486 BUSY response; and then the CCAS sends the 181 "Call is being forwarded" to the calling party, and the INVITE to the target of the forwarding.

7.11.6 Call barring

7.11.6.0 Introduction

The call barring supplementary service triggers the failure of calls when some conditions are met.

7.11.6.1 Barring of outgoing calls

An authorized user may prohibit a MU from setting up calls (individual and/or group) to defined set of recipients. This barring of outgoing calls triggers the failure of any call attempt by the barred MU to the barred individual or group recipients. The code for failure shall unambiguously indicate the cause of the failure.

NOTE: Barring of an individual MU as a call destination does not imply barring of communications to a group in which that individual is a member. Therefore MU A may be barred from making individual calls to MU B, but may still place calls to a group where MU B is a receiving member.

7.11.6.2 Barring of incoming calls

An authorized user may prohibit a MU from receiving calls (individual and/or group) from a given source or a given set of sources. The calling party shall be notified the cause for failure of the call attempt.

NOTE: In the same way as for outgoing calls, barring of incoming calls from an individual MU does not imply barring of group calls where that individual MU is the talking party.

7.11.7 Call waiting and call hold

Call waiting and call hold enable simple management of the reception of several individual calls which are setup during the same period of time. The process follows normal SIP procedures; examples of such can be found in [i.7].

When a MU receives a call setup (i.e. receives a SIP INVITE) while being already involved in a previous call, it may let the setup of the new call continue but may prevent media from flowing, thus providing the user with an indication of a waiting incoming call. It achieves this by negotiating a call which completes without allowing a media stream to start, i.e. using the SDP information in the 200 OK message.

Alternatively, the CCAS may also inform a MU that is already engaged in a call of a waiting call by the same mechanism, i.e. the INVITE sent from CCAS to MU contains no media. In this second case, the CCAS has effectively intervened in the set up process using knowledge that the called user is busy, and therefore the CCAS has taken the decision not to attempt to present a media flow. In either case, the setup may be later completed and media started when the called unit sends a new INVITE message which allows the media to flow.

If the MU wishes to keep an ongoing call while responding to another call, the former call may be put on hold. This may be achieved in the same way by sending a SIP INVITE removing media content from the call. The call may then be taken out of hold or released: in this case a further INVITE may be used to re-establish the media stream.

7.11.8 Discreet listening

The discreet listening service allows an authorized user to listen an individual or group call without any party of the call being notified of this intervention. The authorized user may release the call at any time.

This function is a system level feature which does not impact MU protocol.

7.11.9 Call transfer

An MU receiving a call may perform a call transfer to another MU once the call has been setup. This step may be performed after a call diversion (or call forwarding unconditional) in order to implement a simple call authorized by dispatcher feature. The process follows normal SIP procedures; examples of such can be found in [i.7].

When the called MU want to perform a transfer to a third party, it may put the existing call on hold, if media transfer is taking place, and may contact the party to whom it wishes to transfer the call by sending an INVITE. The party to be transferred is then sent a SIP REFER to inform it of the new called party. The new call is setup, and the original call shall be released by use of SIP BYE messages.

7.11.10 Area restriction

Area restriction allows limiting the actual coverage of a group communication. This restriction activated by calling party at setup time can restrict the coverage to a pre-programmed sub-coverage or to a sub-coverage dynamically defined based on calling party location (for example, all cells within a radius of x kilometres from that party's location).

7.11.11 Tracing & Recording

Tracing allows an authorized user to subscribe to events linked to an entity (e.g. a user, a group) to get real-time notifications and/or to log those events. The CCAS shall log at least the following items for logged calls, messages and data transfers: start time and date, user identities, group identity, location information of transmitting parties, end time, call reason and call type (normal, imminent peril, emergency, regroup, individual or group, media type), change of selected group.

Recording shall be possible for any type of media stream or data exchanged between or within entities. Recording shall be achievable at the home system of the recorded entity (individual or group). If end-to-end encryption is in use, the recording process shall preserve the end-to-end confidentiality of the communication.

Tracing and Recording are system level features which do not impact MU protocol but have an impact on the routing of calls and data to ensure the home system of the recorded entity is able to capture the media or data in order to deliver the feature.

7.11.12 Remotely triggered call

An authorized user may remotely request an MU to set up a call. The user of the affected MU shall be notified when this occurs. Both individual and group calls may be triggered in this way, with the affected MU requesting immediate permission to transmit.

NOTE: An ambience listening call (clause 7.11.1) is a remotely triggered call where the user is not notified that the call has been set up.

7.11.13 Over-the-air configuration

The CCA provides the means for an authorized user to use an MU to query and change user profiles, group profiles device profiles and CCAS service parameters stored by the CCAS (see clause 9). Profiles are stored by the CCAS in XML configuration access protocol (XCAP) documents (see clause 9.1).

The authorized user employs a SIP SUBSCRIBE message to obtain an HTTP URI for a profile. An HTTPS connection (see IETF RFC 2818 [23]) shall be used to read or write the profile. Reading an XCAP document is done with HTTP GET, creating or modifying is done with HTTP PUT and removal of a document is done with HTTP DELETE (see IETF RFC 4825 [27]).

NOTE 1: Other methods editing the profiles and configuring MUs are outside the scope of the present document.

NOTE 2: Care should be taken to avoid overloading of the communications links when changing the profile of a group to which a large number of MUs are affiliated.

Clause 7.2.3.8 describes how the MU obtains the CCAS service parameters and the MU's device, user and group profiles following registration with the SIP core, and enrols to receive notifications about changes to the information. When the MU receives a notification about changes to the information, it shall retrieve the full profile or only the changed items using the method and sequence described in clause 7.2.3.8 for retrieving the CCAS service parameters and the MU's device, user, and group profiles following registration with the SIP core. Clause 9.1 gives additional information about how the MU can obtain changes to a profile.

7.12 Principles for mobility management

7.12.1 Roaming and Migration

As described in clause 7.2, two configurations have to be considered for roaming and registration, depending on whether a single CCAS or multiple CCASs are involved.

If the transport network (e.g. LTE Core Network) allows direct access to the home CCAS of the user, then roaming is transparent to the user and to the application, it is entirely managed at the transport network level.

In case the transport network does not allow direct access to the home CCAS of the user, i.e. if local breakout is imposed, then the MU shall access its home server(s) through the local CCAS. In this configuration, the MU may have access to both its home and local services (e.g. groups from its home system and groups from the local system).

In case the home server(s) of the MU are not reachable from the CCAS, i.e. in case of isolation of the systems, the MU should be able to register with local server(s) with a default profile. The MU can have access to local services only.

7.12.2 Media gateway re-allocation

A Critical Communication Application can comprise several media interfaces, in order to provide redundancy and/or load balancing and/or geographic zones.

It can therefore be necessary or desirable to switch an MU from one media interface to another media interface, while staying attached to the same CCAS. The decision to switch media interface can be triggered by MU payload information, such as the MU's current LTE cell, which may be carried with the regular heartbeats exchanged between the MU and the CCAS.

In order to perform a seamless handover between the two media interfaces, the system uses a "make before break" procedure. This procedure consists in setting up a new permanent secure channel between the MU and the new media interface. Once this new secure channel is established, the CCAS updates the SDP of every group call and individual call to have them redirected on the same 5-tuple as the new channel, i.e. to the new Media Gateway, using a SIP UPDATE method.

In case the "make before break" is not possible, e.g. in sudden unavailability of the current media interface, the system proceeds with the set up of a new secure channel between the MU and an available media interface before using call restoration procedures to re-established the ongoing calls. In that case, the switching of the media interface is not seamless.

8 Multiple User Instances

8.1 User Instances

Clause 6.1.0 describes the CCA user identity and clause 6.1.1 defines CCA application identities.

A user instance is a unique combination of a CCA individual identity, a user profile and a CCA client instance. As there is a one-to-one mapping of the CCA individual identity to a CCA user identity, multiple user instances with the same CCA individual identity all represent the same CCA user. A user who registers with two or more devices exists in the CCAS as two or more user instances. When the CCAS needs to communicate with the user rather than a particular device, the CCAS may contact any or all of his user instances, as appropriate.

EXAMPLE: In a control room with several dispatchers the same CCA individual identity, user profile and CCA functional identity might be provided to each dispatcher. Alternatively, each dispatcher might have his own CCA individual identity and user profile but share the same CCA functional identity. In either case an emergency call should be sent to the control room's CCA functional identity. Control room logic can route the call to one or several dispatchers. If the caller wishes to call the same dispatcher again, the caller should address the call to the dispatcher's contact address (i.e. the dispatcher's GRUU - see clause 7.2.3.5).

8.2 List identifiers

List identifiers are used for the implementation of functions such as list addressing or list search call in existing narrowband systems. It allows a call to be directed to a set of individuals (for example dispatchers), without knowing which one will answer. The various individuals in the list are polled at call setup and one of the individuals acknowledging the call is the actual called party.

It is not specified whether the polling is sequential, parallel or a combination of both methods.

8.3 Use of multiple MUs

One user may be registered and authenticated via multiple MUs at any one time; i.e. the user can possess separate registered user instances on different MUs. For each user instance, the user shall authenticate to the CCAS independently through the relevant MU. The user may affiliate to different groups on the different MUs. The user may configure his user profile and the device profiles to indicate which MU is the preferred receiver of different types (e.g. half-duplex, full-duplex, voice, data, video) of incoming individual calls. When the CCAS receives an individual call request, it shall route the call to the preferred MU based on an inspection of the user profile and device profile in use by each user instance.

8.4 Multiple users of one device

A single MU may support more than one user instance. The MU's CCA client creates a separate CCA client instance for each user instance. The MU's user instances may be for different users or for the same user. The MU obtains a unique GRUU for each of its CCA client instances during SIP registration (see clause 7.2.3.5). Each CCA client instance acts on behalf of one user instance. Depending on the capabilities of the MU, each CCA client instance may communicate with its user via a separate user interface or the CCA client user interfaces may share a single user interface - how that may be done is outside the scope of the present document. The CCAS's SIP application server can use the GRUU to communicate with a specific CCA client instance, and thus with a particular user of the MU.

NOTE: Where the MU supports more than one user instance, it should attempt to rationalize some types of communications such as location information, so that the same information is not sent multiple times (once for each user instance).

8.5 Participant types

The "participant type" is a functional category of a CCA user (e.g. first responder, second responder, dispatch, dispatch supervisor). The CCA user's permitted participant types are typically defined by a CCA administrator authorized to control CCA service parameters and user profiles, etc. (see clause 9). A CCA user possessing multiple MUs may assume a different participant type for each MU. At any moment in a call, only one participant type shall be used per CCA individual identity and CCA client identity combination.

9 Profiles and Service Parameters

9.1 General

The CCAS shall maintain user profiles, supplementary configurations, device profiles, group profiles and CCAS service parameters. Each MU shall store and maintain a copy of its device profile, copies of the user profiles of its current users, copies of the group profiles of its affiliated groups (see clause 7.2.3.8) and a copy of the CCAS service parameters. Suitably authorized users may use an MU to read and modify user, device and group profiles (see clause 7.11.13). An MU needs only retain supplementary configurations for the duration of its stay on a visited CCAS.

Profiles and CCAS service parameters are stored by the CCAS in the form of XML configuration access protocol (XCAP) documents (see IETF RFC 4825 [27]) with one sub-document per user profile and an HTTP "put" selection describing the node. (For a specification of XML see W3C Recommendation 16 "Extensible Markup Language (XML)" [28].) Access to XCAP documents is controlled by an XCAP server. There is a separate user profiles document for each CCA user. All the user profiles for a single CCA user are stored in that document. Each user profile is thus a separate XCAP resource and can be individually addressed by the CCA client instance. Similarly, there is a single XML document containing all the group profiles of groups owned by the CCAS.

NOTE 1: Profile information that is not downloaded to the MU is stored separately by the CCAS.

NOTE 2: The method by which supplementary configuration information (see clause 9.3) is stored is outside the scope of the present document.

Each XCAP resource within an XCAP document is provided with an entity tag (etag). Whenever an XCAP resource within the document is changed, that XCAP resource is assigned a new etag and all other XCAP resources within the document are assigned the same etag value. When the CCA client instance downloads an XCAP document from the XCAP server, or makes any change to the document stored by the XCAP server, the XCAP server sends the new etag to the CCAS client. The XCAP server allows conditional requests based on the value of the etag. Thus, when the CCA client instance wishes to update its copy of an XCAP document or XCAP resource within a document, the CCA client instance can use a conditional GET in order to reduce network usage if its cached copy is still valid. (See IETF RFC 4825 [27] section 8.5).

The XCAP root URI is pre-configured in the MU client (clause 9.7). It should be provided as an HTTPS URI.

The Open Mobile Alliance (OMA) specifies a method of storing XML documents known as the XML Document Management System (XDMS) [34]. Documents stored according to this method are known as XDM documents. XDMS makes use of XCAP and XDCP (XDM command protocol). If the CCAS uses XDMS for storing profiles, the MU may use a "Differential Read XDCP request" to obtain the difference between a profile stored by the CCAS and the version of the profile identified by the supplied etag.

The MU is pre-provisioned with the MU's device class and device capabilities (see clause 9.7). However the MU's device class and device capabilities may change from time to time (e.g. by user selection or interconnection of peripheral equipment, etc.). The CCAS maintains a copy of that information (see clause 9.5.3). The MU shall send its device class and/or device capabilities to the CCAS using SIP PUBLISH if either changes. This should not be delayed beyond the MU's next successful SIP registration with the CCAS server.

9.2 User Profiles

The CCAS shall maintain a user profile for each CCA user. In addition, the CCAS shall maintain a default user profile that defines the services available to unauthenticated users. A user profile can be an individual user profile or a functional user profile. Functional user profiles contain one of more CCA functional identities by which the user can be called in the operational role for which the functional user profile is intended.

The user profile may contain the following items:

- user identity;
- home CCA server identity;
- name of user's CCA organization;
- user profile identifier;
- user profile version number;
- user profile status (enabled or disabled);
- CCA individual identity;
- displayable name of CCA individual identity;
- list of zero or more CCA functional identities used by this profile; for each identity a set of:
  - CCA functional identity;
  - displayable name of CCA functional identity;
- participant type - one of:
  - individual;
  - first responder;
  - second-responder;
  - dispatcher;
  - dispatch supervisor;

- system administrator;
- etc.;

- user type - one of:
  - personal user;
  - non-shareable functional identity;
  - shareable functional identity;
- list of groups to which this user profile may affiliate - for each group a set of:
  - CCA group identity;
  - the group's home CCA server identity;
  - displayable name of group (defined by either the 7-bit GSM default alphabet (see ETSI TS 100 900 [20]) or the UTF-8 character set (IETF RFC 3629 [21]));

NOTE 1: If present, "displayable name of group" overrides its equivalent in the group profile.

  - affiliation type; one of:
    - automatically by the CCAS;
    - on request by a user or the CCAS;
  - relative presentation priority in the event of multiple incoming group calls;
  - receive-only group;
  - user priority for the group;
  - participant type for the group;
  - call type (open-session, discrete or no preference);

NOTE 2: The affiliation type needs to be consistent with the affiliation type specified in the group profile.

- CCA group identity to be used for imminent peril group call requests (or selected group if not specified);
- CCA group identities to be used for emergency group call requests (or selected group if not specified);
- CCA individual identity for emergency individual call request (or user selected if not specified);
- recipient identities for an emergency alert (or user selected if not specified);
- priority for group call setup;
- maximum permitted number of affiliations;
- call set up and transmit request priority (8 levels), including dependence on hours of operation and duty hours;
- current hours of operation and duty hours;
- types of individual voice calls the user is permitted to request, e.g.:
  - hook-switch controlled;
  - requested automatic answer;
  - forced automatic answer;
  - half-duplex;
  - full-duplex;

  - none;

- sets of CCA individual identities to which an individual half-duplex voice call may be requested (no restriction if empty);
- sets of CCA individual identities to which an individual full-duplex voice call may be requested (no restriction if empty);
- sets of CCA individual identities to which other call types (e.g. data, video) may be requested (no restriction if empty);
- CCAS-defined phone book;
- user-defined phone book;
- sequence of calling a CCA individual identity that is registered with multiple devices:
  - call each device at the same time until one device answers; or
  - only call most preferred device that is currently registered; or
  - call each device that is currently registered in order of device preference;
- sequence of calling a CCA functional identity that is using multiple devices:
  - call each device at the same time until one device answers; or
  - only call most preferred device that is currently registered; or
  - call each device that is currently registered in order of device preference;
- device preference level for reception of full-duplex voice calls;
- device preference level for reception of individual half-duplex voice calls;
- device preference level for reception of group voice calls;
- transmission timeout pre-warning time;
- transmission timeout pre-warning enabled;
- incoming emergency alert indication method (e.g. audible, visual, tactile);
- incoming imminent peril alert indication method (e.g. audible, visual, tactile);
- incoming non-emergency alert notification;
- location information delivery (excluding imminent peril and emergency events):
  - MU to CCAS during individual call;
  - MU to CCAS during group call;
  - CCAS to dispatcher during call;
  - CCAS to other participant in an individual call;
  - CCAS to other participants in a group call;
- location information enablement for imminent peril and emergency events;
- maximum number of simultaneous audio streams the user may receive;
- number of simultaneously receivable group calls;
- list of foreign CCA server identities that this user profile is permitted to use;

- list of permissions, each consisting of three items corresponding to operation on the home CCAS, operation on visited CCASs, and to visitors from other CCASs that are operating on this user's home CCAS:
  - restrict provision of individual call setup failure reasons;
  - override transmissions in an individual call;
  - revoke transmit permission;
  - create, edit, delete, enable and disable user profiles for other CCA users;
  - enable or disable users;
  - temporarily disable MU applications and enable temporarily-disabled MU applications;
  - permanently disable MU applications;
  - temporarily disable devices and enable temporarily-disabled devices;
  - permanently disable devices;
  - create, edit and delete displayable names for other CCA users;
  - create a temporary group for reception of broadcast group calls;
  - make pre-emptive transmission request within a call;
  - make imminent peril call;
  - cancel in-progress imminent peril;
  - make emergency group call;
  - make emergency individual call;
  - cancel in-progress emergency in a group call;
  - cancel in-progress emergency in an individual call;
  - send emergency alert;
  - cancel any device's emergency alert;
  - alter device's emergency indication method;
  - make emergency individual call;
  - cancel individual call emergency priority;
  - change location information enablement;
  - initiate dynamic group merging operations;
  - locally-trigger an ambience listening call;
  - remotely-trigger an ambience listening call;
  - remotely-trigger non-ambience listening calls;
  - remotely cancel a user's transmit permission;
  - view which users are registered on the CCAS;
  - view which users can participate in individual calls;
  - view by users the state of this user's CCAS registration;
  - view another user's affiliated groups;

  - view group members;
  - view affiliated group members;
  - propose changes to group affiliations of other users;
  - change group affiliations of other users;
  - exhibit displayable names;
- proprietary user profile information.

9.3 Supplementary Configuration

Supplementary configuration may be provided to a visiting user to add group memberships relevant to the visited CCAS. A URI for the supplementary information is sent automatically by the visited CCAS in SIP NOTIFY message so that the supplementary information can be downloaded using HTTP. The supplementary information is applicable only for the duration of the visit.

- list of groups to which this user profile may affiliate - for each group a set of:
  - CCA group identity;
  - the group's home CCA server identity;
  - displayable name of group (defined by either the 7-bit GSM default alphabet (see ETSI TS 100 900 [20]) or the UTF-8 character set (IETF RFC 3629 [21]));

NOTE 1: If present, "displayable name of group" overrides its equivalent in the group profile.

  - affiliation type; one of:
    - automatically by the CCAS;
    - automatically by the MU;
    - by user request;

NOTE 2: The affiliation type needs to be consistent with the affiliation type specified in the group profile.

  - relative presentation priority in the event of multiple incoming group calls;
  - receive-only group;
- local CCAS phone book (temporarily supplements the CCAS-defined phonebook in the user profile (clause 9.2);
- list of denied permissions (temporarily cancels individual permissions granted in the user profile - see clause 9.2 for details).

9.4 Group Profiles

9.4.1 General

The CCAS shall maintain a profile for each defined group.

9.4.2 Group profile items provided to group members

The following items in the group profile may be provided to group members:

- CCA group identity;
- the group's home CCA server identity;

- name of group's CCA organization;
- group profile version number;
- default displayable name of group (defined by either the 7-bit GSM default alphabet (see ETSI TS 100 900 [20]) or the UTF-8 character set (IETF RFC 3629 [21])) - overridden by displayable name in user and device profiles and supplementary configuration (if present);
- call type (open-session, discrete or no preference);
- current status of the group: enabled or disabled;
- indication if temporary group;
- level within group hierarchy (applicable only for a group-broadcast group);
- level within user hierarchy (applicable only for a user-broadcast group);
- imminent peril calls permitted;
- emergency calls permitted;
- emergency alerts permitted;
- timeout value for cancellation of in progress imminent peril group call;
- timeout value for cancellation of in progress emergency group call;
- group call model (discrete call or open-session call);
- group-call hang time;
- security requirements:
  - signalling confidentiality and integrity;
  - floor control confidentiality and integrity;
  - end-to-end media confidentiality and integrity;
- geographical area where users are required to acknowledged group call setup;
- geographical area where call can be setup;
- primary geographical area;
- hours of operation and duty hours;
- group call priority in primary geographical area and duty hours;
- group call priority outside primary geographical area or duty hours;
- pre-emption of this group permitted;
- permission for this group to pre-empt other users;
- preferred voice codec (including rate information);
- preferred video codec (including rate and format information);
- permission to request list of members of this group;
- permission to request list of affiliated members of this group.

9.4.3 Group profile items not normally provided to group members

The following items in the group profile are not included in the group profile provided to group members:

- maximum permitted group call duration;
- maximum permitted imminent-peril group call duration;
- maximum permitted emergency group call duration;

NOTE 1: The remaining call duration may be provided to MUs in the call.

- group members - list of:
  - CCA individual identity;
  - affiliation type - one of:
    - automatically by the CCAS;
    - on request by a user or the CCA;
  - user priority for the group;
  - participant type for the group;
  - receive-only;
  - requirement to acknowledge setup before group call proceeds;

NOTE 2: The affiliation types need to agree with the information provided to the group members in user profiles.

- list of group members (CCA individual identities) permitted to select the group;
- list of receive-only group members;
- list of CCA individual identities currently affiliated to the group;
- maximum permitted number of group members;
- minimum permitted number of group call participants;
- minimum permitted number of group call setup acknowledgers;
- geographical area where acknowledgement of all affiliated users is required before start of audio transmission;
- acknowledged call setup timeout;
- action following call setup acknowledgement failures: proceed or abandon;
- ability to pre-empt other users;
- ability to be pre-empted.

9.5 Device Profiles

9.5.1 General

The CCAS shall maintain a profile for each device.

9.5.2 Device profile items provided to the MU

The following items in the CCAS's copy of the device profile may be sent to the MU:

- maximum number of simultaneous transmissions device is permitted to receive in the event of override in a single group call;
- maximum permitted number of simultaneous individual calls per device;
- set of services available prior to user authentication, e.g. emergency call, emergency alert;
- list of user-independent groups to which device may affiliate - for each group a set of:
  - CCA group identity;
  - home CCA server identity of the group;
  - displayable name of group (defined by either the 7-bit GSM default alphabet (see ETSI TS 100 900 [20]) or the UTF-8 character set (IETF RFC 3629 [21]));

NOTE 1: If present, "displayable name of group" overrides its equivalent in the group profile.

  - relative presentation priority in the event of multiple incoming group calls;
  - receive-only group;
- incoming emergency alert indication method (e.g. audible, visual, tactile);
- user permission to alter emergency alert indication method;
- incoming imminent peril alert indication method (e.g. audible, visual, tactile);
- user permission to alter imminent peril alert indication method;
- location information enablement (excluding imminent peril and emergency events);
- location information enablement to called and calling parties in individual and group calls;
- location information enablement for imminent peril and emergency events;
- user permission to change device's location information enablement;
- preference level among multiple active MUs for reception of individual full-duplex calls;

NOTE 2: This may be overridden (e.g. by user choice) during SIP registration.

- proprietary device profile information.

9.5.3 Device profile items not normally provided to the MU

The following items in the CCAS's copy of the device profile are not normally included in the device profile sent to the MU:

- CCA client identity;
- CCA client status:
  - enabled;
  - temporarily disabled;
  - permanently disabled;
- maximum supported number of simultaneous CCA client instances;
- device class (supported or not-supported features) - see clause 9.7 for details;

NOTE 1: The device class in the device profile is a copy of the device class pre-provisioned in the MU as subsequently altered by addition or subtraction of accessories (e.g. a high resolution display or remotely-controlled video camera) - see clause 9.7. The MU notifies the CCAS when its device class changes and the CCAS can ask the MU to send the device class to the CCAS.

- device capabilities (see clause 9.7 for details);

NOTE 2: The device capabilities in the device profile is a copy of the device capabilities pre-provisioned in the MU. The MU notifies the CCAS when its device capabilities change and the CCAS can ask the MU to send the device capabilities to the CCAS.

- set of currently affiliated groups per registered user.

9.6 CCA Service parameters

9.6.1 Service parameters provided to the MU

Services supported by the CCAS:

- Voice:
  - individual half-duplex calls;
  - individual full-duplex calls;
  - group calls;
- Messaging (SDS);
- Video.

The following CCA service parameters may affect the operation of MUs:

- the maximum time for which an MU is permitted to transmit in a half-duplex call;
- time remaining when the CCAS warns MU of imminent transmit time expiry;
- individual call hang time;
- time remaining when the CCAS warns MUs of imminent call time expiry;
- permission for merged groups to use encryption;
- automatic affiliation of MUs into temporary groups created by group merging;
- character set used for identifiers;
- sets of pre-stored group merging parameters.

NOTE 1: The MU should reload the CCA service parameters when it registers with a new CCAS.

NOTE 2: The method by which the CCAS modifies the CCAS service parameters for calls between CCASs with different values of these parameters is outside the scope of the present document.

9.6.2 Service Parameters not provided to the MU

The following service parameters are stored by the CCAS but are not normally sent to the MU:

- maximum permitted individual call duration;
- maximum permitted emergency individual call duration;

NOTE 1: Where a call transits between CCASs, the shortest of the relevant timers applies.

- destination address for logging and recording information;
- maximum number of simultaneous audio streams that may be sent to an MU.

NOTE 2: The device profile parameters "maximum number of simultaneous audio streams the device can receive" and "maximum number of simultaneous transmissions device is permitted to receive in the event of override in a single group call" may be lower than this.

9.7 MU configuration data

Before it can be used for the first time, the MU needs to be configured with essential information. This includes:

- CCA client identity;
- the MU's home CCA server identity;
- for each CCAS that this MU is configured to use, a set of:
  - CCA server identity;
  - APN;
  - IP address or FQDN or URI of the CCAS's application control interface;
  - TCP and UDP port numbers for access to the CCAS's functional entities;
  - device and user authentication requirements:
    - device authentication required by the CCAS;
    - user authentication required by the CCAS;
    - redirect HTTPS URI pre-registered at the OpenID provider [31];
  - XCAP root HTTPS URI (see clause 9.1);
- for each PLMN that this MU is configured to use:
  - for each CCAS that this MU is configured to use, a set of:
    - CCA server identity;
    - local APN;
- method of CCAS selection. One of:
  - locked to home CCAS;
  - selection by user;
- imminent peril CCA group identity;
- emergency call CCA group identity;
- device class (set of supported features);
  - dispatch terminal;
  - hook-switch operation;
  - half-duplex voice;
  - full-duplex voice;
  - text message store and display;
  - photograph store and display;

- low resolution video display;
- full-duplex low-resolution video calls;
- high-resolution video display;
- full-duplex high-resolution video calls;
- remotely-controllable low-resolution video transmission;
- remotely-controllable high-resolution video transmission;
- automatic number-plate recognition;
- air-to-ground support;
- reserved items;

NOTE 1: The device class is pre-provisioned in the MU but may be modified by addition or subtraction of accessories (e.g. a high resolution display or remotely-controlled camera). The CCAS maintains a copy of the device class in the device profile (see clause 9.5.3). The MU notifies the CCAS when its device class changes and sends the device class to the CCAS on demand.

- device capabilities:
  - list of CCA standard version numbers supported;
  - list of access network types supported (e.g. LTE, WiFi, IP-based wired access, etc.);
  - list of supported voice codecs;
  - list of video codecs supported;
  - list of end-to-end encryption methods and algorithms supported;
  - E-MBMS capabilities:
    - E-MBMS supported;
    - number of MBSFN bearers that can be simultaneously received;
    - SC-PTM supported;
  - location information capabilities (protocols, constellation types, AGNSS support);
  - maximum number of simultaneous audio streams the device can receive;
  - maximum number of simultaneous video streams the device can receive;
  - reserved items;

NOTE 2: The MU's device capabilities are pre-provisioned in the MU. The CCAS maintains a copy of the MU's device capabilities (see clause 9.5.3). The MU notifies the CCAS when its device capabilities change and sends the device capabilities to the CCAS on demand.

- proprietary device information.

Annex A (informative): Analysed services and requirements

This clause contains listed requirements for the CCA derived from the User Requirements Specification for Mission Critical Broadband [i.1] and implied from existing functionality within TETRA derived from TETRA Interoperability Profile documents. A list of functions which are specified in TIPs can be found in [i.2]. The tables of requirements can be used to cross check the architecture solution described in the present document, and in protocol specifications compliant to this architecture.

Table A.1 identifies function requirements applicable to the CCAS to MU interface. Table A.2 identifies function requirements applicable to the equivalent interface for a base station operating in base station fallback mode. Table A.3 identifies performance requirements for the interface.

Table A.1 categorizes each service listed in the table according to predicted impact on an underlying broadband IP network as well as impact (i.e. standardization requirement) on the CCAS to MU interface. The sources of each requirement are identified as follows:

URS: Taken from User Requirements Specification [i.1]. Requirements are numbered according to URS clause.

TIP: Taken from the named TETRA Interoperability Profile specification and implied to be necessary for the MU to CCAS interface based on existing TETRA functionality. A list of functions for which TIPs have been written is given in [i.2].

SS: Taken from set of TETRA Supplementary Service specifications [i.3].

The "Clause" column in table A.1 indicates which clause within the present document satisfies the relevant requirement.

Table A.1: List of services for CCAS to MU interface

Service	Transport layer impact	Application layer impact	Source	Clause
Identities and addressing				
Support 500 000 group (address)s per system	No	Yes	URS 4.2-15	6.1.1
Functional addressing by role	No	Yes	URS 4.2-20	7.6
Location dependent addressing of dispatcher	No	Yes	URS 4.2-21	7.6
Registration				
Registration of user/identity	Yes for IMSI	Yes for application layer identity	Core TIP	7.2
Use of ASSI	Yes for IMSI	No for application: identity protected	Core TIP	N/A
Energy saving mode	Yes	No (see note 1)	Core TIP	N/A
Periodic location update	Yes (as required by network)	Yes - keep alive for application, also if needed for any IP connection	Core TIP	7.2.4
Mobility related location update	Yes	Potential need for application to be aware of its location (resource management, etc.)	Core TIP	7.2.4
Deregistration	Yes	Yes for application	Core TIP	7.2.5
Entry to dual watch	TBD - technology dependent	TBD - technology dependent	Core TIP	7.2.5
Entry to DMO	TBD - technology dependent	TBD - technology dependent	Core TIP	7.2.5
Subscriber class	Yes See note 5	No: network access function	Core TIP	N/A
Individual call				
Half-duplex	No	Yes	Core TIP	7.3
Full-duplex	No	Yes	Core TIP	7.3
Hook signalling/direct call	No	Yes	Core TIP	7.3.1, 7.3.2
Calling/Talking party identity	No	Yes	Core TIP	7.11.2

Service	Transport layer impact	Application layer impact	Source	Clause
Call proceeding indications	No	Yes	Core TIP	7.3.1, 7.3.2
Transmission control grant	No	Yes	Core TIP	7.5
Call waiting function	No	Yes	SS list SS_CW	7.11.7
Call modification				
Direct to hook	No	Yes	Core TIP	7.6
Half-duplex - full-duplex (both ways)	No	Yes	Core TIP	7.6
End of transmission	No	Yes	Core TIP	7.5.2
End of call	Yes - bearer release under application control	Yes	Core TIP	7.5.6
Call queue	No See note 6	Yes	Core TIP URS 4.3-5	7.3.1, 7.3.2
Call hold (full-duplex call)	No	Yes	SS Call Hold	7.11.7
Call maintenance				
Call maintenance information transmission (see note 1)	No	Yes	Core TIP	7.3.1, 7.3.2
Emergency/priority				
Emergency individual call	Yes - pre-emptive bearer demand	Yes	Core TIP URS 4.2.1-3	7.7.2
Emergency speech item request	Yes - pre-emptive bearer demand	Yes	Core TIP	7.7.3
Emergency call set up modification	No	Yes	Core TIP	7.7.2
Pre-emptive priority individual call	Yes - pre-emptive bearer demand	Yes	Core TIP URS 4.3-2	7.7.2
Priority call - terminal demanded priority	No	Yes	Core TIP	7.7.2
Priority call - SwMI configured priority	No	Yes	Core TIP	7.7.1
Group management				
Broadcast address	Yes	Yes	Core TIP	7.4.1
Single group attachment (affiliation)	No	Yes	Core TIP URS 4.2-2	7.4.4
Multiple group attachment (affiliation)	No	Yes	Core TIP	7.4.4
Selected group attachment (affiliation)	No	Yes	Core TIP	7.4.4, 7.7.4
Class of use - scanning - 8 values	No	Yes	Core TIP	7.7.4
SwMI initiated attachment (affiliation)	No	Yes (see note 2)	Core TIP URS 4.2-3b	7.4.4
SwMI rejection of MU attachment (affiliation) request	No	Yes	URS 4.2-1	7.4.4
SwMI acceptance of MU attachment (affiliation) request	No	Yes	URS 4.2-3a	7.4.4
SwMI forced detachment (de-affiliation)	No	Yes	Core TIP	7.4.4
Scanning on/off indication	No	Yes	Core TIP	7.8.1.6
Attachment (affiliation) lifetime	No	Yes	Core TIP	7.4.4
MU initiated detachment (de-affiliation)	No	Yes	Core TIP	7.4.4
Group call	Yes - for group bearer	Yes		
Calling/talking party identity	No	Yes	Core TIP URS4.2-5	7.11.2
Suppression of talking party identity (set by CCAS, not user)	No	Yes	URS clarification	7.11.2
Notify MU if only group member at call set up	No	Yes	URS 4.2-4	7.4.5
Call queuing when not all resources available ("all start")	No	Yes	URS 4.2-11, 4.3-5	7.4.7.3.1, 7.4.7.3.2
Call partial completion when not all resources available ("fast start")	No	Yes	URS 4.2-12	7.4.7.3.1, 7.4.7.3.2
Ringing group call	No	Yes		7.4.7.4
Transmission control	No	Yes	Core TIP	7.5
End of transmission	Yes - bearer release	Yes	Core TIP	7.5.2

Service	Transport layer impact	Application layer impact	Source	Clause
Transmission interrupt	No	Yes	Core TIP URS 4.2-6, 4.2.2-3, 4.2.2-5	7.5.4
Indication of attempted interruption	No	Yes	URS 4.2-7. 4.2.2-8	7.5.4
Dispatcher hears interrupted and interrupting parties	No	Yes	URS 4.2-8, 4.2.2-6	7.4, 7.5.4
Call disconnection	Yes - bearer release	Yes	Core TIP	7.5.6
Call maintenance (wait)	No	Yes	Core TIP	7.5.5
Late entry - roaming	Yes (reconnection of bearer on roaming)	No	Core TIP	7.4.6
Late entry - late group selection	No	Yes	Core TIP URS 4.2-10	7.4.6
Late entry - resources become available	No	Yes	URS 4.2-13	7.4.6
Call bearer modification (LTE unicast/multicast)	Yes See note 7	Yes - if application controlled	Core TIP	7.4.7.3.1, 7.4.7.3.2
Multipoint to point-point	No	TBD - TETRA function used for out of area call diversion to dispatcher. Can be an application above the standard (achieved using standard signalling)	Core TIP	7.6
Local/wide area call	No	Yes	SS Area Selection	7.4.2
Call waiting indication (incoming individual call)	No	Yes	SS CW	7.11.7
Multiple media types in same group	No	Yes	URS 4.2-16	7.4
Multiple instances of same media type in same group	No	Yes	URS 4.2 clarification	7.4
Video "push" call	No	Yes	URS 4.2 clarification	7.4
Independent transmission control for different media in same group	No	Yes	URS 4.2-17	7.4.5
Rejection/suspension of user from call if cell capacity reached	No	Yes	URS 4.2-34	7.5.5
Signalling of congestion with rejection for capacity reasons	No	Yes	URS 4.2-35	7.5.5, 7.7.5
Emergency/priority call				
Emergency group call highest priority	Yes - pre-emptive bearer demand	Yes	Core TIP URS 4.2.1-5, 4.3-3	7.7.2
Emergency group call can include group members and dispatcher	No	Yes	URS 4.2.1-11	7.7.2
Emergency speech item request	Yes - pre-emptive bearer demand	Yes	Core TIP	7.7.3
Emergency call set up modification	No	Yes	Core TIP	7.7.2
Emergency call patching	No	Yes	URS 4.2.1 clarification	7.11.3
Pre-emptive priority group call	Yes - pre-emptive bearer demand	Yes	Core TIP URS 4.2.1-6, 4.2.1-18, 4.3-2, 4.3-8	7.7.2
Signalling to talking party that some group members have been lost due to resource pre-emption	No	Yes	URS 4.3-18	7.7.5
Priority call - terminal demanded priority	No	Yes	Core TIP & URS 4.2 clarification	7.7.2
Priority call - SwMI configured priority	No	Yes	Core TIP	7.7.1
Broadcast call	Yes	Yes	Core TIP	7.4.1, 7.4.4
Priority group scanning	No	Yes	Core TIP	7.4

Service	Transport layer impact	Application layer impact	Source	Clause
Area related emergency call	No	Yes	URS 4.2.1-4	7.4.1, 7.4.2
Termination of emergency call by user	No	Yes	URS 4.2.1-7	7.5.6
Termination of emergency call by dispatcher	No	Yes	URS 4.2.1-8	7.5.6
Termination of emergency call by system (e.g. time-out)	No	Yes	URS 4.2.1-9, 4.2.1-19	7.5.6
Ringing/alerting emergency call	No	Yes	URS 4.2.1-12	7.4.7.4
Alert authorized users of emergency call if they are in other calls	No	Yes	URS 4.2.1-13	7.7.2
Accept or reject ringing emergency call	No	Yes	URS 4.2.1-14	7.4.7.4
Imminent peril call (pre-emptive, pre-emptable by emergency call)	No	Yes	URS 4.2.1-16; Clarification	7.7.2
Priority (general)				
Degrade QoS of lower priority sessions (data)	Yes	Yes	URS 4.3-6	7.7.5
Move lower priority sessions to queue in congestion (data)	Yes	Yes	URS 4.3-7	7.7.5
Cell reselection	Yes	No		
Broadcast of network area information	Yes	Yes (to configure the broadcast)	Core TIP	7.8.2.1
Status message	No	Yes	Core TIP	
Status individual to individual	No	Yes	Core TIP	7.8
Status to group	No	Yes	Core TIP	7.8
Emergency status	No	Yes	Core TIP URS 4.2.1-1	7.8.1.1
Pre coded status	No	Yes	Core TIP	7.8
Telephone call				
PSTN call - direct LTE routed	Yes	No	Core TIP	N/A
PABX call	No	Yes	Core TIP	7.3.3, 7.3.4
PSTN call - home application routed	No	Yes	Core TIP	7.3.3, 7.3.4
DTMF overdial	Yes (direct LTE routed)	Yes (home application routed)	Core TIP	7.3.3, 7.3.4
Call disconnect	Yes	Yes (application routed)	Core TIP	7.3.3, 7.3.4
Emergency phone call	Yes (direct LTE, 112, etc.)	Yes (home application routed)	Core TIP	7.3.3
Incoming and outgoing number presentation	No	Yes	SS list	7.11.2
Outgoing number presentation restricted by CCAS (not user set)	No	Yes	SS list & URS clarification	7.11.2
Call hold	No	Yes	SS list	7.11.7
Transmit inhibit	Yes (if it is possible)	Yes (if LTE supports; for application information)	Core TIP	7.8.1.7
Short Data Service	No	Yes		7.8.2
SDS-TL	No	Yes	SDS TIP	7.8.2
Predefined service types for SDS-TL (e.g. text, AVL, etc.) See note 2 and note 3	No	Yes	SDS TIP	7.8.2
Notification of available video	No	Yes	URS 4.2 clarification	7.8.2
Individually addressed SDS	No	Yes	SDS TIP	7.8.2
Group addressed SDS	TBD: could make use of MBMS/GCSE	Yes	SDS TIP	7.8.2
Store and forward of messages	No	Yes	SDS TIP	7.8.2
Message validity time for store and forward	No	Yes	SDS TIP	7.8.2
Message reports	No	Yes	SDS TIP	7.8.2

Service	Transport layer impact	Application layer impact	Source	Clause
Multiple forms of message addressing	No	Yes - at least application level address, TETRA addressing and external subscriber number	SDS TIP	7.8.2
Support of SS control application	No	Yes	SS list	7.8
Support of (existing TETRA) DMO management application (DOTAM)	No	Yes	SS list	7.8
Support of management of ProSe operation through the CCA	FFS	FFS		FFS
DGNA				
Assignment of groups	No	Yes	DGNA TIP URS 4.2-32	7.11.3
De-assignment of groups	No	Yes	DGNA TIP	7.11.3
Forced attachment (affiliation) to assigned group	No	Yes	DGNA TIP	7.11.3
Forced detachment (de-affiliation) of assigned group	No	Yes	DGNA TIP	7.11.3
DGNA addressed to individual address	No	Yes	DGNA TIP URS 4.2-32, 4.2-37	7.11.3
DGNA addressed to group address	TBD: could make use of MBMS/GCSE if service needed	TBD: service may be achieved to individual address only.	DGNA TIP	7.11.3
Group merging	No	Yes (see note 3)	DGNA TIP URS 4.2-38	7.11.3
Provision/modification of group mnemonic name	No	Yes	DGNA TIP	7.11.3
DGNA rejection and/or error reporting by MU	No	Yes	DGNA TIP	7.11.3
Authentication				
Mutual authentication (application level)	No	Yes	Auth. TIP	7.2.0.2
Ambience Listening				
AL request from target user	No	Yes	AL TIP	7.11.1, 7.8.1.4, 7.8.1.5
AL setup by SwMI	No	Yes	AL TIP URS 4.2.1-10	7.11.1
AL cleardown by SwMI	No	Yes	AL TIP	7.11.1
End to End Encryption	No	Yes	URS 6-1	5.4.7
Clear voice override	No	Yes	E2EE TIP	5.4.7
Algorithms to be upgradable	No	Yes	URS 6-2	5.4.7
Enable/disable				
Enable/disable of UE	Yes - whichever LTE mechanisms apply (possibly network barring only)	No	En/Dis TIP	N/A
Enable/disable of application	No	Yes	En/Dis TIP	7.11.4
Disable of the UE by application action (c.f. disable of ME)	Yes (UE) (FFS)	Yes	En/Dis TIP	7.11.4
Call authorized by dispatcher				
Call transfer by SwMI	No	Yes (if required)	CAD TIP	7.11.9
Call acceptance or rejection by dispatcher	No	Yes (if required)	CAD TIP	7.11.5.1
Air to Ground	Yes	No	A2G TIP	N/A
Location Information Protocol		See note 4	LIP TIP	7.10
Unsolicited location reports	No	Yes	LIP TIP	7.10.1
Trigger based reporting	No	Yes	LIP TIP	7.10.1
Control of reporting	No	Yes	LIP TIP	7.10.1
Net Assist protocol	No	Yes	SS list	7.10.2
Call forwarding Configured in SwMI				7.11.5
Call forward telephone calls	Yes	No	CF TIP	7.11.5
Call forward PTT calls	No	Yes	CF TIP	7.11.5

Service	Transport layer impact	Application layer impact	Source	Clause
Callout				
Alerting, terminal response and user response	No	Yes	Callout TIP	7.8.2
Group call information phase	Yes - for group bearer	Yes	Callout TIP	7.8.2
Barring of incoming calls	No	Yes	SS list SS-BIC	7.11.6.2
Barring of outgoing calls	No	Yes	SS list SS-BOC	7.11.6.1
Call forwarding - individual calls	No	Yes	SS list SS-CF	7.11.5
Call forward on busy	No	Yes	SS list SS-CFB	7.11.5.2
Call forward on no reply	No	Yes	SS list SS-CFNR	7.11.5.2
Call forward on not reachable	No	Yes	SS list SS-CFNRy	7.11.5.2
Call forward unconditional	No	Yes	SS list SS-CFU	7.11.5.2
Discreet listening (by dispatcher only)	No	Yes	SS list SS-DL	7.11.8
Dual Watch				
Monitor infrastructure group calls when in ProSe	Yes	Yes	URS 4.10-1	FFS
Switch between infrastructure and ProSe modes	Yes	Yes	URS 4.10-2	FFS
Simultaneously listen to infrastructure and ProSe calls	Yes	Yes	URS 4.10-3	FFS
Detect an emergency ProSe call when in infrastructure or ProSe mode	Yes	Yes	URS 4.10-4	FFS
Interoperability with legacy systems				
Communicate via gateway	No	Yes	URS 4.5-1	4.2.3; N/A
Data transfer to/from legacy systems	No	Yes	URS 4.5-1	4.2.3; N/A
Voice calls to/from legacy systems	No	Yes	URS 4.5-1	4.2.3; N/A
Share groups with legacy system	No	Yes	URS 4.5-1	4.2.3; N/A
End to end encrypted calls with legacy system	No	Yes	URS 4.5-1	4.2.3; N/A
Priorities consistent with legacy system	No	Yes	URS 4.5-1	4.2.3; N/A
Miscellaneous				
Adequate speech performance in noisy environments	No	Yes	URS 5-1	6.2.1

NOTE 1: Application layer may need to control the way that UE saves energy to achieve call setup, etc. performance requirements.
NOTE 2: To be checked whether the same as DGNA with forced attachment.
NOTE 3: Not specifically specified in TETRA TIPs, but application can provide the function using TIP mechanisms.
NOTE 4: The actual protocol is TBD.
NOTE 5: Need to consider how to achieve air to ground and similar cell steering.
NOTE 6: Feedback from the network when bearer released.
NOTE 7: Could be under application control or network function.

Table A.2 lists the set of services derived from the same source for base station fallback mode.

Table A.2: List of services required in Base Station fallback mode

Service	IP layer impact	Application layer impact	Source
BS fallback	Yes - TBD	TBD - network; Yes - UE app.	Core TIP
BS fallback - neighbour cell state	Yes	No	Core TIP
Group call services	Yes	Yes	URS 4.2.3-1
Group multimedia services	Yes	Yes	URS 4.2.3-2
Disconnection or continuation of calls at point of disconnection	TBD	TBD	URS 4.2.3-3
Indication of serving cell fallback state	Yes	TBD	URS 4.2.3-4
Continue to use normal addressing	No	Yes	URS 4.2.3-6
Maintain security in fallback mode, including encryption	TBD	Yes	URS 4.2.3-8
Authentication in fallback mode, which may be implicit	TBD	Yes	URS 4.2.3-9
BS provides list of served users to others receiving service from that BS	TBD	TBD	URS 4.2.3-10
Restrict list of served users to those within same group	TBD	TBD	URS 4.2.3-11
Cancel local service indication when reconnected to infrastructure	Yes	TBD	URS 4.2.3-13

NOTE 1: Call maintenance signalling includes signalling in circumstances such as impending disconnection warning, call timer extension.

NOTE 2: The SDS message types which should be supported include at least the following:

- Text messaging, including immediate text messaging.
- End to end encrypted messaging.
- End to end encryption key management.
- Location reporting and control of reporting.
- Wireless Datagram Protocol WAP.
- Wireless Control Message Protocol WCMP.
- Managed DMO service.
- PIN authentication.
- Net Assist Protocol.
- Messages with user data header.

NOTE 3: Current TETRA theoretically can support concatenated text messages of up to 2 048 bytes x 255 messages.

Table A.3 lists performance requirements for the services, where specified. All are taken from the URS [i.1].

Table A.3: Performance requirements

URS clause	Requirement
4.2-9	Talker changeover, with delay no longer than initial call setup
4.2-14	MU support for 5 000 groups
4.2-22	Call setup within 300 ms
4.2-23a	Minimal audio delay within a call
4.2-23b	Minimal difference in delay for users in same cell, and nearby users on different cells
4.2-24	Efficient use of resources
4.2-25	Group size from 2 participants to all on system
4.2-26	Group size within a cell from 1 to all users within the cell
4.2-29	High speed handover, 300 km/h, preferably 500 km/h
4.2-30	At least 36 simultaneous group calls per cell/sector
4.2-31	At least 2 000 users per cell/sector
Clarification URS 4.2	One group may contain all (2 000) users in a cell/sector
4.2.1-14	Ringing emergency call: same capacity and performance requirements as normal call
5-2	No echo on voice
5-3	Consistent quality with range of speeds up to 300, pref. 500 km/h
ETSI TS 122 179 [i.4] (V13.3.0) R-6.15.4.2-003	Maximum Late call entry time for calls without application layer encryption within one CCA system to be less than 150 ms for 95 % of all late entry requests
ETSI TS 122 179 [i.4] (V13.3.0) C-4	There may be group call participants in every cell
NOTE: The performance requirements in this table apply for terrestrial use only and only when users are under coverage of the same network.	

Annex B (normative): Media control protocol

B.1 General

This annex lists the messages required for the Media Control Protocol, together with the parameters required by the messages.

B.2 Media Control Protocol message table

Table B.1 lists the downlink MCP messages and parameters.

Table B.1: Downlink MCP messages

Message name	Purpose	Parameters
MCP D-TX Granted	Indicates to talking party that he has transmit permission	Flow identification [m] (see notes 2 and 3); Replacement flow identification [o] (see note 3); Transmission duration [m]; Call duration [o].
MCP D-TX Granted to another	Indicates to a receiving party that another talking party has transmit permission	Flow identification [m] (see note 4); Transmission request permission [m]; Talking party identity [o]; PTT priority [m]; Current call priority [m]; Request for acknowledgement [m]; Location information of talking party [o].
MCP D-Setup	Indicates to a receiving party that a call is being setup, sent over a multicast bearer where there is no session in progress	Flow identification [m] (see note 4); Media parameters [m].
MCP D-Queued	Indicates that a request for transmission has not been granted and indicates that the user has been placed in a queue	Flow identification [m] (see note 2); Queue position [o]; Request for acknowledgement [m].
MCP D-Reject	Indicates that a request has been rejected	Flow identification [m] (see note 2); Rejection cause; Request for acknowledgement.
MCP D-Info	Provides additional information related to a call	Flow identification [m] (see note 4); Information provided [m]; Request for acknowledgement [m].
MCP D-TX Interrupt	Sent to a talking party to indicate that his transmit permission has been revoked	Flow identification [m] (see note 4); Overridden flow identification [m] (see note 5); Request for acknowledgement [m].
MCP D-TX Ceased	Sent to receiving parties to indicate that the talking party has finished transmission	Flow identification [m] (see note 4); Request for acknowledgement [m].
MCP D-Clear	Informs all parties that a call has been cleared, and that they should return to an out of call state	Flow identification [m] (see note 4); Request for acknowledgement [m].
MCP D-Acknowledge	Sent to acknowledge reception of an uplink message, if a corresponding downlink message is not to be sent immediately	Flow identification [m] (see note 2).

NOTE 1: [m] indicates that a parameter is mandatory in the message, and [o] indicates that a parameter is optional in a message.
NOTE 2: The "flow identification" parameter in the "MCP D-TX Granted", "MCP D-Queued", "MCP D-Reject" and "MCP D-Acknowledge" messages shall match the "flow identification" parameter in the uplink message to which they are responding.
NOTE 3: If present, the value of the "replacement flow identification" parameter shall be used by the MU to identify uplink media flow; otherwise the value of the "flow identification" parameter shall be used by the MU to identify uplink media flow.
NOTE 4: The "flow identification" parameter in this message identifies the downlink flow.

NOTE 5: The "overridden flow identification" parameter in the "MCP D-TX Interrupt " message identifies the uplink flow that is being interrupted.

Table B.2 lists the uplink MCP messages and parameters.

Table B.2: Uplink MCP messages

Message name	Purpose	Parameters
MCP U-TX Demand	Request for transmission	Talking party identity [m]; Target group identity [m]; PTT priority [m]; Flow identification [m] (see note 2); Retention demand [o]; Location information [o].
MCP U-Acknowledge	Response to specific request for acknowledgement that was received in a downlink message	Flow identification [m] (see note 3).
MCP U-TX Ceased	Indication of end of transmission, or cancellation of a queued or not executed call request	Flow identification [m] (see note 4); Talking party identity [m]; Location information [o]; Request for acknowledgement [m].
MCP U-Clear	Request to clear an ongoing call	Flow identification [m] (see note 3); Request for acknowledgement [m].
MCP U-Leave	Request to leave an ongoing call, without clearing it	Flow identification [m] (see note 3); Request for acknowledgement [m].
MCP U-Info	Provides additional information from that user	Information provided [m]; Request for acknowledgement [m].
MCP U-Resume	Request to resume unicast downlink delivery	Flow identification [m] (see note 3); Location information [o].
MCP U-Stop	Request to stop unicast downlink delivery	Flow identification [m] (see note 3); Location information [o].
NOTE 1: [m] indicates that a parameter is mandatory in the message, and [o] indicates that a parameter is optional in a message. NOTE 2: Proposed identifier for requested uplink flow. NOTE 3: Downlink flow identifier. NOTE 4: Proposed or actual uplink flow identifier.		

Table B.3 describes the parameters used in downlink and uplink MCP messages.

Table B.3: MCP message parameters

Parameter	Downlink or uplink use	Description
Call duration	Downlink	Remaining time in the call (can include "infinite")
Current call priority	Downlink	Priority of the current call with respect to other ongoing calls
Flow identification (see note)	Downlink	Identity of media flow to which message refers
	Uplink	MCP U-TX Demand: flow identifier which MU proposes to use for uplink media MCP U-TX Ceased: flow identifier which MU has been using (or proposed to use if transmit permission has not yet been granted) for uplink media MCP U-Acknowledge: flow identifier provided in the downlink message that this uplink message acknowledges MCP U-Clear, MCP U-Leave, downlink flow identifier in use in call which MU will clear or leave
Information provided	Uplink	Information provided
	Downlink	Information provided
Location information	Uplink	Location information relating to transmitting MU
Media parameters	Downlink	Description of media for the forthcoming call
Overridden flow identification	Downlink	Uplink flow identifier of media stream which has been overridden, and so will cease
Pre-emption capability	Uplink	Requested allowability of being pre-empted (binary: yes/no)
PTT priority	Downlink	Priority of the current transmission of the talking user
	Uplink	Requested priority of this transmission
Queue position	Downlink	Position in transmit queue
Rejection cause	Downlink	Reason for transmission request rejection
Replacement flow identification	Downlink	Flow identifier to be used for uplink media
Request for acknowledgement	Downlink	Requires that the MU sends an acknowledgement in response
Retention demand	Uplink	MU's request to allow pre-emption or not
Talking party identity	Downlink	CCA individual identity of currently talking party
	Uplink	CCA individual identity of MU sending the uplink message
Target group identity	Uplink	Reference to identity of group to which requests are sent
Transmission duration	Downlink	Granted maximum transmission time (can include "infinite")
Transmission request permission	Downlink	Indicates that another user is or is not allowed to attempt to interrupt an ongoing transmission
NOTE: The flow identification parameter may be used to synchronize the media encryption process so should be non-repeating and different for each party in the call. (The encryption synchronization method is required to be such that a replay cannot occur.)		

History

Document history		
V1.1.1	January 2015	Publication
V1.2.1	June 2017	Publication