ETSI TR 102 022-2 V1.2.1 (2018-01)

User Requirements Specification;
Mission Critical Broadband Communications;
Part 2: Critical Communications Application

Reference
RTR/TCCE-01204

Keywords
evolution, requirements, 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

Important notice

The present document can be downloaded from:
http://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the only prevailing document is the print of the Portable Document Format (PDF) version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status.
Information on the current status of this and other ETSI documents is available at
https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

Contents

Intellectual Property Rights 5
Foreword 5
Modal verbs terminology 5
Introduction 5
1 Scope 7
2 References 7
2.1 Normative references 7
2.2 Informative references 7
3 Definitions and abbreviations 8
3.1 Definitions 8
3.2 Abbreviations 8
4 Critical Communications Application Requirements 10
4.1 General 10
4.1.0 Introduction 10
4.1.1 Description of Interfaces in Figures 1 to 3 12
4.2 Group Addressed Services 16
4.2.0 General 16
4.2.1 Emergency communication 18
4.2.2 Dispatcher Override 19
4.2.3 Local Fall Back 19
4.3 Priority and Pre-Emption Services 20
4.4 Off Network Services 21
4.4.0 General 21
4.4.1 Public Safety Specific Requirements for Off Network Services 21
4.4.2 Local network Extension 22
4.5 Calling/Talking Party Identity Restriction 23
4.6 Interoperability with Legacy Systems 23
4.7 Support for White Boarding and other Multi-Media Operations 24
4.8 Dispatching - a Video Case 24
4.9 Video Briefing 24
4.10 Net Preference 24
4.11 Dual Watch 24
5 Voice Requirements 24
5.0 General 24
5.1 Intelligibility in Noisy Environments 25
5.2 Call Set up Time 25
6 Security 25
7 Priorities for Functionality 25
8 Summary of Baseline TETRA and Tetrapol Services and Exceptions to their Transfer to Broadband Requirements (adopted from TETRA04(13)000074r2-Use-of-TETRA-services) 29
Annex A: Functionality Split Proposal for Group Addressed Calls from 3GPP (Preliminary view) 34
Annex B: Visualization of Relay Node Use 36
Annex C: Possible Progression of Interoperability Requirement 38
Annex D: Extract from 3GPP TS 22.278 V12.4.0 (2013-09) 41
Annex E: Requirements from Project Broadmap 44

History 45

Intellectual Property Rights

Essential patents

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.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

Foreword

This Technical Report (TR) 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 the User Requirement Specification (URSs) Mission Critical Broadband Communications, as identified below:

Part 1: "Mission Critical Broadband Communication Requirements";

Part 2: "Critical Communications Application".

Modal verbs terminology

In the present document "**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.

Introduction

The Terms of Reference for TC TCCE approved at ETSI Board meeting #42, 2013 is to produce ETSI deliverables (and maintenance thereafter) in accordance with the following requirements:

a) To identify requirements for mission and business critical broadband services that will enable an evolution of digital narrowband PMR services to mobile broadband.

b) To identify and fill standardization gaps such as:

   1) Architectural design of critical communications services to be delivered over mobile broadband systems.

   2) The development of standards for secure services and interfaces into private and commercial broadband systems.

   3) Interconnection of external PMR interfaces to critical communications systems.

c) The provision and development of proportionate security measures for TETRA and mission critical communications services.

d) The selection and development of suitable CODECs for audio and video services.

e) The evolution and enhancement of TETRA and critical communications services as required by the market with the provision of new services, facilities and functionality made possible by new technology innovations and standards.

f) To identify requirements for the further development of the TETRA standard.

g) The maintenance of the TETRA standard.

Technical Objective:

- The present document provides the User Requirement Specifications for the Critical Communications Application that facilitates digital PMR services over LTE™.
- The URS is required by TC TCCE to guide the design of the critical communications application to facilitate broadband voice and data communications for critical communications users.

1 Scope

The present document provides the User Requirement Specifications for the Critical Communications Application needed to support Broadband Mission Critical Communications over IP communications networks such as LTE.

The present document describes the functionalities which are most needed by users and the requirements they make on the technology. The present document is applicable to the specification of broadband mission critical communications equipment.

The user requirements contained in the present document are described in non-technical terms and are based on discussions in TC TCCE WG1, TC TCCE WG4, LEWP RCEG and TCCA's CCBG SA and UR Groups.

2 References

2.1 Normative references

Normative references are not applicable in the present document.

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 TS 122 468 (V12.1.0): "LTE; Group Communication System Enablers for LTE (GCSE-LTE) (3GPP TS 22.468 version 12.1.0 Release 12)".

[i.2] ETSI TS 122 278 (V12.5.0): "Universal Mobile Telecommunications System (UMTS); LTE; Service requirements for the Evolved Packet System (EPS) (3GPP TS 22.278 version 12.5.0 Release 12)".

[i.3] ETSI TR 102 022-1: "User Requirement Specification; Mission Critical Broadband Communication Requirements".

[i.4] NPSTC Recommendations for Push To Talk over Long Term Evolution Requirements, Public Safety Broadband. A NPSTC Public Safety Communications Report.

[i.5] ETSI EN 300 392-9: "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 9: General requirements for supplementary services".

[i.6] ETSI EN 300 392-12 (sub-parts 1, 3, 7, 8, 10, 16 and 22) : "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 12: Supplementary services stage 3".

[i.7] 3GPP TS 22.278 (V12.4.0): "Service requirements for the Evolved Packet System (EPS)".

[i.8] Proximity-based Off Network Public Safety Use Case S1-113165 to 3GPP TSG-SA WG1 from NIST et al.

[i.9] Requirements associated with Public Safety Off Network Use Case S1-113165 to 3GPP TSG-SA WG1 from NIST.

[i.10] Tetrapol Specifications PAS 0001-1-2 (V3.0.1): "Part 1: "General Network Design: Part 2: Voice and Data Services in Network and Direct Mode".

[i.11] WG4 WI DTR/TCCE-04186: "TCCE Critical Communications Architecture Reference Model".

[i.12] ETSI EN 300 392-1 (V1.4.1): "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 1: General network design".

[i.13] TETRA04(13)000074r2-Use-of-TETRA-services (Work in progress for ETSI TCCE04).

[i.14] "Finlands 5 Steps to Critical Broadband", Vinkvist, Pesonen and Peltola, Radio nResource International Q4 2014.

3 Definitions and abbreviations

3.1 Definitions

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

Base Station (BS): set of equipment on a single site (which may be more than just a radio function)

mission critical broadband communications: work programme within ETSI Technical Committee TETRA and Critical Communications Evolution to facilitate and enhance the services and facilities of digital PMR such as TETRA operating over LTE in order to meet new user requirements for data and voice

3.2 Abbreviations

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

AL	Ambience Listening
ASSI	Alias Short Subscriber Identity
AVL	Automatic Vehicle Location
BS	Base Station
CA	Conventional Access
CCA	Critical Communications Application
CCBG	Critical Communications Broadband Group
CCS	Critical Communication System
CLIR	Calling Line Identification Restriction
COMM	Common
DA	Direct Access
DGNA	Dynamic Group Number Assignment
DISC	DISCovery

NOTE: Not in the ETSI list.

DMO	Direct Mode of Operation
DTMF	Dual Tone Multi Frequency
EPC	Evolved Packet Core
ETSI	European Telecommunications Standards Institute
E-UTRAN	Evolved Universal Terrestrial Radio Access Network
FFS	For Further Study
GCSE	Group Call Service Enablers
GPS	Global Positioning System
GSCE	Group Communication System Enablers
IP	Internet Protocol
ISI	Inter System Interface
KPI	Key Performance Indicator
LEWP	Law Enforcement Working Party
LMR	Land Mobile Radio
LTE	3GPP Long Term Evolution (4G)
MC	Mission Critical
MCPTT	Mission Critical Press to Talk

ME	Mobile Equipment
MM	Mobility Management
MS	Mobile Station
MU	Mobile Unit comprising UE plus CCA
MVNO	Mobile Virtual Network Operator
NIST	National Institute of Standards and Technology (USA)
NPSTC	National Public Safety Telecommunications Council (not in the ETSI list)
OPS	Operations
PABX	Private Automatic Branch eXchange
PMR	Private Mobile Radio
PPDR	Public Protection and Disaster Recovery
ProSe	Proximity Services
PSTN	Public Services Telephone Network
PTT	Press to Talk
QoS	Quality of Service
RCEG	Radio Communications Experts Group, a working group of LEWP
RF	Radio Frequency
SA	System Architecture

NOTE: Technical Specification Group of 3GPP.

SDS	Short Data Service
SDS-TL	SDS-Transport Layer
SIM	Subscriber Identity Module
SLA	Service Level Agreement
TA	Tracking Area
TCCA	TETRA + Critical Communications Association
TCCE	TETRA and Critical Communications Evolution
TL	Transport Layer
TPI	Talking Party Identity
TR	Technical Report
UE	User Equipment
UR	User Requirements
URS	User Requirement Specification
USIM	Universal Subscriber Identity Module
UTRA	Universal Terrestrial Radio Access
UTRAN	Universal Terrestrial Radio Access Network

4 Critical Communications Application Requirements

4.1 General

4.1.0 Introduction

In order to ensure that IP communications networks such as LTE are able to meet the requirements of critical communications some changes to the 3GPP™ standards are needed. The most critical have been proposed first and are called Group Communication System Enablers (GCSE) [i.1] and Proximity Based Services (ProSE) [i.2]. These have resulted in 3GPP Work Items for Release 12. There are likely to be further requirements. In order to benefit from the market scale available for public LTE and the attendant benefits such as lower cost, open standards, supplier choice, fast development of features and long term evolution of capability the changes proposed to date have been kept to a minimum to improve the chances of them being implemented by manufacturers. This means that to deliver the full mission critical/critical communications functionality there has to be a Critical Communications Application (CCA) that sits above the LTE protocol. This application will need to provide the services required for critical communications [i.3]. (One of these services is push or press to talk, and NPSTC have recommended requirements for Public Safety in the US [i.4]. Outside of North America the PTT voice functionality of TETRA [i.5], [i.6], [i.12] and Tetrapol [i.10] is taken as an assumed baseline on top of which further functionality appropriate to broadband is added. To avoid describing all the many standards a summary of this functionality and the exceptions, that is baseline functionality not needed in broadband are listed in clause 8). The application will need to have implementations in the infrastructure and in terminals with a standardized interface between them so that different vendors can be used.

It is important that the standardization of the CCA should be rapid and co-ordinated to match planned releases of the 3GPP standard containing the appropriate enablers. A phased approach is considered but whilst most user groups want to focus on data services there are some groups, for example in the UK working on their future mission critical communications, who want to rapidly transition to voice services as well. This means that the first release of the CCA has to support core voice and data requirements with extensions in functionality coming in later releases.

There are different needs for supporting migration away from legacy systems depending on the plans in the various user groups for the rate of migration. Some users groups see little need to operate with legacy systems and others see a sustained period of inter-working. The level of interoperability required also varies but there is clearly a need for the first release of the CCA to support some interaction with legacy systems with fuller integration coming later for those who wish to operate their legacy systems for voice and narrowband data for a longer period alongside broadband data or voice and data systems. This is dealt with in more detail in clause 7.

Some thoughts have been given to the partition between functionality to be supported in 3GPP and that by the CCA (annex A). This led to a model of the architecture for Mission Critical Broadband Communications from TCCA CCBG WG SA that defined the requirements of the CCA. This model is being developed in TCCE WG4 [i.11] and a version of this is shown below purely to illustrate the scope of the requirements to be addressed. This diagram will not be updated in this URS.

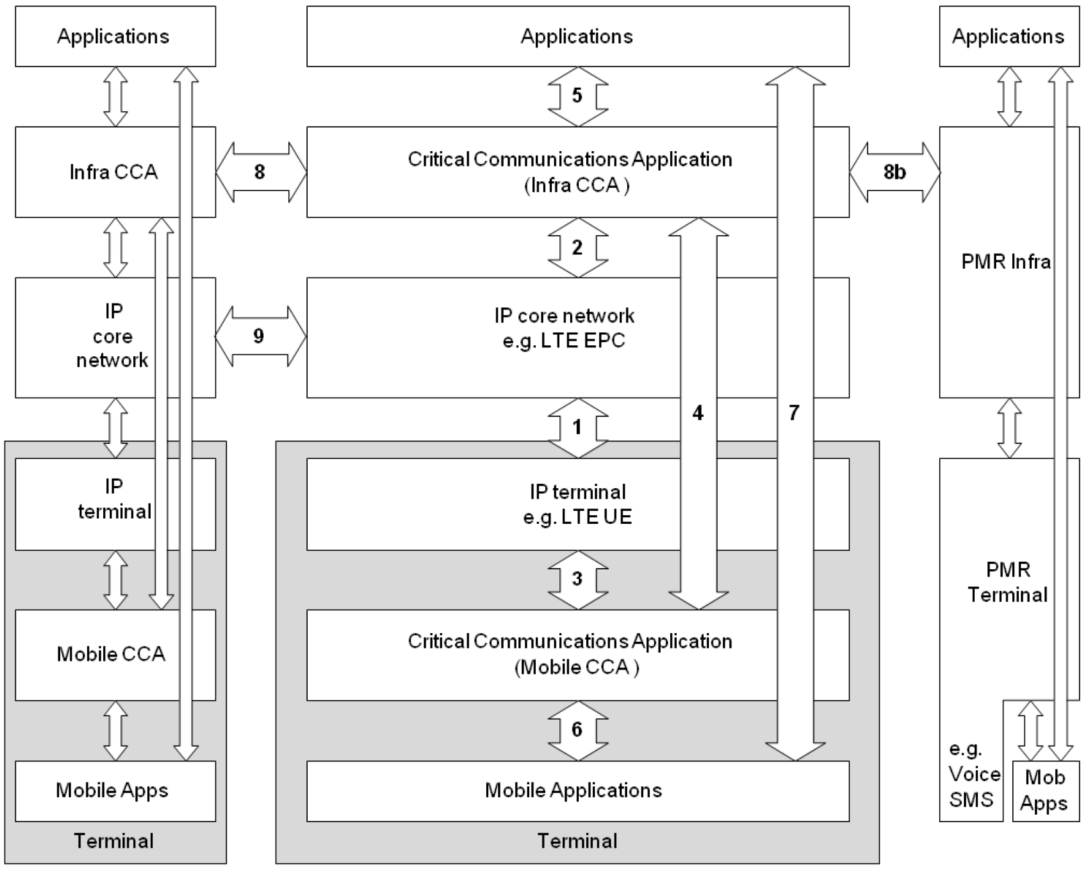

Figure 1: CCS Reference Model

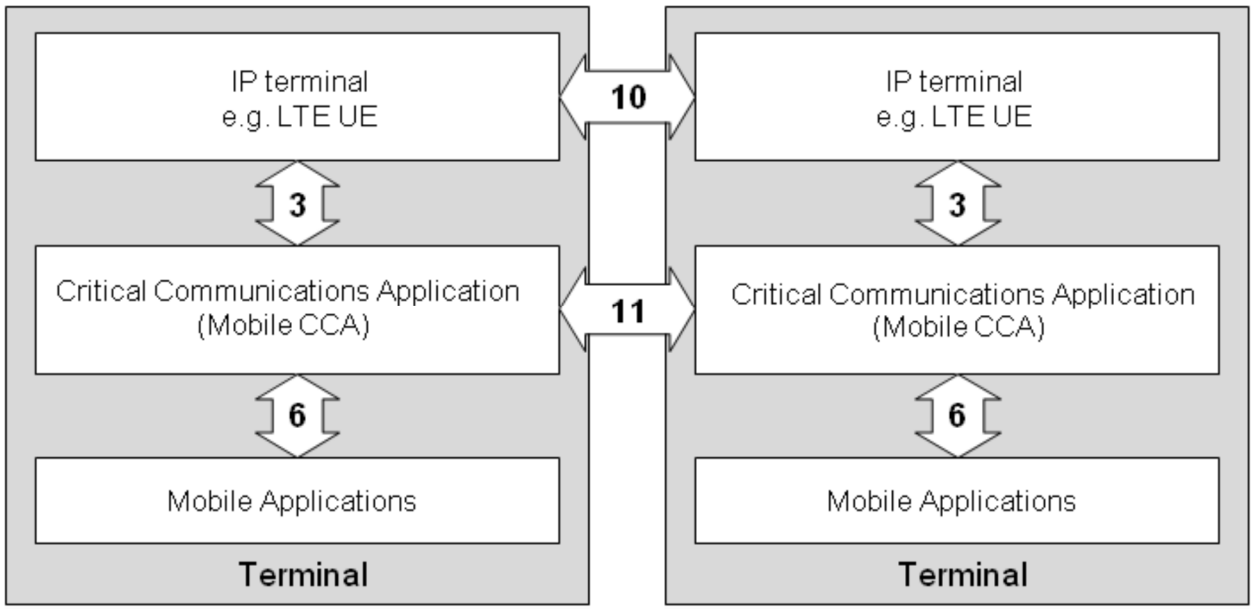

Figure 2: Proximity Services Reference Model

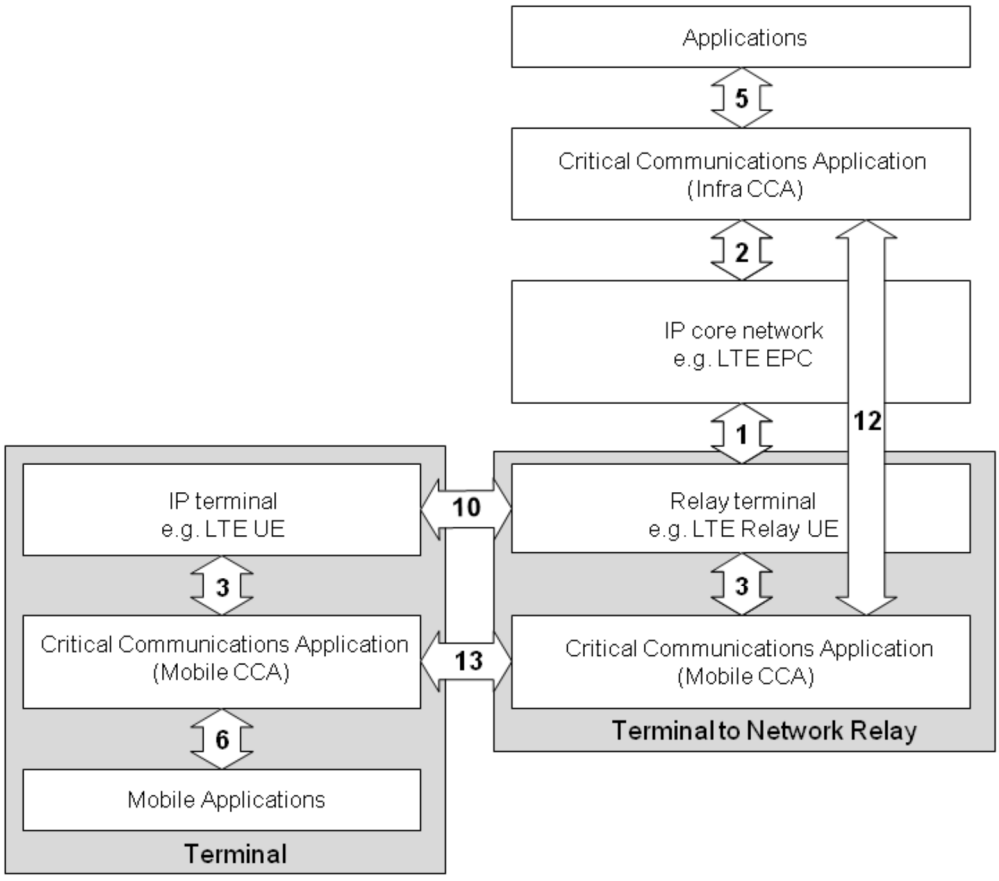

Figure 3:Terminal to Network Relay Reference Model

4.1.1 Description of Interfaces in Figures 1 to 3

Interface 1 LTE Core Network - UE

This interface is specified according to the network protocols of the underlying IP network. Where the underlying network is LTE, it consists of the 3GPP specified standardized LTE UE to EPC interfaces.

Interface 2 Infra CCA - LTE Core Network

This interface is specified according to the network protocols of the underlying IP network.

Where that underlying network is an LTE EPC, it consists of existing Rx and SGi interfaces, plus the GC2 interface developed in the GCSE-LTE work item from 3GPP Release 12, to allow use and control of LTE broadcast bearers.

Interface 3 LTE UE to Mobile CCA

This interface relies on the services available from the IP network terminal.

In an LTE environment, it utilizes the interfaces provided by the UE to any application and may evolve to include developments related to GCSE-LTE work item from 3GPP Release 12.

This interface itself is not fully standardized since it is dependent on the terminal implementation and operating system.

Interface 4 Infra CCA to Mobile CCA

The objective of this interface is to allow interoperability between a CCA infrastructure and terminals from different manufacturers.

This interface provides similar functionality to existing digital PMR Layer 3 Air Interface messages, supporting, but not limited to, user registration, setup and control of individual and group communications, media transfer and management and short data transport.

Interface 5 Infra CCA to Application

The objective of this interface is to allow easy integration of Applications in a CCA environment, and portability of those applications to CCAs from different manufacturers.

This interface is made of two main components:

- A Call interface, to provide control of sessions (C-Plane) and of media transport (U-Plane) within a communication. This interface may be similar to a Dispatch interface in existing PMR systems, extended to Multimedia.

NOTE 1: A single communication session can be an organized set of one or more communications used to transport the same information to or from one or several mobiles. Independent sessions implies that there can be several separate communications taking place between different sets of parties which can be accessed through this interface.

- A Routed Transport interface to transport and route data messages (e.g. signalling, geo-location information, text messages) and data files (e.g. picture, map) between mobiles and applications.

Interface 6 Mobile CCA to Mobile Application

The objective of this interface is to allow easy integration of Mobile Applications in a CCA environment, and portability of those applications between terminals from different manufacturers.

Interface 7 Application to Mobile Application

Some components of this interface may be defined by standards, for specific applications that require generic formats to ensure interoperability between mobile applications and control room application for instance: geo-location, video format, vocoder, etc.

Interface 8 Inter CCA

The objective of this interface is to allow interoperability and interworking between CCS.

This interface supports interconnection of communications between users operating on different CCS.

This interface should support mobility of users between different CCS.

Interface 8b CCA to Legacy PMR

The objective of this interface is to allow interworking between a CCS and existing legacy PMR systems such as TETRA, TETRAPOL and P25.

This interface is intended to support interconnection of communications between users operating on a CCS and on a legacy PMR system.

Interface 9 Core Network to Core Network

This interface is determined by the underlying core IP network. Where the underlying network is an LTE EPC, it makes use of 3GPP standard interfaces.

This interface provides support and control of mobility and roaming of terminals between different core networks.

NOTE 2: Where the underlying core networks use different technologies, a standardized interface may not be available.

Interface 10 Terminal to Terminal

This interface is determined by the terminal technology.

Where the terminals are LTE Ues, this interface will be a standard 3GPP interface, defined under the Proximity Services (ProSe) work item in 3GPP Release 12.

This interface supports direct communications between terminals and also the terminal to Network Relay configuration.

Interface 11 Mobile CCA to Mobile CCA

The objective of this interface is to provide control of direct CCA Services between two or more terminals without any infrastructure path. Where the terminals are LTE Ues, it relies on underlying services defined by 3GPP ProSe.

Interface 12 Infra CCA to Relay CCA

The objective of this interface is to support the specific configuration of a Terminal to Network Relay. This interface can be considered to be a subset of the interface 4 Infra CCA to Mobile CCA.

Interface 13 Mobile CCA to Relay CCA

The objective of this interface is to support the specific configuration of a Terminal to Network Relay. This interface can be considered to be a subset of the interface 11 Mobile CCA to Mobile CCA.

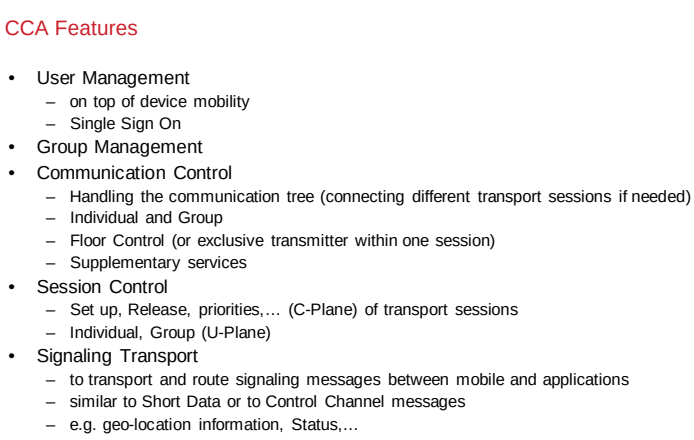

Figure 4: Critical Communications Application Features

The CCA then is broadly being asked to:

For Systems:

- Interface to legacy systems (TETRA, P25, Tetrapol) to allow a degree of interoperability. Is it assumed 3GPP will manage the fallback from 4G to allow interoperability on a best efforts basis with 3G.
- Interface to other CCAs in the same or other networks. The intent is that initial CCA core functionality will be standardized and that further functionality will be defined for subsequent releases that will in part depend and be aligned with supporting feature releases from 3GPP.
- Interface to other LTE systems to allow roaming. There are two types of roaming to be supported; where 'LTE roaming' is utilized (i.e. the user device is provided with an IP link back to their serving CCA via the roaming networks), and application level roaming where the MU registers onto a visited CCA and communicates with users there (interface 8 on the architecture reference model).
- The system (including the CCA) should support an Inter System Interface (ISI) for roaming of home subscribers to other neighbour networks. It supports full dynamic subscriber migration.
- Group handling.
- Call control.
- Manage Priorities.
- Interaction with other 3GPP services.
- Performance management.

For LTE:

- Interface to EPC to allow GCSE and other services to be managed.

For Applications:

- Allow portability of different suppliers applications on the CCA.

For Mobiles:

- Interface to mobile CCA to allow
- Control access
- Manage groups
- Establish sessions for group communication between mobiles
- Manage priorities
- Transport and route signalling messages between mobiles and applications

In order to detail these requirements of the CCA the features that it needs to support today or for the future are described below.

4.2 Group Addressed Services

4.2.0 General

This is the classic public safety and PMR situation whereby one addresses many in a voice or data call and it has the following detailed requirements:

- The group call application should be able to allow or bar MU access to each group.
- When the user selects a group, the MU should request access to the group and the MU should inform the user whether access is granted or not. There is also a need for infrastructure directed attachment.
- There should be an indication to the user if they are the only one on the group [i.4]. This indication to be given at call time rather than attachment time. If a dispatcher is a member of the group and on the call then the indication does not need to be made.
- Recipients of the call should receive an indication of the identity of the talking party.
- Subject to configuration and PTT priorities of the Group members, the system should be able to permit or deny a second party to interrupt the talking party. If interruption is successful, both original and new talking parties should receive an indication of their new state.
- For North America there has to be the ability to listen to both overriding and overridden calls [i.4].
- Once the current talking party has ended the transmission, another member of the group may request to transmit to the group. The delays associated with the changeover should be no greater than the delays associated with the original call setup.
- An MU should be able to join a group whilst a call is ongoing.
- Depending on the system configuration, if resources are not enough for all group members to receive the call, calls can either be:
  - queued, and the call should be set up once resources are available; the requesting party should receive an indication of both the initial queued condition, and the granting of transmit permission once resources are available; or
  - continued with parties whose serving cells have enough resources to support the call.

  These are sometimes known as "all start" and "fast start" respectively. For fast start it should be clear to the talking party that some group members will not hear.
- If a call can start without all available parties, then those parties should be added to the call as soon as sufficient resources become available.
- An MU should support access to in excess of 5 000 groups. This can include groups that have been dynamically downloaded over the air to reduce the number that have to be continually available on the terminal. The system should be able to handle in excess of 500 000 groups.
- The system should be capable of managing different types of media for the same group with the same priority level and same coverage (where coverage is all used cells with RF range).
- The system should be capable of managing independent floor controls for concurrent communications within a given group for different types of media.
- For all calls including video briefing (one to a large group) the system should be capable of providing information to a dispatcher on the participants of a group call.
- It should be possible to share video without forcing it to be taken by sending a message that video is available and the user pulling it when they are ready. The intent of this is a "notify and pull" approach probably with a time validity given with the message such as "take by(next hour) with today's date" or "(specified hour) next day" etc. There is a possibility that an acknowledgement to the notification may be needed with a time to co-ordinate a later group push to avoid lots of individual calls.

- A "push" service where the user elects to accept the video or not is also considered a (lower priority) requirement. A group "push" service in general with no option to decline is a requirement.

- Two further elements are functional addressing, which is addressing roles rather than radios or aliases, and location dependant addressing, where the address of the controller (dispatcher) changes as an MU moves through the network.

The following requirements have implications for the 3GPP domain as well as the application domain:

- When an authorized user sets up a call to the group, he should receive an indication of success (or failure) within 300 ms of the call setup, and recipients of the call should receive an indication of the start of the call within 300 ms of the originator's call setup. For clarity the start of the call is measured from PTT press.

- Audio should be conveyed from the transmitting party to all recipients with minimal delay. There should be no noticeable difference in audio delay experienced by recipients on the same cell.

- Resources should be allocated efficiently, such that many recipients may share the same resources for the call.

- A group can have any number of members from 2 up to the total number of users on a system. Within a cell where there is a user who can use that group, the number of users can range from 1 up to the total number of users on that cell.

- Groups can be carried on any number of cells from 1 up to the total number of cells on the system. The system decides how many cells are needed based on the presence of users.

- There is a special requirement known as a "ringing group call" that is initiated in the field or by a dispatcher where there is a need for the recipients to act in concert in an operation and so it is important to know who has acknowledged the call and is going to participate. For this to work there has to be a fast acknowledgement process and a listing displayed of all those who will participate. This need is further detailed in clause 4.2.1.

- The system should support mobility for MUs transmitting and receiving a group call. Transmitting Mus should retain transmit permission after a mobility event. There should be minimal loss of audio, video or other data due to the mobility event.

- Mobility events such as handovers between cells should meet the requirements above for MUs moving at speeds between 0 - 300 km/hr, ideally 500 km/h.

- A cell or sector should be able to support a number of simultaneous group calls. By way of guidance most needs could be met if this number was at least 36.

- Similarly a cell or sector should be able to support a large number of users participating in different group calls. If at least 2 000 users could be supported it would meet anticipated requirements.

- The system needs to support the dynamic addition of groups to MUs over the air to allow groups to be configured with appropriate talkgroups as they move location and/or attend incidents.

- It may occasionally happen during events or incidents that 500 users or more within a cell or sector may be participating in the same group. When whatever the upper limit of the system is reached it is permissible to reject the next user beyond the stated capacity. The user who has been rejected due to this should receive a message stating "overload" or "congestion" as the reason for rejection. No ongoing call should be interrupted due to the stated capacity being exceeded.

- The system should be capable of setting up several communication paths concurrently and independently for the same set of devices. In general this will apply to different services but for the override situation where the overridden voice call still needs to be heard as well this will apply to speech. There are other use cases such as communications up and down organizations where concurrent speech calls are required.

- There is a need for groups to be managed dynamically over the air.

- The system should support patching to allow a call to be sent to more than one group.

4.2.1 Emergency communication

This is where in an emergency situation a user needs to send an emergency message for assistance. This is normally an alarm which is a predefined change of status tagged with location but conceivably can be voice text or video. The derived requirements are:

- The MU should send an Emergency Alarm with pre-emption when the Emergency Button (or similar feature that is easy to locate even in the dark, single functioned and with positive tactile feedback) is pushed on an MU. This emergency alarm should include user id and location.

- The System should route the Emergency Alarm to the Dispatchers associated with the Group of the MU in Emergency and to the Dispatcher associated with the agency of the Unit in Emergency. This information is part of the agency and group provisioning of the System.

- There are situations such as when emergency gateways or dispatchers who are connected via an MU are used that individual rather that group calls are required.

- For rail use the system supports the Railway Emergency Call. This is a pre-emptive group call which is initiated from a mobile and involves both the controller (dispatcher) and all relevant users in the local area of the call originator.

- The Emergency alarm is normally followed by a Emergency call from the Unit in Emergency, giving details about the actual emergency. For this call the System should apply an Emergency Priority which is the highest priority for resource allocation and retention. Any communication with an Emergency Priority should pre-empt resources from existing non-emergency communications if needed.

- There are various requirements regarding the termination of emergency calls. They include termination by the dispatcher, termination by the end user or a pre-programmed time out. All of these should be supported individually or in combination.

- The MU should support the Ambience Listening feature.

- There should be the facility to allow a professional user to create or share any type of emergency call with the members of a Group including the dispatcher. The situation where the create capability might be needed is if the user in an emergency cannot push the emergency button and another user initiates the call on that user's behalf. The sharing could arise when another group or individual who could help need to be patched into the call.

- Some group communications should be able, as they are established, to ring all their authorized MUs, even if those MUs are already participating in another communication. Those MUs are so alerted that an emergency communication is ongoing and that they are invited to participate.
  Such "ringing group" communications:

  - should have the same characteristics as any normal group communication (number of MUs or group of Mus, number of supported eNodeB, etc.);

  - should have a particular ringing tone (may be defined as a parameter);

  - only ring at the establishment.

  In case an MU is switched on after the ringing group call establishment, and if this ringing group communication is always opened, the MU should be notified of the ringing group communication without being ringed.
  An MU should be able to accept or refuse to enter a ringing group call.

- For North America there is a need to recognize a second level of priority for Imminent Peril calls. (Situations which are not yet an emergency but are at high risk of becoming so). Such calls can be pre-empted by an emergency call. Specifically [i.4]:

  - The PTT Service SHOULD support imminent peril calls.

  - The PTT Service SHOULD ensure that emergency and imminent peril calls have the highest priority over all other PTT Group transmissions.

- The PTT Service SHOULD provide a mechanism to ensure that emergency and imminent peril calls, including their content and signalling, have pre-emptive priority over all other types of PTT Group transmissions.

- The PTT Service SHOULD support emergency calls that persist until being acknowledged and terminated based on criteria created by a Public Safety Entity Administrator.

4.2.2 Dispatcher Override

This is where a dispatcher decides to override communications to a group to share information. The derived requirements are:

- The system should manage a priority level **within a group** associated with each member of the group **for floor control** in an active communication.

- There should be four (4) different priority levels for floor control.

- The system should support a pre-emptive priority level within a group for floor control in an active communication.

NOTE: Those priorities are only intended for floor control within a communication and are distinct from the communication priorities which are intended to arbitrate resource allocation between communications.

- The highest priority could be available to both a wired user (Conventional dispatcher) or a MU configured as a dispatcher. The latter will need support to have the highest possible resources available at all times.

- The system should be able to stop an ongoing MU transmission to a group.

- For North America the system should permit [i.4]:

  - When an authorized user overrides a PTT Group transmission, authorized users SHOULD be able to listen to both the overriding and overridden PTT Group transmissions.

  - When an authorized user overrides a PTT Group transmission, a Public Safety Entity Administrator SHOULD be able to configure which PTT Group transmission a user receives, overriding and/or overridden.

  - When an authorized user overrides a PTT Group transmission, the PTT Service SHOULD provide a means of notifying the overridden talker that the transmission has been overridden.

4.2.3 Local Fall Back

When through accident or intent an MU cannot connect to any base station that is connected to the network it should be able to temporarily fall back into operating on the local base station or isolated group of base stations only in a fall back mode with restricted services. The requirements of this are:

- If disconnected from the Central Switching Network a base station or group of interconnected base stations should ideally be able to provide local multimedia and data communications to all users under the coverage of the Base Station(s). As a minimum group voice services should be supported for each organization using the local base station(s).

- When the base station goes into the disconnected state, it may disconnect all calls in progress, or it may maintain calls already in progress between users under the coverage of that base station.

- While in the disconnected state, the base station should provide an indication of local area service only to all users under its coverage.

- Once in the disconnected state, the base station should allow users under its coverage to set up and maintain multimedia and data calls with other users under this same base station.

- The normal addressing of users and groups needs to be continued in Fall back mode (implies some part of the CCA needs to be supported in some way in the total equipment at the BS).

- Only critical communications users should have access to a base station in fall back mode.

- Whilst in the disconnected state, the base station should maintain an appropriate level of communications security, including encryption. This should include a check of authenticity of served users, which may be implicit.
- In the disconnected state, the base station may provide a list of served users and/or served groups to all users under the coverage of the base station. Lists may be restricted according to security policy, for example information on users and/or groups within a served user's organization may only be provided to that served user, and information on users may only be provided to other users within the same group.
- When the link becomes available again, the base station should automatically reconnect to the Central Switching Network.
- When it returns to the connected state, the base station should withdraw the local service indication to users under its coverage, and may provide an explicit notification of wide area service.

4.3 Priority and Pre-Emption Services

In order to gain priority of access over other users or to pre-empt existing users on the system there has to be a protocol to access and use the system that allows this to occur.

The following requirements apply to the 3GPP layer and to the Application layer:

- The system should support at least eight different priority levels and probably as many as thirty. The reason is that priorities will need to be set by user, type of communication, application and event for each organization supported and relative to each (i.e. a matrix of relative priorities) plus some dynamically allocatable priority.
- The system should support pre-emption, that is the ability to have immediate access over other users (not moving to first in queue but getting straight in).
- The maximum system priority level will be reserved for Emergency calls, e.g. those activated via the MU's emergency button or through some other means.
- In general priority will be set by the user group but there should be a user group selectable capability for individual users to be able to manually set their own call priority for group or individual calls.
- At times of resource congestion, the system should be able to allocate available resource and maintain QoS to the Point-to-Point or Point-to-Multipoint session on the basis of higher priority first. When sufficient resources are not immediately available a means to queue data sessions should be provided.
- At times of resource congestion, for any session having the highest priority level the system should be able to trigger one of the following:
  - the degradation in quality of lower priority sessions;
  - the commencement of queuing for lower priority sessions when the session is a real time data session;
  - termination of lower priority sessions.
- The prioritization of an individual communication will depend on a combination of the MU, the End User ID, Group, type of communication, application, event, and Point-to-Point data flow type. To allow this, the system will enable:
  - An authorized public safety user to assign a priority to each of the public safety MUs used by their organization. Each Individual MU will only have one priority level assigned to it at any one time.
  - An authorized public safety user to assign a priority to each of the public safety End User Ids within their organization. Each End User ID will only have one priority level assigned to it at any one time.
  - An authorized public safety user to assign a priority to each of the public safety Groups used by their organization. Each Group will only have one priority level assigned to it at any one time.

  - An authorized public safety user to assign different priorities to different Point-to-Point public safety data application within their organization .e.g. Voice, email, file sharing, video, remote control, telemetry, browsing etc. Each Point-to-Point public safety data flow types will only have one priority level assigned to it at any one time.

  - An authorized public safety user to assign a priority to Point to Point data flow types which would normally be classed as best effort data.

  - An authorized public safety user or command and control system to dynamically change priority settings for individual public safety Mus, End User Ids, Talk Groups and Point-to-Point data flow types in advance of and during public safety incidents. The new priority settings will take effect immediately for new and ongoing sessions.

- Upon initiation of a session by a public safety user the application layer will determine the appropriate priority that will be used for that session in the event of Priority Arbitration, as being the Higher of:

  - the End User ID priority setting if it is available, if not then the MU priority setting; or

  - the priority setting of the appropriate session type, Point-to-Point, Point-to-Multipoint or Distress Call.

- The system should provide an indication on the Public Safety MU that its allocation of resource has been queued.

- The system should provide an indication on the Public Safety MU that its allocation of resource has been pre-empted. If this happens in one cell of a group call there should be two configurable options, end call or continue in others with the current talking party being informed in the latter case.

- For North America the system should permit [i.4]:

  - When an authorized user overrides a PTT Group transmission, authorized users SHOULD be able to listen to both the overriding and overridden PTT Group transmissions.

  - When an authorized user overrides a PTT Group transmission, a Public Safety Entity Administrator SHOULD be able to configure which PTT Group transmission a user receives, overriding and/or overridden.

  - When an authorized user overrides a PTT Group transmission, the PTT Service SHOULD provide a means of notifying the overridden talker that the transmission has been overridden.

4.4 Off Network Services

4.4.0 General

Where it is not possible or desirable to connect to the network public safety users need the ability to operate terminal to terminal in "walkie-talkie" mode for voice and data. This facility is called Direct Mode Operation in PMR parlance. It is proposed that in LTE proximity services (ProSe) is used. Terminals operating in this mode should be able to work with relays to extend coverage. In PMR parlance the extension of range in DMO can be achieved by a repeater and connection back to the network (extending the coverage of the network) by a gateway.

4.4.1 Public Safety Specific Requirements for Off Network Services

Whatever technology is used authorized public safety terminals should be able to exchange voice and data directly with others without use of the network. This may even be required if there is network coverage.

Requirements were proposed by TCCA CCBG SA as part of their use case development and input into 3GPP the response has been 3GPP TS 22.278 [i.7] which is the normative source. The relevant sections are shown in annex D.

The need is to be able to make secure calls for authorized users without use of the network to individual users or groups of users. These calls should authenticate users, will need to be encrypted and support voice and data transfer. It is understood that the range that this can be achieved over depends on a number of variables including the terrain, the nature of interfering materials, the power of the Ues, the weather and the package size of data being transferred. It is therefore desirable that users are aware of the proximity of other users with which they can communicate and when they are going out of range of such off network services. In order to set some level of expectation and recognize the changing range with data rate/application one country has proposed normally a 3 - 5 km line of site is required and it is suggested that this would reduce to 2 km for critical high speed data and 500 m - 1 km for very high speed data. The range expectation along with other requirements for the US have been proposed by NPSTC and are included below. Elsewhere there are some special needs such as forest fire fighting where ranges of 10 km are needed for line of site communication between elevated platforms.

Where the range needs to be extended it is expected that repeaters (PMR or LMR terminology, relays in LTE) will be available and where network services need to be extended then gateways between MUs operating off network and the network. Where MUs are used as repeaters (relays) they should be capable of being configured as such by the user when required.

Users are used to having dedicated channels for off network calls and it is assumed that there will need to be some allocated spectrum to support this for broadband and that MUs can be configured to access this when required.

The following requirements are based on the use case S1-113165 [i.8] from NIST et al as detailed in their follow up S1-113166 [i.9].

Proximity Communications Requirements

General

[COMM] The direct mode of operation should function if the individual user/device, upon power up, has not attached to a macro network.

[DISC] Discovery should function if the individual user/device, upon power up, has not attached to a macro network.

[DISC] Discovery should be supported in sufficient density to enable both a pedestrian and vehicular mobility model and peer/MU distribution.

Direct Mode - General

[COMM] The direct mode of operation should provide the capability for an emergency message to be transmitted from an individual user/device to all individual users/devices, regardless of group membership.

[COMM] The direct mode of operation should provide an emergency message the highest priority.

[COMM] The direct mode should provide a mechanism to communicate directly between a group of devices in such a manner where delivery of a transmission to the group of devices requires a single, simultaneous transmission.

Proximity System Operational Requirements

Communications - General

[OPS] The operator and authorized users should be capable of configuring individual users/devices into multiple pre-configured and ad hoc user groups while solely in direct mode.

The range to be achieved between communicating devices may vary from several hundreds to thousands of feet (100 m to 1 000 m say).

4.4.2 Local network Extension

There are times when extra capacity needs to be provided locally at an incident. The requirements are:

- A nomadic relay node (that might for example be mounted on a vehicle) that can be moved to an incident area, connect there to a wide area network and provide local coverage and capacity extension.
- Systems support for such a nomadic relay node t in the wide area network.
- Relay node device that provides MU capability simultaneously.

The way in which it is proposed to use LTE Relay nodes to extend coverage or increase capacity at events is outlined visually in annex C.

4.5 Calling/Talking Party Identity Restriction

- Talking Party Identity restriction, i.e. suppression of the talking party identity to provide anonymity, is occasionally required for individual and group calls within the CCA, or in 'ISI-equivalent' calls between CCAs in order to, for example, protect covert users.
- Similarly it can be anticipated that Calling Party Identity Restriction is required, i.e. suppression of the outbound MS-ISDN/telephone number of a mobile unit within a Critical Communications environment, when that mobile unit is engaged in telephone calls routed through the CCA to an external user. This could apply to both PABX and PSTN calls. (Note that CLIR would need to be separately provided for calls routed by the CCA, when compared with calls routed 'normally' as a telephone call through the LTE network, which connects directly to PSTN).
- CLIR and TPI should be customisable on/off for user groups, users and dispatchers . The user has not traditionally had this freedom but it could be considered if this allows the rest of the system to be more standard.
- There needs to be some override to allow identity to be preserved for calls where this is never hidden e.g. 112 calls.

4.6 Interoperability with Legacy Systems

The System should be able to interwork with narrow-band systems such that:

- An MU should be able to communicate by a gateway between systems with devices used in the narrow-band systems.
- An MU should be able to send and receive data (e.g. status messages, text, location, IP data) to/from devices used in the narrowband system.
- An MU should be able to send and receive voice communications (PTT and all advanced voice critical communications services) to/from devices used in narrowband systems.
- It should be possible that an MU and devices used in the narrow-band systems are affiliated (or registered) to the same communication group.
- An MU should be able to send and receive communications (voice and data) that use end-to-end encryption to/from devices used in the narrowband system.
- The System also ensures that the priorities and quality of service of narrowband data applications, and narrowband voice applications when transmitted on the broadband network have a consistent setting with respect to the narrowband system.

The possibilities for interoperability that might be envisaged based on the speed and nature of migration from legacy systems are outlined visually in annex D and further detailed in clause 7 based on surveys of European operators and organizations.

For clarification there is a need for interoperability between different systems both for MUs with roaming and for network to network connectivity. There are likely to be two cases for roaming: using an IP connection provided between the 3GPP networks to obtain CCA services on the home server, and the case where the UE acts as a visitor on a local server in the visited network:

- For North America there are specific requirements for interoperability with legacy systems defined in [i.4].

4.7 Support for White Boarding and other Multi-Media Operations.

Based on the separation between the 3GPP domain and the Application layer, the following requirements apply to the Application layer:

- The system should be capable of managing different types of media for the same group with the same priority level and same coverage.
- The system should be capable of managing independent floor controls for concurrent communications within a given group for different types of media.

4.8 Dispatching - a Video Case

Included as a line in group addressed calls plus.

Based on the separation between the 3GPP domain and the Application layer, the following requirements apply to the Application layer:

- The system should be capable of managing different types of media for the same group.
- The system should be capable of managing independent floor controls for concurrent communications within a given group for different types of media.

4.9 Video Briefing

This is where video/multi-media is pushed to a group to brief them. Covered above.

4.10 Net Preference

Requirement is on 3GPP only.

4.11 Dual Watch

There is a need when in ProSe to monitor for GCSE and be able to switch over. Furthermore:

- The MU should be able to switch between GCSE_LTE and ProSE modes via user interaction with the radio.
- The MU should be able to listen simultaneously to a set of GCSE_LTE and ProSE communications.
- All MU should be able to detect a pre-defined Emergency ProSE call while engaged into GSCE or ProSE mode of communications.

5 Voice Requirements

5.0 General

Covered in group addressed calls to a large extent. The need is for clear, high quality audio in a variety of environments both with an earpiece and without. The audio has to be capable of being sufficiently loud that communications can be understood in noisy environments and when the MU is worn on the waist.

At the same time the audio and user interface has to manage such that the user cannot unknowingly enter a setting that will cause noise induced deafness. Speech quality should be constant over the range of speeds specified for use (0 - 300, ideally 500 km/h). There should be no echo on the voice.

For some situations the user will not want to speak at normal volume into the MU microphone and so there needs to be an adaptive gain control capability for the MU.

5.1 Intelligibility in Noisy Environments

There is a need to be able to make and receive clear communications on an MU when standing adjacent to vehicles with sirens operating and/or helicopters and aircraft with their engines running. For TETRA this was assisted by the use of a specific CODEC and something similar is needed here.

There is also a need to be able to communicate outside in windy conditions without negatively impacting audio quality.

5.2 Call Set up Time

Covered under group addressed calls.

6 Security

The CCA has to address the facilitation of end to end encryption between MUs so that coupled with the air interface encryption of LTE a similar level of encryption to that already available on mission critical communications can be achieved. The algorithms used for encryption should be capable of being upgraded over time to maintain the level of security.

7 Priorities for Functionality

At the TCCA CCBG meeting in Amsterdam in June 2013 attendees were asked what their priorities for functionality were given that there would probably be a phased release. The questions posed are summarized in figures 5 and 6.

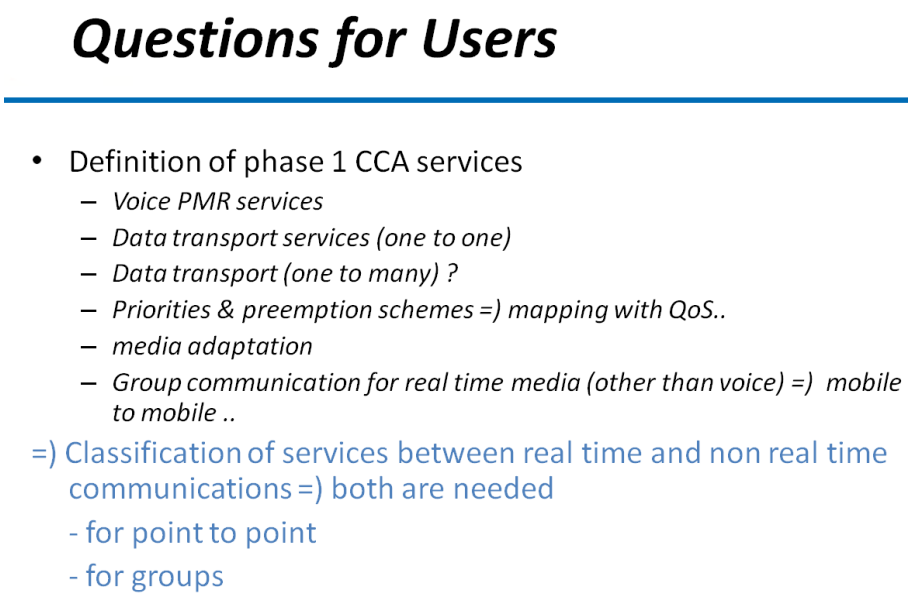

Figure 5: Questions for Users (slide 1 of 2)
(extract of slides with the consent of TCCA)

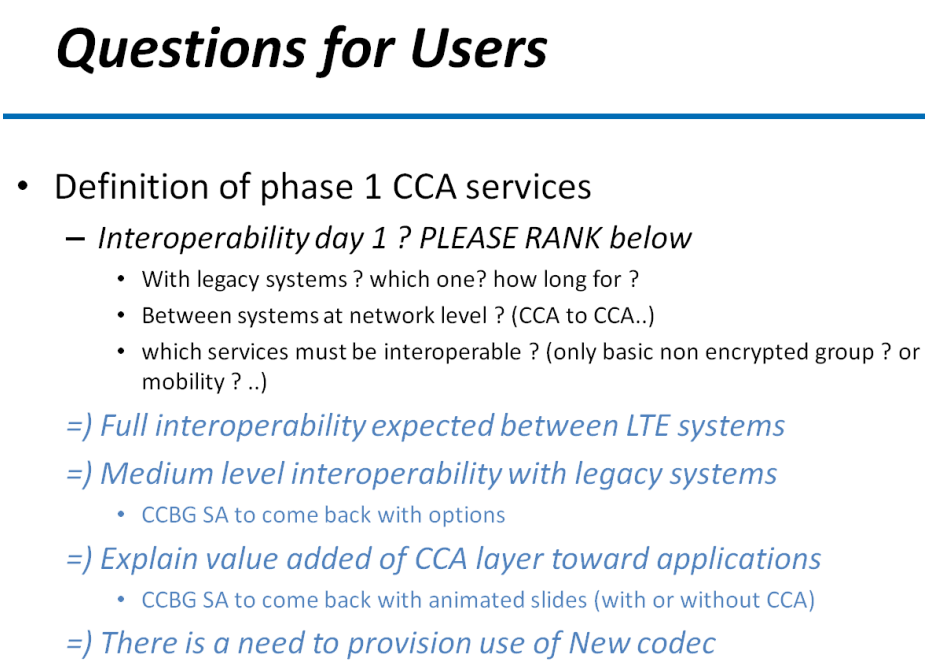

Figure 6: Questions for Users (slide 2 of 2)
(extract of slides with the consent of TCCA)

It is clear that different user groups have different priorities regarding voice and data. Those wanting to replace legacy systems need a core public safety voice capability from the start and are content to see data functionality developed over time from an entry level offering. Others see the need for an early significant data capability and are willing to wait for voice. There is probably agreement that:

- Voice or data calls within a network are prioritized over those going out to other networks.
- Group addressed communication over LTE has to be addressed as a priority.
- With video the need to share mobile to mobile is probably lower than having the ability to push selected video from control to users or make clips available to be pulled.
- Pre-emption especially for emergencies and priority needs to be an early deliverable as this is not dealt with satisfactorily for LTE.

Regarding interoperability with legacy systems the consensus is that it would be acceptable to have this at a low level initially and perhaps even long term by which is meant:

- interfacing to the control room of both legacy and LTE;
- connection at audio level but not full mobility;
- legacy data should interoperate with LTE data but not vice versa;
- two box working rather than integrated solutions;
- some protocol on how to handle encryption.

In the Spring of 2016 nine significant European operators/user organizations were surveyed to see if, based on the good progress with standardizing Mission Critical functionality in LTE, their interworking needs had changed.

Two operators see a sustained period of TETRA and LTE co-existence. For them the progression is from non-mission critical data alongside TETRA to mission critical data alongside TETRA and then eventually, for many but not all needs, LTE for data and voice. They therefore need:

- the ability for the interface to support SDS, alert and location services;
- emergency calls to be managed between systems and for end to end encrypted calls to be supported;

- for there to be a consistent, predictable priority of call made between networks;
- for there to be the facility for late entry to calls that may include users in both systems;
- for the user ID to be in some way visible;
- for DGNA and patch and re-group services to be supported for groups who may be on either system.

There were other operators who did not make a formal reply but supported the idea that there would need to be a sustained period of interworking. (There have also been reports from North America that anticipate the need for a sustained period of inter-working between legacy LMR systems and LTE).

Another of the organizations contacted stated that due to the amount of mission critical functionality being standardized in 3GPP that a more rapid transition than they previously anticipated in their inputs to CCBG and WG1 would be likely and therefore reduce the need for a standardized interface. In their view there is no need to enable fully integrated use of MCPTT and TETRA.

They do see a need for interworking between MCPTT and TETRA, primarily at international level. In their view at least a back-to-back solution will be required for connection to partner countries that use legacy systems. A more advanced interworking solution would be nice to have. When designing a more advanced interworking solution the investments for development and implementation of such an interface both at MCPTT side and on the TETRA side should be a leading criteria.

Another organization supported the consensus view of the CCBG in June 2013, i.e. it would be acceptable to have interoperability of LTE with legacy systems at a low level by which is meant:

- interfacing to the control room of both legacy and LTE;
- connection at audio level but not full mobility;
- legacy data should interoperate with LTE data but not vice versa;
- two box working rather than integrated solutions.

Regarding encryption they assume that:

- Air interface encryption will be available in LTE.
- Users needing end to end encryption should:
  - have all their users on a single system; or
  - accept decryption en re-encryption in an interface/gateway between a legacy system and LTE.

At the other end of the spectrum two organizations has said that it has no interest in standardization because they expects that they will transition from TETRA or Tetrapol to LTE quickly and before any standard is available and adopted by manufacturers. They recognized that they would need some degree of interworking during transition but would rely on a proprietary solution for this.

Requirements relating to the Transition from TETRA to LTE.

For those operators/users who see that they will eventually migrate from TETRA to LTE for voice and data there are a number of possible routes. One is the much publicized five step model proposed by Vinkvist, Pesonen and Peltola [i.14].

This has been described as follows:

Step one is to set up a data mobile virtual network operator (MVNO) to address the increased everyday data requirements. This will be accomplished by extending the subscriber and services provisioning system to support provisioning users on a broadband network. At first an official can use externally purchased subscriber identity module (SIM) cards, but eventually the second step will be to own and control subscribers in the LTE core.

In this second step, the critical voice and messages will run in the narrowband network, and high-speed non-critical (but secure) data will run in the commercial broadband network. The natural follow-up - step three - is to expand the owned LTE core to an owned dedicated broadband radio access in chosen locations, providing critical-grade data services.

Once the critical voice over LTE standardization is ready and the TETRA supplier supports group call over LTE functionality in the TETRA side, then the two networks can be connected, which will be the fourth step. This way the large development investments in TETRA group communications functionalities, such as prioritization, could be used. Then the same voice services are available both in narrowband and broadband - in the dedicated networks on critical service levels and in the commercial operators' networks up to the levels they can provide.

The final fifth step is dismantling the TETRA radio access once broadband service availability and reliability meets public safety's requirements. In some - most of all rural - areas, this might take place first when the narrowband network spare parts stock runs out.

During these five steps, the narrowband TETRA network will transform to a TETRA critical voice service server, the operator will gain knowledge and understanding about how to operate a broadband network, and users will have access to a high-speed data service that enables them to benefit from data applications and to develop information-centric ways of working.

This model seems to be fulfilling the following requirements for transition:

1) Control of the migration with a secure fall-back for voice communications at all times to maintain essential services at the expected level of performance.

2) Time to develop appropriate data centric operational procedures (taking account of the opportunity offered by the technology but considering legal, security, integrity and robustness requirements).

3) The setting up and running a MVNO for non-critical mobile data:

    a) Gain early experience of provisioning for broadband and assessing applications and appropriate operational procedures for the future.

    b) Gain experience in contracting for services from commercial operators.

4) The ability to provision services and support on a broadband network.

5) Owning a LTE core or purchasing services under a strong SLA such that mission critical grade services can be provided (resilience, accessibility, coverage, hardening of sites, etc.). A hybrid of these is another possibility:

    a) Gain experience in operating a broadband network or working with a commercial partner to achieve the desired result.

    b) Bring operational procedures for information - centric ways of working to maturity.

6) Interworking of TETRA and LTE for group communications. Same voice functionality in both networks, possibly same TETRA data functionality in both networks:

    a) Predictable inter-system performance (need not be completely seamless).

    b) A method for SDS, Flash messaging, status message and location interworking.

7) Inter-systems operation (between different TETRA networks and MC enabled LTE, different MC LTE networks and MC and standard LTE networks.

Analysing the above (and supported in some discussions with operators on requirements) the specific technical items requiring standardization from this would seem to be:

1) Agreed interfaces and protocols between the various networks in 7) above.

2) Agreed interfaces and protocols for how TETRA/LTE interworking is to be achieved for voice and some if not all TETRA data services.

3) Some generic requirements or a validation/proving process for applications proposed for mission critical use so that the availability and integrity of data in the network is not compromised.

8 Summary of Baseline TETRA and Tetrapol Services and Exceptions to their Transfer to Broadband Requirements (adopted from TETRA04(13)000074r2-Use-of-TETRA-services)

Modes of operation

- CA/DA selection
- Transmission mode (message, transmission, quasi transmission)

Registration

- Registration of user/identity
- Use of ASSI
- Energy saving mode
- Periodic location update
- Mobility related location update
- Deregistration
- Entry to dual watch
- Entry to DMO
- MM STATUS

Group attachment

- Subscriber class

Individual call

- Semi duplex
- Full duplex
- Early/late channel assignment
- Hook signalling/direct call
- Calling/Talking party identity
- Call proceeding indications
- Transmission control grant
- *Call modification*
    - Direct to hook
    - Hook-direct
    - Simplex-duplex (both ways)
    - Point-point to multipoint (i.e. individual to group call)
    - End of transmission

  - End of call
  - Call queue
- *Call maintenance*
  - Presence check
  - Impending disconnection warning
  - Call timer extension
- *Emergency/priority*
  - Emergency individual call
  - Emergency speech item request
  - Emergency call set up modification
  - Pre-emptive priority individual call
  - Priority call - terminal demanded priority
  - Priority call - SwMI configured priority

Group management

- Broadcast address
- Single group attachment
- Multiple group attachment
- Selected group attachment
- Class of use - scanning - 8 values
- SwMI initiated attachment
- SwMI forced detachment
- Scanning on/off indication
- Attachment lifetime
- MS initiated detachment
- SwMI initiated group reporting

Group call

- Temporary address
- Calling/talking party identity
- Presence checking at start of call
- SwMI modified priority
- Transmission control
- End of transmission
- Transmission interrupt
- Call disconnection

- Call maintenance (wait)
- Late entry - roaming
- Late entry - late group selection
- Call bearer modification (LTE unicast/multicast)
- Multipoint to point-point
- Area selection
- *Emergency/priority call*
    - Emergency group call
    - Emergency speech item request
    - Emergency call set up modification
    - Pre-emptive priority group call
    - Priority call - terminal demanded priority
    - Priority call - SwMI configured priority
    - Broadcast call
    - Priority group scanning

Cell reselection

- Broadcast of network area information

Status message

- Status individual to individual
- Status to group
- Emergency status
- Pre coded status

Telephone call

- PSTN call - direct LTE routed
- PABX call
- PSTN call - home application routed
- Early/late routing
- DTMF overdial
- Call disconnect
- Emergency phone call

BS fallback

- BS fallback - neighbour cell state

Layer 2 operation

Transmit inhibit

Packet mode data service

Circuit mode data

Multi-slot data

Concurrent voice and data

Short Data Service

- All SDS types 1-4
- SDS (not TL)
- SDS-TL
- Predefined service types for SDS-TL (e.g. text, AVL etc)
- Individually addressed SDS
- Group addressed SDS
- Store and forward of messages
- Message validity time for S&F
- Message reports
- Multiple forms of message addressing
- Concatenated SDS

DGNA

- Assignment of groups
- De-assignment of groups
- Forced attachment to assigned group
- Forced detachment of assigned group
- DGNA addressed to individual address
- DGNA addressed to group address
- Group merging
- Provision/modification of group mnemonic name
- DGNA rejection and/or error reporting by MS

Authentication

- One way authentication of MS
- Mutual authentication (application level)

Ambience Listening

- AL request from target user
- AL setup by SwMI
- AL cleardown by SwMI

End to End Encryption

- Clear voice override

Enable/disable

- Enable/disable of UE
- Enable/disable of application
- Disable of the UE by application action (cf disable of ME)

Call authorized by dispatcher

- Call transfer by SwMI
- Call acceptance or rejection by dispatcher

Air to Ground

Location Information Protocol

- Unsolicited location reports
- Trigger based reporting
- Control of reporting

Call forwarding

- Configured in SwMI
- Call forward telephone calls
- Call forward PTT calls

Callout

- Alerting, terminal response and user response
- Group call information phase

Discreet listening

- The following TETRA services are not seen as being required for Mission Critical Broadband Communications:
    - Circuit mode data

Annex A:
Functionality Split Proposal for Group Addressed Calls from 3GPP (Preliminary view)

Category	Requirements	description	Non-3GPP scope	3GPP scope	Note
group handling	Group attributes management	create/delete group add/remove group member definition of group area maintenance of all other group attributes such as subscription per group, etc.	YES	NO	Due to difference per application, this should be done fully under application layer
	Temporary linking groups	To dynamic merge at least two groups together for a temporary communication	YES	FFS	The dynamic link is also a service layer management and can be invisible to 3GPP. It is left open for now because 3GPP may need to avoid radio resource waste if duplicated resources might be allocated, FFS
Call control	Talking party identification	To allow application server to identify talking party and notify other members	YES	NO	Fully service layer requirement and can be solely done by application server
	Listening party identification	To allow application server to identify members who already join the call and the number of the group	YES	NO	Fully services layer requirement and can be solely done by application server
	Application layer arbitration	To allow members with higher priority to pre-empt the current talking party	YES	NO	Fully services layer requirement and can be solely controlled by application server
Interoperability	Interworking with narrow-band group communication systems	To allow group communication between narrow-band and broad-band system	YES	NO	Fully services layer requirement and can be solely managed by interoperability mechanism between different application servers
Interaction with other services	Interaction with other ordinary 3GPP services	When having other 3GPP services like ordinary voice calls, data applications, the priority/precedence to handle these services should be treated	YES	YES	The network has to be able to know priorities of different applications for transport resource allocation precedence

Category	Requirements	description	Non-3GPP scope	3GPP scope	Note
Application layer Addressing	Group addressing for incoming group communications	To address group member within 3GPP network	YES	NO	The group is managed and identified by the application layer
Radio resource efficiency	The 3GPP radio resource efficiency should be enhanced for group communication	To avoid duplicated/unnecessary radio resources allocated for different group members in a certain cell To minimize impact on signalling plane for the network	FFS	FFS	3GPP network is fully responsible for the radio resource management as providing transport functionality, including any 3GPP layer group-based addressing. The application may also be able to indicate usage of broadcast/multicast bearers
Service continuity	The group communication should be seamless handed over to enhance user experience	When the group member is moving between 3GPP cells, the group communication should not be interrupted and seamless handover should be supported	NO	YES	Such mobility management is fully under 3GPP network control and therefore service continuity is managed by the 3GPP network
Indication of geographical area	To enable the application layer know when a MU moves between different application-layer defined geographical area		YES	FFS	For example, the Cell ID or Tracking Area (TA) could be passed to the application layer
Capacity	Group capacity	the [maximum] number of groups the [maximum] number of members per group the [maximum] number of active group calls in parallel	YES	FFS	The number comes from the service layer, and it might have impact on 3GPP system for the radio resource capacity and MU capability to support these requirements and therefore 3GPP prefer it to be open now
Performance	Performance KPI for the group communication transmission	group communication setup time Voice Grant time (application layer only) end-to-end delay Interrupt time	YES	YES	Both need to be taken into account since the E2E delay includes both parts. However it needs to be reminded that such performance requirement might vary due to different applications

Annex B:
Visualization of Relay Node Use

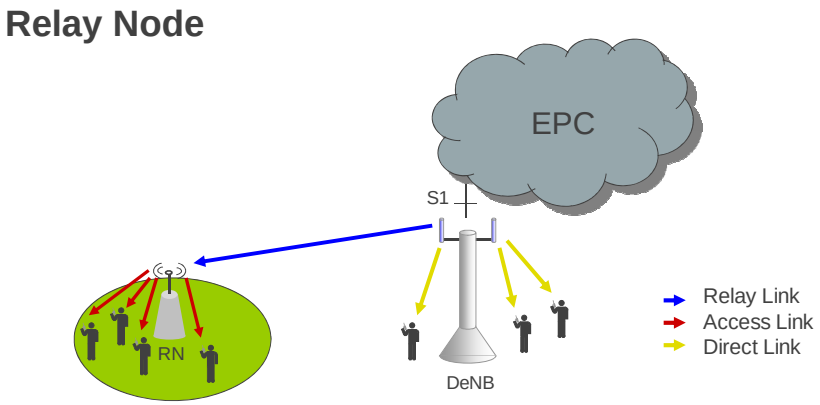

Figure B.1

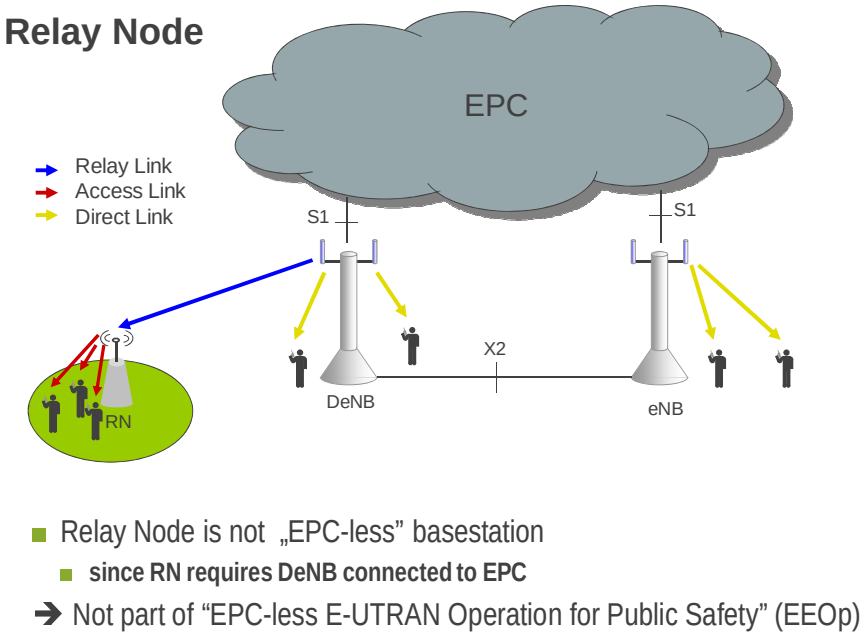

Figure B.2

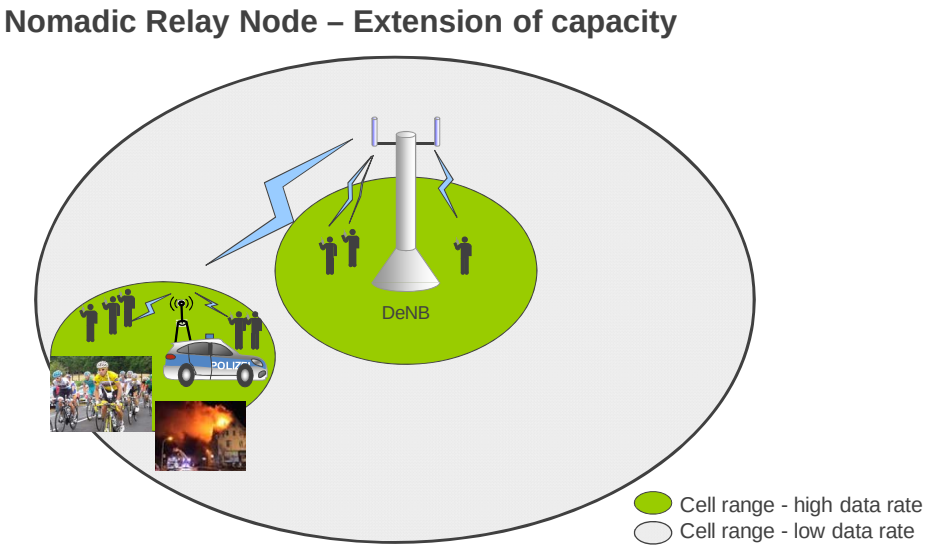

Figure B.3

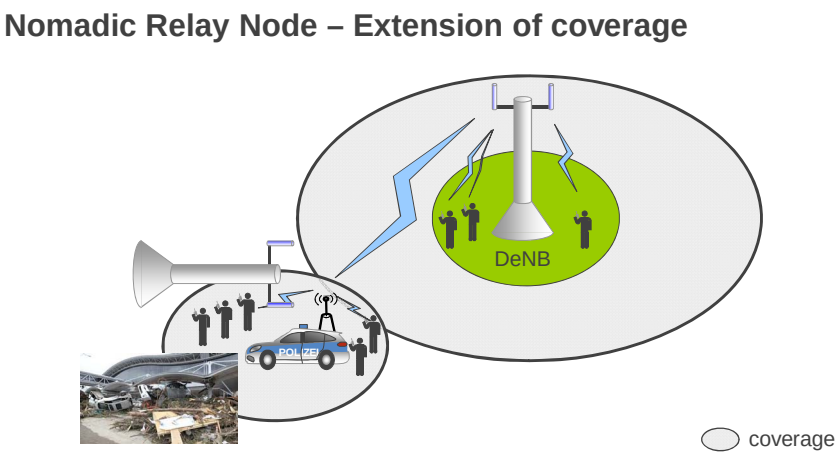

Figure B.4

Annex C:
Possible Progression of Interoperability Requirement

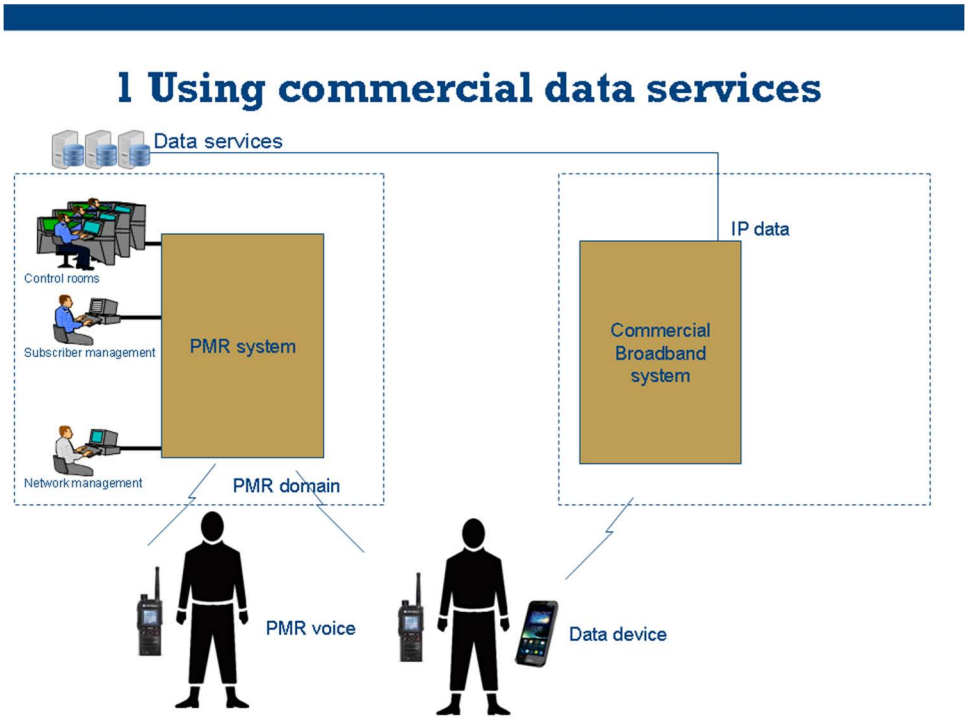

Figure C.1

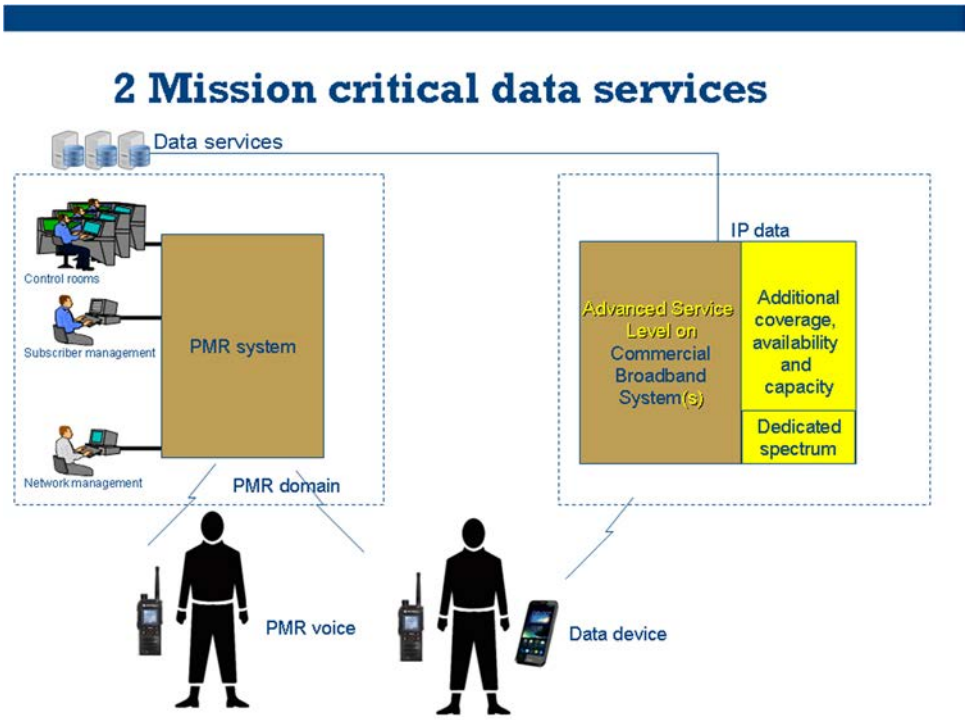

Figure C.2

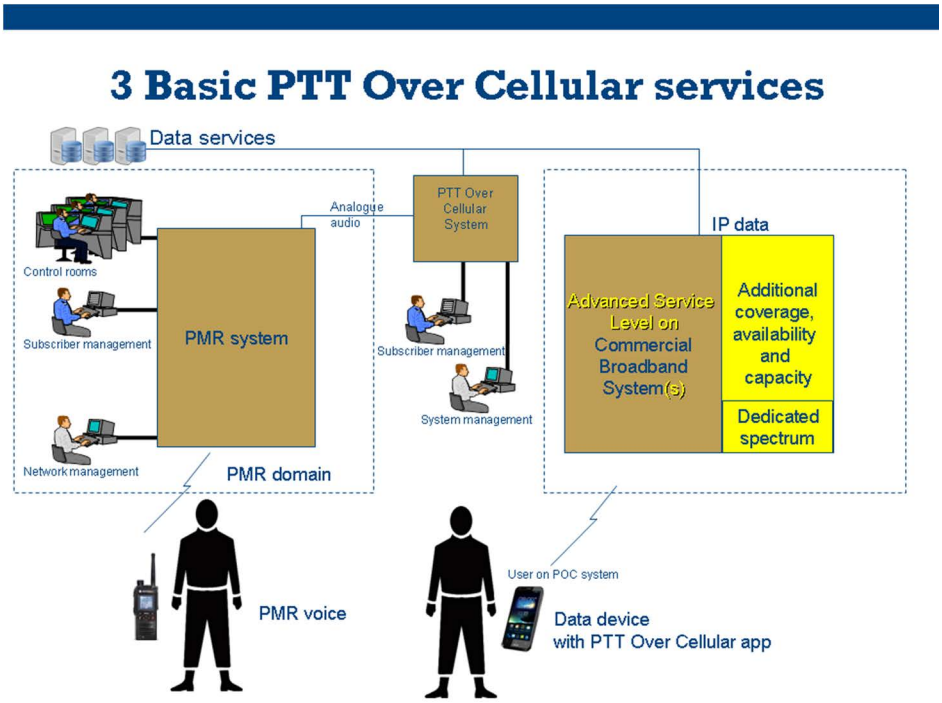

Figure C.3

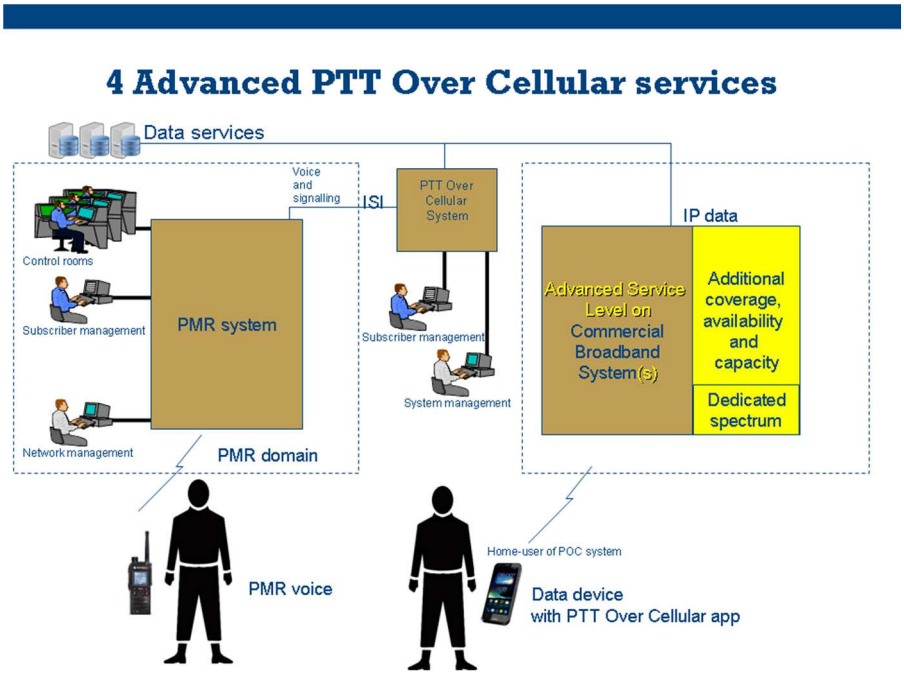

Figure C.4

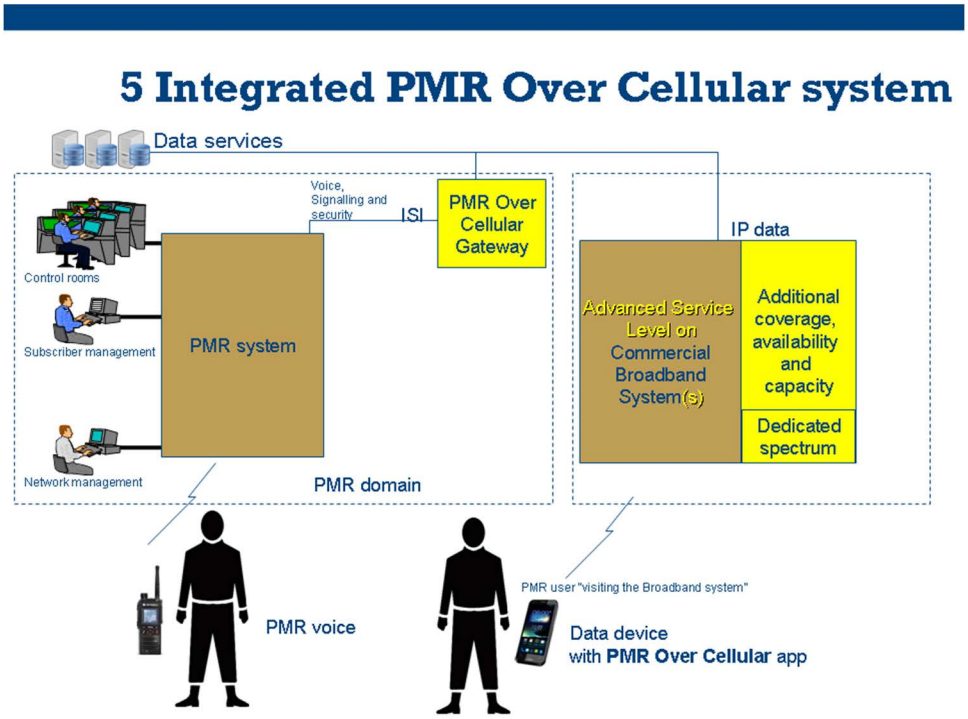

Figure C.5

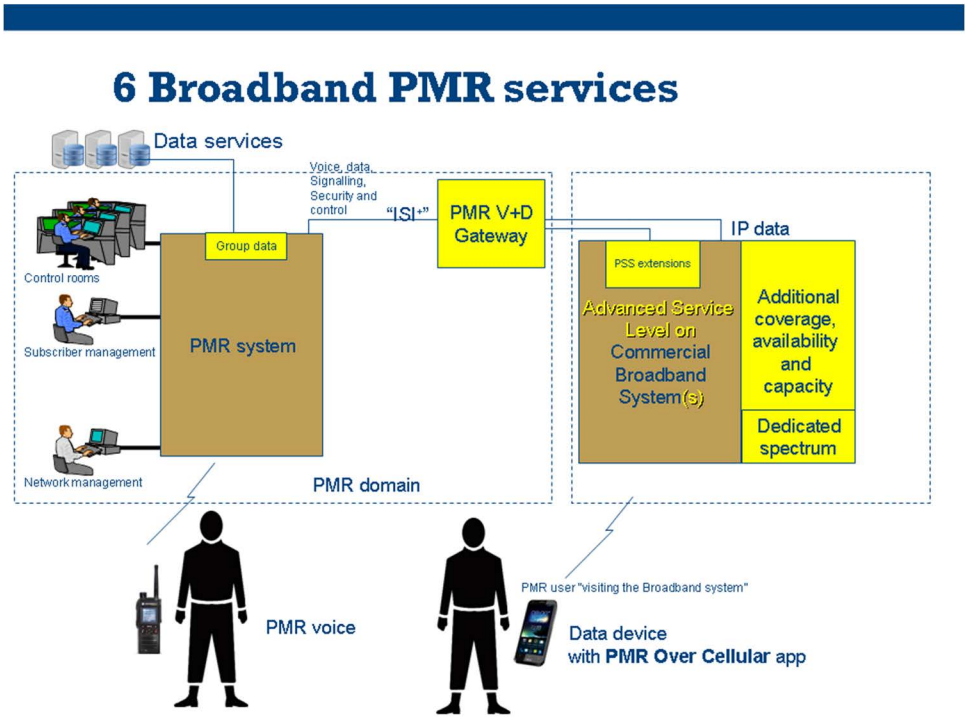

Figure C.6

Annex D:
Extract from 3GPP TS 22.278 V12.4.0 (2013-09)

"A Public Safety ProSe-enabled UE with ProSe Discovery enabled for discovery of other public safety Ues should be able to discover other discoverable public safety Ues, without network interaction if allowed by the operator, even when served by E-UTRAN whether or not ProSe E-UTRA Communication is used (including whether or not ProSe Group Communication or ProSe Broadcast Communication are used).

NOTE: A network operator can provide additional services for public safety Ues that are under 3GPP network coverage, such as providing accurate location information through GPS data.

A user of a Public Safety ProSe-enabled UE should be able to activate or deactivate the UE's ProSe Discovery feature while served by E-UTRAN, if allowed by the operator whether or not ProSe E-UTRA Communication is used (including whether or not ProSe Group Communication or ProSe Broadcast Communication are used).

ProSe should not be available to ProSe-enabled Ues not served by E-UTRAN, except in the following cases:

- *Public Safety ProSe-enabled Ues can use ProSe when operating on public safety spectrum even when not served by E-UTRAN. In this case, at least a one-time pre-authorization to use ProSe is needed.*
- *A Public Safety ProSe-enabled UE with ProSe Discovery enabled should be able to discover other discoverable Public Safety ProSe-enabled Ues when some or all of the Public Safety ProSe-enabled Ues involved in ProSe Discovery are not served by E-UTRAN, whether or not ProSe E-UTRA Communication is used (including whether or not ProSe Group Communication or ProSe Broadcast Communication are used).*

A Public Safety ProSe-enabled UE should be capable of determining autonomously whether or not a discovered ProSe-enabled UE is a public safety UE.

The configuration of a Public Safety ProSe-enabled UE that allows the Public Safety ProSe-enabled UE to discover other discoverable Public Safety ProSe-enabled Ues should be independent from its configuration to allow or not to allow other Public Safety ProSe-enabled Ues to discover it.

Public Safety ProSe-enabled Ues whether they are served by E-UTRAN or not, should be capable of establishing a secure ProSe E-UTRA Communication on a ProSe E-UTRA Communication path and exchange user traffic on public safety spectrum, assuming they are in Communication Range, are authenticated and authorized. This requirement applies to ProSe E-UTRA Communication between two Public Safety ProSe-enabled Ues, ProSe Group Communication and ProSe Broadcast Communication.

The operator should be able to authorize, via network control, Public Safety ProSe-enabled Ues to establish ProSe Communication when at least one of the two Public Safety ProSe-enabled Ues is served by EUTRAN.

The operator should be able to pre-configure Public Safety ProSe-enabled Ues (e.g., in the USIM or ME) with the permission to use ProSe Discovery and/or Communication services for Public Safety, without the need for the Public Safety ProSe-enabled Ues to connect to the network to get this initial configuration. This requirement applies to any ProSe E-UTRA Communication between two Public Safety ProSe-enabled Ues, ProSe Group Communication and ProSe Broadcast Communication.

The system should enable Public Safety ProSe-enabled Ues to mutually authenticate each other when not served by E-UTRAN.

Assuming Public Safety ProSe-enabled Ues are in Communication Range, are authenticated and are authorized, a Public Safety ProSe-enabled UE on public safety spectrum, whether or not it is served by E-UTRAN, should be capable of establishing multiple one-to-one ProSe E-UTRA Communications using multiple ProSe E-UTRA Communication paths, and of exchanging user traffic with each Public Safety ProSe-enabled UE across these multiple paths.

A Public Safety ProSe-enabled ProSe-enabled UE, whether or not it is served by E-UTRAN should be capable of transmitting data to a group of Public Safety ProSe-enabled Ues using ProSe Group Communications with a single transmission, assuming they are within Communication Range, authenticated and authorized.

Authentication should allow for security-enablement of large groups, regardless whether group members have discovered each other when served by E-UTRAN or not.

A Public Safety ProSe-enabled UE whether or not it is served by E-UTRAN should be capable of receiving a ProSe Group Communications transmission, of which it is a group member, regardless of whether or not it has been discovered by the transmitting Public Safety ProSe-enabled UE.

An authorized Public Safety ProSe-enabled UE, whether or not it is served by E-UTRAN should be capable of sending a broadcast message to all authorized Public Safety ProSe-enabled Ues within Communication Range, regardless of group membership, using ProSe Broadcast Communication in a single transmission.

An authorized Public Safety ProSe-enabled UE, whether or not it is served by E-UTRAN, may be capable of acting as a relay for other public safety Ues.

An authorized Public Safety ProSe-enabled UE should be capable of acting as a relay for ProSe E-UTRA Communication between two Public Safety ProSe-enabled Ues, ProSe Broadcast Communication, and ProSe Group Communication.

A ProSe UE-to-UE Relay and a ProSe UE-to-Network Relay should be able to relay data for a group of Public Safety ProSe-enabled Ues using ProSe Group Communications regardless of their group membership.

An authorized Public Safety ProSe-enabled UE, whether or not it is served by E-UTRAN, should be capable of being enabled/disabled by a user or the system to act as a relay for other Public Safety ProSe-enabled Ues.

The user of a Public Safety ProSe-enabled UE acting as a relay should not perceive service degradation due to its use as a relay, regardless whether or not the Public Safety ProSe-enabled UE is served by E-UTRAN.

There should be a maximum of one ProSe UE-to-Network Relay between a Public Safety ProSe-enabled UE and E-UTRAN.

There should be a maximum of one ProSe UE-to-UE relay between two Public Safety ProSe-enabled Ues.

A ProSe UE-to-UE Relay serving as a relay for other Public Safety ProSe-enabled UE should be able to be served at the same time by the UE serving as a relay for it.

A ProSe UE-to-UE Relay should be capable of relaying communications for one or more Public Safety ProSe-enabled Ues that are within Communication Range of the ProSe UE-to-UE Relay.

A Public Safety ProSe-enabled UE should be capable of acting as a ProSe UE-to-Network Relay between a UE and E-UTRAN if it is authorized to act as a relay and served by this E-UTRAN.

A Public Safety ProSe-enabled UE should be capable of acting as a relay regardless of whether or not it has been discovered by a Public Safety ProSe-enabled UE using it as a relay if they are within Communication Range.

In the case where communication is relayed by a ProSe UE-to-Network Relay between an E-UTRAN and a Public Safety ProSe-enabled UE there should be no ProSe UE-to-UE Relays between the Public Safety ProSe-enabled UE and E-UTRAN.

An authorized Public Safety ProSe-enabled UE should be capable of communication using both the network infrastructure and ProSe Communication with Public Safety ProSe-enabled Ues not served by E-UTRAN in parallel whether or not ProSe Discovery is used.

An authorized Public Safety ProSe-enabled UE should be capable of being enabled/disabled to act as a relay to/from E-UTRAN for other Public Safety ProSe-enabled Ues unable to access E-UTRAN.

Based on operator policy and user choice, the system should be able to move a user traffic session of a Public Safety ProSe-enabled UE that is losing connection to the network to a direct ProSe Communication path via a Public Safety ProSe-enabled UE acting as a ProSe UE-to-network relay, which is in direct Communication Range and has connectivity to the network. A mechanism to support service continuity should be provided and may apply when the traffic is moved. This requirement is not applicable to ProSe Group Communication and ProSe Broadcast Communication.

Based on operator policy, the operator network should be able to control the relaying of network services between Public Safety ProSe-enabled Ues communicating by means of ProSe.

In addition, the system should be able to move the user traffic session back to the EPC Path once the Public Safety ProSe-enabled UE is served by E-UTRAN. The user may inhibit the switch back to the EPC Path.

Based on operator policy, the operator network should be able to control ProSe E-UTRA Communication between Public Safety ProSe-enabled Ues that are in ProSe E-UTRA Communication with a Public Safety ProSe-enabled UE that is served by E-UTRAN and acting as their ProSe UE-to-network relay. This requirement applies to any ProSe E-UTRA Communication between two Public Safety ProSe-enabled Ues, ProSe Group Communication and ProSe Broadcast Communication.

It is desirable that an authorized Public Safety ProSe-enabled UE, whether or not it is served by E-UTRAN, supports the capability to exchange data via ProSe from within a building to Public Safety ProSe-enabled Ues outside the building using a power class 3 E-UTRA UE.

Authorized Public Safety ProSe-enabled Ues, whether being served or not by E-UTRAN, should be able to communicate with other authorized Public Safety ProSe-enabled Ues whether or not ProSe discovery is used.

A Public Safety ProSe-enabled UE should provide the ability for the end user to activate/deactivate ProSe E-UTRA Communication whether or not the UE is served by E-UTRAN and whether or not ProSe discovery is used. This requirement applies to any ProSe E-UTRA Communication between two Public Safety ProSe-enabled Ues, and to ProSe Group Communication and ProSe Broadcast Communication.

A Public Safety ProSe-enabled UE should support independent activation/deactivation of ProSe Discovery and ProSe E-UTRA Communication whether or not it is served by E-UTRAN. This requirement applies to any ProSe E-UTRA Communication between two Public Safety ProSe-enabled Ues, ProSe Group Communication and ProsSe Broadcast Communication.

Re-authorization and specific configurations, including spectrum configurations, of Public Safety ProSe-enabled Ues should be subject to public safety operator policy.

An operator should be able to configure a Public Safety ProSe-enabled UE with the permission to be discoverable or not by one or more Public Safety ProSe-enabled Ues, without prior registration to the network.

Subject to operator policy and/or network authorization, a user of a Public Safety ProSe-enabled UE should be able to select the ProSe Communication path (direct or routed via local eNB) when the Public Safety ProSe-enabled UE is being served by E-UTRAN. This requirement applies to any ProSe E-UTRA Communication between two Public Safety ProSe-enabled Ues, ProSe Group Communication and ProSe Broadcast Communications. The network authorization should consider the current traffic condition in the specific area.

A Public Safety ProSe-enabled UE should be able to operate in spectrum allocated exclusively for ProSe and spectrum allocated for both ProSe and other services."

Annex E:
Requirements from Project Broadmap

In April 2017 the EU Horizon 2020 Project called Broadmap reported. The primary goal of the BROADMAP project is to, "Collect and validate the PPDR (Public Protection and Disaster Relief) organisations' existing requirements with the aim to establish a core set of specifications and roadmap for procurement, to achieve future evolution of EU broadband applications and interoperable radio communication solutions".

This project collected PPDR broadband requirements from a number of European public safety users and operators. It compared them with the functionality being specified in 3GPP for critical communications and concluded that there were two gaps. These were:

1) "Missing support for MC apps to minimize interruptions to other on-going MC services."

2) "Missing generation of service status advice for MC users."

Whilst 2) is sufficiently clear as a requirement there may be a need for further clarity on how 1) should work given that different Mission Critical applications may be supplied by different providers and have different levels of security. Further it seems likely that no MC application should be aware of use of other MC services other than the ones that it is making use of itself implying it would need to be a more centralized element with the authority to see resource usage across groups for instance. There will presumably need to away to prioritize one data service above another.

History

Document history		
V1.1.1	January 2015	Publication
V1.2.1	January 2018	Publication