NTNU

Norwegian University of
Science and Technology

Public safety networks towards mission critical mobile broadband networks

Milan Stojkovic

Master of Telematics - Communication Networks and Networked Services

Submission date:	June 2016
Supervisor:	Bjarne Emil Helvik, ITEM
Co-supervisor:	Eirik Larsen Følstad, ITEM

Norwegian University of Science and Technology
Department of Telematics

Problem description

The TETRA network is a narrowband public safety network for critical communication, which provides highly reliable and secure narrowband services for many public safety organizations across Europe and in the other parts of the world. Lately there is an increasing need for introducing broadband services into critical communication networks. To provide broadband services in public safety networks TETRA's standardization body, ETSI, and LTE's standardization body, 3GPP, have started developing common standards which will enable LTE to provide features which are now inherent only for mission critical networks.

The idea of TETRA migration/evolution towards broadband communication is relatively new, the idea was born in 2012. Also, in 2012 government of US adopted the law of building nationwide wireless broadband network dedicated to public safety. First feasibility studies and requirements researches by 3GPP are done in 2013 while the latest standards are released in December 2015. At the same time, in December 2015, TETRA network became nationwide public safety network in Norway and the government of UK has signed a contract for creating their own broadband network dedicated to public safety.

Until today we do not have fully operative broadband network for public safety use, first transitions are yet expected. Implementations of the 3GPP standards released in 2014 are expected for this year, while the implementation of the standards released in December 2015 are expected at the end of 2017. UK has predicted to do the transition between 2017 and 2020 while predictions for global transition towards mission critical mobile broadband networks go beyond 2020.

The facts that standards are still in development and that the field for transition is in the preparation make work on this project open for innovations and highly motivated by novelty and originality which could be introduced. Innovation can be reflected through the solutions proposed for Public Safety LTE, meaning implementation strategy. Creation of transition scenarios, estimation of their benefits and risks will be a challenge of this project.

The main objective of this master thesis is to perform an assessment of the different options for introducing mission critical communication for public safety organizations in the LTE network(s), to identify possible advantages but also to detect possible problems.

The focus will be on the standards developed by 3GPP Work Groups which should enable LTE to support mission critical communication. Methods and goals of these standards will be described. The security aspects like Authentication, Air Interface Encryption (AIE) and End to End encryption, will be paid additional attention and undergo an evaluation.

Different scenarios of possible migration/evolution from TETRA to LTE will be described and their feasibility and timing will be discussed. The TETRA network in Norway will be taken as a case study.

Abstract

Lack of broadband data applications in dedicated public safety networks has pushed public safety users to seek for the solutions in commercial LTE networks. However, LTE communication systems are missing functionalities like group and device-to-device communication, push-to-talk (PTT) feature, etc., which are essential for public safety users. To address those shortcomings, in the past 5 years 3GPP has been developing new functionalities for LTE that should make LTE suitable for public safety networks. Besides that, 3GPP is also working on definition of a robust LTE migration roadmap towards public safety networks solution.

This thesis 1) assesses whether new LTE functionalities match with the functionalities available in public safety communications systems today; 2) proposes security protocols for user authenticating when two new Public Safety LTE features are used; 3) evaluates different alternatives for deployment of future public safety LTE network; 4) proposes transition scenario for Norway's public safety network, i.e. roadmap for migration from TETRA to LTE network.

The assessment of the new LTE functionalities has shown that LTE will be able to provide the same communication functionalities as provided today by specialized radio communications systems for public safety networks, such as TETRA. Group Communication System Enablers for LTE (GCSE_LTE) will enable group calls in LTE, Proximity Services (ProSe) will enable device-to-device communication, Mission Critical Push To Talk (MCPTT) over LTE will provide PTT service in LTE and Isolated E-UTRAN Operation for Public Safety (IOPS) will enable LTE's base station to operate without a backhaul connection. These functionalities are expected to become available late 2017.

Analysis of security protocols proposed has shown that proposed protocols are able to meet all security requirement defined by 3GPP and establish high level of security.

Evaluation of deployment alternatives for future LTE public safety networks has shown that the choice of the right deployment model will largely depend on needs, interests and possibilities of public safety organizations. Those willing to have full control over the network and provide the most reliable services to its users will chose Dedicated LTE network model, in return they will have high costs, longer waiting time before network becomes operative and they will have to lobby for the spectrum. Public safety organizations not willing to wait long, deal with the problem of spectrum allocation and invest much will go for Commercial LTE networks model, however services they get will not be adapted to the needs of public safety users, they will have to accept that they have reduced control over the network and services and that the service availability is not high as in dedicated networks, unless network undergo upgrades, in which case each of these aspects can be improved. Third evaluated model, Hybrid solution, represents a combination of two previously mentioned models. Hybrid solution is flexible and allows public safety organizations to combine different aspects of Dedicated and Commercial LTE networks. This allows them to adapt the network to their specific needs. Exactly this feature favors this model compared to other two. However, Hybrid model can raise problems of networks interoperability and spectrum sharing, which nevertheless can be solved.

The case study has confirmed the claims on Hybrid solutions model. By using the hybrid model approach we were able to ensure seamless transition from TETRA to LTE for Norway's public safety network, Nødnett.

Acknowledgments

I would like to thank my supervisor Eirik L. Følstad and my responsible professor Bjarne E. Helvik, for guidance, support and valuable advices throughout the process of writing this master's thesis.

Contents

List of Figures

List of Tables

Abbreviations

AI	Air Interface
AIE	Air Interface Encryption
AMR	Adaptive Multiple Rate
AUC	Authentication Center
AVL	Automatic Vehicle Location
BS	Base Station
CA	Certificate Authority
CAPEX	Capital Expenses
CCBG	Critical Communications Broadband Group
CIA	Confidentiality, Integrity and Availability
CO	Contractor Owned/Contractor Operated
DCK	Derived Cipher Key
DGNA	Dynamic Group Number Assignment
DM	Direct Mode
DMO	Direct Mode Operation
DNK	Direktoratet for NødKommunikasjon
DSA	Digital Signature Algorithm
EAP	Extensible Authentication Protocol
EDGE	Enhanced Data rates for GSM Evolution
EPC	Evolved Packet Core
EPS	Evolved Packet System
ESMCP	Emergency Services Mobile Communications Programme
ESN	Emergency Services Network
ETSI	European Telecommunications Standardization Institute
FCC	Federal Communications Commission
GCS	Group Communication Service
GCSE	Group Communication System Enablers
GO	Government Owned
GPRS	General Packet Radio Service
HSD	High Speed Data
HSS	Home Subscriber Server
ICCA	International Critical Communications Awards
IdMS	Identity Management Server
IMS	IP Multimedia Subsystem
IOPS	Isolated E-UTRAN Operation for Public Safety
IP	Internet Protocol
ISI	Intra-System Interface

LSA	Licenced Shared Access
LSB	Least Significant Bits
LTE	Long Term Evolution
MAC	Message Authentication Code
MBMS	Multimedia Broadcast/Multicast Service
MCPTT	Mission Critical Push-To-Talk
ME	Mobile Equipment
MITM	Man-In-The-Middle
MME	Mobility Management Entity
MNO	Mobile Network Operator
MoU	Memorandum of Understanding
MS	Mobile Station
MSB	Most Significant Bits
MSC	Mobile Switching Center
MSPD	Multi Slot Packet Data
MVNO	Mobile Virtual Network Operator
NAS	Non-Access Stratum
NATO	North Atlantic Treaty Organization
NeNB	Nomadic eNB
OMC	Operations and Management Center
OPEX	Operating Expenses
OTAR	Over The Air Re-keying
PABX	Private Automatic Branch eXchange
PCC	Policy and Charging Control
PCRF	Policy and Charging Rules Function
PDN	Packet Data Network
PDP	Packet Data Protocol
PEK	ProSe Encryption Key
PIK	ProSe Integrity Key
PPP	Public-Private Partnership
PS	Public Safety
PSTN	Public Switched Telephone Network
PTT	Push-To-Talk
RAN	Radio Access Network
RF	Radio Frequency
RFC	Request For Comments
RRC	Radio Resource Control
SA	System Aspects
SAE	System Architecture Evolution
SCK	Static Cipher Keys

SDS	Short Data Service
SFPG	Security and Fraud Protection Group
SIM	Subscriber Identity Module
SIP	Session Initiation Protocol
SLA	Service Level Agreement
SwMI	Switching and Management Infrastructure
TBS	TETRA Base Station
TCCA	TETRA and Critical Communication Association
TCO	Total Cost of Ownership
TEAP	Tunnel Extensible Authentication Protocol
TEDS	TETRA Enhanced Data Service
TETRA	Terrestrial Trunked Radio
TLS	Transport Layer Security
TLV	Type-Length-Value
TMO	Trunked Mode Operation
TR	Technical Report
TS	Technical Specification
TSG	Technical Specification Groups
UE	User Equipment
UICC	Universal Integrated Circuit Card
UMTS	Universal Mobile Telecommunications System
USIM	Universal Subscriber Identity Module
VPN	Virtual Private Network
WI	Work Items
WLAN	Wireless Local Area Network

Chapter 1

1 Introduction

Nowadays, most of the public safety organizations across the globe use dedicate communications systems like TETRA, TETRAPOL or P25 [1], which were conceived more than 20 years ago, in the 1990s. These systems have primarily been designed and deployed to provide highly reliable and secure mission critical narrowband voice-centric services designed to match special requirements of the public safety communications users. The specialized services they provide include group and priority call with push-to-talk feature, 'device-to-device' communication (Direct Mode Operation (DMO)), etc. And while voice services are on satisfactory level, the data transmission capabilities of these public safety communications systems is rather limited. The focus on voice-centric services has led to situation where technology used in public safety communications is far behind technology used in commercial domain in terms of available data rates. Now, public safety community is seeking to overcome this problem and introduce broadband data services into public safety communications.

1.1 Background and Motivation

Behavior of public safety network users is changing. Their need for voice-centric services is slowly being substituted by data-centric applications. Over the time it was realized that usage of applications like picture or video transmission, live video or audio streaming, high-speed Internet access, etc., could be beneficial for public safety. It was recognized that these data applications can change the way how public safety communications are perceived today and improve the communication among the users which may further lead to improved public safety.

Whether due to difference in priorities, needs or different size of user market (bigger market imply bigger financial support for development), commercial cellular systems and public safety communications systems have evolved at different speeds. Development of technology for public safety communications systems has fell into certain stagnation, which result in limited data transmission capabilities. The most widely used public safety communications systems today are not able to cope with new user requirements and provide support for bandwidth-hungry data applications. On the other side, technology in commercial domain was evolving much faster which has led to the situation that commercial cellular systems have better data transmission capabilities and are able to support even the most demanding data applications.

Unavailability of data applications in communications systems used in public or rather, their inability to support those application, has forced some of the public safety organizations to seek for alternatives and rely on commercial networks for data services. However, soon it was realized that commercial networks are lacking functionalities needed for normal operational work of public safety users, like group communication, push-to-talk feature, and device-to-device communication.

Realizing that changes in public safety communications are inevitable, public safety community has started creating a solution which will put the entire public safety communications under one roof. Commercial LTE networks have good support for data applications but they do not have support for specialized services important in public safety communications. On the other side, public safety TETRA networks have support for specialized services but do not have good support for data applications which requires higher throughput. Solution was to develop a single standard which will satisfy the users' needs for data applications but at the same time provide specialized services important for their operations. Since TETRA standard cannot expand to support broadband applications, another solution had to be found. It was decided that LTE will be the future single global standard for public safety communications. Next step was to improve LTE and add the necessary functionalities.

Work on improvements in LTE, to create so called Public Safety LTE (PS LTE), started recently. Their development represents a major turnaround not only for LTE but also for public safety communications. For LTE, which has been developed for commercial network and ordinary users, it is a huge challenge to meet the high level requirements of public safety users and achieve the same level of reliability and services availability provided by existing public safety networks. For public safety networks which rely on systems proven to be secure and reliable this is a big step into unexplored.

These enormous changes were not a subject of many researches and they have not been described by large-scale, which sets a high motivation for exploring these topics. Therefore, it is interesting to see whether, and how well LTE succeed to cover all the necessary functionalities and whether it will be suitable for public safety networks. Also, it will be interesting to examine how public safety networks can switch from one technology to another. In that context, it will be useful to investigate different transition models for public safety networks, to see in which directions this transition can go and how sustainable those transition models are.

1.2 Objective

The aim of this thesis is to perform an assessment of the ongoing changes in public safety communications. One objective is to discuss the ability of LTE standard to take the place of TETRA standard in public safety networks i.e. to evaluate, can new LTE features for public safety replace proven TETRA services, with special emphasis on security implementation. Another objective is to evaluate different transition scenarios of public safety networks, i.e. deployment models for future public safety networks.

In particular, this thesis will:

- Identify the characteristics of the TETRA systems used today in public safety networks
- Identify the differences between public safety networks and commercial cellular networks
- Provide details on LTE standardization evolution and discuss new LTE features for public safety
- Propose protocols which will help in security establishment when new LTE features are used
- Discuss different alternatives for transition/migration from TETRA to LTE network(s)
- Examine how transition alternatives could be applied on a concrete network model

1.4 Methodology

Qualitative research method was used throughout this thesis. Firstly the data on TETRA technology were collected. These were collected mostly from the TETRA standard specifications and official reports. This was to identify characteristics of communications systems used in public safety networks and their advantages and limitations which was later used as a basis for technologies comparison. In the same way the data were collected for LTE technology, from LTE standard specifications. Similar was done for public safety and commercial cellular networks, data were collected to identify the properties of these networks. Which means that research is based on collecting the relevant data which were used to obtain the necessary information and draw the conclusions. Exceptions are methods used in Chapter 5 and Chapter 7. In Chapter 5 security analysis was conducted and based on security requirements, and according to defined frameworks, authentication protocols were proposed for two new features in LTE. In Chapter 7 knowledge gained throughout this project was used to propose transition scenario for Norway's public safety network.

1.5 Thesis Structure

This document is organized in eight chapters of which first two provide introduction and background, chapters 3-7 represent the main part of the project and they are dealing with the analysis and problem solving of a given task, and the last chapter, Chapter 8 gives a conclusion and provides findings of this project. This thesis project consists of two parts, accordingly the analysis part is split on two parts:

- **Part I** – which includes Chapters 3, 4 and 5 deals with the analysis of future mobile broadband public safety communications systems, i.e. analyses which characteristics future public safety communications systems should have; performs an assessment of the new LTE functionalities for public safety communications; and proposes security protocols for new LTE features
- **Part II** – which includes Chapters 6 and 7 deals with the analysis of future public safety networks, i.e. evaluates deployment models for future public safety network which public safety organization can apply in transition from TETRA to LTE networks and applies those findings in a case study

Brief description of each chapter follows:

Chapter 1 provides a justification and motivation for this project, sets the objectives of this project and explains the methodology used.

Chapter 2 describes communications systems and technology used in public safety networks nowadays. In this chapter TETRA system, one of the most widely used system in public safety networks was taken as a representative to describe the characteristics of such systems. Chapter 2 describes what TETRA standard defines, which kind of services provides, what type of communications modes supports and how security in such system is implemented.

Chapter 3 aims to identify differences between public safety and commercial cellular networks as well as differences in technologies they use. Comparative approach should illustrate advantages and disadvantages which one side has over another. In some way Chapter 3 serves as a guideline for future public safety network, by showing all the necessities that this network should have. Furthermore, this chapter provide examples of countries which have already started changing their public safety networks, to illustrate through real examples how and on which way present public safety networks can evolve and do the transition towards public safety mobile broadband networks.

Chapter 4 provides insight in standardization work for Public Safety LTE and describes new LTE functionalities. Here, ability of new LTE functionalities to match the functionalities available in TETRA was discussed. Finally, an answer to the question when these features may become available in LTE networks, was also given.

In **Chapter 5** protocols which should help in security establishment for new LTE features are proposed. Proposed protocols should ensure user authentication when using two new LTE features, ProSe and MCPTT.

Chapter 6 describes and evaluates three different deployment models for future public safety networks. These deployment models can be used for transition from TETRA to LTE network(s).

In **Chapter 7** case study was conducted. Based on the findings from Chapter 6, suitable transition scenario for Norway's public safety network was proposed. Possible challenges of that particular transition scenario were identified and suggestions for overcoming these challenges were proposed.

Chapter 8 summarizes and concludes the work done. In this chapter main findings of this project are presented.

Chapter 2

2 Background

Public safety (PS) networks are dedicated telecommunication networks used by public safety organizations, such as police, fire, emergency medical service, etc., for critical communications [2]. Public safety communications systems are communication systems used in public safety networks to deliver communication services needed. Most of the public safety organizations today, use dedicated systems based on telecommunication standards developed especially for public safety communications, like Terrestrial Trunked Radio (TETRA), ARCP Project-25 (P25) and TETRAPOL, which use narrowband technology [2]. These systems are designed and deployed to provide highly reliable and secure narrowband services.

This chapter provides the background of one of the narrowband communications systems used in public safety networks. Terrestrial Trunked Radio (TETRA) system will be taken as a representative and its services, features and characteristics will be described.

2.1 Terrestrial Trunked Radio – TETRA

The TETRA (Terrestrial Trunked Radio)[1] is an open telecommunication standard for public safety communications systems, developed by European Telecommunications Standardization Institute (ETSI). The TETRA standards define series of open network interfaces between the TETRA network infrastructure (Switching and Management Infrastructure (SwMI) in TETRA terminology) and other network elements encompassed by the TETRA system.

2.1.1 TETRA Release 1

The first set of specifications for TETRA, developed by ETSI, are named ‘TETRA Voice + Data’. As the name says, TETRA Voice + Data standard was standardizing elementary voice services and basic data service. Later when TETRA standards have continued to evolve this standard became known as TETRA Release 1. Beside network elements and interfaces, Release 1 has also standardized services for TETRA network, and as the name of the standard indicates, services can be divided in two groups, Voice services and Data services.

Voice services:

- **Individual call** - service that enables one-to-one communication on a half-duplex or full duplex basis between two TETRA mobile stations. This is a basic service for any mobile radio network. When individual call is realized as half-duplex only one

[1] *In telecommunications, **trunking** is a method for a system to provide network access to many clients by sharing a set of lines or frequencies instead of providing them individually (https://en.wikipedia.org/wiki/Trunking)
*A **trunked radio system** is a complex type of computer-controlled two-way radio system that allows sharing of relatively few radio frequency channels among a large group of users (https://en.wikipedia.org/wiki/Trunked_radio_system)

participant of communication can transmit (speak) at the time while in full-duplex mode both participants can transmit (speak and be heard) at the same time. Individual call can be established as half-duplex and full-duplex when TETRA mobile station uses TMO (trunked mode operation) mode, while in DMO (direct mode operation) mode only half duplex individual call can be made. TETRA modes of operation will be explained shortly.

- **Group call** – service that enables one-to-many communication on a half-duplex basis. This is one of the key services of TETRA system. The group call function as a broadcast/multicast communication where one "member" of a group is transmitting (speaking) by holding a button on his mobile station (MS), while other members are receiving (listening) what that member is transmitting. The listeners can only start transmitting when the member who was transmitting is finished, i.e. when he/she releases the button.
- **Pre-Emptive Priority Call (Emergency Call)** – The usage of TETRA Emergency call service provides the highest priority to this call among all call services. This means that Emergency call gets highest priority access to network resources and the highest uplink priority. In the case that network is busy when Emergency call is activated the lowest priority communication will be dropped in order to enable network to handle the Emergency call. The Emergency call is initiated by using a dedicated switch located on a mobile station carried by the user. For more refer [3].
- **Call Retention** – service which ensures that the call will not be dropped, i.e. it protects a call from being forced off the network when the network is busy as it is the case with low priority call when Emergency call enters the busy network. For more refer [4].
- **Priority Call** – service which provides different levels of priority to the users for accessing the network resources. The TETRA has 16 levels of priority which gives great flexibility to the network. For more refer [5].
- **Dynamic Group Number Assignment (DGNA)** – service which allows authorized users to create, modify, delete and interrogate group(s). Group participants can be from different public safety organizations (for ex. Police, Ambulance, Fire, etc.). Dynamic Group Number Assignment (DGNA) can also group participants in an already ongoing call. For more refer [6].
- **Ambience Listening –** service that enables a Dispatcher to perform some form of "eavesdropping" of the mobile station user(s). A Dispatcher can set his/her mobile (or other kind of) station, into Ambience Listening mode and listen to the conversation and background noises within range of the mobile stations' microphone of the mobile station user. The mobile station user cannot be aware that Ambience Listening is being performed since he is not notified about the action performed and there is no notification on the mobile station. For more refer [7].
- **Call Authorized by Dispatcher** – service which gives to Dispatcher a role of Authorizer, i.e. a Dispatcher can allow or not allow call requests to be proceeded. For more refer [8].
- **Area Selection –** service which in essence defines which users can operate in which areas (base station coverage). It makes it possible for a Dispatcher to select over which base station certain calls will go through. This service can improve network loading by providing one kind of load-balancing, while Area Selection can be chosen on a "call by call" basis. For more refer [9].
- **Late Entry -** is not a real service but an air interface feature that allows new users to join a communication channel in the ongoing call. It is performed automatically by control channel which diverts the user's mobile station to a talk group call if the user's

mobile station was out of the coverage or turned off when the conversation started. For more refer [10].

Data services:

- **Short Data Service –** is a message service which enable users to exchange short pre-defined or user-defined messages – e.g. emergency message, basic status message, location information etc., or free form text messages. The Short Data Service (SDS) includes both point-to-point and point-to-multipoint capabilities and can be used in parallel with an ongoing speech call. The SDS service can provide up to 256 bytes of data. For more refer [11].
- **Packet Data Service** – also called TETRA Packet Data Protocol (PDP) service is a service that provides mechanisms which convey different higher layer protocols to extend TETRA to act as an IP subnet. For more refer [12].

2.1.2 TETRA Release 2

The second set of specifications for TETRA bear the name 'TETRA Release 2', and represents the evolution of the TETRA standard. TETRA Release 2 provides additional enhancements driven by the user needs. Those enhancements resulted in the following services and facilities being standardized as part of TETRA Release 2 [13]:

- Trunked Mode Operation (TMO) Range Extension
- Adaptive Multiple Rate (AMR) Voice Codec
- Mixed Excitation Liner Predictive, enhanced (MELPe) Voice Codec
- TETRA Enhanced Data Service (TEDS)

Trunked Mode Operation (TMO) Range Extension – is the ability for TETRA to operate beyond the 58 km range limit. The TMO range of TETRA is extended up to 83 km.

Adaptive Multiple Rate (AMR) Voice Codec – is the AMR codec, operating in the 4.75 kbits/s only mode, has been chosen for possible future applications in TETRA. However, completion of the Air Interface Standard to accommodate the AMR codec is suspended in TETRA until sufficient market need is identified. For more refer [14].

Mixed Excitation Liner Predictive, enhanced (MELPe) Voice Codec – The STANAG 4591 (MELPe codec), to use its correct NATO reference, has been standardized by NATO for its own military communication applications because of its low bit rate (2400 bit/s), immunity to high background noise and acceptable voice quality performance. Because of TETRA's suitability for certain military communication applications TC TETRA carried out a technical feasibility study to see if could be supported on TETRA [15].

TETRA Enhanced Data Service (TEDS) – TEDS is a new TETRA High Speed Data (HSD) service meant to improve data transfer in TETRA system. For more refer [16].

From enhancements in Release 2, TEDS is particularly interesting, since it represents an improvement of limited data services defined in Release 1.

2.1.3 TETRA System Architecture

The TETRA system architecture consists of a number of system entities and defined interfaces. Figure 2.1 provides an overview of system elements and interfaces covered by TETRA standard.

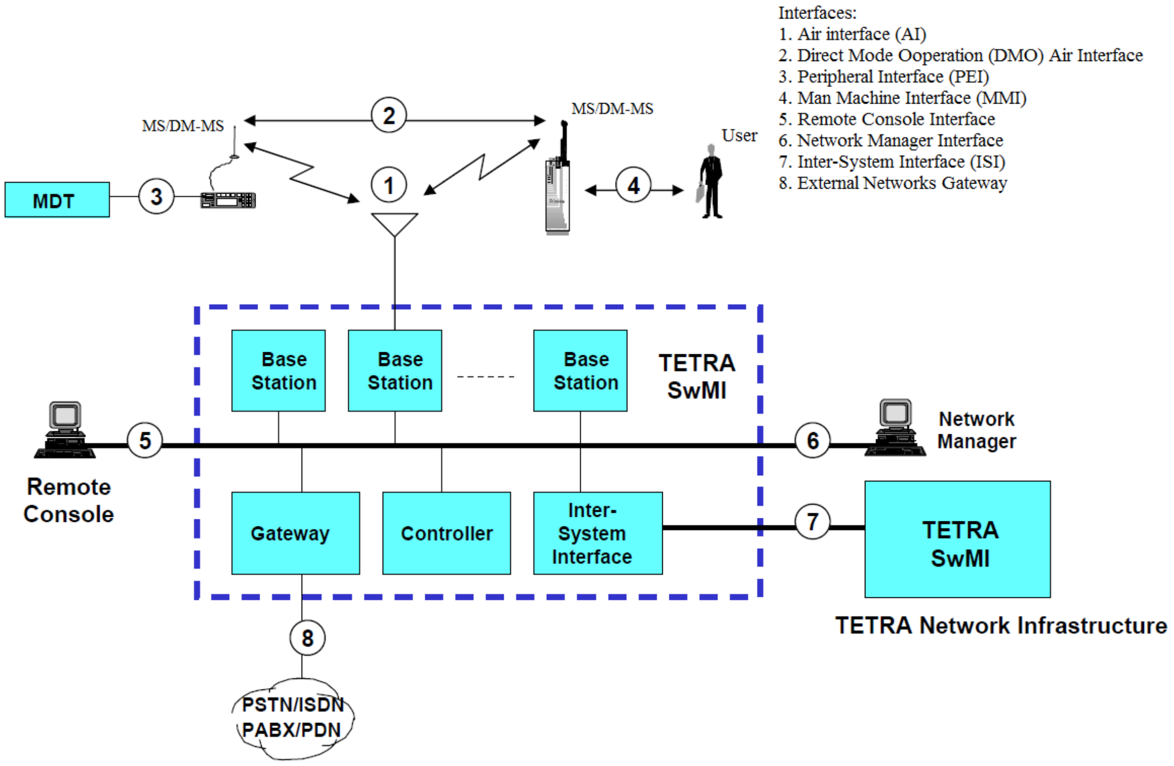
Interfaces:
1. Air interface (AI)
2. Direct Mode Ooperation (DMO) Air Interface
3. Peripheral Interface (PEI)
4. Man Machine Interface (MMI)
5. Remote Console Interface
6. Network Manager Interface
7. Inter-System Interface (ISI)
8. External Networks Gateway
MS/DM-MS
MS/DM-MS
User
MDT
1
2
3
4
5
6
7
8
Base Station
Base Station
Base Station
TETRA SwMI
Remote Console
Network Manager
Gateway
Controller
Inter-System Interface
TETRA SwMI
TETRA Network Infrastructure
PSTN/ISDN PABX/PDN

Figure 2.1: TETRA system architecture with standard interfaces [17]

System components are:

- Individual TETRA network (TETRA Switching and Management Infrastructure (SwMI))
- Mobile Station (MS)
- Direct Mode Mobile Station (DM-MS)
- Remote Console (RC)
- Network Management Unit
- Gateway
- Mobile Data Terminal (MDT)

All system components together with the interfaces between them are standardized by TETRA standard, except the internal architecture of the individual TETRA network (TETRA SwMI). Only periphery of the TETRA system is covered by the TETRA specification. That implies standardization of following interfaces (numbers in parentheses follow the numbers with which interfaces are marked on Figure 2.1).

Air Interface(s) (1 and 2) define interface between base station (BS) and mobile station (MS), and Direct Mode Operation (DMO) interface between two radios which allows them to communicate without network infrastructure. Air interface is the most important and the most complex interface of TETRA standard, for more refer [12].

Peripheral Equipment Interface (3) standardizes the connection of the MS to an external device. It also supports data transmission and to some extent control within the MS from the external device, for more refer [18].

Remote Console Interface (5) intended to standardize connection to the dispatcher consoles like in the control rooms, but it is dropped by ETSI due its complexity and mainly to allow different manufacturers to define their own interfaces since different public safety organizations were using services of different control room manufacturers.

Network Manger Interface (6) standardization of this interface is also dropped as for the Remote Console Interface since defining common network management interface was impractical. Work done on the beginning of standardization for this interface is now as a guide to assist users in defining network management requirements.

Inter-System Interface (7) allows interoperability between two or more networks which use infrastructure from different TETRA manufacturers, for more refer [19]

External Network Gateway Interface (8) standardize connections between TETRA network and external networks, like PSTN (Public Switched Telephone Network), ISDN (Integrated Services for Digital Network) and/or PABX (Private Automatic Branch eXchange), for more refer [20].

The main purpose of defining a series of open interfaces is to enable independent manufacturers to develop infrastructure and terminal products that would fully interoperate with each other as well as meet the needs of traditional public safety user organizations [21].

2.1.4 TETRA Network

In the Figure 2.1 part framed by a dotted line presents Switching and Management Infrastructure (SwMI). SwMI includes all the sub-systems that comprise a TETRA network including the base stations (BSs). Everything inside SwMI, including the base station interface and internal interfaces is not standardized to allow infrastructure manufacturers freedom and flexibility in design when finding the most cost-effective network solution. The individual TETRA network can include local switching center, mobile switching center (MSC), base station (BS), gateways, switches, operations and management center (OMC) and the associated control and management facilities.

Figure 2.2 illustrates high level overview of a TETRA network.

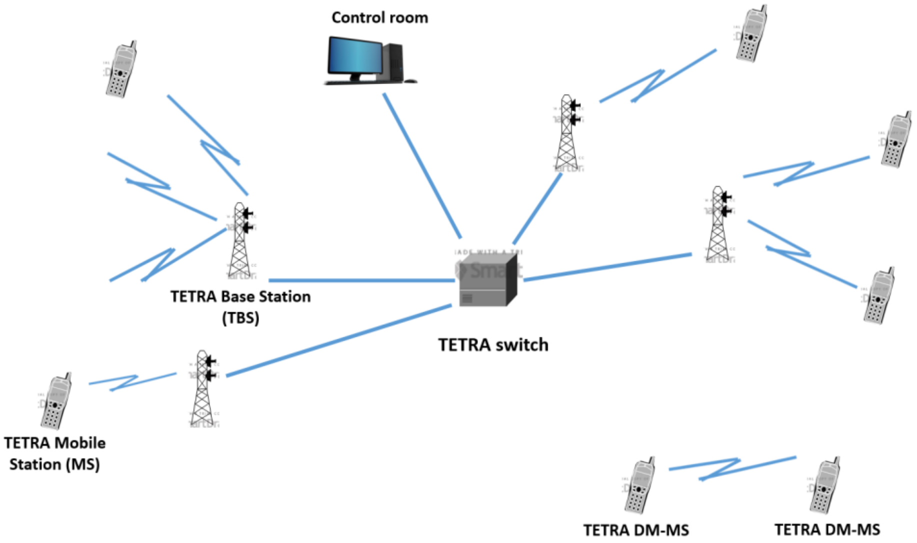

Figure 2.2: TETRA network overview [22]

Figure 2.2 provides basic TETRA network overview. Figure 2.2 shows core part of the network represented by TETRA switch and control room, then access part of the network represented by TETTRA base stations and the end-user equipment presented by TETRA mobile stations. TETRA Direct Mode mobile stations (DM-MS) work in Direct Mode Operation which will be explained shortly.

The **TETRA switch** is one functional entity of the TETRA network, it holds the database with information of the MSs together with the services assigned to them, and performs basic switching operations.

The **TETRA base station** (TBS) is an access point towards TETRA network for MSs, it sends out microwaves/radio signal thereby providing coverage for MSs and receives the TETRA signals send out by the MSs. The base stations are directly connected via backhaul links to the TETRA network switch.

Control rooms or **dispatchers** can be added to the network and they present central point of the voice communication. Control rooms (dispatchers) can communicate with end-users (which hold the MSs) and can also prioritize call from one MS over another, or enable/disable MS, authorize calls, perform Ambience Listening, etc.

Mobile Stations (MSs) are simple transceivers able to send and receive radio signals, however they are not part of the TETRA network but overall TETRA system.

2.1.5 TETRA Modes of Operation

The TETRA system allows TETRA mobile stations (MSs) to communicate in two different modes of operation:

- Trunked Mode Operation (TMO), and
- Direct Mode Operation (DMO).

2.1.5.1 Trunked Mode Operation (TMO)

Trunked Mode Operation (TMO) [23] implies using TETRA mobile station (MS) in combination with network infrastructure (SwMI). The signal transmitted from mobile station goes over the uplink to the selected TETRA base station (TBS), then over the downlink from TBS to MS if MSs are in the same coverage area, if not then signal from the TBS goes further through the switching element(s), (TETRA swith), which select proper base station for downlink, and again over another base station to the intended recipient(s), which are in the same *talkgroup*. A talkgroup represents an assigned group of mobile stations that participate in a same conversation on a trunked radio system. The TMO configuration is illustrated on Figure 2.3, here mobile station 1 is transmitting while other mobile stations (2, 3, 4 and 5, members of the same talkgroup) are receiving message.

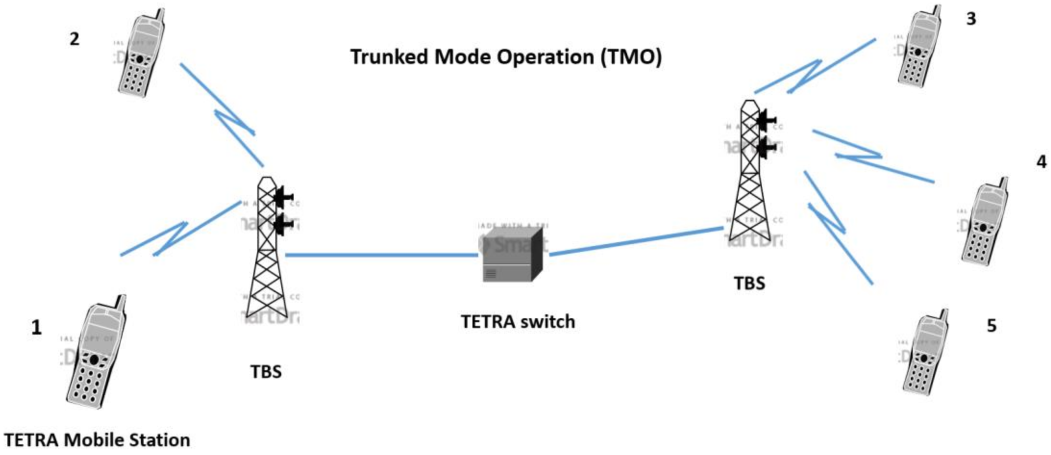

Figure 2.3: Trunked Mode Operation (TMO)

Special case when switching elements are not involved (required) for communication and only base station is needed is called *Dispatch* mode.

Dispatch Mode

In this configuration we have centralized Dispatcher connected to a base station, through which all communication goes. Two channels for uplink (mobile station to base station) and downlink (base station to mobile station) exist. Messages from the dispatcher on the downlink are/can be received by all MSs or it can be sent individually to a specific MS, while uplink messages are received only by dispatcher, so the communication between the MSs is possible only via the dispatcher, as illustrated in Figure 2.4. Connections to external networks (e.g. PSTN) are also possible only via the dispatcher.

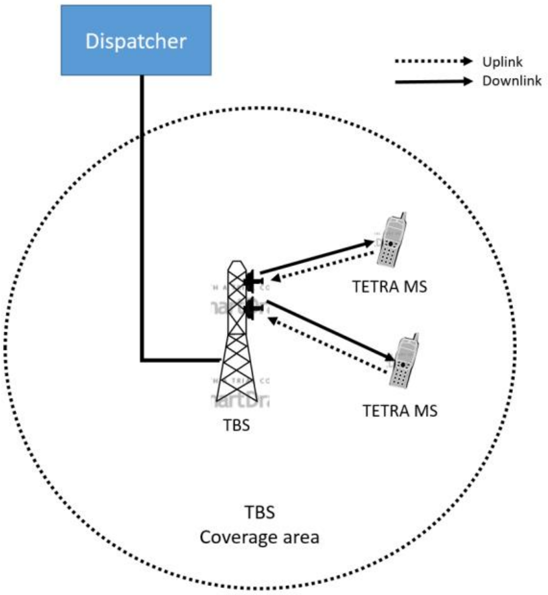

Figure 2.4: Dispatch mode configuration

Another special case only requires base station from overall network infrastructure is *Talkthrough* mode.

Talkthrough Mode Operation

In this mode of operation base station serve to extend the range of mobile stations by working as a repeater, in that way serving only as a "talkthrough" device so that central dispatch and SwMI are not necessary. As illustrated in Figure 2.5, base station only retransmits message received, for example, from TETRA MS 1, then TETRA MSs 2 and 3 (which are in the coverage of this base station) will receive that message.

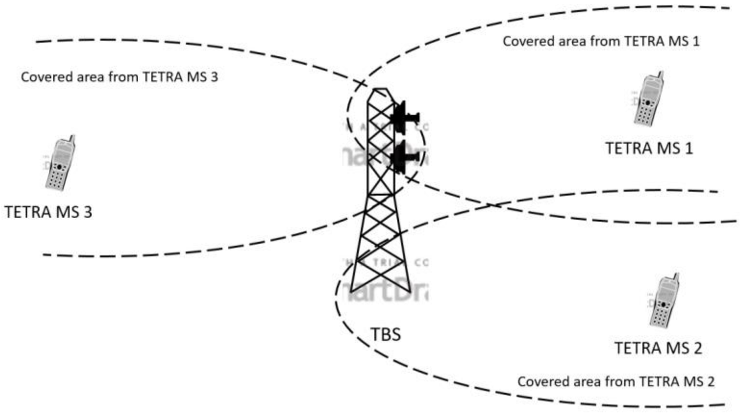
Covered area from TETRA MS 1
Covered area from TETRA MS 3
TETRA MS 1
TETRA MS 3
TBS
TETRA MS 2
Covered area from TETRA MS 2

Figure 2.5: Talkthrough Mode Operation

2.1.5.2 Direct Mode Operation (DMO)

Direct Mode Operation (DMO) [24] essentially imply direct device-to-device communication between mobile stations without network infrastructure. However, yet there are 4 operational modes of TETRA DMO [25]. They are:

- **"Back-to-back"** - direct MS to MS communication
- **Direct Mode (DM) Repeater** - serve to extend DMO MS's coverage
- **Direct Mode (DM) Gateway** - relay between DMO and TMO
- **Dual Watch** - MS scans for both DMO and TMO

"Back-to-back" mode

"Back-to-back" mode [26] implies direct communications between MSs without the need for TETRA base station (TBS). All terminals within the range of a single MS receive the message(s), as illustrated in Figure 2.6. Private communication between two MS is also possible as well as group communication within specific group (talkgroup) based on a frequency(s) selected [27].

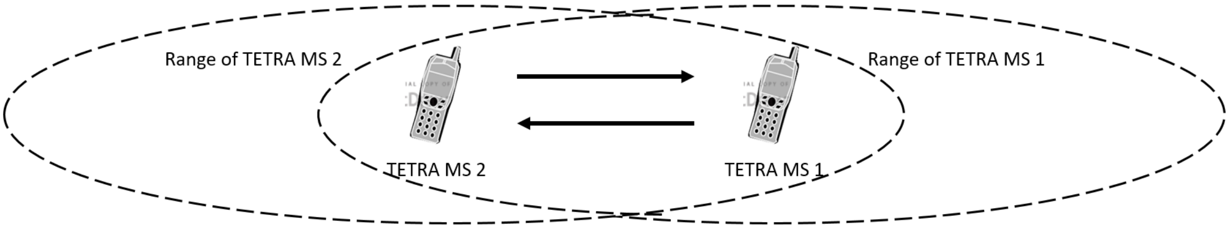

Figure 2.6: "Back-to-back" DMO

DM Repeater

In DM Repeater [28] mode of operation DMO enabled MS acts as a repeater, i.e. repeater only retransmits (repeats) the message it receives thereby enabling the communication between the MSs which are not in the range of each other, or so to say extend the range of those MSs, as illustrated in Figure 2.7. Here we see that MS of the officer on a motorcycle is not in the coverage area of the MS of the other officer so direct "back-to-back" communication between them is not possible, but the DM repeater placed on a vehicle is in the range of MSs from both officers so it serves as a repeater and the messages between these two officers, or rather their MSs, go through the DM repeater.

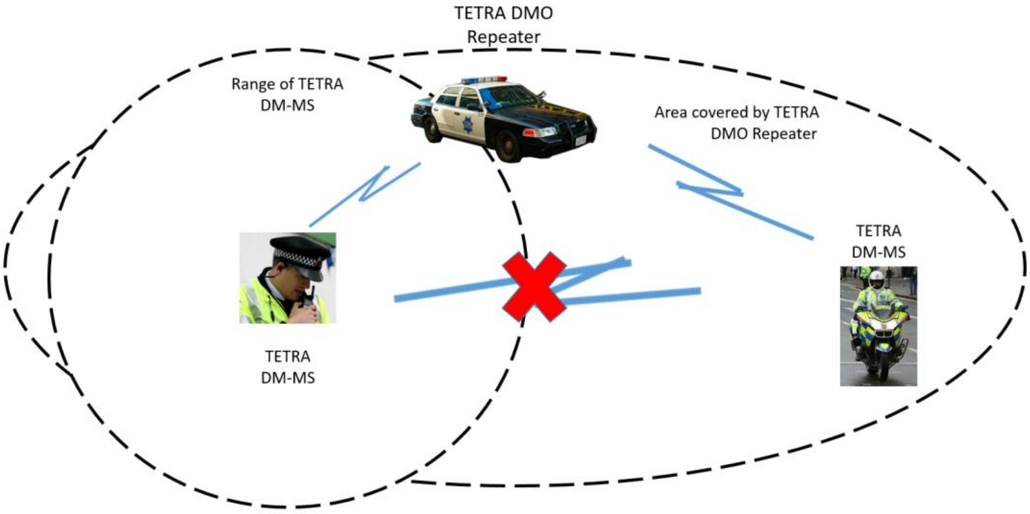

Figure 2.7: DM Repeater

DM Gateway

Special MSs can operate as DM Gateways [29]. The DM Gateway act as a “gate” between DM-MS and TMO network, and it is used to provide the coverage for hand-held MSs which have smaller range than DM repeaters (acting as gateways in this case) due to lower power restricted by battery. The DM Gateway is actually a repeater that just relays the messages between DMO and TMO. Figure 2.8 illustrates how DM Gateway works, hand-held MS is not in the coverage of the base station but the repeater mounted on the vehicle is, so it acts as a gateway for a hand-held MS which is communicating with the gateway then the gateway relays the message to base station and vice versa. In this way the DM Gateway provide TMO network range extension.

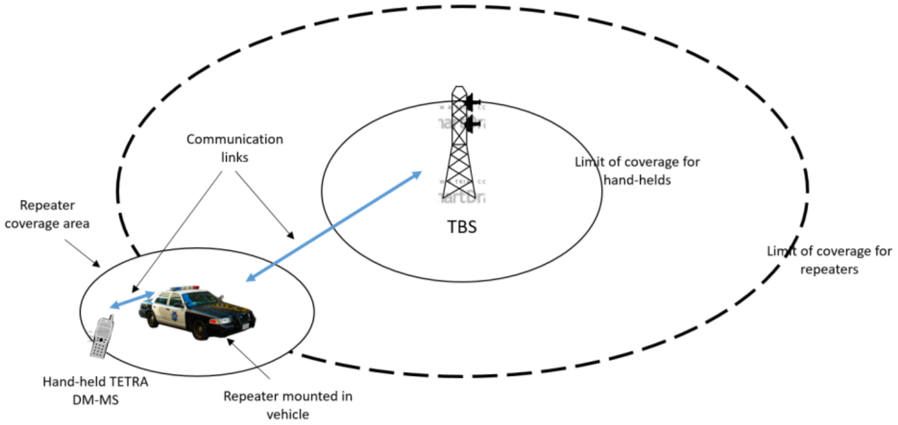

Figure 2.8: DM Gateway

DM Dual watch

Special MS equipment can act as Dual Watch [24] and get in touch with both DMO and TMO worlds simultaneously. This means that if the MS is operational in one of the modes DMO or TMO it simultaneously monitors the other mode (the one which is not used at the moment) for the incoming call. In particular, either if the MS is idle (Idle Dual Watch) or engaged in a call (Full Dual Watch) in DMO it can also receive TMO call or SDS messages from TMO users. The Dual Watch facility is possible for both, hand-held MSs and MSs with larger dimension. For hand-held MS to operate in Dual Watch mode it must be in the coverage of TMO network. Figure 2.9 illustrates TETRA Dual Watch terminal communicating with TETRA TMO and DMO MSs.

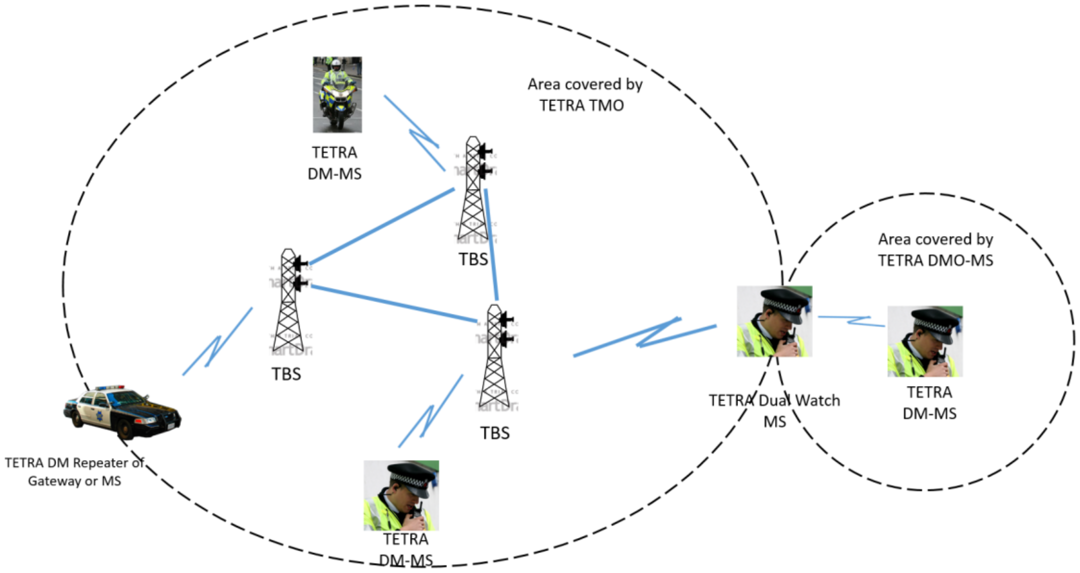

Figure 2.9: DM Dual watch

The DMO can have various applications and provide several benefits, they are [30]:

- Operation outside the coverage of TMO Infrastructure
- Gives extra capacity when TMO network is highly loaded
- Operations in poor signal strength areas
- Fall-back operation when the TMO Infrastructure is inoperative
- Covert Operations – cannot be monitored by Control rooms
- Utilities applications - used by organizations other than public safety, without requiring trunked network capacity
- Communication takes place on a *single* carrier

Direct Mode Operation (DMO) is a specific feature for TETRA (and other specialized public safety communications systems) and it is a key difference that sets it apart from other public and private cellular mobile networks.

2.2 TETRA Security

As public safety network TETRA network has to provide high level of security. The main objective of the TETRA security functions is to protect users' information, which could be speech and data traffic or information related to users' identity and operations. The TETRA security functions are separated in four different categories [31], being:

Security mechanisms. These functions are independent and self-contained, they have specific security objective such as confidentiality and authentication. Security mechanisms are considered as the main building block of a security mechanism.

Security management features. Security management features control, manage and operate the individual security mechanisms. These functions are like blood system in a human body, they connect all the parts (security mechanisms) and make sure that they work as one organism (security system). They also ensure interoperability between security mechanisms over different networks. One of the most important security management function is the Key management.

Standard cryptographic algorithms. Standard cryptographic algorithms present mathematical functions which are standardized and specific for a certain system(s). They are used to provide proper security level for the security mechanisms and the security management features.

Lawful interception mechanisms. Lawful interception mechanisms define functions which are used, in some exceptional cases (regulated by laws on national level), to provide access to information and communication. These functions should not undercut regular system security and they should be controlled through security management features.

2.2.1 Security Mechanisms

The TETRA standard specifies a number of protection mechanisms at various levels of the radio communication protocol layers, from the low level air interface to high level end-to-end user applications [32]. The TETRA standard covers security mechanisms through:

- **Authentication,**
- **Air Interface Encryption (AIE), and**
- **End to End encryption.**

These security mechanisms provide protection against well-known security threats which try to attack:

- Confidentiality – protects from eavesdropping;
- Authenticity – proof that someone is who he claim he is;
- Integrity – assurance that message has not been changed in transport;
- Availability – services are always available;
- Accountability (Non repudiation) - assurance that messages cannot be denied by message originator.

Figure 2.10 [33] illustrates which part(s) of the TETRA system is/are covered by each of the three TETRA security mechanisms, which at the same time present key functions of the TETRA security.

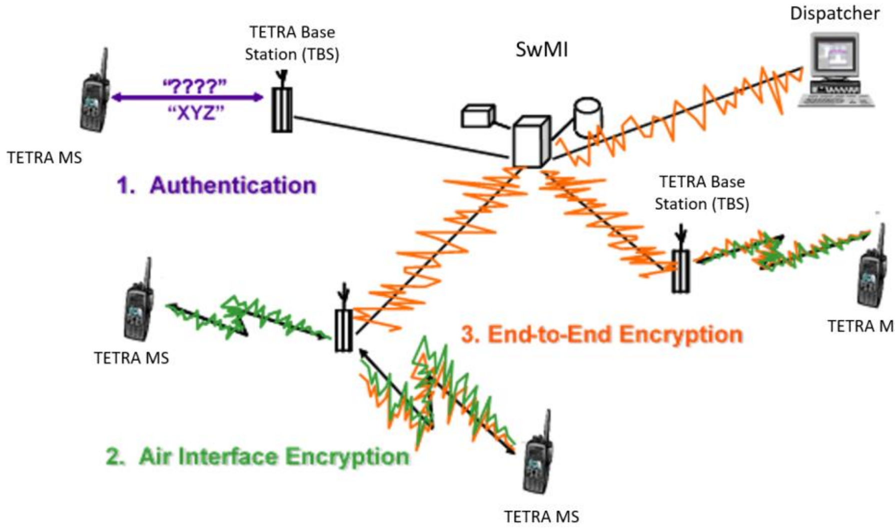

Figure 2.10: Security mechanisms' area of acting

Authentication (marked with purple in Figure 2.10) is carried out between MSs and the network (in this case TETRA Base Station (TBS)). The TETRA system provides mutual authentication, meaning that network authenticates users but the users also authenticate network. This ensures that only valid subscribers have access to the TETRA system and on the other side that subscribers only try and access the authorized TETRA system.

Air Interface Encryption (AIE) (marked with green in Figure 2.10) is in charge for radio link between TETRA mobile station(s) (MS) and TETRA base station (TBS). The role of AIE is to protect all the traffic between these two parties, including signaling and identities.

End-to-End (E2E) Encryption (marked with yellow in Figure 2.10) as the name says operates form one end to another, i.e. from one MS (transmitting end) to another MS (receiving end) or a Dispatcher as shown on the Figure 2.10. The E2E Encryption has the role to protect the information as it passes through the system, which means that message encrypted at one end can only be decrypted at the other end, and not inside the system.

The standard only specifies how the security mechanisms are integrated into the TETRA protocols, it does not specify how they are implemented or which cryptographic algorithms should be used.

2.2.1.1 Authentication

Depending on mode of operation used, TETRA system provide different ways of authentication. The mutual authentication security mechanism is only available for Voice and Data mode [34], and it is graphically illustrated in Figure 2.11 [35]. An explicit authentication is not available for DMO [36] but it is however provided through implicit mutual authentication by using Static Cipher Keys (SCK)[2] [31].

[2] In cryptography, a key is a piece of information (a parameter) that determines the functional output of a cryptographic algorithm or cipher (https://en.wikipedia.org/wiki/Key_(cryptography))

Authentication in TMO

The TETRA standard supports mutual authentication between subscriber(s) (MSs) and TETRA network (SwMI). This ensures controlled access to the network by the TETRA system (MS identity authentication by SwMI) and also guarantees that the network to which MS is attached is trusted (authenticating of the network by MS, prevention from “fake base station” attack). It also gives a possibility to the system to enable/disable Mobile Stations (MSs) or Subscriber Identity Module (SIM) cards, if used, either temporary or permanently.

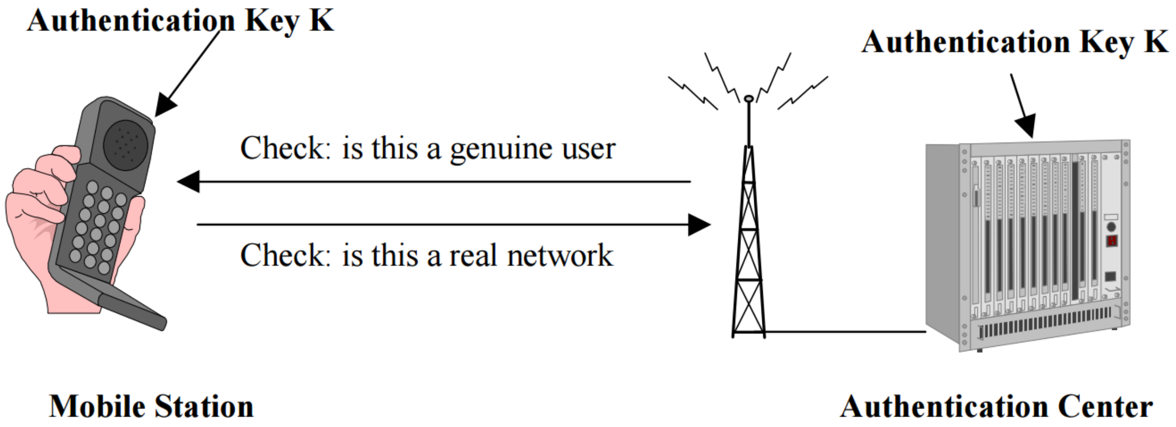

Figure 2.11: TETRA mutual authentication in TMO

Mutual authentication for V+D mode [34] is based on Authentication Key (K) [34]. Authentication Key (K) is unique for every MS. Copies of the key K are stored, one in the MS and one in the network. The network has specific element used for storing the Authentication Keys, which is part of TETRA SwMI and it is called Authentication Center (AUC). The authentication procedure is 2-pass challenge-response protocol, as illustrated in Figure 2.12 [35]. The method is symmetric secret key type, secret is Authentication Key K, known only to two authentication parties, being MS and AUC of the SwMI. The MS is representing the user (subscriber) while the representor of SwMI is not specified and in some cases TBS can be chosen to carry the authentication protocol on behalf of the Authentication Center (AUC), information needed are communicated to the TBS. Two parties, MS and network (SwMI) challenge each other and calculate the response(s) by using the Authentication Key K and challenge as input to an encryption algorithm (not specified but common for both parties), if the response is the same as the one expected then the authentication is successful. (NOTE: Successful authentication is not sufficient to guarantee access to the SwMI.) After successful authentication both parties (MS and TBS) calculate Session Authentication Key (KS) which will be used for Air Interface Encryption (AIE), in this way Authentication Key (K) of the MS is never visible outside the Authentication Centre.

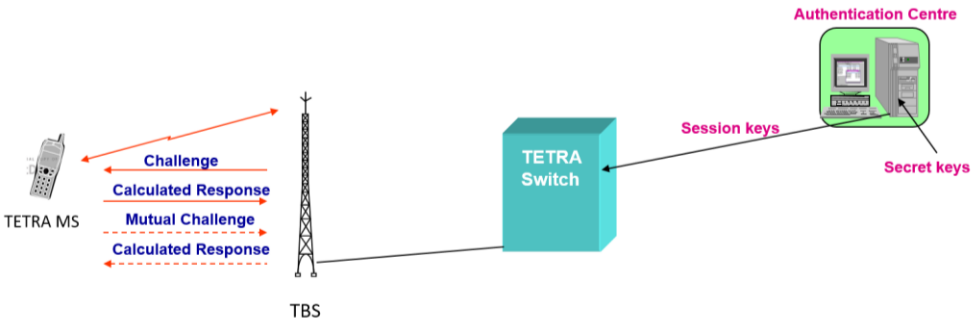

Figure 2.12: Mutual authentication procedure [33]

It is assumed that the intra-system interface (ISI) linking the authenticating entity (in this case TBS) to the authentication center (AUC) is adequately secure [34].

The authentication presents a very first basis for the overall security in TETRA system and can be used for multiple purposes, like:

- Ensure a correct billing in Public Access systems;
- Control the access of the MS to the network and its services;
- Derive a unique session encryption key, the Derived Cipher Key (DCK) which is linked to the authentication, and establish other security parameters
- Create a secure distribution channel for sensitive information such as other encryption keys;
- Control the disabling and enabling of an MS/SIM is a secure way;
- Ensure that TETRA MS's are connected to the legitimate TETRA system.

Authentication in DMO

In DMO explicit authentication between MS is not available. The DMO uses implicit authentication with static cipher keys (SCK) [36]. The fact that static cipher keys are used provides an implicit authentication between MSs and it works in a simple way: If MSs know the SCK they can successfully communicate which means that they are authenticated. The SCKs are generated, controlled and distributed through the DMO system security management which may use the TMO system or may be distributed by a fill gun [36].

2.2.1.2 Air Interface and End-to-End Encryption

The TETRA system provides different levels of encryption security. First level encryption, used to protect information over the radio link is the Air Interface Encryption (AIE), however TETRA also provide End-to-End Encryption as a top level protection in information security. Figure 2.13 [35] illustrates the difference in scopes of protection between the air interface security and end-to-end security.

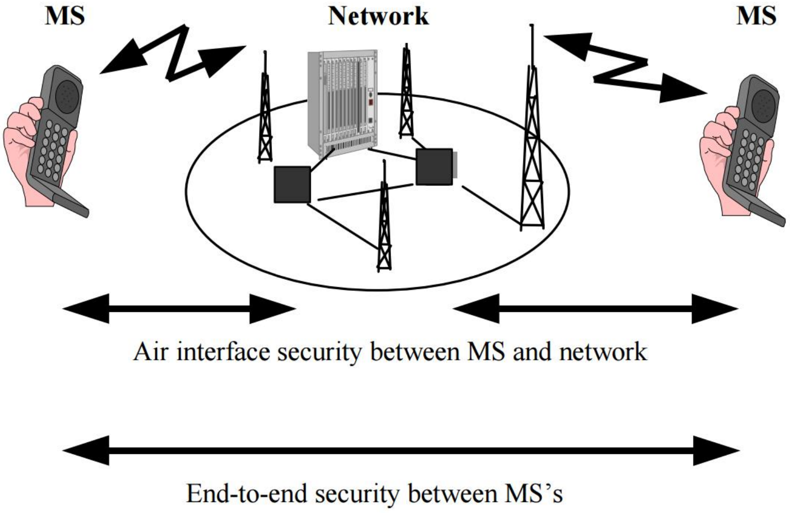
MS
Network
MS
Air interface security between MS and network
End-to-end security between MS's

Figure 2.13: Air interface security versus end–to-end security in TETRA system [35]

Form Figure 2.13 we can see that Air Interface Encryption (AIE) secures information only on the radio link between MS and base station, while End-to-End (E2E) Encryption secures information all the way it travels from one end to another, i.e. from one MS to another MS.

Air Interface Encryption (AIE)

Air Interface Encryption (AIE) comes from the need to protect user and signaling information from eavesdropping while traveling through the air, i.e. to provide confidentiality on the radio link. AIE intention is to secure communication between MSs and the TETRA network (SwMI). AIE is available for both types of communication, individual and group communication as well as for Voice + Data in Trunked Mode Operation (TMO) [34] and Direct Mode Operation (DMO) [36].

AI (Air Interface) traffic encryption protects user speech and data wile AI signaling encryption protects from traffic analysis which could lead to user identification, i.e. discovering users' identity.

End-to-End Encryption

Air interface security is in most of the cases sufficient security measure, on which one network can rely. However, TETRA system are often used by government agencies, police, military and other organizations which require extreme level of security, in those cases AIE is not considered as enough security measure. In cases when information transmitted from one MS to another requires protection not only over the air interface but also within the network, End-to-End Encryption is used.

The TETRA system has standardized support for End-to-End security service, however it does not standardize how End-to-End Encryption will be realized, so it can be realized in many ways. This ensures flexibility and gives freedom to the TETRA users to realize E2E encryption based on their own requirements. Although E2E encryption service is not standardized, TETRA provides standardized support for E2E encryption. ETSI standard [37] contains specific end-to-end specification which should ensure compatibility between infrastructures and terminals. Also, TETRA MoU – Security and fraud Protection Group (SFPG) gives End-to-End Encryption framework and provides detailed recommendation how to realize E2E encryption (E2E service) in TETRA in their report *TETRA MoU SFPG recommendation 2*[3].

End-to-End encryption cannot provide maximum security when used alone [38]. E2E encryption protects user payload, therefore only protects against confidentiality threats but not against integrity and availability threats to the system. To provide maximum protection E2E encryption should be used in conjunction with Air Interface encryption which protects from integrity and availability threats by the use of Authentication [38].

[3] Available for MoU members under a signed non-disclosure agreement; nonmembers need the support of an MoU member; Copies may be obtained from the SFPG Secretariat (Mrs. Marjan Bolle - SFPG@TandCCA.com)

Part I:

Future Mobile Broadband Public Safety Communications Systems

Chapter 3

3 Public Safety Networks and Commercial Cellular Networks Comparison

In this chapter we will compare public safety networks and commercial cellular networks in order to grasp the differences between the systems they use, and to understand how future public safety communications system should look, i.e. which characteristics should have. The networks will be compared in terms of technology, services and the way they are deployed. The TETRA and LTE networks will be taken as representative models of public safety and commercial cellular networks, respectively.

After that, explanation how next generation public safety networks should look will be given. Chapter will be concluded with examples of countries which have already started building their next-generation public safety networks.

3.1 Technology

Over the years public safety networks and commercial cellular networks have had the needs for different types of services, accordingly they were using technologies which could meet their needs.

There are three essential technologies used in communication networks [2]:

- **Narrowband (NB) technology** is designed to deliver voice-centric communication and low-speed data applications. Data rates in type of systems are limited to few tenths of kilobits per second (Kb/s).

Public safety TETRA networks use narrowband technology to deliver its services.

- **Wideband (WB) technology** refers to technologies that can deliver application data rates of several hundred of kilobits per second (384-500 Kb/s).

With Release 2, TETRA has tried to improve its data service by introducing TETRA Enhanced Data Service (TEDS) [13]. TEDS uses WB technology to provide higher data rates, up to several hundreds of kilobits per second (approx 500 Kb/s, but typically much less). However WB technology has not been widely accepted and its data rates are not high enough to support bandwidth-hungry applications [39], like Video Conferencing which requires from several hundred Kb/s up to tenths of Mb/s (megabits per second) [40] or Audio and Video Streaming which requires between 1 and 10 Mb/s [41].

- **Broadband (BB) technology** is technology which can cope with bandwidth-hungry applications. BB technology can support higher-speed data communications than WB, including high-resolution video transmission.

Data rates which BB technology can support go up to 300 Mb/s, in LTE networks. LTE networks use broadband technology to deliver its services, on downlink data rates go between 100 Mb/s and 300 Mb/s while on uplink data rates are in the range from 50 Mb/s to 75 Mb/s [42].

3.2 Services

TETRA shares many basic technology elements with cellular mobile networks, but with added unique mission critical features. Different design requirements have created significant differences between public safety networks, such as TETRA, and commercial cellular networks, such as LTE. Those different design requirements have provided public safety networks with certain services and features which are not present in commercial cellular networks, and which can be seen as TETRA systems' advantages. They are as follows [43]:

- Group calls
- Dispatcher operation
- Fast call set-up
- Supplementary services (Pre-Emptive Priority Call, Late Entry, etc.)
- Direct Mode Operation (DMO)
- Gateway mode
- End-to-end security
- etc.

What characterize public safety users is that they work in groups, accordingly they need to communicate in groups. The communication systems used in public safety have been specifically designed and optimized to meet this fundamental means of working. Commercial cellular communications systems were, on the contrary, been developed for person to person (one-to-one) communications, which makes them unsuitable for public safety communications.

For public safety users possibility to communicate even outside the network coverage is very important to have, DMO allows that type of communication. This is also not available in commercial cellular networks. In the same way rest of the services are also important for public safety users, and they are something that commercial cellular LTE networks cannot provide.

3.3 Networks

Although they cannot praise with advanced technology, what has adorned public safety networks through all these years are high level of control, security and high availability. In a past couple of decades commercial cellular networks and dedicated public safety systems had different design and deployment priorities, accordingly they were designed and deployed on different ways.

Table 3.1 [44] summarize main differences between the public safety network and commercial network models.

Issues	Commercial network operator model	Public safety network model
Goals	Maximize revenue and profit	Protect life, property and state
Capacity	Defined by "busy hour"[4] on a typical day	Defined by "worst case" scenario
Coverage	Population density	Territorial, focused whatever may need protection across a country geography
Availability	Outages undesirable	Outages unacceptable (live lost or threatened)
Communications	One-to-one	Dynamic groups, one-to-many, field crews/control centre
Broadband data traffic	Internet access (mainly downloads)	Traffic mainly within organization (more uploads than downloads)
Subscriber information	Owned by carrier	Owned by organization
Prioritization	Minimal differentiation, by subscription level or application	Significant differentiation, by role and incident level (dynamic)
Authentication	Carrier controlled, device authentication only	Organization controlled, user authentication
Preferred charging method	Per minute for voice, per GB for data, per message for SMS or Subscriptions with pre-defined amount of minutes/GBs/SMSs with fixed price	Quarterly or annual subscription with unmetered use

Table 3.1: Differences between public safety network and commercial network model [44]

Table 3.1 illustrates the differences in priorities concerning the way how networks were deployed and how they were operated. To become suitable for public safety communications, future LTE networks have to bridge these gaps and overcome limitations which are now preventing LTE networks to be used for public safety.

[4] In a communications system, the sliding 60-minute period during which occurs the maximum total traffic load in a given 24-hour period

3.4 Overcoming the Differences

Limitations of TETRA

Although built according to user requirements to provide many specific services, be reliable and secure, TETRA networks are now marked as outdated due to their inability to support advanced broadband applications. Technology these networks use prevents them in doing so. Lack of support for modern data applications was also identified as major TETRA limitation by the TETRA and Critical Communication Association (TCCA)[5] [21]. To overcome this problem TCCA formed a working group in April 2012, named Critical Communications Broadband Group (CCBG), with the mission to "*drive the development of one or more common standards for Mobile Broadband that fulfil the mobile applications needs of users who operate in a Critical Communications environment and will lobby for appropriate harmonized spectrum in which to deploy such services*" [45].

In October same year, TCCA published that LTE (Long Term Evolution) has been chosen to deliver Mobile Broadband solutions for users of Mission and Business Critical mobile communications [46]. As a result TCCA started working with 3GPP on developing standards for LTE which will support functionalities needed for mission critical communications. TCCA also started working with 3GPP to create harmonized standards among Critical Communications user community.

Result of this cooperation are new sets of specifications for Public Safety LTE (PS LTE), which should enable LTE to public safety communications. More on this in Chapter 4.

Need for Broadband

The report from Analysis Mason for the TCCA *'Public safety mobile broadband and spectrum needs'* [47] from 2010 has shown through the usage scenarios that public safety users are moving from voice-centric communications and that the usage is evolving towards information-centric operations which provide different ways of sharing information (voice, data, video). Already existing data application in TETRA systems (e.g. automatic vehicle location (AVL) and tracking, short and status data messaging, and (limited) transfer of video) were proved to be very useful. Studies, like [47], show that introduction of broadband data application, like Intranet/Internet access, Web browsing, video streaming, high-resolution imagery could bring huge gain into the public safety networks.

Besides the direct returns which may result from using above mentioned applications, some other studies, like [48], show that deployment of public safety networks based on broadband technology could potentially generate long term indirect returns in the form of various socioeconomic benefits.

Unification of Two Worlds

The fact that technology for public safety networks were developed separately and specifically for public safety market had its cost, technology for commercial networks has evolved much faster due to much bigger market and bigger financial benefit [49]. However, each of these two types of networks still have some advantages. Now, the time has come to unify those two worlds. The public safety networks will have to evolve and provide their users with services

[5] The TETRA and Critical Communication Association (TCCA) represents TETRA and all interested parties (uses, manufacturers, applications providers, operators, etc.)

which are now available only in commercial mobile broadband networks. This will require certain migration from TETRA to LTE networks. This will not be an easy change, LTE networks will need to adapt it to special requirements of public safety users. Future public safety networks should sustain the same level of control, security and high availability as currently deployed narrowband public safety networks, and also provide the advanced applications today present only in commercial networks.

User Requirements

Transition from TETRA, to LTE will not be an easy process no matter of all attractive new features which LTE could be provide. Public safety users are accustomed to standard services provided by TETRA systems, which are very important for public safety communications. Accordingly their requirements still hold true today. As identified by TCCA in [50] and [51], to completely substitute TETRA, future public safety network has to be able to provide following service:

- **Group Communications -** communications across groups of users and multiple groups of users (and other services related to group communication, such as group management, late entry, dynamic groups, etc.)
- **Device-to-device communication** – communications between mobile devices independent of the network
- **Push-to-talk (PTT) service -** communication over mobile radio network in which users press a "talk key" to activate the voice transmission path before speaking
- **Prioritization** and **pre-emption** – ability to allow the most important calls to be connected at times of congestion
- **Emergency Calls** – calls prioritized above other traffic

Beside the mentioned services, one public safety network needs to have following characteristics [44], regardless of technology used:

- **Coverage –** radio coverage should cover close to 100% of the country geographical area (for national networks) plus the possibility to operate even out of the networks' coverage (with device-to-device communication)
- **Scalability** – varying cell load, symmetric uplink/downlink usage pattern, availability of services at different speed
- **Availability** – high level of network resilience and service availability (close to 99,999% at all times, which means less than 5 min of downtime per year)
- **Security** – multiple levels of encryption to meet the needs of public safety organizations, both end-to-end and air interface
- **Interoperability** – ability to interwork with other public safety networks

Public Safety Networks Migration

Before LTE public safety networks become reality, LTE networks themselves will have to pass through personal evolution, following the user requirements described in previous sub-section. For that time public safety organizations will have to migrate from TETRA to LTE networks.

According to [49] there are three techno-economic aspects which are driving the transition of public safety networks from TETRA to LTE, those are:

- Technology dimension,

- Network dimension, and
- Spectrum dimension

Each of these dimensions plays almost equally important role in adoption of LTE as a future mobile broadband technology for public safety networks. **Technology dimension** reflects through standardization work done by 3GPP to enable LTE to become a technology of choice for public safety networks. These standards should introduce necessary functionalities in LTE systems in order to provide services which are now available only in specialized public safety systems, such as TETRA. Technology dimension will be elaborated in Chapter 4. **Network dimension** reflects through different delivery and business models which could be applied in transition from TETRA to LTE public safety networks. Network dimension will be elaborated in Chapter 6. At last, **spectrum dimension** reflects through various of regulations which should be adopted on a local and global level in order to find a spectrum which could be used for public safety needs and which will possibly be uniform across the globe. Spectrum dimension will not be elaborated in separated chapter but its significance will be explained through analysis in Chapter 6.

Deployment Models

The evolution of public safety networks will require some form of transition from the currently used systems to the future public safety communications systems. In that transition finding the right deployment scenario and associated business model for the future public safety network may have one of the crucial roles. In that sense, different implementation options need to be considered. As possible deployment models following options are identified [44]:

- LTE dedicated networks – LTE networks built for public safety communications
- LTE commercial networks – LTE commercial networks which can be used for public safety communications
- Hybrid solutions – combination of dedicated and commercial LTE networks or a combination of dedicated/commercial LTE network and legacy public safety network such as TETRA

LTE dedicated networks are specifically designed and built with the special purpose to be used only for public safety communications. These networks should be built to meet the requirements of the public safety users.

LTE commercial networks option means that public safety organizations are using the commercial LTE networks for public safety communications. In that way public safety services can be provided over existing LTE networks.

Hybrid solutions imply several different delivery options that are based on combination of dedicated and commercial (mobile broadband) network infrastructures or a combination of LTE and TETRA network infrastructures.

These delivery models will be further discussed in Chapter 0.

3.6 Transition from TETRA to LTE - Current Initiatives

Many government agencies around the world have recognized the need and benefits of having a broadband communication in their public safety networks, and some of them have already started preparing the field for future mobile broadband public safety communications systems. Some of the pioneers in this transition are Australia, Canada, New Zealand, United States, South Korea, and in Europe those are United Kingdom and Belgium. Different countries are using different deployment models, and while US are building LTE dedicated network for public safety use, Belgium is using LTE commercial network to provide data-centric application for public safety users. In addition to Belgium, Finland and France are also considering to apply the same model.

3.6.1 FirstNet in US

It could be said that US is one of the first countries that started transition towards mission critical mobile broadband networks. On February 22, 2012 contract was signed about building completely independent mobile broadband network for public safety communications, the project was named FirstNet. Development of the FirstNet [52] started by allocating spectrum dedicated only for public safety use, which is considered as one of the crucial things due to problem of its (un)availability. FirstNet project has the task to architect, deploy, operate and maintain a public safety broadband network in a given spectrum, this network should be based on a single national architecture based upon the LTE technology. US is using LTE dedicated network deploy model, which means that network is being built for public safety, with option to make their resources available to other type of users.

3.6.2 Emergency Services Network (ESN) in UK

Opposite from US, UK is using LTE commercial network model. The UK was also one of the first countries that started transition towards public safety mobile broadband networks. Currently, Airwave [53] is a network operator in charge for UK's public safety network, which is based on the TETRA technology. Since TETRA is unable to provide broadband data services and contact with Airwave expires between 2016 and 2020, UK's Home Office has decided to replace Airwave critical voice services by enhancing a commercial mobile network. The project was named 'Emergency Services Mobile Communications Programme’ (ESMCP) [54], project's task is to provide next generation communication system for public safety users. This system will be called the emergency services network (ESN) [54]. At the moment (April 2016) the ESN is in the mobilization phase, while transition is expected between 2017 and 2020.

3.6.3 ASTRID in Belgium

Belgium has chosen hybrid model. Government-owned operator ASTRID [55] has been chosen to provide services for public safety users. ASTRID operates national radio communication, paging and dispatching network which was specially designed for emergency and security services. Radio network is based on TETRA technology. To provide broadband data services to public users ASTRID has started project called Blue Light Mobile [56], in April 2014. ASTRID uses MVNO (Mobile Virtual Network Operator) model by offering services via third-party networks, i.e. public safety organizations have the option to use commercial 3G and 4G networks via a specific service [55]. Users are provided with ASTRID SIM cards which should ensure priority of public safety traffic over the non-public safety traffic. ASTRID SIM cards have 'preferred' network but are able to switch to another networks if they are out of coverage of preferred network [55]. Security aspects, like confidentiality and integrity are intended to be achieved by creating a secure VPN (Virtual Private Network) connection between mobile terminals and data centers [57], VPN connections create a kind of ‘tunnel’ for traffic. Since TETRA network is still used in parallel with 3G/4G networks, mobile terminals have to be compatible with both, 3G/4G and TETRA. Blue Light Mobile is seen as a temporary solution [57].

Chapter 4

4 LTE Technology for Public Safety Communications

After the great success of its ancestors GSM (Global System for Mobile Communications) and UMTS (Universal Mobile Telecommunications System), LTE (Long-Term Evolution) [58] became the first cellular communication technology that has brought the entire mobile industry to a single technology footprint [49]. This means that LTE standard is adopted globally. As such, it has strong technical and economic support for development. Besides that, it has plenty of advantages [49], like high bit rate, low latency, possibility to provide data-rich services etc.

Success of LTE has attracted much attention of public safety community [51], so it was not a surprise that LTE was chosen by TCCA as the future mobile broadband standard which will replace narrowband TETRA technology in public safety communications [59]. Having such standard available public safety community decided that it is better to improve LTE and adjust it to the needs of public safety communications than to develop completely new standard. One of the main reasons was that development of standards and technology for public safety market cannot attract the same level of investments as commercial domain. Improvements to LTE which will make it suitable for public safety communications were imposed as reasonable solution.

Here we describe those improvements, i.e. how LTE plans to develop and cover the needs of public safety communications.

This chapter should give an answer to question whether and when LTE could meet the public safety user requirements for services, and provide the same functionalities as TETRA, meaning:

- Group communication
- Device-to-device communication and
- Push-to-talk service
- Isolated, independent work of base station (Dispatch and Talkthrough mode)

4.1 LTE as Public Safety Mobile Broadband Standard

LTE is a standard for mobile broadband communication, developed by the 3rd Generation Partnership Project (3GPP). The LTE standardization work within 3GPP started in 2004, in Release 8 document series, and it was completed at the end of 2008 with minor enhancements described in Release 9.

The first specification for Public Safety (PS) LTE started in Release 11, which was active from 2010 until 2013, but public safety specifications were not so widespread in Release 11. Following Releases, Release 12 & 13, which have been developed in the range from 2011 to 2016, contain many specifications for PS LTE. This chapter addresses those specifications. In the following sections we describe what those specifications tend to achieve and how LTE intends to become technology of choice for public safety communications.

The Tetra and Critical Communications Association (TCCA) [21] which represents the views of TETRA and other critical communication technology users and manufacturers, is actively involved in creation of PS LTE specifications. In mid-2012 the TCCA said [60]:

"The TETRA and Critical Communications Association (TCCA) has an objective of driving the development of Mobile Broadband solutions for the users of Mission Critical and Business Critical mobile communications. Having reviewed existing technologies the TCCA believes that LTE holds the greatest prospect for delivering such solutions. As a result the TCCA intends to work with 3GPP to include the functionality necessary within the LTE standard to meet that objective."

Within TCCA a Critical Communications Broadband Group (CCBG) [61] was established to [49]:

- Drive the standardization of common, global mobile broadband technology solutions for critical communications user
- Lobby for appropriate (and as far as possible (globally) harmonized) spectrum for deployment of critical communications broadband networks

TCCA and CCBG are providing inputs to 3GPP for PS LTE specifications. Besides the standardization roadmap, TCCA, CCBG and 3GPP are also working on definition of a robust LTE migration roadmap for public safety and other critical communications network solutions. This migration roadmap should ensure safe transition from existing TETRA networks, used now for public safety, to LTE networks, which will be used for public safety in some foreseeable future.

4.2 Standardization Roadmap towards Public Safety LTE

3GPP standardization body has structured work in developing the standards for LTE Public Safety. The work is separated on Work Items, each Work Item has defined objectives and roadmap within their technical area [60]. These Work Items are developing standards which should enable LTE to support and provide services for Public Safety Communications Systems. The list of Work Items [62], classified by Releases in 3GPP, is provided below:

Release 11:

- Public Safety Broadband High Power UE for Band 14 for Region 2

Release 12:

- Study on Proximity-based Services (FS_ProSe)
- Group Communication System Enablers for LTE (GCSE_LTE)
- Proximity-based Services (ProSe)
- Study on LTE Device to Device Proximity Services - Radio Aspects (FS_LTE_D2D_Prox)
- Study on Group Communication for LTE (FS_LTE_GC)

Release 13:

- Study on Isolated E-UTRAN Operation for Public Safety (FS_IOPS)
- Mission Critical Push To Talk over LTE (MCPTT)
- Isolated E-UTRAN Operation for Public Safety (IOPS)
- Service Requirements Maintenance for Group Communication System Enablers for LTE

- Enhancements to Proximity-based Services (eProSe)

Release 14:

- Mission Critical Improvements (MCImp)
- Mission Critical Push to Talk over LTE Realignment (MCImp-MCPTTR)
- Mission Critical Services Common Requirements (MCImp-MCCoRe)
- Mission Critical Video over LTE (MCImp-MCVideo)
- Mission Critical Data over LTE (MCImp-MCData)

NOTE: Release 14 specifications are yet to be developed. Above-mentioned WIs for Release 14 have defined requirements for planned improvements and further work is expected.

Generally, overall work for PS LTE can be grouped in (for now) four main areas (without taking Release 14 into account), in which 3GPP is developing LTE enhancements to address public safety applications, those are [60]:

- **Proximity Services (ProSe)**, which should provide support for device-to-device communication when no coverage is available from the LTE network and enable mobile devices in physical proximity to discover (detect) each other
- **Group Communication System Enablers (GCSE)**, which should support group communication, such as one-to-many calling and dispatcher working and allow streaming of voice and video to multiple devices using a single downlink data stream
- **Mission Critical Push-To-Talk (MCPTT)**, which should enable one-to-one and one-to-many voice communication services. Users should be able to use those services by pressing the "talk key" to start talking, where Push-To-Talk operation is used to provide call set-up in group communications, and for that reason MCPTT is often considered as part of GCSE,
- **Isolated E-UTRAN Operation for Public Safety (IOPS)**, for isolated operation of LTE base stations when no backhaul link to the LTE core infrastructure is available. The features to be developed for MCPTT and IOPS are closely linked to ProSe and GCSE features.

However, it is important to note that work of many Work Items is interrelated and they cannot be clearly separated, same applies for specifications within one Work Item. In that sense, it is often the case that specification from one Work Item refer to specification from another Work Item or specification within the same Work Item.

Seen from an overall functionality point of view, these features are the functionalities that separate TETRA from LTE and they are the essential features that LTE **must** have before it completely substitute TETRA in public safety communications.

Releases Timeline

The production of a new 3GPP standards release usually takes between 18 and 24 months [63], and from the start to the end date of Release passes even more time [64] (up to 3 years). From the Releases' end date until the first implementations of the same Release becomes available approximately 18 months pass [65]. Figure 4.1 shows 3GPP Releases timeline, i.e. illustrates how 3GPP Releases were/will be developed through the years as well as the period in which implementations of those Releases are expected. Figure legend shows which are those new features, while matching colors illustrate in which Release they are specified.

These certain Releases are important for public safety communications since they contain specifications that define new features which will be added to LTE and which are now only inherent for public safety communications systems.

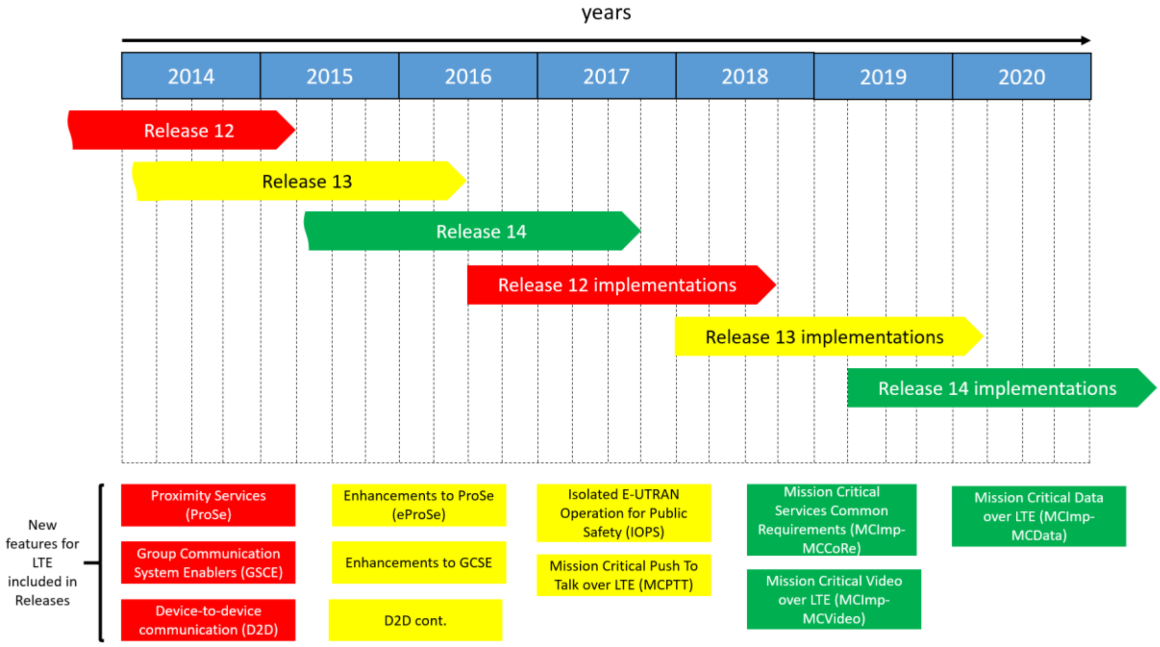
years
2014
2015
2016
2017
2018
2019
2020
Release 12
Release 13
Release 14
Release 12 implementations
Release 13 implementations
Release 14 implementations
New features for LTE included in Releases
Proximity Services (ProSe)
Group Communication System Enablers (GSCE)
Device-to-device communication (D2D)
Enhancements to ProSe (eProSe)
Enhancements to GCSE
D2D cont.
Isolated E-UTRAN Operation for Public Safety (IOPS)
Mission Critical Push To Talk over LTE (MCPTT)
Mission Critical Services Common Requirements (MCImp-MCCoRe)
Mission Critical Video over LTE (MCImp-MCVideo)
Mission Critical Data over LTE (MCImp-MCData)

Figure 4.1: 3GPP Releases' timeline

It is also worth noting that introduction of new major features into the standards typically spans several Releases, so specification for certain new feature can start in one Release and be completed in some of the next Releases. How certain features for Public Safety LTE were developed throughout Releases is illustrated in Figure 4.2. Features are represented by their respective Work Items (WIs).

Figure 4.2 presents somewhat different timeline, it graphically illustrates progress of the respective Work Items throughout Releases, including Work Items set for the next Release, Release 14. Arrows indicate that standardization work of the specific WI may be continued in the future Release(s).

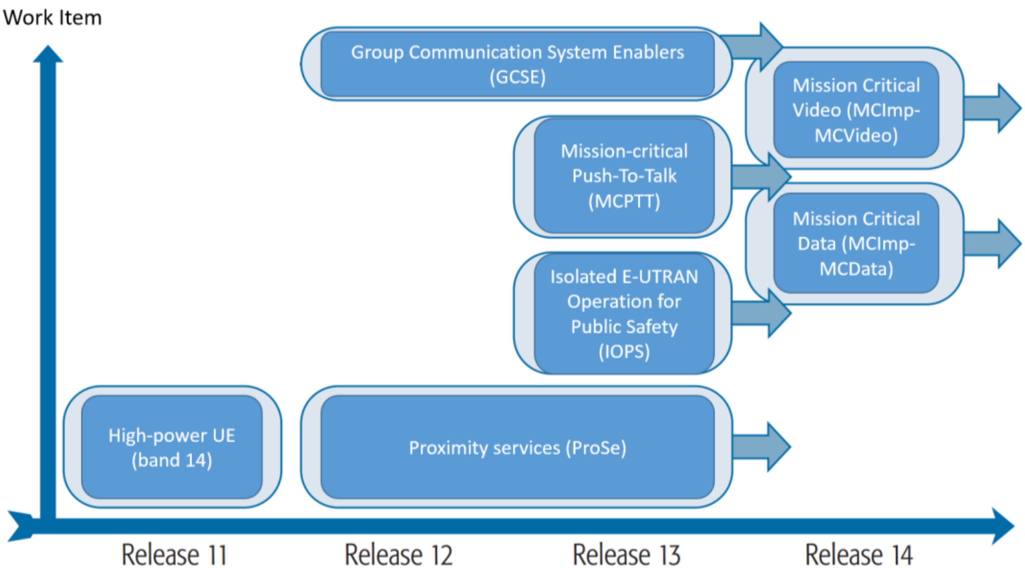
Work Item
Group Communication System Enablers (GCSE)
Mission Critical Video (MCImp-MCVideo)
Mission-critical Push-To-Talk (MCPTT)
Mission Critical Data (MCImp-MCData)
Isolated E-UTRAN Operation for Public Safety (IOPS)
High-power UE (band 14)
Proximity services (ProSe)
Release 11
Release 12
Release 13
Release 14

Figure 4.2: 3GPP Public Safety oriented WIs throughout Releases

Specifications Development

The technical work of the Work Item(s) is conducted in three stages [60]:

- Stage 1 – Requirements;
- Stage 2 – Architecture and system design;
- Stage 3 – Protocol development and solution implementation.

Within Work Items several different Technical Specification Groups (TSGs) [66] can work to address different parts of the system. In that context we have: GSM EDGE Radio Access Network (GERAN) TSG, Radio Access Network (RAN) TSG, Service & Systems Aspects (SA) TSG and Core Network & Terminals (CT) TSG.

4.3 Proximity-based Services (ProSe)

Direct communication between mobile devices when network coverage is not provided (available) is one of the central capability of the TETRA system, and can be used in several ways and for many applications, as explained in section *2.1.5 TETRA Modes of Operation* of this document. To cope with that, 3GPP started working on device-to-device communication standards in its Release 12, known in 3GPP terminology as Proximity-based Services (ProSe). In that way 3GPP is trying to become the platform of choice to exploit device-to-device communication and public safety communications in general.

4.3.2 Standardization Work

The following Work Items (WIs) within 3GPP have been developing specifications for ProSe [67]:

- Study on Proximity-based Services (FS_ProSe) [68], initiated in Release 12
- Proximity-based Services (ProSe) [69], initiated in Release 12
- Study on LTE Device to Device Proximity Services - Radio Aspects (FS_LTE_D2D_Prox) [70], initiated in Release 12
- Enhancements to Proximity-based Services (eProSe) [71], initiated in Release 13
- Study on Security for Proximity-based Services (FS_ProSe_Sec) [72], initiated in Release 12 and moved to Release 13

Table 4.1 below summarize 3GPP's technical specifications/technical reports (TS/TR) developed within WIs mentioned above. Table 4.1 includes their 3GPP index (TS/TR xx.xxx), name, release in which they are initiated, technical work stage, TSG which developed specification/report and short description.

TS or TR/ Name	Release/ Stage/ TSG	Description
TR 22.803 - Study on Proximity-based Services (FS_ProSe)	12/1/SA	Normative technical report developing use cases for ProSe
TS 22.115 - Service aspects; Charging and billing	12/1/SA	Normative requirements added for ProSe
TS 22.278 - Service requirements for the Evolved Packet System (EPS)	12/1/SA	Normative requirements added for ProSe
TR 23.703 - Study on architecture enhancements to support Proximity-based Services (ProSe)	12/2/SA	Informative technical report containing candidate architectural proposal for ProSe
TS 23.303 - Proximity-based services (ProSe); Stage 2	12/2/SA	Normative specification work of the functional architecture
TR 33.833 - Study on Security issues to support Proximity Services	12/1/SA	Study on security issues
TS 33.303 - Proximity-based Services (ProSe); Security aspects	12/2/SA	Normative specification work for ProSe security
TS 23.401 - General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access	12/2/SA	Normative requirements added for ProSe
TS 29.244, TS 29.343, TS 29.345, TS 24.333, TS 24.334 - CT aspects (ProSe–CT)	12/3/CT	Normative specification work for ProSe core network and terminals
TR 23.713 - Study on extended architecture support for proximity-based services	13/2/SA	Normative requirements document for ProSe enhancements
TR 36.843 - Study on LTE device to device proximity services; Radio aspects (FS_LTE_D2D_Prox)	12/1/RAN	Feasibility study concerning radio access

Table 4.1: 3GPP documents covering Proximity-based Services

Above listed specifications are aiming to adapt LTE system to the new type of communication, device-to-device communication, previously unknown to commercial systems. How that reflects on LTE systems is explained in the following sub-section.

4.3.4 ProSe Functional Architecture

NOTE: Readers not familiar with LTE architecture should first refer *to Appendix A (LTE Architecture).*

ProSe introduce fundamental change in how calls are routed in LTE systems, which is illustrated in Figure 4.3 [60].

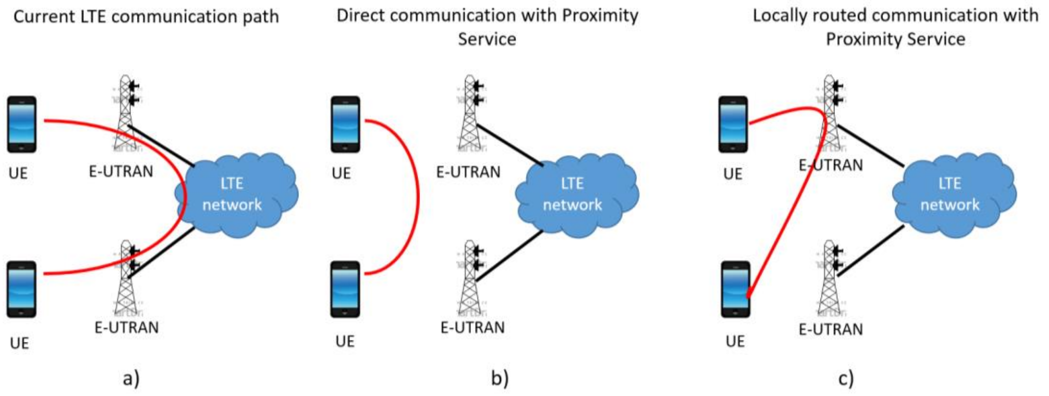
Current LTE communication path
Direct communication with Proximity Service
Locally routed communication with Proximity Service
UE
E-UTRAN
LTE network
UE
E-UTRAN
a)
UE
E-UTRAN
LTE network
UE
E-UTRAN
b)
UE
E-UTRAN
LTE network
UE
E-UTRAN
c)

Figure 4.3: Call routing in LTE with and without ProSe [60]

In commercial LTE network(s) each call (communication between two UEs) goes over access network (Evolved UMTS Terrestrial Radio Access Network (E-UTRAN)) and through the LTE core network, Figure 4.3 a). Figure 4.3 b) and c) show how call can be established in LTE with the use of Proximity Service, directly between the UEs without any help of network infrastructure (Figure 4.3 b)) and by use of access network infrastructure (Figure 4.3 c)), with the fact that the call is not routed through core network.

Beside the fact that this feature provides LTE with the service needed to become a public safety system, it can also considerably contribute to reducing the load of the network, save the network resources by not using network' help to establish communication and it can also provide communication in areas outside network coverage, which is original intention [73].

ProSe Functional Architecture

Figure 4.4 illustrates ProSe functional architecture in LTE system, with new functional entities introduced by ProSe. Beside the standard LTE entities (HSS - Home Subscriber Server, MME - Mobility Management Entity, S/P-GW – Serving/ PDN Gateway) [74], the new functional entities are:

- **ProSe Application.** The application is located on the UE side, and it uses the features provided by ProSe [67].
- **ProSe Application Server.** The application server is in charge for storage and mapping of applications and user identifiers [67].
- **ProSe Function.** It is the logical function that is used for network related actions required for ProSe [67]. The ProSe Function plays different roles for each of the features of ProSe.

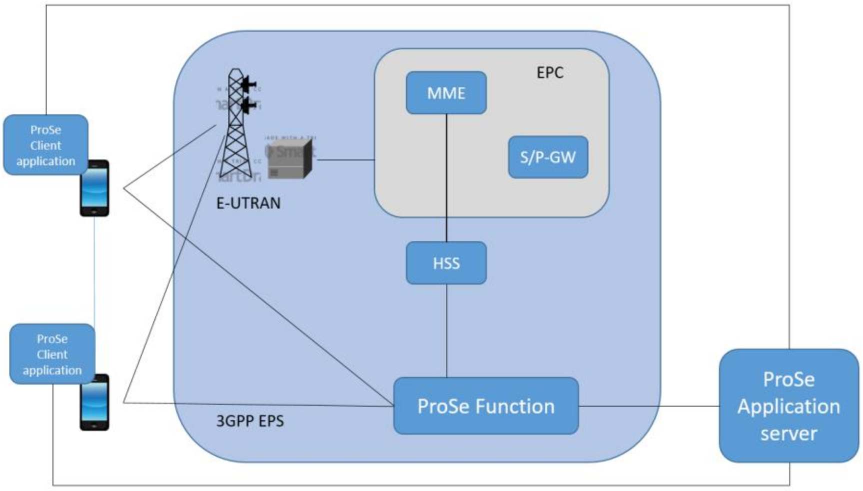

Figure 4.4: ProSe functional architecture

Light blue square represents LTE architecture (3GPP EPS - Evolved Packet System) and the grey square indicates LTE core network (EPC - Evolved Packet Core). We see from the figure that ProSe function entity will be part of LTE's architecture while ProSe Application Server may be application level solutions and it is not necessarily a physical entity but it may be part of some general Application Server located in the network.

Detailed specification on functional entities shown in the Figure 4.4, and reference points between them can be found in TS 23.303 [75].

4.3.5 ProSe Capabilities

Proximity-based Services (ProSe) WIs task is to enable direct mode or proximity ('device-to-device') services in LTE. ProSe services are based on LTE User Equipment[6] (UEs) being in proximity one to another [75] and should enable communication between UEs even when network is down or when UEs are out of coverage. Those services include [75]:

- **ProSe Discovery.** These mechanisms should allow a device to find (discover) other device when they are in physical proximity, by using direct radio link (with or without network infrastructure), denoted as ProSe Direct Discovery, or by using EPC (Evolved Packet Core), denoted as EPC-level Discovery.
- **ProSe Communications.** This should allow a device to communicate with one or more ProSe enabled devices which are within communication range. This service can work without the help of network infrastructure, communication goes directly between ProSe-enabled UEs (ProSe Direct Communication) or it can be routed via local eNB(s) (ProSe E-UTRA Communication).
- **ProSe UE-to-Network Relay.** This should allow the UE to act as a relay between network infrastructure and ProSe enabled device which is not within network coverage (similar to DM Gateway in TETRA system).
- **ProSe UE-to-UE Relay.** This should allow one UE to act as a relay between two other UEs which are out of direct communication range of each other.

[6] User Equipment (UE) in 3GPP terminology is the equivalent to Mobile Station (MS) in TETRA terminology

- **ProSe Group Communication** and **ProSe Broadcast Communication.** This should allow group and broadcast communication among a number of UEs.

ProSe Discovery

ProSe discovery between UEs can be done with or without network infrastructure help. The one that imply networks' help is called ProSe EPC-level Discovery while the opposite one is called ProSe Direct Discovery. Definition of *ProSe Direct Discovery* describes it as a process in which one UE detects another UE in proximity using E-UTRA (Evolved Universal Terrestrial Radio Access) direct radio signals (with or without E-UTRAN) [75]. Figure 4.5 illustrates the difference between Direct and EPC-level discovery. In ProSe Direct Discovery E-UTRA radio links are used and communication path goes directly between UEs (with or without E-UTRAN), while in ProSe EPC-level Discovery communication path is routed through EPC.

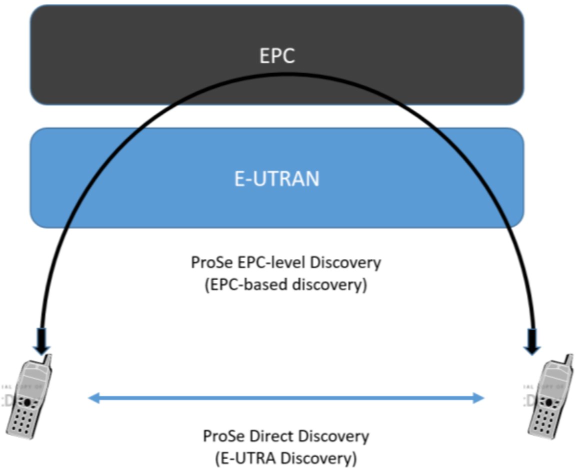

Figure 4.5: ProSe Direct Discovery vs. ProSe EPC-level Discovery

Two types of ProSe Direct Discovery exist [75]:

1. **Open** – no explicit permission from the UE is needed in order to be discovered, and
2. **Restricted** – UE has to give explicit permission in order to be discovered.

ProSe Direct Discovery defines two specific functions for public safety use [75], those are:

1. **UE-to-Network Relay Discovery** [75] - this type of discovery involves the use of pre-provisioned parameters to first discover a UE-to-Network Relay, and a subsequent communication link establishment [75]. Because only Remote UEs[7] with valid credentials and some form of pre-affiliation can successfully perform this procedure, it is restricted procedure.
2. **Group Member Discovery** [75] - this type of discovery is also a form of restricted discovery type since only users that are affiliated with each other are able to discover each other.

[7] Remote UE: A ProSe-enabled Public Safety UE that communicates with the network via a ProSe UE-to-Network Relay.

ProSe Direct Communication

ProSe Direct Communication [75] enables communication between two or more ProSe-enabled UEs that are in ProSe communication range and can apply when the UE is served by E-UTRAN and when the UE is outside of E-UTRA coverage [75]. First option include small help of network infrastructure, where only eNB is used to locally route the call and no backhaul connection with the core network is required. Second option imply direct communication between UEs, without any help of the network. Figure 4.6 illustrate the difference between ProSe Direct Communication and ProSe E-UTRA Communication. The difference is ProSe Direct Communication does not require network infrastructure in order to establish communication.

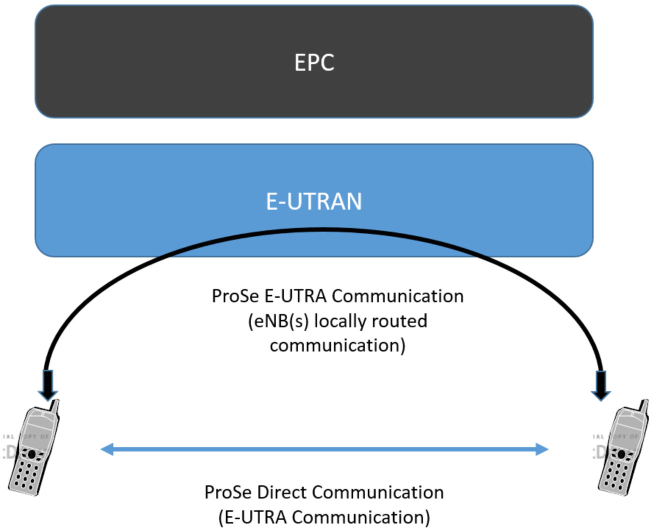

Figure 4.6: ProSe Direct Communication vs. ProSe E-UTRA Communication

In addition, ProSe Direct Communication can also be realized via ProSe UE-to-Network Relay or ProSe UE-to-UE Relay (under or off-network control). Also, it is important to note that ProSe Direct Communication can be performed in one-to-many (ProSe Group Communication) or one-to-all (ProSe Broadcast Communication) manner (under or off-network control), as described in [75].

ProSe UE-to-UE and UE-to-Network Relay

Generally, ProSe has two main features, ProSe Discovery and ProSe Communication; ProSe Relay capability can be considered as one of the functions that ProSe Discovery and ProSe Communication features can have.

The ProSe UE-to-Network Relay [75] is a functionality of an entity to support connectivity to the network for Remote UEs. A Remote UE can be located within E-UTRAN coverage or outside of E-UTRAN coverage. Figure 4.7 [75] shows architecture model using a ProSe UE-to-Network Relay. We can see that one entity behaves as a relay between Remote UE and E-UTRAN (eNB) where all the traffic goes through that entity. The ProSe UE-to-Network Relay can be used for both, one-to-one and one-to-many ProSe Direct Communication.

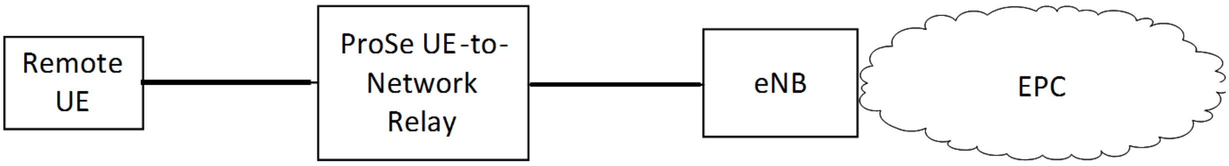

Figure 4.7: Architecture model using a ProSe UE-to-Network Relay

ProSe UE-to-UE Relay works in a similar way as UE-to-Network Relay, the only difference is that connects two UEs instead UE and the network.

4.4 Group Communication System Enablers (GCSE)

Group call, is another essential service for public safety users, both mobile users on the scene and fixed users (dispatchers) working in a control center. These capabilities are well supported in TETRA and they have been identified by TCCA's Critical Communications Broadband Group (CCBG) as one of the key applications for critical communication which should be standardized by LTE [76]. LTE systems based on releases that preceded Release 12 are optimized for one-to-one communications and they are not capable of providing group communication.

3GPP intention is to develop a Group Communication Service (GCS) for LTE, to provide a fast and efficient mechanism to distribute the same content to multiple users in a controlled manner. In TETRA, the primary use of a Group Communication Service is to provide Push-to-Talk (PTT) functionality, so a GCS based on 3GPP architecture, using LTE radio technology, should also enable PTT voice communications [77]. Moreover, Group Communication Service (GCS) is expected to support, voice, video or, more general, data communication.

4.4.1 Standardization Work

Specification development has started in Release 12 and it has been concluded under Release 13 [78]. The following Work Items (WIs) have been established within 3GPP to develop specifications for group communication and PTT application over LTE:

- Group Communication System Enablers for LTE (GCSE_LTE) [79], initiated in Release 12
- Study on Group Communication for LTE (FS_LTE_GC) [80], initiated in Release 12
- Service Requirements Maintenance for Group Communication System Enablers for LTE (SRM_GCSE_LTE) [81], initiated in Release 13

Table 4.2 summarize 3GPP's technical specifications/technical reports (TS/TR) developed within WIs mentioned above. Table 4.2 includes their 3GPP index (TS/TR xx.xxx), name, release in which they are initiated, technical work stage, TSG which developed specification/report and short description.

TS or TR/ Name	**Release/ Stage/ TSG**	**Description**
TS 22.468 - Group Communication System Enablers for LTE (GCSE_LTE)	12/1/SA	Normative requirements document
TR 23.768 - Study on architecture enhancements to support Group Communication System Enablers for LTE	12/1/SA	Informative technical report containing candidate architectural proposal for GCSE_LTE
TS 23.468 - Group Communication System Enablers for LTE (GCSE_LTE)	12/2/SA	Normative specification work of the functional architecture
TR 36.868 - Study on Group Communication for LTE (FS_LTE_GC)	12/1/RAN	Group communication requirements for evaluation of E-UTRA
TR 33.888 - Study on security issues to support Group Communication System Enablers (GCSE) for LTE	12/2/SA	Study on security issues
TS 33.246 - 3G Security; Security of Multimedia Broadcast/Multicast Service (MBMS)	12/2/SA	Normative specification work for GCSE security
TS 22.468 - Service Requirements Maintenance for Group Communication System Enablers for LTE (SRM_GCSE_LTE)	13/2/SA	Normative requirements document
TS 29.468, TS 29.213, TS 29.214, TS 29.468, TS 29.212, TS 29.274, TS 23.007, TS 23.008, TS 24.301 - CT aspects (GCSE_LTE-CT)	12/3/CT	Normative specification work for GCSE core network and terminals
TS 36.413 - Group Call Embms congestion management for LTE: Core Part (GCSE_LTE-MBMS_CM_Core)	12/3/RAN	Normative specification work for GCSE_LTE improvements

Table 4.2: 3GPP documents covering Group Communication System Enables for LTE

What is meant to be achieved with above listed specifications is to develop extensions, denoted as Group Communication System Enablers for LTE (GCSE_LTE). GCSE are modular functions and open interfaces (e.g. a resource efficient distribution mechanism) that can be used to design Group Communication Services. Among other, GCSE should enable priority and pre-emption services, and interaction with Proximity-based Services (ProSe), another important functionalities for public safety communications.

4.4.2 Group Communication System Functional Architecture

Figure 4.8 illustrates group communication system functional architecture in LTE system, with new functional entities introduced by GCSE. Beside the standards LTE core entities (HSS, MME, S/P-GW, PCRF), new functional entities added are [82]:

- **GCS Client Application.** The application is located on the UEs side, and it uses the features provided by GCS.
- **GCS Application Server.** 3GPP's Group Communication Service (GCS) concept is based on the GCS Application Server (GCS AS) [82]. GCS AS uses enablers to provide GCS, these enablers are denoted as Group Communication System Enablers (GCSE). This should enable one-to-one and one-to-many type of communication. The GCS AS uses EPC (Evolved Packet Core) bearer services and/or MBMS (Multimedia Broadcast Multicast Service) bearer services for transferring application signalling and data on the downlink towards UEs (in some situations they can be used in parallel), UEs can only use EPC bearer services for the same purpose in the uplink direction towards GCS AS [82].

MBMS-GW (MBMS Gateway) and BM-SC (Broadcast Multicast Service Centre) functional entities are added to MBMS.

- **BM-SC** – provides functions for MBMS user service provisioning and delivery [78].
- **MBMS-GW** – provides the interface for the entities that are actually using the MBMS bearers [78].

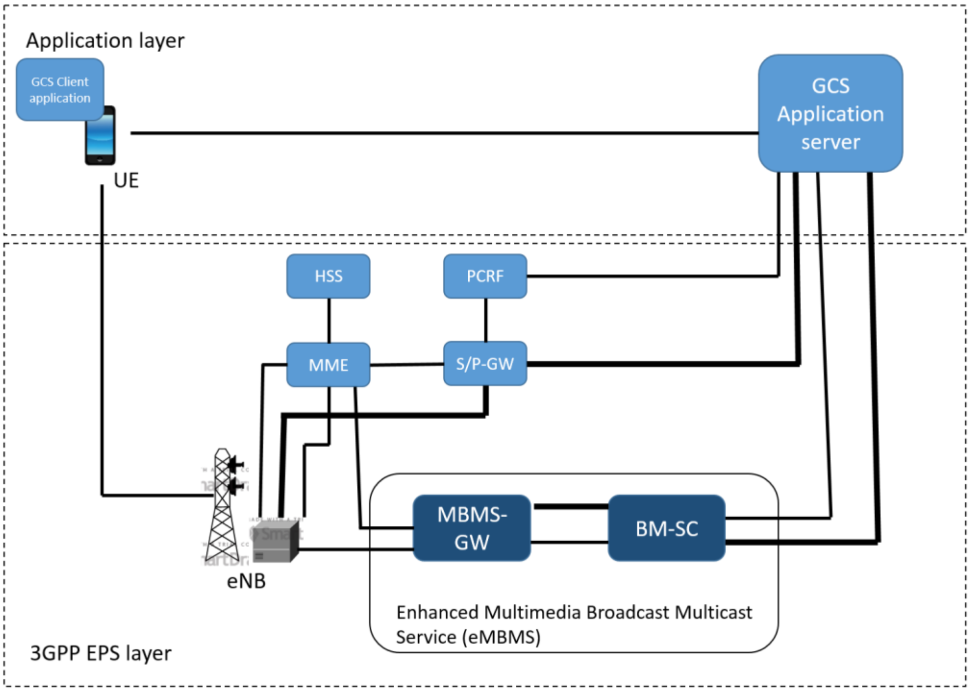

Figure 4.8: GCSE functional architecture

As shown on the Figure, the architectures is split into two separate layers (framed with dotted lines) [78]:

1. The **application layer**. This layer hold the core functionalities of the group communication service, which could be distributed between Group Communication Service Application Server (GCS AS), on the network side, and a GCS Client Application (GCS CA) running on a UE terminal.
2. The **3GPP EPS layer**. This layer enables information flow between the application layer entities. This, so called, delivery service includes both, unicast and multicast delivery. Multimedia Broadcast Multicast Service (MBMS) is a solution developed by 3GPP (denoted also as evolved MBMS (eMBMS) in LTE) to provide multicast/broadcast delivery

mode. For that reason MBMS functions are also included in the 3GPP EPS layer. In this way application layer can use unicast EPS bearer services and MBMS bearer services[8] to support GCS.

More information on network entities shown in Figure 4.8 and reference points between them can be found in [82].

4.5 Mission Critical Push-To-Talk (MCPTT)

PTT describes communication over mobile radio network in which users press a "talk key" to activate the voice transmission path before speaking. PTT can be used to realise one-to-one or one-to-many calls. PTT service usually imply simplex type of communication, that is, only one user is allowed to speak and be heard at the time, although full duplex communication is also possible in some technologies (not in TETRA). The user speaking/transmitting is said to hold the 'floor'.

WI MCPTT is complementing the work done by ProSe WIs and GCSE WIs, with further features that are needed to support an MCPTT service over LTE. In some way, MCPTT service presents realization of Group Communication Service (GCS) by giving GCS a real application.

4.5.1 Standardization Work

Specification development was initiated and completed in Release 13. Entire work was conceived within one Work Item, named Mission Critical Push To Talk (MCPTT). Table 4.3 summarize 3GPP's technical specifications/technical reports (TS/TR) developed within this WI.

[8] In telecommunications, **Bearer Service** is a service that allows transmission of information signals between network interfaces (https://en.wikipedia.org/wiki/Bearer_service); The **MBMS bearer** is used to transport data on the downlink from the GCS AS to the UE [82].

TS or TR/ Name	Release/ Stage/ TSG	Description
TR 23.779 - Study on Application Architecture to support MCPTT	13/1/SA	Informative technical report containing candidate architectural proposal for MCPTT
TS 23.179 - Functional architecture and information flows to support MCPTT	13/2/SA	Normative specification work of the functional architecture
TS 22.179 - Mission Critical Push To Talk (MCPTT) over LTE	13/2/SA	Normative requirements document
TS 33.179 - Security of MCPTT	13/2/SA	Normative specification work for MCPTT security
TR 33.879 - Study on Security Enhancements for MCPTT	13/2/SA	Normative specification work for MCPTT security improvements
TR 26.879 - Study on media, codecs and MBMS enhancements for MCPTT	13/2/SA	Normative specification work for MCPTT improvements
TS 26.179 - MCPTT Codecs and media handling	13/2/SA	Normative requirements document
TR 24.980 - IMS Profile to support MCPTT (MCPTT-Prof)	13/2/CT	Normative requirements document
TS 24.379, TS 24.380, TS 24.382, TS 24.383, TS 24.384, TS 29.165, TS 23.003, TS 23.008, TS 29.283, TS 31.102, TS 31.103 - CT aspects (MCPTT-CT)	13/3/CT	Normative specification work for MCPTT core network and terminals

Table 4.3: 3GPP documents covering MCPTT over LTE

Key requirements that MCPTT specifications should meet are summarized below:

- Support for one-to-many communication groups
- Dynamic group creation
- Monitoring of multiple PTT groups
- Authentication, authorization and security control for PTT groups
- One-to-one private call
- Announcement group calls
- Support of ruthless pre-emption
- Support of imminent peril and responder emergency calls including prioritization above normal PTT calls
- Identity and personality management
- Location information for PTT group members

- Support of off-network PTT communications and its operation together with on-network PTT at the same time

These requirements at the same time represent the features that MCPTT Service should provide, and features which LTE is missing to completely replace TETRA.

4.5.2 MCPTT Functional Architecture

The MCPTT service over LTE is an application level solution and it builds on the LTE system architecture extended with the GCSE and ProSe capabilities, but specific MCPTT functional architecture is not defined.

The functional model for the support of MCPTT defines two separate planes. This should allow a breakdown of the MCPTT architectural description. Each plane operates in an independent manner, however planes are interconnected to provide each other services when requested.

MCPTT functional model defines two different planes:

- **Application plane.** This plane is responsible for providing all services provided by MCPTT and required by the user, it also provides necessary functions to support media control and transfer. To support those requirements it uses services provided by signalling control plane.
- **Signalling control plane.** This plane provides the necessary signalling support to establish the association of users involved in an MCPTT call or other type of call and other services. It also offers access to and control of services applicable to calls.

Each of above mentioned planes has its specific functional architecture, both, for on-network and off-network scenarios, with plane specific functional entities described in TS 23.179 [83].

4.5.3 MCPTT Capabilities

The MCPTT Service provides a method by which two or more users may engage in communication [84]. The MCPTT Service will support group calls (communication between several users) and private calls (communication between pair of users). Users will request the permission to talk by pressing the ‘talk key’ on their UE, these request will be regulated by ‘floor control’. In situations when multiple requests occur decision which user gets permission to talk will be determined based on priorities, this will also allow users with higher priority to interrupt the current talker. Time in which one user can talk (hold the ‘floor’) will be limited with ‘Hold the floor’ mechanism in order to enable users with the same or lower priority to gain the floor, i.e. get permission to talk. Late call entry will also be possible to allow user to join an already established MCPTT group call. Also, priority and pre-emptive call services will be realized through MCPTT.

The MCPTT Service will be available within the network coverage and outside the network coverage, based on ProSe. Although MCPTT service focus on the use of LTE it will be also possible to access the MCPTT Service through non-3GPP access technology and for such purpose special interfaces will be designed.

More applications are expected to be added with Release 14.

4.6 Isolated E-UTRAN Operation for Public Safety (IOPS)

In public safety networks, the benefit of ensuring the ability to communicate between public safety officers on the ground is of the utmost importance, even though they may be moving in and out of LTE network coverage or following the loss of backhaul communications [85]. In TETRA network these are ensured with Dispatch and Talkthrough modes of operation. As two main reasons for introducing this possibility in LTE following scenarios are listed:

1. When UE-to-UE direct communication ensured by Proximity Services may not be enough to provide voice, video, and data communication service for public safety officers who are out of LTE network coverage so public safety organizations may deploy a dedicated eNB(s) for nearby Public Safety UEs.
2. When some major incident interrupts the backhaul and/or the link(s) between the eNBs but the eNBs are still operational.

In such situations it is expected from eNBs to act alone, isolated from the network, and provide isolated operation to ensure communication between public safety officers.

This was also recognized by 3GPP as one of the crucial capabilities that should be added to LTE in order to be suitable for public safety communications.

4.6.1 Standardization Work

Specifications development was initiated and completed in Release 13. Entire work was conceived within one Work Item, named Isolated E-UTRAN Operation for Public Safety (IOPS). Table 4.4 summarize 3GPP's technical specifications/technical reports (TS/TR) developed within this WI.

TS or TR/ Name	Release/ Stage/ TSG	Description
TR 22.897 - Study on Isolated Evolved Universal Terrestrial Radio Access Network (E-UTRAN) Operation for Public Safety (FS_IOPS)	13/1/SA	Normative technical report developing use cases for IOPS
TS 22.346 - Isolated Evolved Universal Terrestrial Radio Access Network (E-UTRAN) operation for public safety; Stage 1	13/1/SA	Normative requirements document
TS 23.401 - General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access	13/2/SA	Normative specification work of the functional architecture
TS 33.401 - 3GPP System Architecture Evolution (SAE); Security architecture	13/2/SA	Normative specification work for IOPS security
TS 31.102 - CT aspects	13/3/CT	Normative specification work for USIM applications

Table 4.4: 3GPP documents covering IOPS

Isolated E-UTRAN Operation for Public Safety (IOPS) is fully defined through above listed specifications, starting from TR 22.879 [86] which defines different use cases for IOPS, over TS 22.346 [87] which defines service requirements and TS 23.401 [88] which provides implementation and deployment guidelines to TS 33.401 which describes IOPS security solution, finally TS 31.102 [89] define Universal Subscriber Identity Module (USIM) application dedicated for IOPS. Result should be ability of LTE's base stations (eNBs) to work independently.

4.6.2 IOPS Capabilities

Isolated E-UTRAN Operation for Public Safety (IOPS) provides the ability to maintain a level of communications for public safety users, via an IOPS-capable eNB (or set of connected IOPS-capable eNBs), following the loss of backhaul communications [88].

Standalone IOPS-capable eNBs, so called Nomadic eNBs (NeNBs) can be used to establish serving radio access network without backhaul communications which will provide support for local services to public safety users in the absence of normal LTE infrastructure availability. This gives a possibility of creation of isolated public safety networks using a Local EPC (Evolved Packet Core). Isolated public safety networks using a Local EPC concept is based on assumption that the IOPS-capable eNB is co-sited with, or can reach, a Local EPC instance which is used in IOPS mode [88]. The Local EPC instance includes at least MME, SGW/PGW and HSS functionality. The Local EPC acts as an IP router among the UEs locally attached to the same IOPS network. When operating in IOPS mode IOPS-enabled UEs only use the appropriate USIM (Universal Subscriber Identity Module) credentials defined in the UICC (Universal Integrated Circuit Card), i.e. those defined exclusively for use in an IOPS network.

4.7 Standardization Work Overview and Evaluation

Much has been done in the development of standards for Public Safety LTE. 3GPP has taken public safety market seriously which can be seen through the mass of public safety related standards published in the latest Releases. Intention of 3GPP is to enable LTE to provide services which are inherent for TETRA system (and other systems of that kind).

This chapter shows that 3GPP Public Safety LTE (PS LTE) specifications cover all TETRA key services in Release 12 & 13, through ProSe, GCSE, MCPTT and IOPS. For now, these PS LTE services will only be equivalent to voice-centric TETRA services, but with Release 14 true benefit of LTE will be added to them, by introducing Mission Critical Video over LTE (MCImp-MCVideo) and Mission Critical Data over LTE (MCImp-MCData).

Planned capabilities for ProSe will provide LTE with functionalities which are now provided to TETRA by DMO. Fundamental functionality of device-to-device communication (DM 'Back-to-Back') outside the network coverage is covered with ProSe Communication feature, DM Repeater functionality will be replaced by UE-to-UE Relay while UE-to-Network Relay will replace DM Gateway functionality. It remains unclear does Dual Watch functionality will also be implemented in LTE. However, ProSe adds one new functionality that may be useful, that is ProSe Discovery, i.e. possibility to discover other ProSe enabled devices in proximity. Real potential of this functionality is yet to be explored.

GCS (Group Call Service) presents big turn in a way how communication could be carried out in commercial cellular communication systems. Traditionally, only one-to-one type of communication is available in such systems. GCSE will enable one-to-many type of communication in LTE system and bring it one step closer to public safety communications. GCSE should setup the environment for creating different kind of services which are based on group communication, Group Call before all, which is one of the essential service in public safety communications systems.

MCPTT service will exactly build upon that beforehand created environment. GCSE and ProSe provide LTE system with functionalities needed to support an MCPTT service. MCPTT service exploits those functionalities by using them to provide different applications, like dynamic groups, prioritization and pre-emption, late entry, etc.

It is worth noting that there are existing initiatives and commercial solutions for PTT over LTE which are available today. These solutions are offered in form of [44]: **a)** software application that provides PTT on a legacy network or a network that does not offer it as a core service (e.g. WAVE application by Motorola Solutions) or; **b)** as a vendor solution for the dedicated deployment and operation of a specific user base (e.g. Samsung's solution for South Korea). Samsung, which is deploying Korea's Public Safety LTE network has already demonstrated MCPTT over LTE in mid-2015 [90], and they also did some testing for GCSE in the beginning of 2016 [91]. However, these solutions are Proprietary LTE solutions and they are not compliant to 3GPP standards.

IOPS itself is not a service, but it is a useful functionality for public safety communications systems. It contributes to network services availability and to the robustness of the network itself by enabling eNBs to work independently, without a backhaul communications with the core network. As we explained in section 4.6, IOPS-capable eNB could complement somewhat 'limited' capabilities of ProSe, when ProSe E-UTRA Communication is used.

Cooperation between ProSe and IOPS is not a unique case. Most of these services are based on functionalities provided by other service or they are complementing each other. ProSe Group Communication and ProSe Broadcast Communication will not be possible without GCSE implemented in the system, just as MCPTT service off-network will not be possible without ProSe, etc. Taking this fact into account, we see the importance of standardized solutions which can seamlessly interwork.

4.7.1 The Availability of Technology and the Timeline

In the past few years 3GPP has done huge work to bring LTE closer to the public safety communications. It is doubtless that is some near future LTE will become number one technology for mission critical communication. Before that becomes a reality LTE will have to prove that it is a decent successor of a current public safety communications systems.

First steps in creating the environment for mission critical mobile broadband networks have been made, a lot of new specifications for Public Safety LTE are adopted, especially in the latest 3GPP's Releases, Release 12 & 13. However, work in this area is relatively new. Decision to start standards development for mission critical mobile broadband networks has been made in 2012 and the first step has been done in 2013 in Release 11 when 3GPP published first standards that should create environment for Public Safety LTE, with the working title "*Public Safety Broadband High Power UE for Band 14 for Region 2*". Next Release, Release 12 contained much more standards which addressed Public Safety LTE, they were mainly focused to provide support for direct communication between devices, without network infrastructure (Proximity-based Services (ProSe)) and support for group communication (Group Call System Enablers for LTE). Freezing date for Release 12 was set for December 2014, however that happened in March 2015. Work on ProSe and GCSE_LTE has been continued in Release 13. Release 13 also addressed other important parts of public safety systems, those were *Mission Critical Push To Talk over LTE (MCPTT)* and *Isolated E-UTRAN Operation for Public Safety (IOPS)*.

For the sake of comparison, most of the currently operational LTE networks are based on Releases 8 & 9 [92], although some of the networks, like in South Korea [93] are running LTE-Advanced solutions whose development started from Release 10 onwards. To understand the timing concept, Release 8 and 9 (on which most of the worldwide LTE networks are based) were developed from 2008 and 2009 until 2010 and 2011 respectively, while Release 12 and 13 (which contain specifications for Public Safety LTE) from 2011 and 2012 until 2015 and 2016 respectively. Taking into account that most of the LTE networks are based on specifications from Release 8 and 9, completed in 2010-2011, it is reasonable to think that it will pass some time before first implementations of specifications from Release 12 and 13 for Public Safety LTE become available.

The same way as Release 9 complements Release 8 with necessary enhancements, the Release 13 complements Release 12 with enhancements needed to establish Public Safety LTE. Implemented solutions based only on Release 12 would be incomplete. Release 13 was frozen in March 2016 [94]. Current status, in April 2016, of features developed for PS LTE is: ProSe - 94% defined, GCSE_LTE - 99% defined, MCPTT - 93% defined and IOPS – 100% defined [95].

Release 12 timeline [65] predicts that first implementations from this Release will be available in the mid-2016, while Release 13 first implementations are expected to be available in late 2017 [65]. In the mid-2016, when this document was written, there was no sign of implementation of any Public Safety LTE feature, which shows that Release 12 timeline predictions were wrong. Taking into account all the circumstances, and that specifications for new LTE features are near the end or just finished, it is more realistic to expect that first implementation of any new LTE feature become available late 2017.

Countries which are implementing Public Safety LTE solutions on the individual basis (like South Korea, UK, Qatar [96]) are accelerating development. Although they use proprietary LTE solution, this may encourage other countries to start deploying Public Safety LTE which could help standardized LTE solutions to be implemented sooner than expected in the years that come.

4.8 Chapter Summary

This chapter has provided insight in ongoing evolution in LTE standardization towards public safety communications. Here we have reflected on the work done by 3GPP Work Items responsible for PS LTE specifications development. We have explained how work within these Work Items is structured and how these Work Items are grouped according to feature for which they are developing specifications. Special emphasis was on describing the functionality of intended features. We have then described, from the functional level, how these features are supposed to work and what their functionality is. The importance of presenting functional architectures reflects in creating the picture of the changes which should be made on the standard LTE system in order to introduce these features. These changes imply introduction of new network entities. New LTE functionalities, ProSe, GCSE, MCPTT and IOPS should enable LTE to provide services similar to those provided in TETRA networks, meaning device-to-device communication (DMO), group call, Push-to-talk service with priority, pre-emptive and late entry functionality, as well as Dispatch and Talkthrough mode, respectively.

Chapter 5

5 Security Enhancements for Public Safety LTE Features

Security plays important role in any mobile network, however public safety networks are used for the purpose of creating a stable and secure environment, maintaining law and order and more importantly protecting life and values of citizens [2]. Therefore, security in those networks has one of the top priorities. Given that the features presented in Chapter 4 are new for LTE system and commercial cellular communications system at all, and that they are intended to be used in public safety communications systems, features will first have to undergo profound tests and security checks before being put into use.

As we indicated in Chapter 1 in this thesis special attention will be paid to security of the new LTE features, i.e. security enhancements will be proposed where there is room for improvement. In Chapter 2, we saw which security mechanism are used in TETRA network, those are: Air Interface Encryption (AIE), Authentication and End-to-end (E2E) encryption. Therefrom, first two are familiar to LTE and used in LTE networks, while E2E encryption is not available in present LTE networks. New LTE features however require new types of authentication procedures. These authentication procedures will be the subject of our analysis.

By examination of security specification documents for ProSe [97], GCSE [98], MCPTT [99] and IOPS [100] it has been concluded that security procedures for GCSE and IOPS are fully specified, those security procedures are already used in LTE networks, and they are proven to be secure. On the other side, User Authentication procedures for ProSe and MCPTT were left unspecified of set up for further study. Those procedures will be subjects of our analysis. In this chapter we will propose some security protocols which could help to establish security on those places where security procedures are not (yet) defined.

5.1 ProSe Security

ProSe includes several features which can be deployed as stand-alone service, each of those features has its own **Individual security procedures**. However, some of those features can also share common procedures, so in that sense **Common security procedures** can be defined.

Common security procedures refer to [97]:

- Network domain security (interfaces between ProSe network entities),
- Security of UE to ProSe Function interface, and
- Security of the PC2 reference point (reference point between ProSe Function and ProSe Application Server)

Individual security procedures for ProSe features include [97]:

- Security for ProSe direct discovery
- Security for One-to-many ProSe direct communication
- Security for EPC-level discovery of ProSe-enabled UEs

- Security for EPC support WLAN (Wireless Local Area Network) direct discovery and communication
- Security for One-to-one ProSe Direct communication
- Security for ProSe Public Safety Discovery

In this thesis, we will take a closer look at the individual security procedures for One-to-one ProSe direct communication and propose some security enhancements. More precisely, we will propose a protocol for user authentication when One-to-one ProSe direct communication feature is used.

5.1.1 Security of One-to-One ProSe Direct Communication

In commercial cellular networks, like LTE, security on air interface between UEs and network infrastructure is well defined [101], and considered secure. However, device-to-device communication is new for LTE and yet not completely explored in security aspect.

We will propose security protocol which will authenticate the UEs who participate in communication and establish a secure channel for communication between them, all that according to requirements defined in 3GPP TS 33.303 [97].

Security Requirements:

Communication is considered to be secure if it is able to maintain CIA (Confidentiality, Integrity and Availability) triad. In TS 33.303 [97] 3GPP identifies following requirements for ProSe Direct Communication:

1. Different security contexts should be supported
2. Direct link signalling ciphering shall be supported and may be used
3. Direct link user plane ciphering shall be supported and may be used
4. Direct link signalling integrity protection and replay protection shall be supported and used
5. Direct link user plane packets between UEs shall not be integrity protected
6. Establishment of the security between the UEs shall be protected from man-in-the-middle attacks
7. The system should support mutual authentication of public safety UEs out of network coverage
8. Compromise of a single UE should not affect the security of the others
9. Authentication credentials should be securely stored in UE

5.1.2 Security Establishment for One-to-one ProSe Direct Communication

As defined in [97], security establishment of ProSe Direct One-to-one communications is performed in four steps, illustrated in Figure 5.1 [97]. Figure 5.1 provides high level overview of the of security establishment of ProSe Direct One-to-one communications. More details for each step will be described shortly, what is important to bear in mind is that step 2 may involve several messages. 3GPP does not define Step 2 and its message(s) depend on the type of the Long term key(s) (more on keys in the following section). In section 5.1.3 that follows, we propose how Step 2 could be implemented.

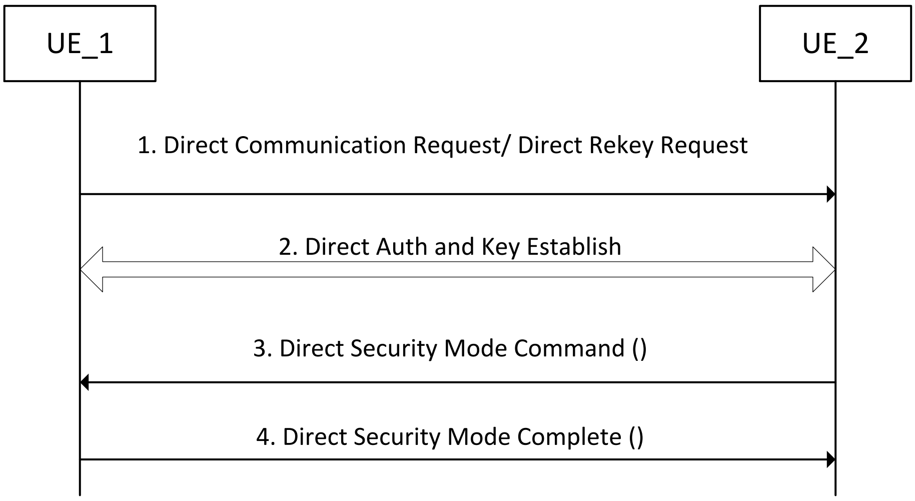
UE_1
UE_2
1. Direct Communication Request/ Direct Rekey Request
2. Direct Auth and Key Establish
3. Direct Security Mode Command ()
4. Direct Security Mode Complete ()

Figure 5.1: Overview of security establishment of ProSe Direct One-to-one communications [97]

Keys

Security establishment of one-to-one ProSe Direct communication involves use of different keys, those keys are split in four different levels [97], being:

1. Long term key – provisioned into the UE. It may be symmetric or public/private key pair. It is identified by Long term ID.
2. K_D – Key shared between two UEs communicating using ProSe Direct Communication. K_D ID is used to identify K_D.
3. K_{D-sess} – This key is used to protect the transfer of data between the UEs. Keys used for confidentiality and integrity protection are derived from this key. It is identified by K_{D-sess} ID.
4. PEK and PIK – ProSe Encryption Key and ProSe Integrity Key, used for confidentiality and integrity protection.

3GPP also defines three possible security states in which UE can be with respect to another UE, they are:

Provisioned-security: UE only has its own long term keys.

Partial-security: UE has K_D which is used in a recent communication with another UE.

Full-security: UE has K_D, K_{D-sess}, PEK and PIK and it is communicating with another UE.

Security Establishment with Security Steps Explained

Figure 5.2 [97] below illustrates security establishment on a connection set-up, as defined by 3GPP in TS 33.303 [97]. Figure 5.2 shows messages exchanged between two UEs, together with the security parameters included in the messages [97].

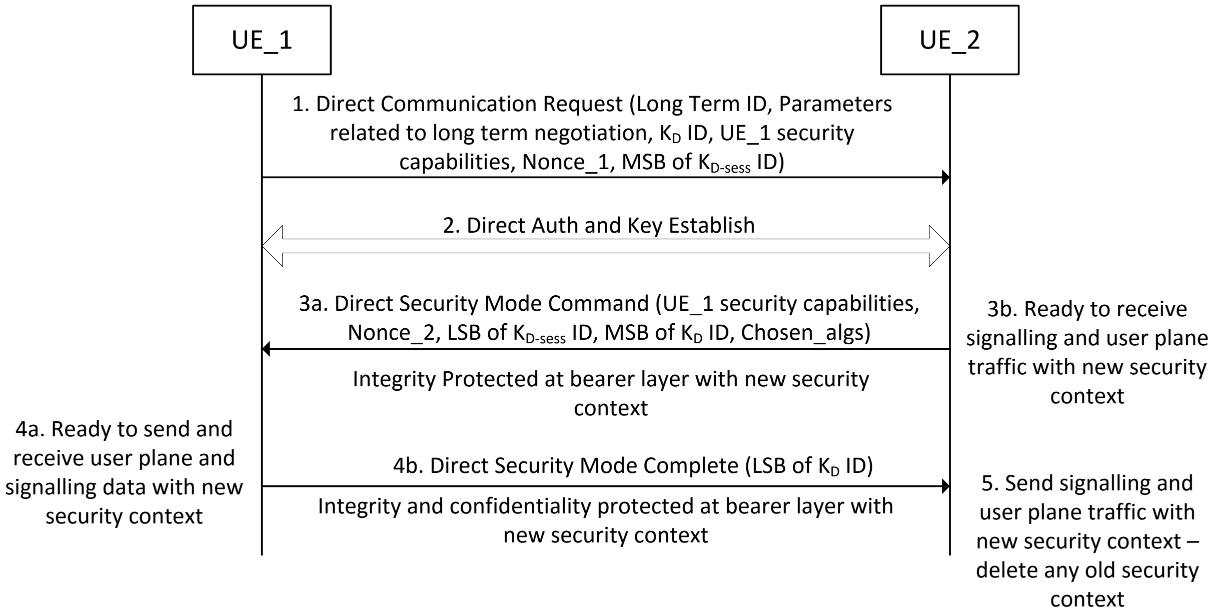
UE_1
UE_2
1. Direct Communication Request (Long Term ID, Parameters related to long term negotiation, K_D ID, UE_1 security capabilities, Nonce_1, MSB of K_D-sess ID)
2. Direct Auth and Key Establish
3a. Direct Security Mode Command (UE_1 security capabilities, Nonce_2, LSB of K_D-sess ID, MSB of K_D ID, Chosen_algs)
Integrity Protected at bearer layer with new security context
3b. Ready to receive signalling and user plane traffic with new security context
4a. Ready to send and receive user plane and signalling data with new security context
4b. Direct Security Mode Complete (LSB of K_D ID)
Integrity and confidentiality protected at bearer layer with new security context
5. Send signalling and user plane traffic with new security context – delete any old security context

Figure 5.2: Security establishment at connection set-up [97]

- Step 1: UE_1 sends Direct Communication Request to UE_2. The message contains: Long Term ID, Parameters related to long term negotiation, K_D ID, UE_1 security capabilities, Nonce_1 and MSB (Most Significant Bits) of K_{D-sess} ID. Long Term ID is the information needed by the UE_2 to identify proper Long term key. Parameters related to long term negotiation provide some addition info to UE_2 if needed. UE_1 security capabilities is the list of accepted security algorithms by UE_1. K_D ID is included only if these two UEs have existing K_D, same goes for the MSB (Most Significant 8-Bits) of K_{D-sess} ID, and they are used to locally identify security context created by this procedure. Nonce_1 is used for session key generation.
- Step 2: Direct Authentication and Key Establishment procedure for ProSe Direct Communication is initiated. This step is required if these two UEs do not have existing K_D and K_D ID pair, in that case this step is mandatory. Step 2 should produce root key for security establishment.
- Step 3: UE_2 sends the Direct Security Mode Command to UE_1. This message includes: most significant bits of K_D ID, in the case that fresh K_D is generated, Nonce_2 needed for session key generation, Chosen_algs parameter serves to inform UE_1 which security algorithms will UE_2 use to protect the data, UE_1 security capabilities are included to provide protection against bidding down attacks[9], LSB (Least Significant Bits) of K_{D-sess} ID are also used for local identification.

  NOTE: Message sent in Step 3 is integrity protected. After this step UE_2 is redy to receive both signalling and user plane traffic protected with the new security context. K_{D-sess} ID is formed from MSB received in Step 1 and LSB received in Step 3.
- Step 4: UE_1 calculates K_{D-sess} and the confidentiality and integrity keys, and checks returned UE_1 security capabilities against those sent in Step 1. UE_1 also checks the integity protection on the message. If both these checks pass, then UE_1 is ready to send and receive signalling and user traffic with the new security context. If MSB of K_D ID were included in Step 3 then UE_1 generated LSB of K_D ID, these two parameters uniquely

[9] Bidding down attacks has for the purpose to make UE_1 use week or no security

identify K_D. Direct Security Mode Complete message is confidentiality and integirty protected. UE_1 also forms K_{D-sess} ID from the MSB sent in Step 1 and LSB received in Step 3.

5.1.3 Proposed Authentication and Key Establishment Protocol for One-to-one ProSe Direct Communication

Here we will propose a protocol for Authentication and Key Establishment, Step 2 in security establishment for ProSe Direct Communication. Proposed protocol will ensure mutual authentication between the UEs communicating and derive the root key (K_D). For that purpose we will also define the type of the Long term key(s), which in our case will be public/private key pair.

Assumptions: UEs are provisioned with long term keys, i.e. public keys of the other UEs, these keys can be refreshed/changed by network infrastructure in OTAR (Over The Air Re-keying) procedure. Also, UEs are provisioned with the sets of prime and primitive root modulo pairs which are identified by IDs (Long Term ID), further we assume that UEs generate perfectly random numbers and have good computational power. As an adversary model we consider the Dolev-Yao adversary model [102] which assumes that attacker has fully control over the wireless channel. We also assume that communicating UEs are not compromised, thereby we design protocol only to prevent the attacker to compromise communication between them.

Protocol design: In this project we propose security protocol for direct (mutual) authentication and key establishment for ProSe Direct Communication. In this type of communication, communicating UEs themselves are responsible for authentication and key establishment since there is no network infrastructure participating which can help in authentication and key distribution process. Proposed solution is based upon Authenticated Diffie-Hellman key exchange protocol [103]. Reason for not using standard Diffie-Hellman key exchange protocol is that the messages are not authenticated, which makes one UE unable to determine the source of the message(s), i.e. to authenticate the other UE with whom is communicating, and it is also vulnerable to the man-in-the-middle (MITM) attack [104]. Proposed protocol follows.

Proposed Protocol

Two UEs, namely UE-A and UE-B, are the two parties who want to establish ProSe Direct Communication. Before the start of the protocol UEs are in **Provisioned-security** state.

Step 1. UE-A and UE-B agree on using same p and g for the Authenticated Diffie-Hellman protocol, where p is a large prime[10] number and g is a primitive root modulo[11] p, and they are a public knowledge.

UE-A and UE-B then generate random numbers a and b, respectively, where $0 \leq a, b \leq p - 1$.

Step 2a. UE-A calculates $g^a \, mod \, p$ and sends it (over insecure channel) to UE-B, together with its UE-A ID, which is used to match UE with its public key.

[10] A **prime number** (or a **prime**) is a natural number greater than 1 that has no positive divisors other than 1 and itself (https://en.wikipedia.org/wiki/Prime_number)

[11] In modular arithmetic, a branch of number theory, a number g is **a primitive root modulo** n if every number a coprime to n is congruent to a power of g modulo n (https://en.wikipedia.org/wiki/Primitive_root_modulo_n)

Step 2b. UE-B calculates $g^b \, mod \, p$ and sends it back to UE-A together with UE-B ID and message signed by UE-B, $Sig_{UE-B}(UE - B \, ID, UE - A \, ID, g^b, g^a)$.

Step 2c. UE-A checks the signature received from UE-B, if the signature is invalid UE-A will abort communication, if the signature is valid UE-A calculates root key for ProSe Direct Communication between these two UEs $K_D = (g^b)^a = g^{ab} \, mod \, p$, sign the message $Sig_{UE-A}(UE - A \, ID, UE - B \, ID, g^a, g^b)$ and sends it to UE-B. Similarly, UE-B will verify signed message, if it is invalid it will abort the communication if not it will calculate root session key $K_D = (g^a)^b = g^{ab} \, mod \, p$.

In this way UE-A and UE-B have authenticated each other and as a result of this protocol they share common secret, root key K_D. UEs are now in **Partial-security** state. K_D is further used as an input together with Nonce_A and Nonce_B in key derivation function, which can be based on a public hash function, to compute root session key K_{D-sess}. PEK and PIK are then directly derived from this key and **Full-security** state is established.

Figure 5.3 illustrates described protocol together with the messages exchanged between two UEs. Protocol steps are repeated below figure to give better overview of the protocol and overall security establishment procedure.

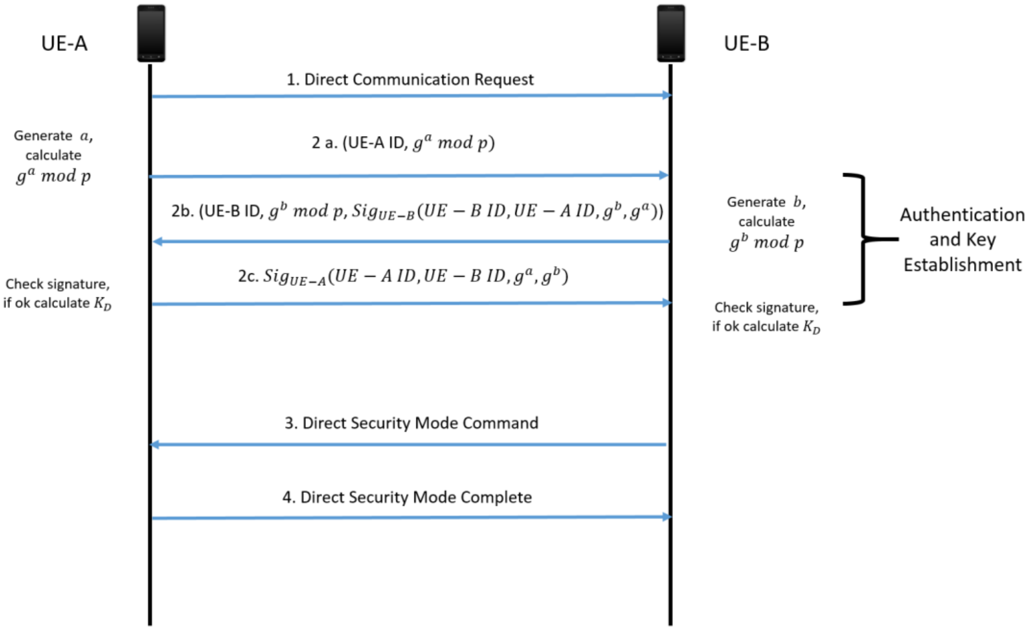
UE-A
UE-B
1. Direct Communication Request
Generate a, calculate $g^a \, mod \, p$
2 a. (UE-A ID, $g^a \, mod \, p$)
2b. (UE-B ID, $g^b \, mod \, p, Sig_{UE-B}(UE - B \, ID, UE - A \, ID, g^b, g^a)$)
Generate b, calculate $g^b \, mod \, p$
Authentication and Key Establishment
2c. $Sig_{UE-A}(UE - A \, ID, UE - B \, ID, g^a, g^b)$
Check signature, if ok calculate K_D
Check signature, if ok calculate K_D
3. Direct Security Mode Command
4. Direct Security Mode Complete

Figure 5.3: Enhanced security establishment in ProSe Direct Communication

- Step 1: Same as in standard security establishment shown in Figure 5.2. Long Term ID is an ID of p, g pair.
- Step 2: 2a. UE-A calculate $g^a \, mod \, p$ and send it together with UE-A ID to UE-B.

  2b. UE-B calculate $g^b \, mod \, p$, sign message $(UE - B \, ID, \, UE - A \, ID, \, g^b, g^a)$ and send those two together with UE-B ID to UE-A.

  2c. UE-A sign message $(UE - A \, ID, \, UE - B \, ID, \, g^a, g^b)$ and send it to UE-B.
- Step 3: Same as in standard security establishment shown in Figure 5.2.
- Step 4: Same as in standard security establishment shown in Figure 5.2.

Protocol analysis: Our proposed solution is based on a public key cryptography and Key distribution using asymmetric cryptography. We use improved Diffie-Hellman key agreement protocol with digital signatures to provide mutual authentication and more. This protocol was chosen because it is able to meet all security requirement listed in section 5.1.1. Starting from the last requirement and going backwards:

- Authentication credentials are securely stored in the UE which is tamper resistant.
- To cope with the requirement that compromise of a single UE should not affect the security of the others, i.e. to provide forward secrecy, UEs can be programmed to automatically delete the list of other UEs public keys on any attempt to forcibly access it, which imply any other access rather than in standard authentication procedures (definition of forced procedures is out of scope of this document).
- Mutual authentication is ensured by using digital signatures – according to the definition of digital signatures [105] only the owner of the private key can generate a correct digital signature.
- MITM attack is prevented by avoiding standard Diffie-Hellman key exchange and using an improved Diffie-Hellman protocol that uses digital signatures, this ensures that if message modification occurs in transmission verification of a digital signature will fail [103] and UE will drop the connection.
- Direct link signalling is integrity protected by sending the same message in clear text and signed (e.g. $UE - B\ ID,\ g^b\ mod\ p$ and $Sig_{UE-B}(UE - B\ ID, UE - A\ ID, g^b, g^a)$).
- Direct link signalling is reply protected by using Nonce(s).
- Direct link user plane ciphering is supported, protocol proposed creates root key used to derive key for encryption and integrity protection of the user plane data.

Possible drawback of this approach could be required computational power. Our proposed protocol uses ephemeral key (keys which are used once and then discarded), to save on computational power and time, static (long-term) private keys (a and b in our case) with corresponding public keys can be used. In this way UE-A and UE-B do not have to compute K_D each time they want to communicate but they can rather find it just by looking up for each other's public key, which also agrees with 3GPP's recommendation. In that case we recommend using El Gamal [106] or DSA (Digital Signature Algorithm) [106] digital signatures which are slightly faster to compute than RSA [106] digital signatures.

Our approach authenticate UEs. If desired, additional authentication of the user(s) can be done verbally or visually after proposed protocol is completed.

5.2 MCPTT Security

As explained in section *4.5.2 MCPTT Functional Architecture*, MCPTT functional model defines two separate planes which operate independently. Consequently, each plane manage its own:

a) Identities - Each plane is responsible for the privacy of that plane's own identities
b) Security – Although individual for each plane, plane can decide either to use offered security from another plane or its own security mechanisms.

Besides individual security for each of the two planes, MCPTT defines security at one more level. These are listed below, together with security procedures within those levels [99]:

1. Application level - Application plane security

    a) Authentication
    b) Authorization
2. Signalling level - Signalling plane security
    a) SIP-1 interface security
    b) HTTP-1 interface security
3. End-to-end level - End-to-end communication security

In this thesis, we will take a closer look at Application plane security. More precisely, we will propose a protocol for MCPPT User Authentication.

5.2.1 MCPTT Application Plane Security

As already said, Application plane security implies Authentication and Authorization security procedures. Here, our focus will be on MCPTT User Authentication. Before proposing the protocol we first have to check the security requirements.

Security Requirements:

Security requirements for MCPTT over LTE are specified in TS 22.179 [107]. Here we provide only those related to MCPTT Authentication and Authorization. They are as follows:

1. The MCPTT Service shall provide the MCPTT User with a mechanism to perform a single authentication for access to all authorized features.
2. The MCPTT Service shall provide a means for an authorized MCPTT UE to access selected MCPTT features prior to MCPTT User authentication.
3. The MCPTT Service shall require authentication of the MCPTT User before service access to all authorized MCPTT features is granted.

NOTE: The MCPTT Service features available are based on the authenticated user identity(s).

5.2.2 Security Establishment for MCPTT Service

Authentication and Authorization procedures are used to establish security when MCPTT Service is used. These procedures should ensure that only users with right credentials can use MCPTT Service. Authentication identifies the MCPTT User and Authorization validates whether or not a MCPTT User has the authority to access certain MCPTT Services.

Figure 5.4 [99] shows defined steps for security establishment for MCPTT Service. Security establishment implies MCPTT Authentication and Authorization.

NOTE: For description of the entities involved please refer to *Appendix B (MCPTT Functional entities description).*

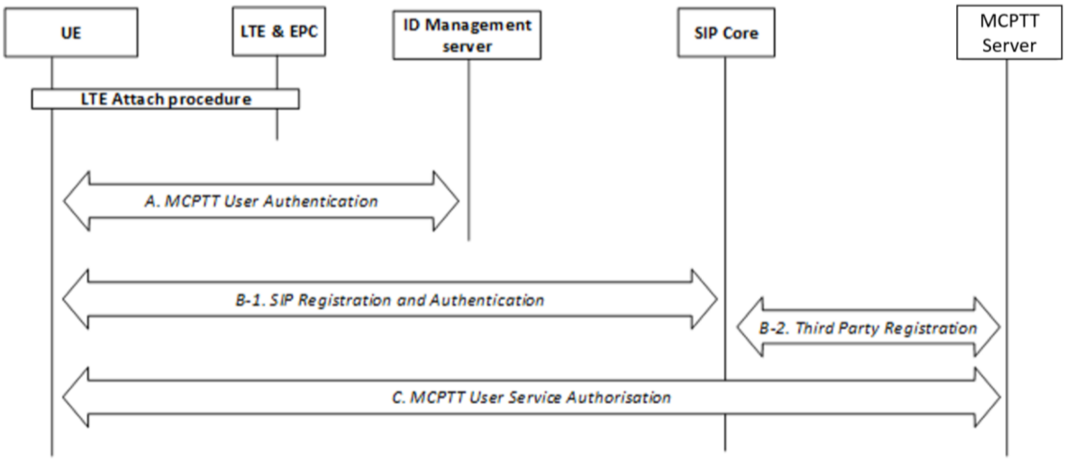
UE
LTE & EPC
ID Management server
SIP Core
MCPTT Server
LTE Attach procedure
A. MCPTT User Authentication
B-1. SIP Registration and Authentication
B-2. Third Party Registration
C. MCPTT User Service Authorisation

Figure 5.4: MCPTT Authentication and Authorization [99]

As shown in Figure 5.4, couple of steps have to be done before MCPTT User can use MCPTT Services. LTE attach procedure uses standard authentication procedure for LTE systems, as specified in TS 33.401 [100]. After being attached MCPTT UE (on behalf of MCPTT User) performs three separate procedures in order to complete the MCPTT Service registration, those procedures are [99]:

- A: MCPTT User Authentication
- B: SIP (Session Initiation Protocol) Registration and Authentication
- C: MCPTT Service Authoriztion.

Steps A and B may be performed in either order or in parallel [99]. The order in which these two steps are done may have an impact in cases when identity bindings between signalling layer identities and the MCPTT user identities exist [99]. In those cases re-registration to SIP core (Step B) is performed to update the registered signalling layer identity.

In case when Step B is completed before Step A and Step C, the MCPTT Server is informed of the registration of the MCPTT UE with the SIP core, though Step B-2. Then the MCPTT UE enters a 'limited service' state, in this state MCPTT User can only use limited services (e.g. an anonymous MCPTT emergency call).

With Step B security requirement No. 2 (The MCPTT Service shall provide a means for an authorized MCPTT UE to access selected MCPTT features prior to MCPTT User authentication) is covered. SIP Registration and Authentication however will not be a part of our analysis, so it is not further discussed. Our focus is on Step A, MCPTT User Authentication, which aims to authenticate the user and produce the means later used in MCPTT User Service Authorization in Step C. These two steps are closely related, Step A has an impact on Step C, since following security requirement No. 3, MCPTT User has to be authenticated before being authorized to access all MCPTT features of MCPTT Service.

Alternatively, MCPTT User Authentication can be done within the Step B if SIP Core is in the same MCPTT Domain as MCPTT Server, but we do not consider that case.

5.2.3 User Authentication Framework

The MCPTT User Authentication is one of the procedures which was not completely defined in MCPTT security specification (TS 33.179 [99]) and it is set for further study. In the next section MCPTT User Authentication Protocol will be proposed, following the basic user authentication framework and security requirements defined in TS 33.179. MCPTT User Authentication framework, as defined in TS 33.179, is illustrated in Figure 5.5 [99].

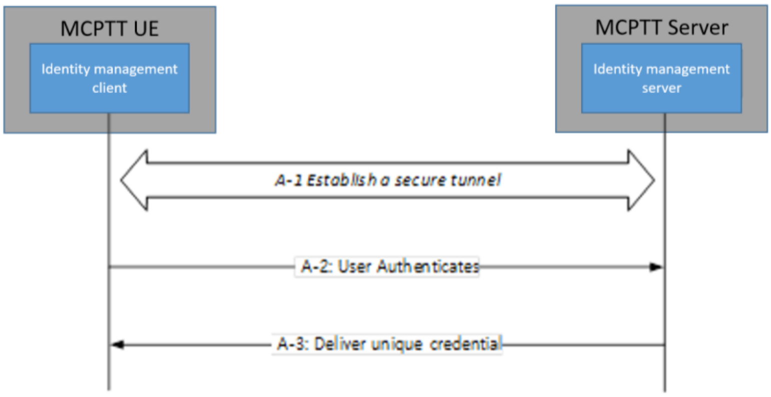
MCPTT UE
Identity management client
MCPTT Server
Identity management server
A-1 Establish a secure tunnel
A-2: User Authenticates
A-3: Deliver unique credential

Figure 5.5: MCPTT User Authentication Framework [99]

The MCPTT User Authentication is carried out between the MCPTT UE (more precisely the identity management client application located in MCPTT UE) and the identity management server (functional entity, part of the MCPTT Server). User Authentication framework splits Step A from Figure 5.4 into 3 sub-steps. Those 3 sub-steps are as follows [99]:

- A-1 – Establish a secure tunnel between the MCPTT UE and Identity Management server (IdMS)/MCPTT Server. Subsequent steps make use of this tunnel.
- A-2 – Perform the User Authentication Process (User proves their identity).
- A-3 – Deliver the credential that uniquely identifies the MCPTT user to the MCPTT client.

Credentials obtained from step A-3 are used to perform MCPTT service authorization, Step C from Figure 5.4.

5.2.4 Proposed MCPTT User Authentication Protocol

Here we propose a solution for MCPTT User Authentication. According to MCPTT User Authentication framework, MCPTT UE, i.e. ID Management Client located in MCPTT UE and ID Management Server (part of the MCPTT Server) should establish secure tunnel before MCPTT User authenticates i.e. before it sends its user identity (MCPTT ID). However, means by which secure tunnel is established are not defined. Here we propose the protocol which creates secure tunnel and authenticates server and the user.

Given that authentication framework supports extensible[12] user authentication solutions, we decided to use TEAP (Tunnel Extensible Authentication Protocol), defined in RFC 7170 [108], and adopted as RFC in May 2014. RFC 7170 defines TEAP as follows: *"TEAP is a tunnel-*

[12] Extensible means that method by which authentication is done is left to be filled in

based EAP (Extensible Authentication Protocol) method that enables secure communication between a peer and a server by using the Transport Layer Security (TLS) protocol to establish a (mutually) authenticated tunnel. Within the tunnel, TLV objects are used to convey authentication-related data between the EAP peer and the EAP server". TEAP provides the way to perform the user authentication in a secure way, as illustrated in Figure 5.6. TEAP consists of two phases: Phase 1 – Tunnel Establishment and Phase 2 – Tunneled Authentication.

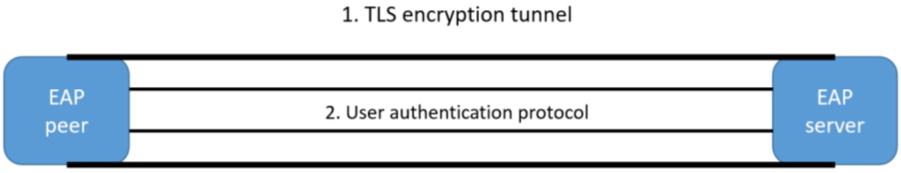

Figure 5.6: TEAP high level illustration

Good side of the TEAP method is that supports different TLS ciphersuites[13] [108], and more importantly it supports anonymous ciphersuites which are used in cases when inner authentication of the user is applied (authentication within the secure tunnel, after the Phase 1). Use of inner authentication method ensures mutual authentication, key generation and resistance to man-in-the-middle attack [108]. We must also note that another reason for choosing TEAP method is because it supports TLS extensions [109], which are one of the key elements that contribute to security strength of this protocol. These will be explained in protocol analysis.

Protocol Overview

Protocol start with the initial EAP Identity request/response exchange, two standard messages exchanged between EAP peer (MCPTT UE in our case) and EAP server (MCPTT Server in our case). These messages are first two messages for every EAP-based protocol [110]. With these two messages TEAP method is initiated.

In Phase 1, TEAP employs the TLS handshake (we use TLS version 1.3) to provide an authenticated key exchange and to establish protected tunnel [108]. Phase 2 starts after Phase 1 is finished, in Phase 2 EAP server (MCPTT Server) and EAP peer (MCPTT UE) are engaging in further conversations to establish the required authentication and authorization policies.

TEAP Phase 1: Tunnel Establishment

Communication between MCPTT UE (i.e. Identity management client) and MCPTT Server starts with EAP request message sent by the MCPTT Server. The MCPTT UE then respond with EAP response message, these two messages indicate the start of TEAP session and negotiate TEAP version to be used. EAP response message sent from the MCPTT UE encapsulates one or more messages related to following TLS handshake. After first two initial messages, regular TLS handshake is performed. At the end of the TLS handshake MCPTT Server and MCPTT UE enter Phase 2. Figure 5.7 illustrates Phase 1 of TEAP.

[13] A **cipher suite** is a named combination of authentication, encryption, message authentication code (MAC) and key exchange algorithms used to negotiate the security settings for a network connection using the Transport Layer Security (TLS) (https://en.wikipedia.org/wiki/Cipher_suite)

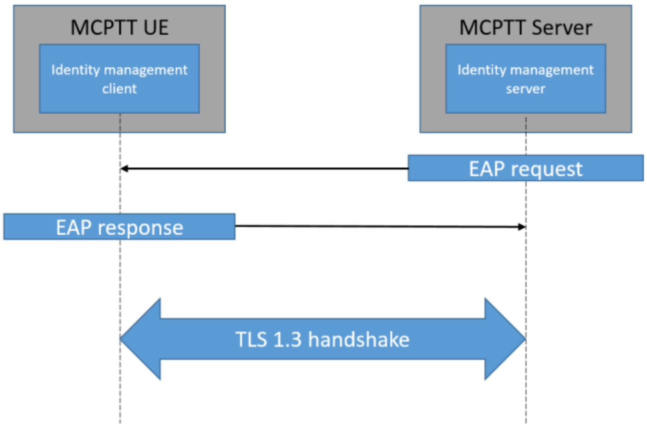

Figure 5.7: TEAP Phase 1

TEAP Phase 1 relies on TLS handshake [111] to establish an authenticated and protected tunnel. Minimum requirement is to support TLS 1.2, however we choose to use TLS 1.3. Although TLS 1.3 version does not have RFC status yet and it is still in a draft form, we opted for this version due to many improvements in handshake protocol which are expected compared to 1.2 version [112]. More on this in the protocol analysis section.

TLS handshake encapsulates several messages. Goal of the TLS handshake between the MCPTT UE and the MCPTT Server is to agree on protocol version (TLS 1.3 in our case), select cryptographic algorithms, optionally authenticate each other (unilateral authentication in our case, only MCPTT Server is authenticated in Phase 1) and establish shared secret keying material [111]. Full content of the TLS 1.3 handshake messages and their aim can be found in [111].

At the end of Phase 1 MCPTT UE and MCPTT Server have secure connection, they have established the tunnel and the server is authenticated.

TEAP Phase 2: Tunneled Authentication

Phase 2 of the TEAP session starts only after successful completion of Phase 1. Phase 2 consists of a series of request and response messages which are aiming to authenticate the MCPTT User. At this point MCPTT User takes its part in authentication process. Until this point MCPTT UE was acting on behalf of user, doing LTE attach procedure, authenticating the MCPTT Server and establishing secure connection. Considering that MCPTT User is to be authenticated, it is necessary to conduct verification of user-specific credentials. This should be provided by the user, by entering its credentials into UE. Our recommendation is that credentials be in form of username and password, which is also recommended by RFC 7170 as an option for inner authentication. Also, TS 33.179 specifies that MCPTT User Authentication Framework must support password-based solution, meaning that username and password authentication is suitable. Figure 5.8 illustrates (successful) authentication of the MCPTT User in Phase 2.

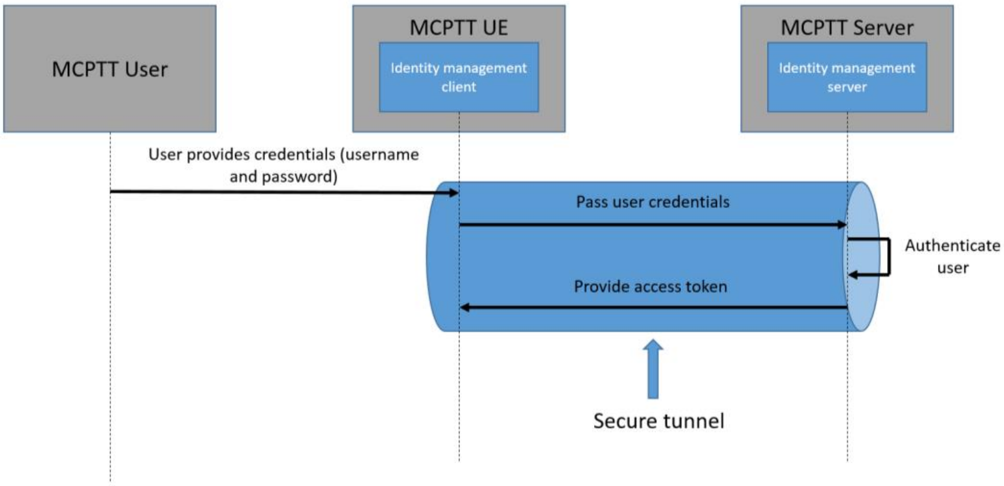
MCPTT User
MCPTT UE
Identity management client
MCPTT Server
Identity management server
User provides credentials (username and password)
Pass user credentials
Authenticate user
Provide access token
Secure tunnel

Figure 5.8: TEAP Phase 2

Result of the successful authentication in Phase 2 is an access token provided by Identity management server to the MCPTT UE, which will be later used for Authorization in Step C. This is to avoid multiple authentications with different entities of MCPTT Server, instead of that MCPTT UE will provide the acquired token to prove its identity and get access to MCPTT features, i.e. to be authorized. This covers security requirement No.1, user should have single authentication.

The general concept of using tokens is to allow user to enter its username and pasword once and by doind that to obtain a token which will later allow the user to fetch a specific resource(s), withouth using their username and password again. This can be seen as some kind of indirect authentication. This could be beneficial for both sides, user and the server that provides resource(s), in this way that do not have to trust to each other, they can rely on the authentication server which has authenticated the user and issued a token for a user. These tokens usualy have limited life-time.

Protocol analysis: In this protocol server is authenticated in Phase 1 based on the certificate[14] provided, while user is authenticated in Phase 2, based on username and password. The reason why only MCPTT Server is authenticated in Phase 1 is to additionally protect MCPTT User by transferring users' credentials within protected (secure) tunnel, but also to ensure that user is not getting services from a false server.

In Phase 1 MCPTT Server is authenticated based on servers' certificate (as defined by TLS 1.3 [111]). User(s) could be also authenticated in a same way in Phase 1 by using users' certificates (Client Certificate in TLS terminology). The reason why we avoid use of user (client) side certificates, even though it provides better security than username/password authentication, is because solution is not sustainable due to client certificates complexity of implementation and the fact that it may also require education of the users how to use the certificates while username and password method is somewhat more susceptive and familiar method to the wide range of users [113].

The TEAP peer (MCPTT UE) does not need to authenticate as part of the TLS exchange but can alternatively be authenticated through additional exchanges carried out in Phase 2 [108].

[14] In cryptography certificates are used for authentication purposes to authenticate certificate owner. Certificates represent identities

The tunnel created in Phase 1 protects information exchanged in Phase 2 (e.g. user identity) from disclosure outside the tunnel. To mitigate man-in-the-middle attack, TEAP provides support for cryptographic protection of the inner EAP exchange and cryptographic binding of the inner authentication method(s) to the protected tunnel.

TEAP's ability tu use TLS extensions comes to the fore in Phase 2. Messages exchanged in Phase 2 are encapsulated in TLV (Type-length-value)[15] objects. These objects are used to provide crypto-binding (RFC 7029 [114]), and Phase 2 must always end with Crypto-Binding TLV exchange. The Crypto-Binding TLV exchange that occurs at the end of the Phase 2 is used to prove that same UE and server have participated in Phase 1 and Phase 2.

Furthermore, TEAP is claimed to support [108]: Mutual authentication, Replay protection, Confidentiality, Dictionary attack protection, Cryptographic binding, among other EAP security requirements [110].

Concerning TLS handshake protocol, although still in a draft from it is very promising since it removes a lot of features which are known to bring security flaws into TLS 1.2 [115]. Security analysis TLS 1.2 draft version 12 (draft-12) claim that authentication and key exchange within handshake protocol are secure from man-in-the-middle attack whenever the server is authenticated. Also, some other studies like [116] have shown that TLS 1.3 was secure even on draft version 5 (draft-05).

Password-based authentication

In ‘Study on security enhancements for Mission Critical Push To Talk (MCPTT) over LTE’ (TR 33.879 [117]) published in March 2016, 3GPP recomends two authentication procedures for MCPTT User Authentication, those are:

- SIP Digest authentication;
- Token based authentication.

Both of these procedures require from user to provide username and password ([118] [119]) in order to be authenticated. This gives indications in which direction 3GPP is going, i.e. using pasword-based authentication. Password based authentication is not considered to be a secure methods for user authentication unless used in conjunction with some external secure system such as TLS [120]. Benefit that this method can provide is separation of users and UEs (they are authenticated separately) which can enable use of shared UEs (one UE can be used by multiple users). However, 3GPP leaves these two mechanisms for futher revision.

[15] TLV stands for **type-length-value** which is an optional information that may be encoded within data communication protocols (https://en.wikipedia.org/wiki/Type-length-value)

Part II:

Future Mobile Broadband Public Safety Networks

Chapter 6

6 LTE Networks for Public Safety Communications

First step towards mission critical mobile broadband networks was made. The necessary functionalities for LTE are defined. However, it will pass some time before LTE networks replace currently deployed public safety networks. On the way to public safety LTE networks, public safety organizations which are using TETRA networks will have to do some form of transition/migration from TETRA to LTE network(s). In that transition, different direction (alternatives) can be chosen, depending on the way how they want to deploy their public safety LTE network(s). For that reason, in this chapter, we investigate different alternatives for deployment of public safety LTE networks.

The definition of the right deployment scenario and associated business model for the delivery of the mobile broadband public safety communications largely depends on interests of public safety organizations and governments around the world. However, in this chapter we provide, what is considered to be, general evaluation of benefits and drawbacks of different deployment models.

We first introduce deployment models. We then explain different factors which could influence their early deployment, where techno-economic factor plays crucial role. Finally, we evaluate them and use current initiatives as living examples to support our claims.

Three delivery models to be analyzed here:

- **LTE dedicated networks** (built for public safety use),
- **LTE commercial networks** (network built for commercial use but also used by public safety users) and
- **Hybrid solutions** (combination of dedicated and commercial LTE networks and/or LTE and TETRA networks).

6.1 LTE Dedicated Networks

The *LTE dedicated network* model is understood as a mobile broadband public safety network which is specifically designed and built for public safety communications and to meet the requirements of the public safety users. This kind of approach was applied for most of the current narrowband public safety networks.

Within the context of dedicated networks various arrangements for the procurement of public safety communications services. These arrangements concern the following things [44]:

Ownership of the infrastructure. Infrastructure can be owned by the government or by some commercial service provider, referred as government-owned (GO) and contractor owned (CO) arrangement, respectively.

Operator of the infrastructure. Infrastructure can be maintained by the owner itself or by third-party company. In accordance with that, three different combinations of the owner-operator exist, they are: government owned and government operated (GO-GO), contractor owned and contractor operated (CO-CO) and government owned and contractor operated (GO-CO).

Users admitted to the network. The network can be used only to serve public safety agencies or it can be shared with other users.

Designation of spectrum for public safety use. The spectrum used can be specifically designed for that purpose (dedicated spectrum), another option is to procure commercial services from commercial operator (no dedicated spectrum).

6.1.1 Model Evaluation

Generally speaking this delivery model could be an ideal solution for any network, for the following reason: It is built to fulfil all user requirements and provides the best services [44], while giving the users a full control over the network. Since it is built to meet all user's requirements it is considered to be the best solution from the user's point of view. From the operators' point of view this model can be a challenge.

Deployment of LTE dedicated system raises the issue of identifying the **spectrum** band(s) and spectrum management model(s) on which these systems can be deployed and operated [49]. The problem arises from the fact that the most promising spectrum to be used for broadband public safety is the same spectrum that commercial mobile operators are willing to use [49] (or they use already), which is the spectrum below 1 GHz and around 700 MHz. This spectrum is also the most expensive one due to its very good characteristics [49], which only contributes to another disadvantage, high costs. Another problem may arise from the need of public safety spectrum harmonization on a global level. The problem with spectrum allocation goes hand in hand with national laws and regulations, which is thoroughly explained in [121].

Costs analysis researches can have different approaches and it is sometimes hard to grasp the actual **network costs**. As reported in study from 2014 for the European Commission [122], network costs can vary considerably and often cannot be properly estimated. There are many factors which can influence network cost. However, most of these reports agree on one thing, rollout of dedicated mobile broadband network for public safety have high costs [123]. Public safety networks have to be built with extra redundancy and with wider coverage than commercial networks while on the other side they have much less users which also contributes to high costs [49].

Let us take the US's network as an example. The total required investment to deploy a nationwide public safety LTE network in US, FirstNet, estimated by Federal Communications Commission (FCC) is $16B, stated in the National Broadband Plan [124]. The US Congress allocated $7B in funding to FirstNet and required from FirstNet to make up remaining $9B through public-private partnership(s) (PPPs). Showing that this model can be expensive even for strong economic countries. High costs could be initial brake for this model to be adopted by many countries.

To cope with high costs, dedicated networks may seek for solution in different cost-saving business strategies. Those strategies are:

- **Infrastructure sharing through public-private partnership** - here public safety organization that owns infrastructure shares it with the private partner (e.g. mobile network operator (MNOs), utilities) to bring down costs of the site acquisition. This strategy can bring cost savings in the range of 40-50% [49].

- **Capacity sharing of private public safety network** - allowing other users who are not part of the public safety organization (e.g. utilities, transport) to use excess capacity. With this strategy costs can be brought down by close to 15% [49].
- **Use if transportable/fast deployable equipment** - deployable systems (e.g. transportable radio Base Stations (BSs)) can help lowering the amount of permanently deployed network infrastructure, improve coverage, increase redundancy and provide extra capacity during incidents. This can result in 30% of costs saving [49].

The procurement process and network buildout can usually take couple of years [44] before it delivers first service to the users, meaning that it takes long **time** before network becomes operative a starts providing service. This is evident on some of the most recent examples. Namely, FirstNet, decision on starting the project was made in February 2012, first Strategic Roadmap was launched in March 2014, and according to information form the latest FirstNet Board Meeting [125] held on March 16, 2016, first activation and testing of the network is planned for August 2018. This is in total more than 6 years from decision on building the network to the first service provided by that network. Another example is Norway's public safety dedicated network, Nødnett. In Norway's case, it took 9 years to build the network, from December 2006, when contract for network development was signed, to December 2015, when network was officially opened [126], without counting the years of research which preceded the contract signing in 2006.

For migration, application of this delivery model implies that TETRA network and TETRA services would be used until LTE network is ready, meaning that users would have to wait until network is fully deployed and tested. This could also be a sudden change for users not accustomed to new services. We should also not forget the fact that technology for Public Safety LTE is not available yet, at least not the one according to 3GPP standards. As we explained in section *4.7.1 The Availability of Technology and the Timeline*, it can be expected to be available in 2-3 years.

Advantages

Main advantage is that these types of network are built especially for public safety use and they are built in that way to meet the requirements set by the users. Meaning that network can be built with suitable coverage and availability criteria. In GO (government owned) dedicated network users have full control over the network while in CO (contractor owned) dedicated network the level of control is regulated. Also, one of the advantages could be that dedicated network is not upset by commercial users during major incidents or at least their influence on the network can be controlled (public safety users/organizations have control over the network).

Disadvantages

The availability of spectrum, timing and high costs stand out as main disadvantages of this model [127].

6.2 LTE Commercial Network

The *LTE commercial network* model is understood as a mobile broadband network which is designed for the needs of commercial users. In that sense, existing commercial networks can be also used by public safety users, in which case they would use non-mission critical services.

However, there is a possibility to upgrade those networks and enable them to provide mission critical services.

Within this model, two different alternatives are possible. These alternatives are different in regard to who operates the network. In that regard we have following alternatives [44]:

- **Take service from standard commercial networks.** In this delivery option individual public safety organization or a public entity on behalf of group of public safety organizations makes an arrangement (commonly known as service level agreement (SLA)) with one or more Mobile Network Operators (MNOs) for the provision of mobile broadband services. These agreements can negotiate [127]: 1. priority access in critical incidents; 2. a response time for network outages; 3. a target for coverage; 4. a target for latency.
- **Operate as a Mobile Virtual Network Operator (MVNO).** In this delivery option MVNO makes a contract with a commercial cellular Mobile Network Operator (MNO) to "buy" access to the MNO's network for its own customers. Level of control which MVNO will have over the services can be specified through the contract. MVNO also have the option to contract more than one MNO, for the sake of greater capacity, availability, resilience or coverage.

Although very similar on the first look, essential difference between these two alternatives are added values which MVNO alternative could introduce. This will be explained through our case study in the next chapter (section 7.3.3 Deployment of Public Safety MVNO).

6.2.1 Model Evaluation

This model is the fastest way to explore the possibilities of broadband services in public safety communications, since commercial networks are already deployed users can considerably save on **time**. Initial **cost**-saving can also be a motivation for applying this model (most of the infrastructure already exist). However, these networks may need to undergo upgrades to meet the requirements of the public safety users. As we have shown in sections *3.2 Services* and *3.3 Networks*, commercial networks do not support services like group call, PTT or DMO, also commercial network and public safety networks are built according to different priorities, so commercial network may need to improve coverage, availability or some other issue. This could be a potential stepping-stone, due to high-level requirements from the public safety users, and the upgrades may not be profitable for the commercial operator. Key for the success of this model lays in "win-win" agreement between the two sides.

Example of this approach is UK's current initiative, Emergency Services Mobile Communications Programme (ESMCP) to create Emergency Services Network (ESN) which will provide the next generation integrated critical voice and broadband data services. The UK intends replace Airwave (TETRA network) critical voice services by enhancing a commercial mobile network [128]. For ESN UK will take existing RAN (Radio Access Network) infrastructure from commercial operator, extend it to provide additional coverage and do the necessary network upgrades to introduce mission critical services into the network. Network procurement is separated in three lots:

- Lot 1 (Delivery Partner)

A Delivery Partner to oversee build out of the network; programme manage transition; provide cross-Lot integration; training support services; and delivery support

- Lot 2 (User Services)

A service provider for end-to-end systems integration; public safety functionality; account management; network and IT infrastructure; technical interfaces to all other lots and services user device management; application hosting; customer support; and service management

- Lot 3 (Mobile Services)

A mobile network operator to provide an enhanced radio access service with highly available full national coverage; and technical interface to Lot 2

Splitting network procurement in three lots aims to "split" the network and avoid the situation in which one mobile network operator (MNO) will have full control over the network and be the only one able to provide public safety communication services (as it is now with Airwave). This will create competitive environment between MNOs, which could impact lower prices for services.

Considering that UK wants to completely replace existing TETRA network and that the commercial network has to undergo changes to provide mission critical services, this will take more **time** than in situation when commercial network is used as it is. The ESN is now in the mobilisation phase before the start of transition. Mobilisation means network design, built (upgrades) and tests while transition imply preparation of users for conversion to ESN [128]. By the ESN timeline, transition is expected between 2017 and 2020, while the first services are expected to be delivered from mid-2017 [54]. However, even this timeline sound aggressive now considering that standardized mission critical services for LTE are not available yet, and as a reminder, according to Release 12 and Release 13 timeline these services are expected to be available some time in 2017., but still they will have to be tested first before their mass implementation. Concerning that 3GPP standards for Public Safety LTE will be immature at the time, the plan is to implement pre-standardized solutions with possibility to upgrade when standards are mature enough [129].

From the very beginning of ESMCP, high **costs** of Airwave's services were mentioned as the main initiator for this transition, which was also repeated many times by Steve Watson [129], director of ESMCP, during the Nødnett days [130] held in Trondheim, April 19-20, 2016. As stated in report explaining the reasons for UK's transition [131], the performance of the TETRA system provided by Airwave was "very good" but "extremely expensive". And indeed, when we look at the costs of some of the currently deployed dedicated TETRA networks [49], total cost of ownership (TCO) per user and per year in Finland (VIRVE) is 475€, in Belgium (ASTRID) is 596€ while in UK (Airwave) TCO per user and per year is 1200€, which is almost three times more than in Finland and two times more than in Belgium. Expiration of the contract with Airwave was seen as a chance to switch to a new system.

For migration, application of this delivery model means getting broadband data applications at the short notice but also implies losing important functionalities (group call, PTT, DMO, etc.), unless network is upgraded beforehand. In case that commercial LTE networks are used as they are, without any upgrades or improvements, public safety organization will enter into certain risk since commercial networks are not designed and constructed according to public safety users' needs, as we saw in section *3.3 Networks*.

Advantages

Key advantage is the fact that these networks are already deployed which can save on time and initial investments, plus they already have allocated spectrum. Also, there is a possibility for new PS LTE features to be early implemented and tested.

Disadvantages

Network is built to meet the requirements of commercial users and not the requirements of public safety users, meaning that essential services for public safety users are not available and due to different design priority they have worse geographical coverage, worse service availability, etc. Users depend on operator's willingness to implement new featured developed for public safety communications, also it may happen that public safety users have to compete for the capacity with the commercial users which can be disastrous in situations of major incidents.

6.3 Hybrid Solutions

The *hybrid solution* is understood as combination, to different extent, of dedicated and commercial LTE networks but sometimes it may refer to combination of TETRA and LTE networks as well. Many combinations of different network aspects can be applied in hybrid solutions, depending on the needs and requirements of the public safety organizations and users. However, most of the hybrid solutions are built around following approaches [44] (following approaches refer to hybrid solutions of LTE dedicated and LTE commercial networks):

- **Support of national roaming for public safety users over commercial network** [44]**.** This approach imply that dedicated mobile broadband network exist only in some parts of the country so to provide full coverage it allows public safety users to roam in commercial networks in order to complement coverage and capacity of the dedicated infrastructure.
- **Deployment of public safety MVNO** [44]**.** In this model one public safety MVNO is established for several public safety organizations in order to avoid individual agreements of each organization with the commercial MNOs. The MVNO takes RAN from MNO(s) but it can built dedicated core network to establish full control over the critical capabilities.
- **RAN sharing with MNOs** [44]**.** In this model dedicated RAN is shared with commercial MNOs.
- **Network sharing of critical and professional networks** [44]**.** In this model, local dedicated networks can be leveraged or integrated in global public safety networks.

Choosing appropriate model depends on situation in which public safety organization is, and the goals it wants to achieve.

6.3.1 Method Evaluation

Due to model's diversity it is hard to claim what are exact advantages and disadvantages of hybrid solution approach. However, flexibility can be segregated as main advantage of this approach, while complexity on the other side could present main disadvantage.

By flexibility we mean openness for different kinds of combinations of a different aspects of the commercial and dedicated networks. These combinations can be done on different levels, which we will explain shortly. In combinations of TETRA and LTE networks the flexibility can reflect through freedom of choice for the services, i.e. which network will provide which services and in which area.

The advantage of the hybrid solutions is also, at the same time a disadvantage of this approach. The mere fact that different networks are combined introduce complexity by itself. In the combination of different networks the interoperability must be ensured, and these are only LTE commercial and LTE dedicated network we are talking about, complexity becomes even bigger if LTE and TETRA networks are combined, due the fact that completely different technologies are used in these two systems.

As we mentioned, dedicated and commercial networks can be combined to different extent, that extent could be expressed through percentages in which one network is represented in the public safety system as a whole (e.g. 50% dedicated network and 50% commercial network). Commercial network could be or could be not specialized for public safety communications. In the former case only services present on the commercial market would be available to public safety users, in the latter case the commercial networks would be upgraded to support services, which are now inherent only for public safety systems. Many combinations of different network aspects can be done, depending on the needs and priorities of the public safety organization.

Public safety organization can create the hybrid network for its needs by combining various network aspects, some of those aspects are listed below:

- Spectrum
- Coverage
- Infrastructure
- Services
- Capacity
- etc.

The main goal of hybrid solutions is to strike the right balance between dedicated and commercial networks or LTE and TETRA networks, where estimating which of above listed aspects is better to take from each networks is the key.

Hybrid solution with MVNO model has already taken its first steps in Belgium, as already described in this document. Belgium's hybrid solution is a combination of dedicated TETRA network and commercial LTE network. Belgium's network operator ASTRID, which operates the national network for public safety and security services uses commercial networks to provide broadband services to the public safety users with possibility to use TETRA as a fall-back solution [57].

ASTRID's solution uses plain commercial networks with no additional upgrades for public safety communications. Solution is based on priorities which public safety traffic has over the non-public safety traffic. Prioritization is the ability of the network to determine and give priority to some connection(s) over others. Based on priorities, network allocates resources accordingly. Prioritization is an important functionality of any network, and it can be a possible way to separate public safety from non-public safety users in cases when public safety users do not have dedicated resources. Priority mechanism is also used in public safety dedicated networks, however the bad side in this approach that public safety users have to compete for the resources even with the commercial users.

In the context of migration, application of hybrid model can be the smoothest way to do the transition. Hybrid model allows using TETRA and LTE networks in parallel which give the possibility to choose between the services, i.e. which services will be provided by TETRA and which by LTE network. Even if only implies a combination of LTE networks, hybrid model also gives the possibility to choose which aspects of the network will be dedicated and which commercial.

6.4 Comparison of Delivery Models

Networks should usually be deployed in the way to meet the user requirements, however, when considering the right deployment scenario user's requirements are not the only factor of influence. Techno-economic factors also play an important role. These factors can have different weight in different public safety organizations and depending on their priorities, public safety organizations can choose among different delivery models.

From three delivery models presented here, the first two (LTE dedicated and LTE commercial) have essential differences while third (hybrid) can be seen as a compromise between the first two.

Control

Starting from the first one, dedicated networks have one big advantage compared to other two models, they are built for the special purpose, they are built according to the user requirements and for the users which gives them exactly what they want with all public safety network characteristics and full control over the network. This is something that is not available in the commercial networks, or at least not on the same level, but may be partly available in the hybrid solutions, how big this "partly" is depends on the business model aplied.

Reduced control over network can be a disadvantage of commercial networks compared to dedicated networks. Control over network means control over network resources which further means control over their allocation. Whenever a user attempts to establish a connection, network determines through the admission control function whether resources will be allocated i.e. whether connection is going to be accepted or not. Besides the admission control, network control also includes control over user prioritization, which can play crucial role when network is overloaded/congested. Additionally, network control covers response time in the case of network disturbance, security, control of subscriber's profiles, etc. Usually, in commercial networks model these control mechanisms are not under control of public safety organizations, but the level of control can be regulated through contracts and SLAs.

Another downside of commercial networks model is the way they are built, commercial networks are more prone to suffer from congestion, service's degradation and sometimes even shutdowns during major incidents, while most of todays' dedicated public safety networks have been built to provide service availability close to 99,999%, which means less than 5 minutes of downtime per year [44]. This is because public safety networks are built to be robust and with extra redundancy.

Timing

The fact that commercial networks are already deployed provides starting advantage in relation to dedicated networks, in the sense that saves on initial investments and time. Timing advantage can be significant considering that public safety organizations can use mobile broadband solutions early and explore the benefits/drawbacks that those solutions bring, also it may be possible to obtain new capabilities as soon as they are released by 3GPP and deployed by

MNOs (e.g. ProSe, GCSE, MCPTT), this however depends on the MNO’s willingness to implement those capabilities.

So, when it comes to timing, commercial networks need the least time to be deployed, they are already available and (non-mission critical) services can be provided in short term. Hybrid scenario can happen in short to mid-term, depending on type of hybrid which will be applied, i.e. hybrid of TETRA and LTE network or hybrid of dedicated LTE and commercial LTE network. In the former case, both, TETRA networks and commercial LTE networks are available now, but the establishment of their interworking can take some time which may be a little longer than deployment of LTE commercial network model. In the latter case, in order to construct the dedicated part of the network standardized solutions for PS LTE need to be available, which, as we explained in Chapter 0, may happen in two to three years. Still, deployment of dedicated LTE network will take the most time. In this case not only that standardized PS LTE solutions must be available but the construction process itself can take long time, up to 7 years as we saw in Norway's case. However, how long it takes to build the network will depend on the starting point, i.e. does some parts of the existing network can be reused or the network will be built from the scratch.

Flexibility

Certain flexibility exist in commercial network approach compared to dedicated network approach. In the case of LTE commercial networks when service is taken from standard commercial networks we see that user(s) can negotiate different aspects for services, through SLAs, which gives the possibility to users to specify the services according to their needs with corresponding price. This can be good alternative for users willing to include broadband services in their system but not willing to invest in dedicated network. However, the biggest flexibility is offered by hybrid solution.

Due its flexibility, hybrid solution approach is often considered as the most likely approach in transition from legacy narrowband dedicated networks to the future mobile broadband public safety network [127]. Hybrid approach offers broad spectrum of possibilities when it comes to business models, however, their sustainability is hard to estimate, accordingly it is hard to prejudge which side, positive or negative, is going to outweigh. This mostly depends on a given circumstances. For public safety organizations MVNO model presents painless solution as a first step in transition towards mobile broadband public safety networks since it does not require sudden changes.

Costs

In terms of costs, different approaches can be taken when evaluating the costs of the network. Studies like [122] evaluate not just the financial cost of the network infrastructure but also its operational value in terms of what it actually offers the user sectors functionally, i.e. value for money. Any additional cost factors that may degrade or enhance the cost-benefit balance are also taken into account. Generally, total cost of ownership (TCO) of a mobile cellular radio network over the long term includes both the initial costs to build the network, largely CAPEX (capital expenses), plus the operational costs, OPEX. Results are examined from the point of view of the overall cost per user, in view of the functional value. This studies' results shown that the CAPEX estimated investment per user, for public safety sector only, are 1.4 times bigger for dedicated LTE network, than CAPEX for commercial LTE network, while operational expenses (OPEX) for the network per year are even approximately 6.7 times bigger in dedicated networks.

Another economic study [132], also compares the costs of these two delivery models – LTE dedicated network and LTE commercial network – but it also includes population density impact. This study presumes that network infrastructure for the commercial network is already built and only additional costs, such as hardening of the existing network, are taken into account in addition to the monthly fee defined according to the heavy business user profile. In the dedicated network case, this study assumes that existing TETRA cell sites and services are utilized when building LTE dedicated network. Results have shown that CAPEX are significantly higher for dedicated network, in densely populated area those expenses are almost two times higher while in the rural are they can be up to ten times higher than in commercial network. Results for annual TCO show that dedicated network is 1.2 times less expensive in highly populated areas while in rural areas dedicated network can be up to 8.4 times more expensive than commercial network. This study concludes that dedicated LTE networks are better choice in the areas where population density is greater than 100…200 persons per km2, while for the areas located in between rural and urban areas, either a dedicated LTE network or a commercial LTE network could be a good solution, depending on the local circumstances of each area.

Costs for hybrid solution deployment are hard to estimate and they depend largely on the model applied, but is assumed that they present balance between the costs of dedicated and commercial network and that the model is chosen to make the costs optimal.

Spectrum

Commercial LTE networks already have assigned frequency spectrum, hybrid solutions can use the same spectrum allocated to commercial LTE networks when they are included in combination, while dedicated LTE networks will have to find a solution for spectrum which will be used for public safety needs (now they do not exist and thereby do not have allocated spectrum).

Table 3.1 summarize advantages and disadvantages of the three above described models for delivery of services. In the table, first model is a representative of LTE dedicated network. The second model is a representative of a standard LTE commercial network (without any additional upgrades). Finally, the third model is an MVNO scenario which could be representative of a hybrid solution and/or commercial LTE network. The MVNO scenario can be applied in hybrid solutions if LTE dedicated and commercial parts of the network exist, but the MVNO can also be setup in commercial networks, as we saw when we were explaining deployment models.

Table includes above discussed aspects, control, timing, costs, spectrum, the only difference is that instead flexibility we compare availability of mission critical services which could be important aspect when comparing and evaluating these models.

	LTE dedicated network	LTE commercial network	MVNO scenario
Supports mission critical services	Yes	No	Only in the areas covered by dedicated network (if any)
Public Safety users have network control*	Yes	Service layer: Yes Network layer: No	Service layer: Yes Network layer: Only in the dedicated part of the network
Requires dedicated broadband Public Safety frequency spectrum	Yes	No	Only if there are areas covered by a dedicated network
Timeline availability	Long term (> 7 years)	Short term (~ 1 year)	Short to mid-term (from 1 to couple of years, depending is it commercial or hybrid solution)
Costs**	Medium to high	Low to medium	Medium

Table 6.1: Comparison of the three delivery models for the future mobile broadband public safety network

* Network control is evaluated through service and network layer, where service layer is concerned with control of the services delivered to public safety users and network layer controls message transport

**Costs refer to the initial network investments to start-up the services

6.5 Chapter Summary

In this chapter we have presented and compared three different delivery models which could be applied in transition from TETRA to LTE networks. We saw that LTE dedicated networks meet the user needs in the best way, however they can turn out as very expensive, require long time for rollout and can raise the problem of spectrum allocation in the future. On the other side, LTE commercial networks are less expensive, require less time to be rolled out, and they already have spectrum allocated, however they usually do not provide same level of control and availability of services, neither are those two aspects in the hands of public safety organizations, besides that they do not provide mission critical services. Hybrid solution can combine different aspects and parts of LTE dedicated and LTE commercial networks in order to create the most suitable model for public safety organizations, and therefore it is often considered as the best way to do the transition. However, even hybrid solution has the downside, this reflects in complexity that can arise when two (or more) networks have to interwork, which introduce the need for interoperability. Conclusion is that there is no advantage which will single out one model as the best transition approach. Delivery models with their advantages and disadvantages could be a right choice in different circumstances, and choosing the most suitable model will largely depend on interests of public safety organization(s), so adoption of each of these models is expected to be seen in the future.

Chapter 7

7 Case Study – Norway’s Public Safety Network

Having analysed different alternatives for deploying public safety LTE network, we will now do a case study of Norway's public safety network. As said, these deployment models can be applied when doing a transition from TETRA to LTE network. Norway's network is an example of nationwide public safety network that uses TETRA narrowband technology and which could migrate towards mission critical mobile broadband (LTE) network in the future.

By taking the current situation and the future plans into account, we will examine which service delivery model suits the best. Then we will describe, what we think that could be the most likely scenario for transition in the next years, we will also identify possible challenges of that approach and we will give some suggestions how those challenges could be overcome.

7.1 Nødnett Description

Nødnett is a dedicated radio network, built over the TETRA standard specifically for rescue and emergency users [126]. Nødnett, as we know it today, was established nationwide in December 2015, before that Norway did not have nationwide dedicated public safety network but instead, there were number of different systems used by the public safety organizations. Nødnett network is government owned (GO). Management of the network has been entrusted to Directorate for Emergency Communication (Norwegian: Direktoratet for nødkommunikasjon (DNK)). DNK is responsible for the creation, management and development of the network on behalf of the Ministry of Justice, meaning that the network is contractor operated (CO). This imply that Norway is using GO-CO (government owned-contractor operated) model.

As TETRA network, Nødnett primarily provides a voice communication for public safety users, but it is also possible to transfer data [126]. During 2016, DNK plans to establish ability for data transfer at up to approximately 12-13 kbit/s using MSPD (Multi Slot Packet Data) on all base stations, while one part (approximately one third) of the base stations will be able to use TEDS (TETRA Enhanced Data Service) which will provide data rates up to 80-90 kbit/s, both uplink and downlink [126]. TEDS coverage will initially be established in urban areas and along the most congested roads. These data rates are in line with what can be achieved with EDGE (Enhanced Data rates for GSM Evolution) [133] in the commercial mobile networks. This is not even close to data transfer speeds and possibility provided in LTE (explained in ***Error! Reference source not found.*** section).

7.2 Nødnett Development

Norway has only recently established completely new dedicated TETRA network, Nødnett. Development of the network took 9 years, required big investment (near 6 560 million

Norwegian crowns) [134] and represented an important project for Norway. This indicates that Norway plans to use TETRA in the years that come. However, there is an open will for further development of the network. Norway is the first country in the world to adopt TEDS in a larger scope [126], which sets it once again as a pioneer in adoption of telecommunication innovations and demonstrates Norway's willingness to future develop its network and follow the latest technologies. To remind ourselves, LTE networks first became publicity accessible in Oslo (Norway) in 2009 [49].

At Nødnett Days, director of DNK, Tor Helge Lyngstøl, pointed out that there are three possible directions in which Nødnett can go [135]:

1. Low involvement
   - Nødnett operated until it is outdated
   - No future orientation, no investment
   - Only emergency organizations use Nødnett
2. Realize maximum gain from the Nødnett investment
   - Nødnett operated, easy development
   - Multiple users interact Nødnett
   - Do not speed-up data
3. Further development of the emergency communications
   - Emergency Network operated and further developed
   - Joint efforts for secure, mobile data solutions, across sectors
   - Strengthened resilience
   - Gradual adaptation to next generation public safety communications (data and voice)
   - Satisfy new safety requirements

Option 1 imply that no further investments and development will be done, network will be used as it is, with existing users until it is outdated. **Option 2** includes introduction of the new users with very small development in order to realize the maximum gain from the existing network. **Option 3** imply further development of the network and transition to broadband data-centric networks.

Tor Helge Lyngstøl expressed his belief that Nødnett will continue to develop in the years that come, but that migration model which will be applied will largely depend on following factors [135]: Cooperation, Ambitions, Knowledge, Finance and Feasibility.

Lack of broadband support in Nødnett was marked as "The Achilles' heel" [136] by Knut Baltzersen, Acting Head of Service and Technology in DNK. In his presentation [136], he proposes two steps for transition to the future mission critical mobile broadband networks:

- **Step 1**: Establish own core network, use the base stations in the commercial networks (MVNO - Mobile Virtual Network Operator)
- **Step 2**: Building a private radio network

By introducing broadband data in the network, DNK also wants to attract more users, which itself is a driving factor for further development [136].

7.3 Transition Approach

First option in transition from TETRA Nødnett to LTE Nødnett is to build a dedicated LTE network. For Norway, building of new national dedicated public safety LTE network from the scratch after just completed construction of dedicated TETRA network, is not the most likely sequence of events since it would require (another) huge investment (as explained in the previous chapter). More cost-efficient way would be to eventually transform existing TETRA network into LTE network, by doing a slow migration. This imply exploiting existing network on any way possible. One of the network parts which could be reused and which contributes a lot to cost-saving are existing TETRA cell sites. Namely, approximately (up to) 70% of any mobile network costs is the radio access network (RAN), and much of RAN costs is not the radio and transmission equipment but the site real estate (either rented or purchased) [49], so instead of building completely new cell sites, those from TETRA should be reused and adapted.

Second option is to use commercial LTE network(s). Use of commercial LTE networks for public safety communications should not be excluded and it is quite possible to happen soon in the years that come due to user demand for broadband data applications. However, following our proposal from the previous paragraph (Nødnett will use TETRA network while evolving), commercial LTE networks could be used for high-speed non-mission critical data services, in the meantime, while Nødnett network is evolving to support LTE functionalities. This can be considered as temporary solution.

Having dedicated LTE network approach eliminated and assuming that commercial LTE networks will be used to satisfy user demands in parallel with TETRA network which will continue to operate for some years, we come to a conclusion that Hybrid scenario is the most suitable for Nødnett's transition.

Our conclusion match the prediction of the leading people from DNK. Accordingly, we will propose hybrid scenario for Nødnett's transition. Proposed transition scenario is described in the following section.

7.3.1 Transition Scenario

To protect the investment made in TETRA network and also to preserve reliability which this network provide, Norway will pick smooth transition scenarios which will exploit TETRA network to the maximum and also satisfy users' requirements for broadband services. In that sense, it is reasonable to think that transition to mobile broadband public safety network will require a period in which networks with narrowband TETRA services and LTE broadband services will coexist and be used in parallel. The TCCA has also predicted coexistence and co-usage of these two types of network at some point. The TCCA predicts that the evolution in public safety communications will take place in the following steps [137]:

- narrowband dedicated public safety network (current situation),
- co-existence of a narrowband dedicated public safety network for voice services and a cooperation with commercial mobile network operator for non-mission critical data services,
- co-existence of a narrowband dedicated public safety network for voice services and a dedicated broadband public safety network for mission critical data services, and
- integrated broadband public safety network for mission critical voice and data services.

According to these steps, TCCA prediction also imply that hybrid solutions will be used in transition(s).

Since hybrid solution transition approach can turn in complex procedure it is important to have strong strategic plan. One should be careful in making plan for transition. One should not be unrealistic and propose ambitious plans, but rather base them on the real possibilities in a given circumstances. For that reason we will use the knowledge of other countries which have gone through this phase. Namely, Finnish TETRA operator, VIRVE, has already established a roadmap towards the implementation of a government-controlled hybrid of dedicated and commercial LTE network which will eventually offer critical voice and broadband data. Important affair which favours Finnish approach stems from the fact that three Nordic countries, Norway, Sweden and Finland have an agreement to harmonize their public safety communication systems [138] meaning creating common technological solutions across national borders, which again implies that they will develop in the same direction. Since the public safety communication systems at the national borders are no different than those used within the country, it may be expected that also their public safety networks will develop in the same direction.

Finnish transition approach follows TCCA's predictions and presents somewhat extended, more detailed, version of the Knut Baltzersen's two steps, which implies deployment of public safety MVNO at the start of the transition process and building a dedicated LTE network as the end goal. VIRVE defines five steps in transition towards critical broadband network [139] (Figures 7.1 – 7.6 are reproduced from Ref. [140]):

NOTE: Understanding of the following figures requires knowledge of LTE architecture. Readers not familiar with LTE's core components should first refer to *Appendix A (LTE Architecture)*. Connections between certain network components may not correspond to the real connections but they are included for illustrative purposes.

- **Step 0.** This step describes current state and it is included only for the illustrative purposes. State in Step 0 is illustrated in Figure 7.1, which presents standard TETRA network.

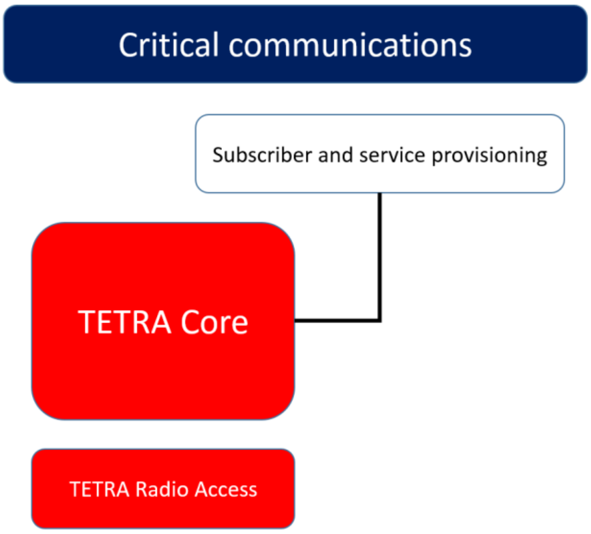

Figure 7.1: TETRA network

- **Step 1.** 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 (somewhat similar to the current solution in Belgium.), but eventually the second step will be to own and control subscribers in the LTE core. State after Step 1 is illustrated in Figure 7.2.

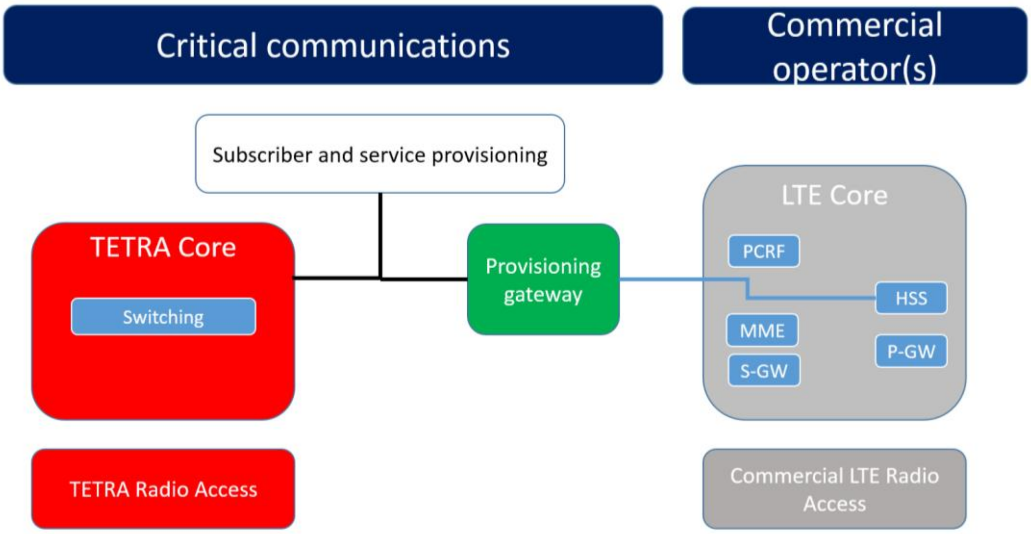

Figure 7.2: TETRA network + commercial (non-mission critical) broadband data provided by commercial operator(s) with own SIM cards

At this point, TETRA network and its services are still used as usual. The public safety users/subscribers are using broadband services from commercial LTE operator. Subscribers' database (Home Subscriber Server (HSS)) is located in the core network of the commercial operator, meaning that, if more than one operator is providing services than each of them will have its own HSS for the same group of users/subscribers. This is important to note, since in this case commercial operators are responsible for performing the operational subscriber management.

Provided services are standard broadband services from a standard LTE network(s) developed for commercial users and they are not adapted for public safety users. The public safety users access the (commercial) LTE network and services by using the special SIM cards, which can be set up to connect to the preferred network (e.g. based on stronger signal power, more available capacity, etc.) while network can be set up to provide priority to the users using those SIM cards. In this way mission critical users could be differentiated from the commercial users. With those SIM cards they can roam in networks of different operators.

- **Step 2.** To control subscribers in an owned LTE core. In this second step, the critical voice and messages will run in the narrowband network, and high-speed non-mission critical, but secure data (with public safety level of security) will run in the commercial broadband network. State after Step 2 is illustrated in Figure 7.3.

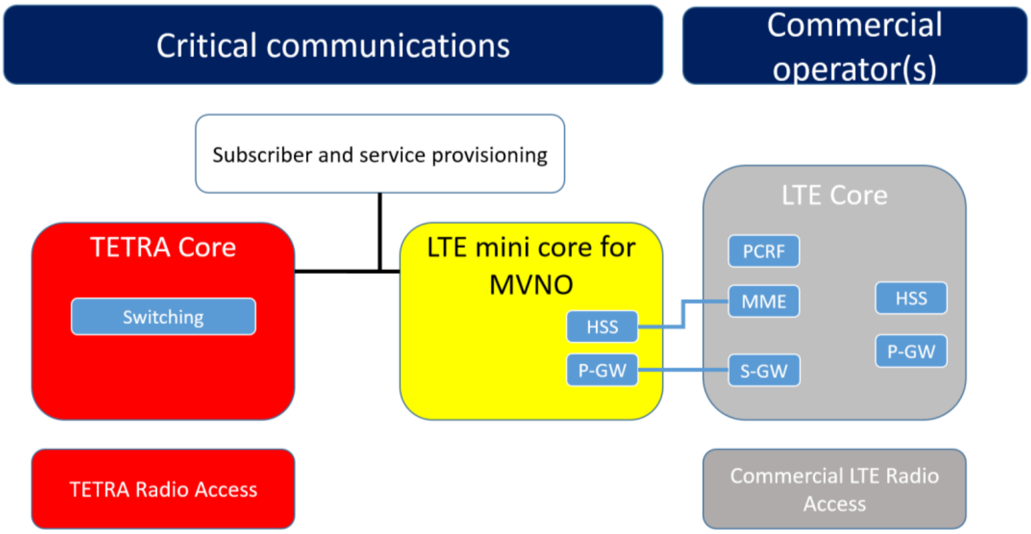

Figure 7.3: TETRA network + MVNO using own LTE-core

At this point users are provided with the same services and in the same way as in Step 1. However, now there is a unique subscribers' database (HSS), located in the dedicated LTE networks' core, which eliminates the need to have multiple databases in different commercial networks and thereby dedicated network becomes users' home network whilst users roam in commercial network. Now MVNO becomes responsible for performing the operational subscriber management. This creates the environment in which is easy switch up from one commercial operator to another, since it does not require the entire database to be moved. Dedicated and commercial LTE network(s) are connected in a standard LTE roaming architecture [74].

In this step construction of dedicated part is started by constructing one part of the core network. At this point, this LTE mini core is used by MVNO to cross from *Light* to *Full* MVNO (see Deployment of Public Safety MVNO).

- **Step 3.** To expand the owned LTE core and add an owned dedicated LTE radio access in chosen locations to complement the coverage of commercial operator(s). Data services provided are mission critical data services. State after Step 3 is illustrated in Figure 7.4.

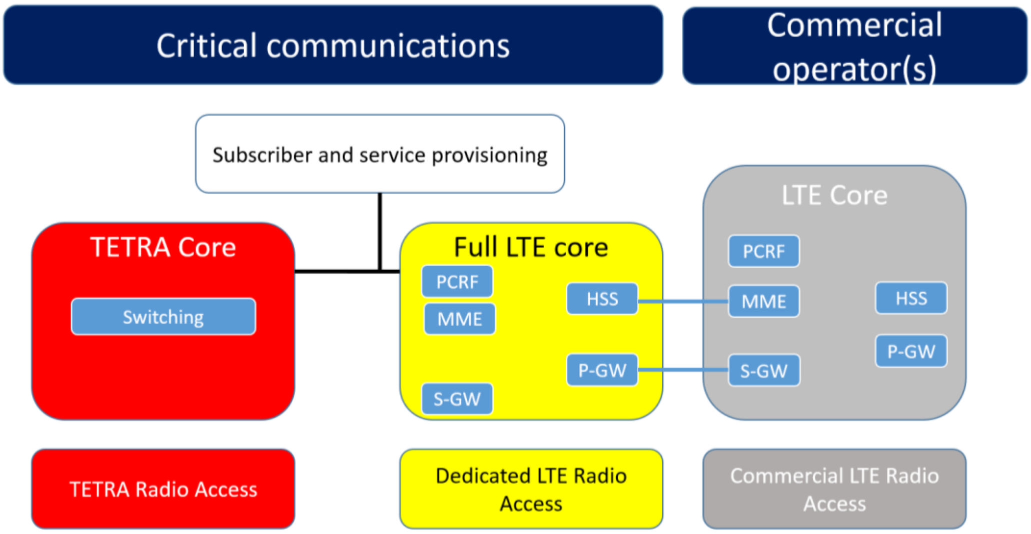

Figure 7.4: TETRA network + dedicated LTE network + commercial LTE network

At this point, TETRA network is still used for voice service, but mission critical data services are now provided by dedicated LTE network.

As already mentioned, this transition process is an implementation of a hybrid of dedicated and commercial LTE network, which should be a final goal. Now, the LTE mini core for MVNO has expanded to full LTE core, containing all standard LTE core elements, and LTE radio access network has been added. MVNO is thereby transformed into dedicated MNO which is now able to operate independently. However, dedicated LTE radio access is only built in the areas lacking the coverage of commercial LTE network(s) so the radio access from commercial LTE network(s) will continue to be used. Dedicated and commercial networks will still be interconnected and interwork in a standard way for LTE networks.

- **Step 4.** To connect the TETRA and the LTE network once the critical voice over LTE standardization is ready and the TETRA supplier supports group call over LTE functionality in the TETRA side. To enable LTE devices to access the TETRA services through LTE network, which is further connected to TETRA network. 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. State after Step 4 is illustrated in Figure 7.5.

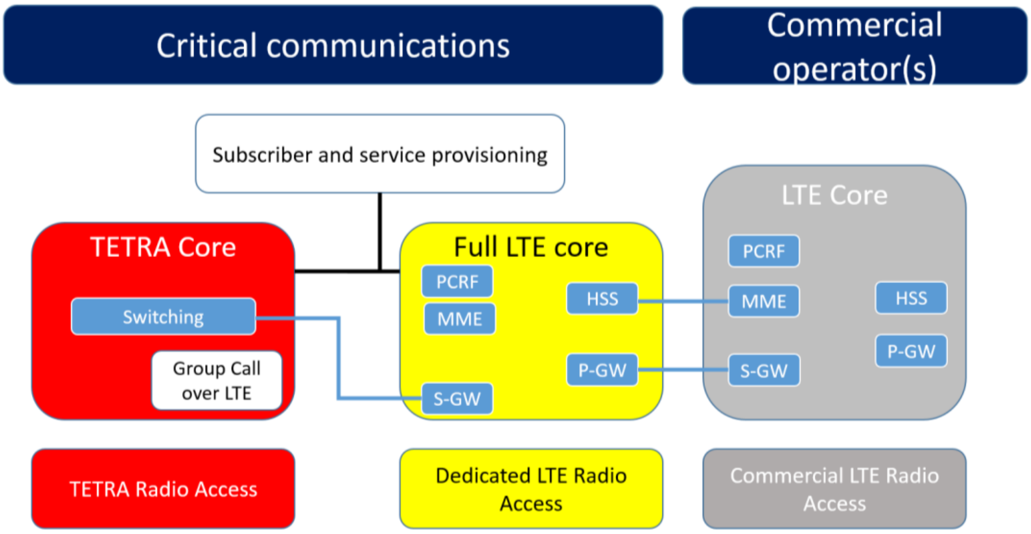

Figure 7.5: TETRA and hybrid LTE

At this point, both, mission critical voice and data services are provided by dedicated LTE network but voice services remain available in TETRA network and can be used as a fallback while commercial LTE networks is used for coverage.

Parallel with deployment of dedicated LTE network, TETRA core network was in the process of upgrading and development which should allow interconnection and interworking with LTE network. These changes should adapt TETRA network to the future needs, meaning support for LTE functionalities in the TETRA side.

- **Step 5.** To dismantle the TETRA radio access once broadband service availability and reliability meets public safety's requirements. State after Step 5 is illustrated in Figure 7.6.

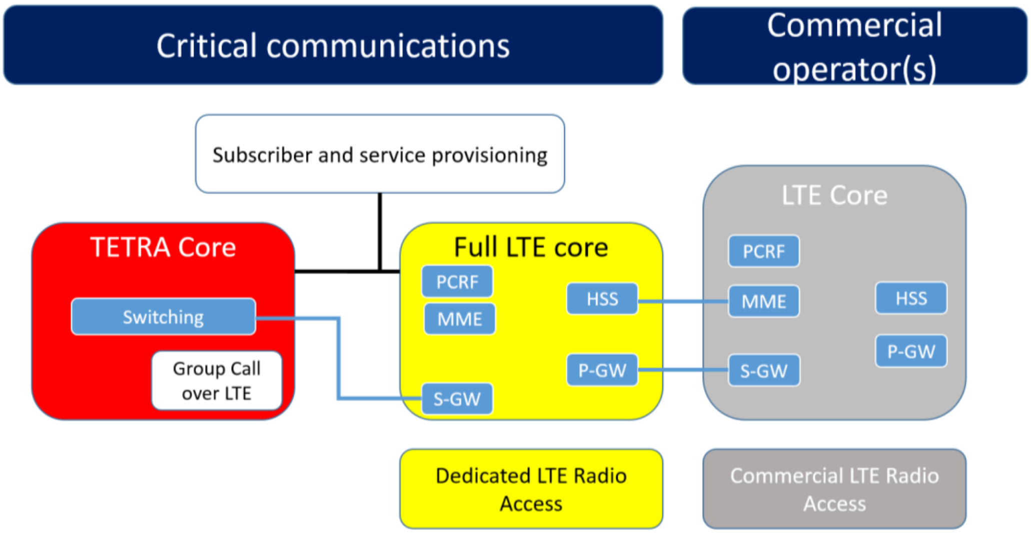

Figure 7.6: Hybrid LTE + TETRA without TETRA RAN (TETRA serves as (voice) application server)

At this point LTE mission critical services are mature enough so TETRA radio access network can be dismantled and TETRA voice services are no longer used as fallback. All services are provided by dedicated LTE network and commercial LTE radio access is used as before.

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 high-speed data service that enables them to benefit from data applications and to develop information-centric ways of working [139].

7.3.2 Timing

Groundworks in Finland have already started, this implies lobby for frequency (spectrum) and prioritization in commercial networks. Critical voice and broadband data are expected to be offered by 2030, meaning that Step 5 will be finished at that time, meaning that Steps 1-5 should be done in period between 2015 and 2030 which gives almost 15 years to do the transition. Figure 7.7 [139] illustrates Finland's timeline for broadband rollout.

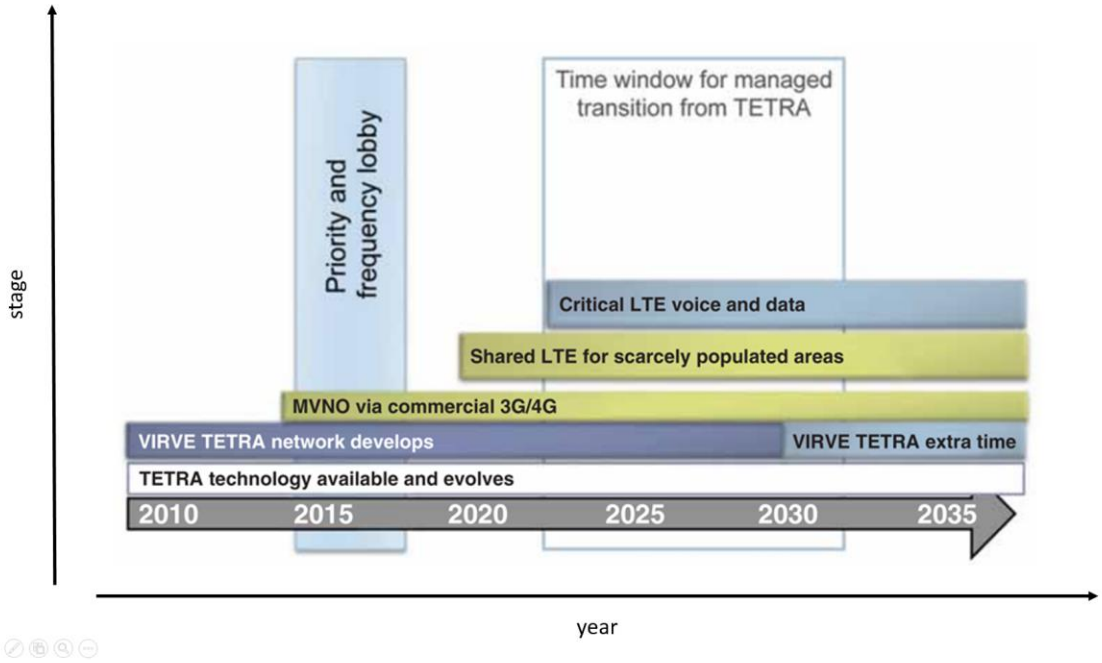

Figure 7.7: Finland’s timeline for broadband rollout [139]

Figure 7.7 shows how the network will evolve and change over time. Y-axis shows stages in the network evolution, from TETRA-based to LTE-based public safety network.

In the sense of timing, this time scale looks reasonable, since by the time when LTE technology for public safety communications should be implemented in the network, it is expected that technology is fully standardized and already tested, also it gives enough time to realize the maximum gain from the TETRA network.

Norway's timeline will look slightly different. In Norway, TETRA network has been put in operation in 2015, so it will pass couple of years before Norway starts grounding works for transition. However, it can be expected that Nødnett offers mission critical broadband data services shortly after VIRVE, that delay should not necessarily be long as initial delay in transition. There are no official documents that show when this may happen, but during Nødnett days there was an impression that Norway is willing to continue developing its network and follow global trend for introducing broadband data services in public safety communications.

7.3.3 Deployment of Public Safety MVNO

Steps 1 and 2 include deployment of an MVNO for public safety/critical communications. The MVNO could be defined as a mobile communication service provider that does not own the network infrastructure and/or does not have an allocation of spectrum, these are provided to MVNO by mobile network operator(s) (MNOs), and in our case we consider them commercial operators. Different MVNO models are possible to implement, depending on level of control which MVNO wants to have over its services. That control depends on how deep MVNO permeates in mobile value chan. Figure 7.8 shows mobile value chain, area in which MVNO can participate and reflects how MVNOs from Step 1 and 2 are set up.

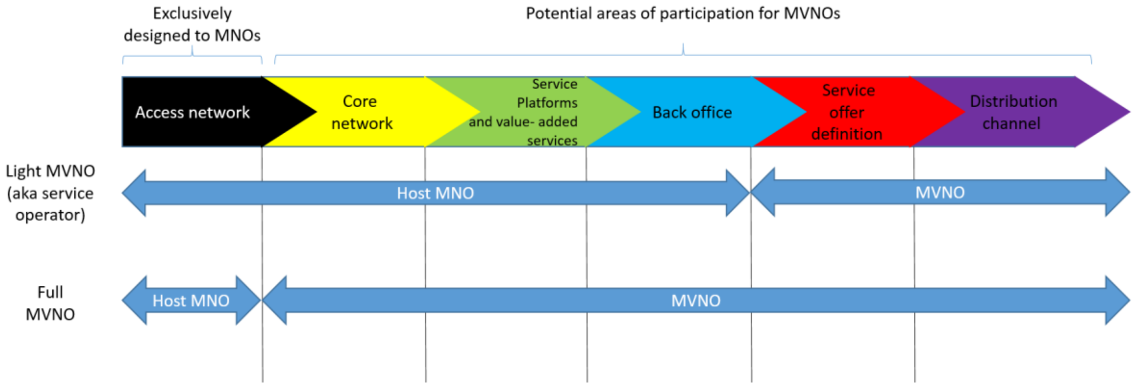
Exclusively designed to MNOs
Potential areas of participation for MVNOs
Access network
Core network
Service Platforms and value- added services
Back office
Service offer definition
Distribution channel
Light MVNO (aka service operator)
Host MNO
MVNO
Full MVNO
Host MNO
MVNO

Figure 7.8: Mobile value chain and areas of participation for MVNOs

Figure is reproduced from Ref. [44].

As shown in the Figure 7.8, potential areas in which MVNO can take participation are [44]: operation of the core network (e.g. switching, backbone, transportation, etc.), the operation of the service platforms and value-added services, the operation of the back-office process to support business processes (e.g. subscriber registration, terminal and SIM logistics, billing, customer care, etc.), the definition of a mobile value offer and the final delivery of the products and services to the client through the distribution channel.

The MVNO set up in Step 1 is a **Light MVNO**, also called **service operator**. This model allows new ventures, to take control over the marketing and sales areas and, in some cases, increase the level of control over the back-office and value-added service definition and operation [44].

The MVNO set up in Step 2 is a **Full MVNO**. In this model the MNO provides only radio access network infrastructure (and sometimes part of the core network), while the new venture provides the rest of the elements of the value chain [44]. The MVNO in our case may not control MNO's core network but it has its own part of the core network.

Deployment of an MVNO may be desirable in situations where MVNO has more knowledge than the MNO of a specific market segment or if MNO does not want to develop itself in that segment, which may be the case in critical communications due to small market. The MVNO stands between user organisations and MNOs, and it manages all the services for the users. However, these services' capabilities and features are dependent on MNO's radio network [141].

Benefits/Drawbacks

The MVNO set up in Step 1 provides all the same services as commercial operators would, but introduces some potential benefits which can be seen as MVNO's added values. The MVNO presenting several organizations may have bigger negotiation power when negotiating the contract agreement with the commercial MNO. That may reflect through following benefits.

Potential added values of MVNO after Step 1 are:

- special SIM card which may operate in all MNOs with certain privileges – if public safety organizations make individual contracts with more than one LTE operator (e.g. for better coverage), they would have to use the same number of SIM cards as the number of operators they have contracts with. Multiple SIM cards can be a certain inconvenience, it may happen that managing multiple SIM cards in single mobile device can be complex task or it may require bigger device, and it can reduce the market (number of manufacturers) who offer such devices, which can increase their price.
- MVNO may negotiate lower prices for the services – although this is not guaranteed it is the most probable outcome
- information exchange among organizations – MVNO presenting multiple organizations can create an environment that will facilitate the exchange of information
- platform for public safety applications development – MVNO can be a platform for development of applications which will be adapted to public safety users' requirements

Other potential added values of MVNO after Step 2 are:

- improved subscriber management - possibility to have one permanent user database which will be located in, dedicated, LTE mini core for MVNO. This eliminates the need to have multiple databases for the same group of users stored in each MNO's HSS (Home Subscriber Server), which facilitates subscribers' management. This will also create the environment for easy switch from one commercial MNO to another if/when needed. The MVNO only needs to re-connect its mini core network to another MNO and will immediately be ready to use the service.
- step towards dedicated LTE network - setting up an MVNO can be a step towards establishing dedicated LTE network for critical communications. The operators and users will have a chance to better understand the potential benefits of mobile broadband services in critical communications.

7.4 Transition Challenges

When we analysed delivery models we pointed out that complexity can be a certain disadvantage of a hybrid solution, here on a concrete example we can point out the challenges that can arise and which cause that complexity.

The mere fact that networks based on different technologies, narrowband and broadband, are used in parallel is a challenge. Challenge can arise if those networks have to interwork or if user terminals need to receive messages from both types of networks. In particular, this raise a challenge of interoperability of:

- terminals and
- infrastructure.

Another challenge can arise if dedicated and commercial LTE network operate on the same spectrum. In that case, spectrum sharing needs to be regulated.

7.4.1 Infrastructure Interoperability

Transition process must ensure that network infrastructures and their appropriate terminals are interoperable.

Migration Path for Installed TETRA Networks

Given that TETRA network will not be fully omitted neither after Step 5, since TETRA supplier will support group call over LTE functionality in the TETRA side, the TETRA network will have to undergo a certain changes, upgrades and improvements in order to cope with the future needs. Before moving further, let us first explain what 'group call over LTE functionality in the TETRA side' means. This means that LTE devices attached to LTE network will be able to use group call service provided by TETRA network. Now, in order for that to be possible, TETRA and LTE networks will have to be interconnected. Those are the future needs for which TETRA network must be ready. This includes creation of open Inter-System Interface (ISI) so that the networks could interconnect in the future.

Today, most of the TETRA networks are interconnected via TETRA ISI and the transport lines between the network gateways in the two TETRA networks are E1 based [142]. Creation of new ISI which will allow interconnection with LTE network will imply phasing out the E1 based lines and substituting them with IP based lines, considering that architecture of LTE is purely IP based [58]. Changes of transport lines will further require changes in TETRA network infrastructure which will have to become all-IP based.

Migration should go towards the unified system, which means:

- allowing TETRA and LTE core components to be implemented on the same hardware
- converged backhaul of LTE and TETRA networks - to share a common transport network
- deploying TETRA base stations which have the possibility to be upgraded with eNB (TETRA/LTE Base Station, e.g. MTS4L [143])

Converged backhaul will be possible when TETRA network do the infrastructure transformation from E1 based to all-IP based infrastructure. Then TETRA can share the same transport lines with LTE network(s).

Hybrid solutions for TETRA/LTE Base Stations are already available on the market (e.g. MTS4L [143] or LTEtraNode [144]). These base stations can be used only for TETRA, only for LTE or both and could be a good solution for smooth transition. TETRA/LTE Base Stations can turn to good account considering that DNK has established cell sites for Nødnett. It is worth noting that only small proportion of those sell sites are dedicated and government owned, most of them are embedded in existing cell sites of commercial telecommunications operators such as Telenor, Norkring and Netcom [145], i.e. they are commercially owned and rented by DNK. Anyhow, established cell sites may be a starting advantage since the existing cell sites can be upgraded.

However, additional cell sites will be required due to limitations of high frequencies used in LTE systems. Namely, TETRA system uses low frequencies (around 400 MHz) which allow better radio propagation and thus better territorial coverage, while working at higher frequencies leads to worse propagation conditions and hence to a higher number of base stations (BSs) required to cover the same territory [146].

LTE Infrastructure

In this migration it may be beneficial to enable access to TETRA network and TETRA services through LTE devices, meaning that users carrying standard LTE devices (e.g. smartphone, tablet, etc.) will be able to use them as if they are TETRA terminals. This could be done by setting up TETRA/LTE gateways (e.g. TASSTA T.BRIDGE [147]). TETRA-LTE gateways are connections between TETRA and LTE networks, they enable LTE devices to access the TETRA network. LTE users can then communicate to TETRA terminals, dispatch services and control centres on the TETRA side. These gateways will also serve to expand the TETRA network coverage since for this solution users are using LTE radio access network (RAN), i.e. they are within LTE networks' coverage and it will also improve co-operation between users.

7.4.2 Terminals Interoperability and Collaboration

Having TETRA and LTE networks work in parallel usually means that no single antenna dual mode (TETRA and LTE) terminals can be used [148], due to different frequency bands in which these two networks operate (in Europe: TETRA at 400 MHz, LTE at 700 MHz). Users will may have to use two devices [149], one for narrowband voice (operating at 400MHz) and one for broadband data applications (operating at 700MHz). This can be a certain inconvenience for the users, since beside carrying two devices they may also receive same information about the event one both devices which leads to waste of time and unnecessary waste of network's resources, or they may receive partly information on each device, which should be presented as a whole. Beside the inconveniences that causes to the users, it may be also challenging for the operators. TETRA terminal and LTE device should be able to collaborate.

This collaboration can be done at the different levels. One type of collaboration could be between devices carried by single user, in which case devices could be connected via Wi-Fi or Bluetooth technology to exchange and share information or to rely the messages of one device on other devices' network (e.g. user uses PTT on the TETRA terminal, that is transmitted to LTE device via Bluetooth, and further on the LTE network), in this way one device could be used for both networks.

Another type of collaboration should ensure direct communication between TETRA terminals and LTE devices when using the same service(s) but when they are in possession of different users. This can be done by using TETRA/LTE gateways, as we already explained, or it could be done at application level by creating a software based interoperable platform able to work on any LTE device with the possibility to communicate with the TETRA users, e.g. WAVE application by Motorola Solution [150] which is already used in Nødnett.

Ultimate goal is to have a single converged device. The latest innovation is a Finmeccanica's PUMA T4-LTE handset which supports both TETRA (at 400 MHz and 700 MHz) and LTE (at 700 MHz) [151]. This handset took the Best Innovation Award at the last ICCAs (International Critical Communications Awards) event [152], held in February, 2016, and it presents the hope that it is possible to use a single device for two different networks

Applications Interoperability

Use of application level solution can however raise a new challenge. Namely, it is quite possible that many applications designed for the same service and coming from the different vendors will appear on the market, for that reason and for the reason of interoperability of LTE public safety networks, those applications need to be tested and certified by some kind of independent Certificate Authority (CA). So far, TCCA has tested and certified TETRA features of terminals [148], but in the future CA for application solutions in PS LTE will be needed.

7.4.3 Spectrum Sharing

As explained in section *6.1.1 Model Evaluation* having a public safety dedicated LTE network can raise a problem of frequency spectrum allocation or spectrum availability. The TETRA systems use 400 MHz frequency band [153], and, as in most European countries [154], in Norway Nødnett, Norwegian (TETRA based) public safety network, has dedicated spectrum blocks in the 400 MHz frequency band [155]. However, for the future mobile broadband public safety communications different frequency band will have to be used, and in Norway 700 MHz frequency band has been chosen [156].

In Norway, NKOM [157], Norwegian Communications Authority (nor. Nasjonal kommunikasjons-myndighet), is the agency responsible for frequency allocation [158]. By the National Table of Frequency Allocations [155], 700MHz frequency band, is currently allocated for broadcasting. It is hard to believe that 700 MHz frequency band will be allocated exclusively to Nødnett in the future, which implies that spectrum will have to be shared. Spectrum sharing is required when sufficient demand for spectrum exists.

By the definition, spectrum sharing refers to the application of technical methods and operational procedures to permit multiple users to coexist in the same region of spectrum [121]. Meaning that, spectrum sharing typically involves more than one user sharing the same band of spectrum for different applications or using different technologies [159].

Spectrum Sharing Models

Different spectrum sharing methods exist, they allow the usage of the same frequencies. The most used methods are:

- geographical separation - this method allows same frequencies to be used in different, distant, geographical areas
- coordinating time usage - same frequency used at different times
- directive antennas - antennas that use the same frequency are directed (focused) in different directions to avoid signal interference

However, spectrum sharing becomes complex when same frequencies are shared in the same geographical area due to signal interference. In that case spectrum sharing models can be classified based on two defining features [121]:

1. Whether the spectrum sharing agreements comprises **primary-secondary sharing** or **sharing among equals**. In primary-secondary model, primary system has higher rights and priority over the spectrum while users of secondary system are allowed to use the spectrum in a way which will not cause interference to a primary system, this is regulated by the spectrum policy. In sharing among equals model, devices from all systems have the same rights for using the spectrum.
2. Whether sharing is based on **cooperation** or **coexistence**. Cooperation model imply that systems or devices sharing the spectrum band must communicate and cooperate with each other to avoid interference. Coexistence model imply that devices from

different systems should in a way "sense" the presence of other systems' device(s) and try to avoid interference without directly communicating with each other.

Proposed Spectrum Sharing Model for Nødnett

The spectrum sharing for public safety use can constitute a credible approach to complement a dedicated assignment of spectrum. The spectrum sharing regulations should specify the amount of spectrum allocated to public safety, this amount can be optimal amount of spectrum needed to perform day-to-day operations. Sharing regulations can also specify that additional spectrum will be provided and guaranteed to public safety in the situations when that it needed (major incident).

In that context, spectrum sharing based on LSA (Licenced Shared Spectrum)[16] approach is imposing as suitable model. LSA spectrum regulatory approach [121], grants LSA licences to each party for a dedicated amount of spectrum (spectrum block) in the same frequency spectrum band, but allows other party/ies to use that spectrum when the party to which spectrum is assigned is not using it. LSA ensures a certain level of guarantee in terms of spectrum access (i.e. each party has individual exclusive access to a portion of spectrum), and avoids occurrence of interference. LSA allows network operators, both, in public safety and commercial domain, to provide predictable quality for their service. This approach may be used to allocate minimum amount of dedicated spectrum to public safety network, which will allow unobstructed (smooth) daily operations, but also give them access to spectrum allocated to commercial networks when available, same goes in the other direction, commercial networks can get access to spectrum allocated to public safety networks, when available. Another option would be to assign more than a minimum amount of spectrum to public safety network, and the public safety network operator can further allow commercial network operator to uses the excess spectrum but keep the right to reclaim the spectrum back in special circumstances (e.g. major incident).

With appropriate spectrum sharing partnerships between Nødnett and commercial networks, public safety users will be able to access licensed public safety spectrum, shared spectrum, as well as commercial networks when the need arises.

7.5 Chapter Summary

Users' need for broadband data services in public safety communications is present. Norway has only recently established nationwide dedicated public safety network based on TETRA technology. However, TETRA network cannot satisfy users' needs for broadband data, so Norway has to seek for solution which will satisfy the user needs but also protect the investment made in TETRA network.

The TETRA based public safety communications systems provide good critical voice and short data messaging capabilities while LTE based communications sytems provide high data rates for broadband data. Golden Grail could be a combination of both technologies in the years that come, while TETRA functionalities and TETRA-like features are migtating to LTE. Coherent solution should be created to satisfy current and future requirements for voice, status, text and

[16] In different literatures name ASA (Authorized Spectrum Access) model often can be found, these two models are equivalent

location messages, picture and video transmission, etc. Transition approach presented in this chapter can succeed in this.

This transition approach maximally exploits the investment made, by using TETRA voice services for years before they are excluded from use and by reusing functionalities developed for group communication to provide Group Call over LTE on the TETRA side even after TETRA network and TETRA services are no longer used for public safety communications.

Besides that it also provides broadband data services in the foreseeable time, before mission critical data services are available, thereby giving operators and users time to adapt to new features. Introduction of non-mission critical services from commercial networks will not require big investment as constraction of dedicated LTE public safety network would, in this way Norway will avoid big initial investment before actually knowing the real value of broadband services.

This scenario can possibly introduce some challenges concerning interoperability and spectrum sharing, which are not impossible to overcome.

Chapter 8

8 Conclusion

This chapter summarize the work of this thesis, provides the main findings, and gives suggestion for future work.

8.1 Summary

The main objective of this thesis was to perform an assessment of whether future LTE networks will be suitable for public safety communications. In that context we have evaluated the ability of new LTE functionalities, designed for public safety communications, to replace the functionalities available in public safety TETRA networks. Special attention was paid to security aspects of two new LTE features, where we proposed security protocols for user authentication. Also, different deployment alternatives for future public safety LTE networks were evaluated.

For the purposes of this assessment, we first had to identify the characteristics of currently used communications systems in public safety networks. This was to understand how one communications system has to look and what it needs to provide in order to be used in public safety network. Widely used system in public safety networks, TETRA, was used as a representative model. It was identified that communications systems used in public safety networks were designed according to public safety user special requirements and that they provide unique services inherent only for public safety networks, of which the most important are: group call with Push-to-talk (PTT) feature, priority call, pre-emptive priority call, call authorized by Dispatcher, etc.. Also, it was noticed that for public safety communications systems it is important to ensure user communication beyond network coverage. This is facilitated by device-to-device communication (Direct Mode Operation (DMO)) functionality.

Comparison of currently deployed public safety and commercial cellular networks has shown that public safety TETRA networks use narrowband technology, which is designed for voice-centric service and does not have good support for data applications. On the other side, commercial cellular LTE networks are more data oriented and they use broadband technology, designed for data applications which require high data rates. In terms of services, public safety TETRA networks have number of services inherent only for those types of networks which are adapted to the user needs, who often work in groups and places where network coverage is not available, therefore they have specialized services like group call and DMO. Commercial cellular LTE networks are designed for one-to-one communication only and do not have support for communication outside the network coverage. Concerning how networks are designed and constructed, public safety networks have better geographical coverage, better service availability, and multiple levels of security, including end-to-end security. Next-generation public safety networks should provide the same functionalities and be constructed as present public safety networks with good support for broadband data applications, as in commercial cellular networks.

Analysis of new LTE functionalities designed for public safety communications have shown that in the future LTE will be able to replace TETRA in public safety communications and provide similar functionalities to those available today in TETRA public safety networks.

Implementation of new functionalities will require changes in LTE architecture which will have to have more network entities, mostly application servers which will be responsible for providing those functionalities. New LTE features will be able to match the TETRA services and meet the public safety user requirements for group and device-to-device communication, through Group Call System Enablers for LTE (GCSE_LTE) and Proximity Services (ProSe) functionalities. Push-to-talk (PTT) service will be provided through Mission Critical Push To Talk (MCPTT) over LTE Service, additionally through MCPTT Service other necessary services will be realized, like Priority call, Pre-emptive call, etc.. Ability of network's base station to operate independently without backhaul connection to the core network and maintain a level of communications between public safety users will also be available in LTE via IOPS-capable eNBs. New LTE functionalities are expected to become available late 2017.

For two new LTE features, One-to-one ProSe direct communication and MCPTT Service security enhancements were proposed. For both of these features User Authentication protocols were proposed. Proposed protocols follow security requirements and frameworks set by 3GPP. For User Authentication when One-to-one ProSe direct communication is used, Authenticated Diffie-Hellman protocol was proposed. Protocol analysis has shown that this protocol is able to confirm user's identity, i.e. the identity of the UE, with certainty and meet all security requirements, thus achieving a high level of security. For user authentication when MCPTT Service is used, TEAP protocol was proposed. This protocol ensures that credentials sent by user for authentication are not compromised. Protocol analysis has confirmed that TEAP protocol is able to meet security requirements for MCPTT User Authentication. It is proposed that user credentials be in form of username and password, since TEAP protocol has good support for this form of authentication. This protocol can verify user credentials and claim whether they are valid or not, however it cannot guarantee that credentials provided are from valid user since credentials are always provided by the end user, a person, which is not under networks' control.

Analysis of deployment models for future public safety networks gave following results. LTE dedicated networks meet the public safety user requirements in the best way, however this model can prove to be very expensive, it requires a long waiting time before services become available and it can raise an issue of spectrum allocation. LTE commercial network model is on the other side, less expensive than LTE dedicated networks model, the fact that these networks are already deployed shortens the time which should pass before services become available, plus these networks already have spectrum allocated. However, these networks are not built according to requirements of public safety users, they do not provide specialized services and are not reliable as dedicated public safety networks, and also they have worse service availability and smaller geographical coverage, as well as lower level of security. All this, however, can be overcome if commercial networks undergo certain upgrades. Hybrid solution model generally imply combination of LTE dedicated and LTE commercial network, however this term can also be used for combinations of TETRA and LTE networks. So, any model that implies combination of two or more networks can be called hybrid scenario. The characteristics of this model is hard to estimate, due to diversity of models implied by this term. However, as combination of LTE dedicated and LTE commercial networks, this model can be a certain compromise between these two models and combine their best properties, thereby achieving the best result. Combination which includes TETRA network as well, is considered to be the smoothest transition approach for public safety organizations from one type of networks to another. Case study for transition from TETRA to LTE network has confirmed those claims.

In case of Norway's public safety network, Nødnett, Hybrid solution model has adapted the best. Proposed transition scenario gives enough time to Norway to exploit the investment made in new TETRA network but also satisfies the users' need for broadband services. At the beginning of transition, hybrid model implies combination of dedicated TETRA network and commercial LTE network, this later develops into combination of dedicated TETRA network and dedicated and commercial LTE network and finally it ends as a combination of dedicated and commercial LTE network. This case study has supported the claims on hybrid model as the smoothest approach for transition from TETRA to LTE. Possible challenges of hybrid model were identified. Those challenges concern the interoperability between TETRA and LTE network(s) and interoperability between terminals used in those networks as well as the spectrum sharing among LTE dedicated and LTE commercial network. Interoperability between networks can be achieved by creating Inter-System Interface (ISI) which will ensure that these networks can interwork, also it is possible to setup gateways which will enable LTE devices to use TETRA services, but this can also be achieved through application level solution. Interoperability between terminals or rather cooperation between LTE and TETRA terminals can be achieved through their connection via Bluetooth or Wi-Fi. Finally, spectrum sharing between LTE dedicated and LTE commercial network, can be regulated by using the LSA (Licenced Shared Access) spectrum sharing model.

8.2 Future Work

Future studies could be related to performance of new LTE features, i.e. whether they are going to be “good” as TETRA services and be susceptive to the users as TETRA services are. Whether call set-up time will be less than 300ms, as in TETRA. Whether LTE ProSe-enabled devices will have the same range as TETRA DM-MSs, due to higher frequency they will use, thus worse signal propagation. Concerning security, new security procedures could be tested after implementation. It will be particularly interesting to see how End-to-end security is planned for LTE, in that sense implementation strategy can be proposed. Also, it can be studied how security will be implemented during the transition phase when TETRA and LTE networks interwork, considering that these two networks use different security protocols.

After some of the transition initiatives is realized, it can be discussed how costly and how beneficial that deployment model was and what have broadband applications brought into public safety communications.

References

[1] Ramon Ferrús, Oriol Sallent, "Preface," in *Mobile Broadband Communications for Public Safety: The Road Ahead Through LTE Technology*, Wiley, August, 2015, pp. ix-xii.

[2] Ramon Ferrús, Oriol Sallent, "Public Protection and Disaster Relief Communications," in *Mobile Broadband Communications for Public Safety: The Road Ahead Through LTE Technology*, Wiley, August, 2015, pp. 1-48.

[3] ETSI, "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 10: Supplementary services stage 1; Sub-part 16: Pre-emptive Priority Call (PPC)," aUGUST 2006. [Online]. Available: http://www.etsi.org/deliver/etsi_en/300300_300399/3003921016/01.03.01_60/en_3003921016v010301p.pdf. [Accessed 22 February 2016].

[4] ETSI, "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 10: Supplementary services stage 1; Sub-part 24: Call Retention (CRT)," April 2000. [Online]. Available: http://www.etsi.org/deliver/etsi_i_ets/300300_300399/3003921024/02_60/ets_3003921024e02p.pdf. [Accessed 22 February 2016].

[5] ETSI, "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 10: Supplementary services stage 1; Sub-part 10: Priority Call (PC)," May 2002. [Online]. Available: http://www.etsi.org/deliver/etsi_en/300300_300399/3003921010/01.02.01_60/en_3003921010v010201p.pdf. [Accessed 22 February 2016].

[6] ETSI, "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 10: Supplementary services stage 1; Sub-part 22: Dynamic Group Number Assignment (DGNA)," January 2002. [Online]. Available: http://www.etsi.org/deliver/etsi_en/300300_300399/3003921022/01.02.01_60/en_3003921022v010201p.pdf. [Accessed 22 February 2016].

[7] ETSI, "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 10: Supplementary services stage 1; Sub-part 21: Ambience Listening (AL)," September 2003. [Online]. Available: http://www.etsi.org/deliver/etsi_en/300300_300399/3003921021/01.02.01_60/en_3003921021v010201p.pdf. [Accessed 22 February 2016].

[8] ETSI, "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 10: Supplementary services stage 1; Sub-part 6: Call Authorized by Dispatcher (CAD)," August 2006. [Online]. Available: http://www.etsi.org/deliver/etsi_en/300300_300399/3003921006/01.04.01_60/en_3003921006v010401p.pdf. [Accessed 22 February 2016].

[9] ETSI, "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 10: Supplementary services stage 1; Sub-part 8: Area Selection (AS)," February 2004. [Online]. Available: http://www.etsi.org/deliver/etsi_en/300300_300399/3003921008/01.02.01_60/en_3003921008v010201p.pdf. [Accessed 22 February 2016].

[10] ETSI, "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 10: Supplementary services stage 1; Sub-part 14: Late Entry (LE)," September 2002. [Online]. Available: http://www.etsi.org/deliver/etsi_en/300300_300399/3003921014/01.02.01_60/en_3003921014v010201p.pdf. [Accessed 22 February 2016].

[11] ETSI, "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 1: General network design," January 2009. [Online]. Available: http://www.etsi.org/deliver/etsi_en/300300_300399/30039201/01.04.01_60/en_30039201v010401p.pdf. [Accessed 22 February 2016].

[12] ETSI, "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 2: Air Interface (AI)," August 2010. [Online]. Available: http://www.etsi.org/deliver/etsi_en/300300_300399/30039202/03.04.01_60/en_30039202v030401p.pdf. [Accessed 04 February 2016].

[13] TCCA, "TETRA Release 2," TCCA, [Online]. Available: http://www.tandcca.com/about/page/12029. [Accessed 28 March 2016].

[14] ETSI, "Terrestrial Trunked Radio (TETRA); Study of the suitability of the GSM Adaptive Multi-Rate (AMR) speech codec for use in TETRA," ETSI, 2001.

[15] ETSI, "Terrestrial Trunked Radio (TETRA); Evaluation of low rate (2,4 kbit/s) speech codec," ETSI .

[16] ETSI, "Terrestrial Trunked Radio (TETRA); Release 2; Designer's Guide; TETRA High-Speed Data (HSD); TETRA Enhanced Data Service (TEDS)," ETSI.

[17] C. Systems, "Mobile Communications II Chapter 4: Tetra," 30 October 2012. [Online]. Available: http://systems.ihp-microelectronics.com/uploads/downloads/MKII-WS2012-04_Tetra.pdf. [Accessed 04 February 2016].

[18] ETSI, "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D) and Direct Mode Operation (DMO); Part 5: Peripheral Equipment Interface (PEI)," July 2010. [Online]. Available: http://www.etsi.org/deliver/etsi_en/300300_300399/30039205/02.02.01_60/en_30039205v020201p.pdf. [Accessed 04 February 2016].

[19] ETSI, "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 3: Interworking at the Inter-System Interface (ISI); Sub-part 1: General design," December 2015. [Online]. Available: http://www.etsi.org/deliver/etsi_en/300300_300399/3003920301/01.04.01_60/en_3003920301v010401p.pdf. [Accessed 04 February 2016].

[20] ETSI, "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 4: Gateways basic operation; Sub-part 2: Integrated Services Digital Network (ISDN) gateway," aUGUST 2000. [Online]. Available: http://www.etsi.org/deliver/etsi_i_ets/300300_300399/3003920402/01_60/ets_3003920402e01p.pdf. [Accessed 04 February 2016].

[21] "TCCA Official Web Page," [Online]. Available: http://www.tandcca.com/.

[22] T. Consultancy, "What is TETRA," TETRA Consultancy, [Online]. Available: http://www.tetra-consultancy.com/index.php?/TETRA/what-is-tetra.html. [Accessed 04 February 2016].

[23] Wikipedia, "Trunked radio system," Wikipedia, 06 December 2015. [Online]. Available: https://en.wikipedia.org/wiki/Trunked_radio_system. [Accessed 23 February 2016].

[24] ETSI, "Terrestrial Trunked Radio (TETRA); Technical requirements for Direct Mode Operation (DMO); Part 1: General network design," December 2011. [Online]. Available: http://www.etsi.org/deliver/etsi_en/300300_300399/30039601/01.02.01_60/en_30039601v010201p.pdf. [Accessed 23 February 2016].

[25] F. Pasquali, "The power of TETRA - Direct Mode Operation," Selex Communications.

[26] ETSI, "Terrestrial Trunked Radio (TETRA); Technical requirements for Direct Mode Operation (DMO); Part 3: Mobile Station to Mobile Station (MS-MS) Air Interface (AI) protocol," December 2011. [Online]. Available: http://www.etsi.org/deliver/etsi_en/300300_300399/30039603/01.04.01_60/en_30039603v010401p.pdf. [Accessed 23 February 2016].

[27] P. Stavroulakis, Terestrial Trunked Radio - TETRA, A Global Security Tool, Berlin: Springer, 2007.

[28] ETSI, "Terrestrial Trunked Radio (TETRA); Technical requirements for Direct Mode Operation (DMO); Part 4: Type 1 repeater air interface," December 2011. [Online]. Available: http://www.etsi.org/deliver/etsi_en/300300_300399/30039604/01.04.01_60/en_30039604v010401p.pdf. [Accessed 23 February 2016].

[29] ETSI, "Terrestrial Trunked Radio (TETRA); Technical requirements for Direct Mode Operation (DMO); Part 5: Gateway air interface," December 2011. [Online]. Available: http://www.etsi.org/deliver/etsi_en/300300_300399/30039605/01.03.01_60/en_30039605v010301p.pdf. [Accessed 24 February 2016].

[30] B. Lovett, "TETRA - Direct Mode Operation".

[31] T. M. association, "TETRA security," TETRA MoU Association , Macclesfield, 2006.

[32] J. Dunlop, D. Girma and J. Irvine, "Operational Aspects of the TETRA Network," in *Digital Mobile Communications and the TETRA System*, John Wiley & Sons, 1999, pp. 383-413.

[33] R. Montañez, "TETRA Security," Motorola.

[34] ETSI, "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 7: Security," July 2012. [Online]. Available: http://www.etsi.org/deliver/etsi_en/300300_300399/30039207/03.03.01_60/en_30039207v030301p.pdf. [Accessed 01 March 2016].

[35] G. Roelofsen, "TETRA Security," *Information Security Technical Report,* vol. 5, no. 3, pp. 44-54, 2000.

[36] ETSI, "Terrestrial Trunked Radio (TETRA); Direct Mode Operation (DMO); Part 6: Security," September 2012. [Online]. Available: http://www.etsi.org/deliver/etsi_en/300300_300399/30039606/01.05.01_60/en_30039606v010501p.pdf. [Accessed 01 March 2016].

[37] ETSI, "Terrestrial Trunked Radio (TETRA); Security; Synchronization mechanism for end-to-end encryption," June 2003. [Online]. Available: http://www.etsi.org/deliver/etsi_en/302100_302199/302109/01.01.01_40/en_302109v010101o.pdf. [Accessed 01 March 2016].

[38] B. Murgatroyd, "End to end encryption in Public Safety TETRA networks," ICTU UK Home Office .

[39] Ramon Ferrús, Oriol Sallent, "Technologies in Use for PPDR Communication," in *Mobile Broadband Communications for Public Safety: The Road Ahead Through LTE Technology*, Wiley, 2015, pp. 22-23.

[40] TrueConf, "Bandwidth Requirements For Video Conferencing," TrueConf, [Online]. Available: http://trueconf.com/support/communication-channels.html. [Accessed 28 March 2016].

[41] Wikipedia, "Streaming media," Wikipedia, 27 March 2016. [Online]. Available: https://en.wikipedia.org/wiki/Streaming_media. [Accessed 28 March 2016].

[42] Wikipedia, "Mobile broadband," [Online]. Available: https://en.wikipedia.org/wiki/Mobile_broadband. [Accessed 20 June 2016].

[43] P. Stavroulakis, "Modern Security Requirements in Private Mobile Communications Systems," in *Terrestrial Trunked Radio - TETRA - A Global Security Tool*, Springer, 2007, pp. 5-42.

[44] Ramon Ferrús, Oriol Sallent, "LTE Networks for PPDR Communications," in *Mobile Broadband Communications for Public Safety: The Road Ahead Through LTE Technology*, Wiley, August, 2015, pp. 193-252.

[45] C. C. B. G. (CCBG), "Mission/Vision Statement," 23 April 2012. [Online]. Available: http://www.tandcca.com/Library/Documents/CCBGMissionv1_0.pdf. [Accessed 29 March 2016].

[46] TCCA, "Statement from the TCCA Board on LTE," October 2012. [Online]. Available: http://www.tandcca.com/Library/Documents/LTEBoardstatement.pdf. [Accessed 29 March 2016].

[47] A. Mason, "Report for the TETRA Association, Public safety mobile broadband and spectrum needs," Analysis Mason, March 2010.

[48] N. Boliari, "Indirect Returns and Use of NPV in Economic Viability Modeling of Critical Communications Networks," *IEEE Journals & Magazines*, vol. 54, no. 3, pp. 38-43, 2016.

[49] Ramon Ferrús, Oriol Sallent, "Future Mobile Broadband PPDR Communications Systems," in *Mobile Broadband Communications for Public Safety: The Road Ahead Through LTE Technology*, Wiley, August, 2015, pp. 81-125.

[50] C. C. B. G. (CCBG), "The Strategic Case for Mission Critical Mobile Broadband - A review of the future needs of the users of critical communications," TETRA and

Critical Communications Association (TCCA), Cambridgeshire, UK, December, 2013.

[51] C. C. B. G. (CCBG), "TETRA AND LTE WORKING TOGETHER," TETRA and Critical Communications Association (TCCA), Cambridgeshire, UK, June, 2014.

[52] F. R. N. Authority, "FirstNet," First Responder Network Authority, [Online]. Available: http://www.firstnet.gov/. [Accessed 29 March 2016].

[53] "Airwave," [Online]. Available: https://www.airwavesolutions.co.uk/home/. [Accessed 30 March 2016].

[54] Home Office, "Emergency services network," UK Government, [Online]. Available: https://www.gov.uk/government/publications/the-emergency-services-mobile-communications-programme/emergency-services-network. [Accessed 30 March 2016].

[55] "ASTRID," ASTRID, [Online]. Available: http://www.astrid.be/Templates/Home.aspx?id=32&LangType=1033. [Accessed 30 March 2016].

[56] "Blu Light Mobile," Blu Light Mobile, [Online]. Available: http://bluelightmobile.be/en. [Accessed 30 March 2016].

[57] O. S. Ramon Ferrús, "Current Initiatives," in *Mobile Broadband Communications for Public Safety: The Road Ahead Through LTE Technology*, Wiley, August, 2015, pp. 109-121.

[58] 3GPP, "LTE," 3GPP, [Online]. Available: http://www.3gpp.org/technologies/keywords-acronyms/98-lte. [Accessed 25 April 2016].

[59] P. Kidner, "LTE is the Future Single Global Standard for Critical Communications".

[60] 3GPP, "Public Safety," 3GPP, [Online]. Available: http://www.3gpp.org/news-events/3gpp-news/1455-Public-Safety. [Accessed 14 March 2016].

[61] "Critical Communications Broadband Group Page," [Online]. Available: http://www.tandcca.com/assoc/page/18100.

[62] 3GPP, "LTE for Public Safety (authority-to-authority) communications_20140630," June 2014. [Online]. Available: http://www.3gpp.org/ftp/Information/WORK_PLAN/Description_Releases/. [Accessed 10 March 2016].

[63] Ramon Ferrús, Oriol Sallent, "LTE Technology for PPDR Communications," in *Mobile Broadband Communications for Public Safety: The Road Ahead Through LTE Technology*, Wiley, August, 2015, pp. 125-192.

[64] 3GPP, "Releases," 3GPP, [Online]. Available: http://www.3gpp.org/specifications/67-releases. [Accessed 02 June 2016].

[65] M. Mustapha, " Developing specifications for LTE," 11 March 2014. [Online]. Available: ftp://www.3gpp.org/Information/presentations/presentations_2014/Critical_comms_Eur_3gpp.pdf. [Accessed 20 April 2016].

[66] 3GPP, "Specifications Groups," 3GPP, [Online]. Available: http://www.3gpp.org/specifications-groups. [Accessed 10 March 2016].

[67] Ramon Ferrús, Oriol Sallent, "Device-to-Device Communications," in *Mobile Broadband Communications for Public Safety: The Road Ahead Through LTE Technology*, Wiley, 2015, pp. 164-174.

[68] 3GPP SP-110638, "WID on Proposal for a study on Proximity-based Services," 3GPP TSG SA Plenary Meeting #53, Fukuoka, Japan, 19 – 21 September 2011.

[69] 3. SP-140574, "Revised Rel-12 WID for Proximity-based Services," 3GPP TSG SA Meeting #65, Edinburgh, Scotland, 15-17 September, 2014.

[70] 3. RP-122009, "Study on LTE Device to Device Proximity Services," 3GPP TSG RAN Meeting #58.

[71] 3GPP SP-140386, "Editorial update of SA1 ProSe phasae 2 WID," 3GPP TSG SA Meeting #64, Sophia Atipolis, France, 16-18 June, 2014.

[72] 3GPP SP-140629, "New Study to create a dedicated SA3 TR on Security for Proximity-based Services," 3GPP TSG SA Meeting #65, Edinburgh, Scotland, 15-17 September, 2014.

[73] T. S. WG1, "WID on Proposal for a study on Proximity-based Services," 3GPP, Fukuoka, 2011.

[74] C. Cox, "Architecture of LTE," in *An introduction to LTE; LTE, LTE-Advanced, SAE and 4G Mobile Communications*, Wiley, 2012, pp. 21-28.

[75] 3GPP TS 23.303 v13.2.0, "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Proximity-based services (ProSe); Stage 2 (Release 13)," 3GPP, December, 2015.

[76] CRITICAL COMMUNICATIONS BROADBAND GROUP, "Mission Critical Mobile Broadband: Practical standardisation & roadmap considerations," TCCA, 2013.

[77] 3GPP TS 22.468 V13.0.0, "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Group Communication System Enablers for LTE (GCSE_LTE (Release 13)," 3GPP, December, 2014.

[78] Ramon Ferrús, Oriol Sallent, "Group Communication and PTT," in *Mobile Broadband Communications for Public Safety: The Road Ahead Through LTE Technology*, Wiley , 2015, pp. 152-164.

[79] 3GPP SP-140433, "Updated WID: GCSE_LTE WID change of Rapporteur," 3GPP TSG SA Meeting #65, Edinburgh, Scotland, UK, 15 - 17 September 2014.

[80] 3GPP RP-131382, "New SI proposal: Group Communication for LTE," 3GPP TSG RAN meeting #61, Porto, Portugal, September 3 - 6, 2013.

[81] 3GPP SP-140228, "New WID on Service Requirements Maintenance for Group Communication System Enablers for LTE (SRM_GCSE_LTE) (from S1-141571)," 3GPP TSG SA Meeting #64, Sophia-Antipolis, France, 16 – 18 June 2014.

[82] 3GPP TS 23.468 V13.3.0, "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Group Communication System Enablers for LTE (GCSE_LTE); Stage 2 (Release 13)," 3GPP, December 2015.

[83] 3GPP TS 23.179 V13.0.0 , "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Functional architecture and information flows to support mission critical communication services; Stage 2 (Release 13)," 3GPP, December, 2015.

[84] 3GPP TR 33.879 V13.0.0 , "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Study on security enhancements for Mission Critical Push To Talk (MCPTT) over LTE (Release 13)," 3GPP, March, 2016.

[85] 3. T. S. M. #62, "Updates to the WID on Feasibility Study on Study on Isolated E-UTRAN Operation for Public Safety (FS_IOPS)," Busan, Korea, 09 – 11 December, 2013.

[86] 3GPP TR 22.897 V13.0.0, "3rd Generation Partnership Project;Technical Specification Group Services and System Aspects; Study on Isolated Evolved Universal Terrestrial Radio Access Network (E-UTRAN) Operation for Public Safety (Release 13)," 3GPP, June, 2014.

[87] 3GPP TS 22.346 V13.0.0 , "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Isolated Evolved Universal Terrestrial Radio Access Network (E-UTRAN) operation for public safety; Stage 1 (Release 13)," 3GPP, September, 2014.

[88] 3GPP TS 23.401 V13.6.1, "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access (Release 13)," 3GPP, March, 2016.

[89] 3GPP TS 31.102 V13.3.0 , "3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Characteristics of the," 3GPP, March, 2016.

[90] Samsung, "Samsung Takes the Lead to Help Emergency Services with Public Safety - LTE," 01 June 2015. [Online]. Available: http://www.samsung.com/global/business/networks/insights/news/samsung-takes-the-lead-to-help-emergency-services-with-public-safety-lte. [Accessed 20 April 2016].

[91] The Korea Times, "SKT to provide public safety network technology overseas," 18 February 2016. [Online]. Available: http://www.koreatimes.co.kr/www/news/tech/2016/02/133_198376.html. [Accessed 20 April 2016].

[92] T. Nakamura, "LTE Release 12 and Beyond," June 2013. [Online]. Available: http://www.3gpp.org/IMG/pdf/lte_africa_2013_3gpp_lte_release_12.pdf. [Accessed 20 April 2016].

[93] SK Telecom, "SK Telecom Launches World's First LTE-Advanced Network," SK Telecom, 26 June 2013. [Online]. Available: http://www.sktelecom.com/en/press/detail.do?idx=1036. [Accessed 20 April 2016].

[94] 3GPP, "SA#71 - Release 13 frozen in Gothenburg," 15 March 2016. [Online]. Available: http://www.3gpp.org/news-events/3gpp-news/1769-rel-13_tsg71. [Accessed 22 April 2016].

[95] 3GPP, "3GPP work programme," [Online]. Available: http://www.3gpp.org/DynaReport/GanttChart-Level-2.htm. [Accessed 22 April 2016].

[96] Radio Resource Mission Critical Communications, "Public-Safety LTE Deployments Accelerate Slowly," 01 April 2014. [Online]. Available: http://www.rrmediagroup.com/Features/FeaturesDetails/FID/440. [Accessed 07 June 2016].

[97] 3GPP TS 33.303 V13.2.0 , "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Proximity-based Services (ProSe); Security aspects (Release 13)," 3GPP, December, 2015.

[98] 3GPP TS 33.246 V13.1.0 , "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Security of Multimedia Broadcast/Multicast Service (MBMS) (Release 13)," 3GPP, December, 2015.

[99] 3GPP TS 33.179 V1.0.0 , "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects Security of Mission Critical Push-To-Talk (MCPTT); (Release 13)," 3GPP, December, 2015.

[100] 3GPP TS 33.401 V13.2.0 , "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3GPP System Architecture Evolution (SAE); Security architecture (Release 13)," 3GPP, December, 2015.

[101] Dan Forsberg, Gunther Horn, Wolf-Dietrich Moeller, Valtteri Niemi, LTE SECURITY, Second Edition, Wiley, 2013.

[102] W. Mao, "Modern Cryptography: Theory and Practice,," Prentice Hall PTR, New Jersey, USA, 2004.

[103] C. A. Boyd, *Lecture 12: Key Establishment and User Authentication,* Trondheim, 2015.

[104] C. A. Boyd, *Lecture 9: Other Public Key Cryptosystems,* Trondheim, 2015.

[105] Wikipedia, "Digital signature," 2016 March 23. [Online]. Available: https://en.wikipedia.org/wiki/Digital_signature. [Accessed 2016 March 28].

[106] C. A. Boyd, *Lecture 11: Digital Signatures and Certificates,* Trondheim, 2015.

[107] 3GPP TS 22.179 V13.3.0 , "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Mission Critical Push To Talk (MCPTT) over LTE; Stage 1 (Release 13)," 3GPP, December, 2015.

[108] RFC 7170, "Tunnel Extensible Authentication Protocol (TEAP) Version 1," Internet Engineering Task Force (IETF), May, 2014.

[109] RFC 3546, "Transport Layer Security (TLS) Extensions," Network Working Group, June, 2003.

[110] RFC 3748, "Extensible Authentication Protocol (EAP)," Network Working Group, June, 2004.

[111] draft-ietf-tls-tls13-12, "The Transport Layer Security (TLS) Protocol Version 1.3," Network Working Group , March, 2016.

[112] T. Taubert, "MORE PRIVACY, LESS LATENCY - Improved Handshakes in TLS version 1.3," [Online]. Available: https://timtaubert.de/blog/2015/11/more-privacy-less-latency-improved-handshakes-in-tls-13/. [Accessed 07 April 2016].

[113] "Certificate based authentication vs Username and Password authentication," [Online]. Available: http://security.stackexchange.com/questions/3605/certificate-based-authentication-vs-username-and-password-authentication.

[114] RFC 7029, "Extensible Authentication Protocol (EAP) Mutual Cryptographic Binding," Internet Engineering Task Force (IETF), October, 2013.

[115] E. Rescorla, "TLS 1.3," [Online]. Available: http://web.stanford.edu/class/ee380/Abstracts/151118-slides.pdf.

[116] Benjamin Dowling, Marc Fischlin, Felix Günther, Douglas Stebila, "A Cryptographic Analysis of the TLS 1.3 Handshake Protocol Candidates," in *ACM Conference on Computer and Communications Security (CCS 2015)*, February, 2016 .

[117] 3GPP TR 33.879 V13.0.0 , "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Study on security enhancements for Mission Critical Push To Talk (MCPTT) over LTE (Release 13)," March, 2016.

[118] RFC 3261, "SIP: Session Initiation Protocol," Network Working Group , June, 2002.

[119] A. Martelli, "What is token based authentication?," [Online]. Available: http://stackoverflow.com/questions/1592534/what-is-token-based-authentication. [Accessed 07 April 2016].

[120] RFC 2617, "HTTP Authentication: Basic and Digest Access Authentication," Network Working Group, June 1999.

[121] Ramon Ferrús, Oriol Sallent, "Radio Spectrum for PPDR Communications," in *Mobile Broadband Communications for Public Safety: The Road Ahead Through LTE Technology*, Wiley, August, 2015, pp. 257-311.

[122] Simon Forge, Robert Horvitz and Colin Blackman, "Study on use of commercial mobile networks and equipment for "mission-critical" high-speed broadband communications in specific sectors," December, 2014.

[123] Federal Communications Commission (FCC), "A BROADBAND NETWORK COST MODEL: A BASIS FOR PUBLIC FUNDING ESSENTIAL TO BRINGING NATIONWIDE INTEROPERABLE COMMUNICATIONS TO AMERICA’S FIRST RESPONDERS," Federal Communications Commission (FCC), May, 2010.

[124] F. C. Commission, "Connecting America: The National Broadband Plan," [Online]. Available: https://transition.fcc.gov/national-broadband-plan/national-broadband-plan.pdf.

[125] FirstNet, "FirstNet Board Meeting," 16 March 2016. [Online]. Available: http://www.firstnet.gov/sites/default/files/March%20Board%20Meeting%20Slides.pdf. [Accessed 2016 April 14].

[126] Direktoratet for nødkommunikasjon (DNK), "Om Nødnett," DNK, [Online]. Available: http://www.dinkom.no/Utbyggingen/Om-Nodnett1/. [Accessed 14 April 2016].

[127] T. a. C. C. A. (TCCA), "A review of options for delivering Mission," December 2013. [Online]. Available: http://www.tandcca.com/Library/Documents/Broadband/MCMBB%20Delivery%20Options%20v1.0.pdf. [Accessed 21 March 2016].

[128] G. Shipley, "Preparing for the Emergency Services Network," 05 November 2015. [Online]. Available: http://bluelightinnovation.co.uk/wp-content/uploads/2015/11/11.30-Gordon-Shipley.pdf. [Accessed 14 April 2016].

[129] S. Watson, "Emergency Services Mobile," 20 April 2016. [Online]. Available: http://www.dinkom.no/PageFiles/14686/01_Steve_Whatson.pdf. [Accessed 06 June 2016].

[130] Direktoratet for nødkommunikasjon (DNK), "Welcome to the Nødnett Days 2016," Direktoratet for nødkommunikasjon (DNK), 22 March 2016. [Online]. Available: http://www.dinkom.no/DNK/Nodnettdagene/English/. [Accessed 23 April 2016].

[131] D. Jackson, "UK seeks to replace TETRA with LTE as early as 2016," 06 October 2013. [Online]. Available: http://www.pscr.gov/downloads/press/broadband-uk_seeks_to_replace_tetra_with_lte_as_early_as_2016_062013-urgent_communications.pdf. [Accessed 23 April 2016].

[132] Matti J. Peltola, Heikki Hammainen, "Economic Feasibility of Mobile Broadband Network for Public Safety and Security," in *IEEE Conference Publications*, 2015.

[133] Wikipedia, "Enhanced Data Rates for GSM Evolution," [Online]. Available: https://en.wikipedia.org/wiki/Enhanced_Data_Rates_for_GSM_Evolution. [Accessed 22 May 2016].

[134] DNK, "Kostnader for utbygging," DNK, 03 May 2016. [Online]. Available: http://www.dinkom.no/Utbyggingen/Om-Nodnett1/Kostnader-for-utbygging/. [Accessed 21 May 2016].

[135] T. H. Lyngstøl, "Nødnettdagene 2016," 19 April 2016. [Online]. Available: http://www.dinkom.no/PageFiles/14686/02_Tor_Helge_Lyngst%C3%B8l.pdf. [Accessed 16 May 2016].

[136] K. Baltzersen, "Robuste datatjenester," 20 April 2016. [Online]. Available: http://www.dinkom.no/PageFiles/14686/01_Knut_Baltzsersen.pdf. [Accessed 16 May 2016].

[137] C. C. B. GROUP, "Mission Critical Mobile Broadband: Practical standardisation & roadmap considerations," February 2013. [Online]. Available: http://www.tandcca.com/Library/Documents/CCBGMissionCriticalMobileBroadbandwhitepaper2013.pdf. [Accessed 16 May 2016].

[138] D. f. E. C. (DNK), "Frequencies for the next generation emergency communication systems," 13 January 2016. [Online]. Available: http://www.dinkom.no/en/About-The-Directorate/News-Archive/Frequencies-for-the-next-generation-emergency-communication-systems/. [Accessed 27 April 2016].

[139] Jarmo Vinkvist, Tero Pesonen and Matti Peltola, "Finland’s 5 Steps to Critical Broadband," 2014. [Online]. Available: http://www.tandcca.com/Library/Documents/Broadband/RRIBroadband(Q4-14).pdf. [Accessed 14 April 2016].

[140] Ilkka Korkiamäki, Jarmo Vinkvist, "Critical Communications TETRA and Broadband Roadmap for 2030," CCW 2015, Barcelona, Spain, May, 2015.

[141] Juyeop Kim, Sang Won Choi, Won-Yong Shin, Yong-Soo Song, and Yong-Kyu Kim, "Group Communication over LTE: A Radio Access Perspective," *IEEE Journals & Magazines,* vol. 54, no. 4, pp. 16-23, 2016.

[142] ETSI, "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 3: Interworking at the Inter-System Interface (ISI); Sub-part 7: Speech Format Implementation for Packet Mode Transmission," ETSI, 2013.

[143] Motorola Solutions, "TETRA and LTE working together," [Online]. Available: https://www.motorolasolutions.com/content/dam/msi/docs/business/product_lines/dimetra_tetra/infrastructure/tetra_base_stations/mst4l/emea/xu-en/j1645_mts4l_specsheet.pdf.

[144] ROHILL, "LTE for Critical Communications," ROHILL, June 2015. [Online]. Available: http://www.rohill.nl/images/pdf-downloads/whitepapers/LTE-for-Critical-Communications-version-1.1.pdf. [Accessed May 2016].

[145] DNK, "Grundig prosess for å få til god dekning," DNK, 17 October 2013. [Online]. Available: http://www.dinkom.no/Utbyggingen/Utbygging-av-Nodnett/Grundig-prosess-for-a-fa-til-god-dekning/. [Accessed 27 May 2016].

[146] Romano Fantacci, Francesco Gei, Dania Marabissi, and Luigia Micciullo, "Public Safety Networks Evolution toward Broadband: Sharing Infrastructures and Spectrum with Commercial Systems," *IEEE Journals & Magazines,* vol. 54, no. 4, pp. 24-30, 2016.

[147] TASSTA, "TASSTA BRIDGE NETWORK INTERCONNECTION," [Online]. Available: https://criticalcommunicationsworld.com/files/49463-TASSTA_Bridge.pdf.

[148] Federal Ministry of the Interior, "On the Future Architecture of Mission Critical Mobile Broadband PPDR Networks," Berlin, Germany, November, 2013.

[149] Radio Resource Mission Critical Communications, "Vendors Say Public-Safety Users Need Two Devices in Data Era," 08 January 2013. [Online]. Available: http://www.mccmag.com/Features/FeaturesDetails/FID/357. [Accessed 18 May 2016].

[150] M. Solutions, "WAVE," Motorola Solutions, [Online]. Available: http://www.motorolasolutions.com/en_us/products/voice-applications/wave-work-group-communications.html#applications.

[151] Selex ES - A Finmeccanica Company, "PUMA T4–TLE (DUAL MODE TETRA – LTE ENHANCED) THE NEW GENERATION OF PROFESSIONAL HANDHELD," Selex ES S.p.A, 2015.

[152] Sam Fenwick, "The ICCAs in review: Critical comms, shining stars," 15 March 2016. [Online]. Available: http://www.tetratoday.com/news/the-iccas-in-review-critical-comms-shining-stars/. [Accessed 18 May 2016].

[153] ETSI, "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 15: TETRA frequency bands, duplex spacings and channel numbering," ETSI, 2002.

[154] E. C. O. (ECO), "ECO Frequency Information System," European Communications Office (ECO), [Online]. Available: http://www.efis.dk/. [Accessed 27 May 2016].

[155] N. C. A. (NKOM), "Search the Norwegian frequency plan," 26 June 2013. [Online]. Available: http://eng.nkom.no/technical/frequency-management/strategy-and-plan/search-the-norwegian-frequency-plan. [Accessed 23 May 2016].

[156] "Access to the 700-MHz frequency band is required for next generation Mission Critical Radio Communication systems," [Online]. Available: http://www.dinkom.no/Global/Dokumenter/Nordic%20white%20paper%20on%20access%20to%20the%20700-MHz%20frequency%20band.pdf.

[157] "Norwegian Communications Authority (NKOM)," [Online]. Available: http://eng.nkom.no/.

[158] N. C. A. (NKOM), "Spectrum strategy for the Norwegian Communications Authority 2015-2016," [Online]. Available: http://eng.nkom.no/topical-issues/news/_attachment/16322?_ts=14b2fa131af. [Accessed 23 May 2016].

[159] International Telecommunication Union ITU, "Spectrum Sharing," [Online]. Available: http://www.ictregulationtoolkit.org/5.4. [Accessed 21 June 2016].

[160] T. -. TETRA, "Direct Mode Operation," TCCA, [Online]. Available: http://www.tandcca.com/about/page/12026. [Accessed 29 January 2016].

[161] 3GPP, "Service and System Aspects," 3GPP, 2016. [Online]. Available: http://www.3gpp.org/specifications-groups/25-sa. [Accessed 10 March 2016].

[162] 3GPP, "SA1 - Services," 3GPP, 2016. [Online]. Available: http://www.3gpp.org/Specifications-groups/sa-plenary/51-sa1-services. [Accessed 10 March 2016].

[163] 3GPP, "SA2 - Architecture," 3GPP, 2016. [Online]. Available: http://www.3gpp.org/Specifications-groups/sa-plenary/53-sa2-architecture. [Accessed 10 March 2016].

[164] 3GPP, "SA3 - Security," 3GPP, 2016. [Online]. Available: http://www.3gpp.org/Specifications-groups/sa-plenary/54-sa3-security. [Accessed 10 March 2016].

[165] N. Networks, "LTE networks for public safety services," NOKIA Networks.

[166] 3GPP, "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Feasibility study for Proximity Services (ProSe) (Release 12)," 3GPP, 2013.

[167] 3GPP, "3rd Generation Partnership Project; Technical Specification Group Radio Access Network; Study on LTE Device to Device Proximity Services; Radio Aspects (Release 12)," 3GPP, 2014.

[168] 3GPP, "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Study on Security issues to support Proximity Services (ProSe) (Release 13)," 3GPP, 2015.

[169] S. WG2, "Update WID: GCSE_LTE WID change of Rapporteur," 3GPP TSG SA Meeting #65, Edinburgh, Scotland, 2014.

[170] 3GPP TR 33.833 V1.6.0, "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Study on Security issues to support Proximity Services (ProSe) (Release 13)," 3GPP, November, 2015.

[171] 3GPP TR 33.888 V12.1.0 , "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Study on security issues to support Group Communication System Enablers (GCSE) for LTE (Release 12)," 3GPP, September, 2014.

[172] Ramon Ferrús, Oriol Sallent, "4.2.4 Security," in *Mobile Broadband Communications for Public Safety: The Road Ahead Through LTE Technology*, Wiley, 2015, pp. 143-149.

[173] Dan Forsberg, Gunther Horn, Wolf-Dietrich Moeller, Valtteri Niemi, "EPS Security Architecture," in *LTE Security*, Wiley, 2013, pp. 109-133.

[174] Dan Forsberg, Gunther Horn, Wolf-Dietrich Moeller, Valtteri Niemi, "EPS Authentication and Key Agreement," in *LTE Security*, Wiley, 2013, pp. 109-133.

[175] 3GPP TS 22.246 V13.0.0 , "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Multimedia Broadcast/Multicast Service (MBMS) user services; Stage 1 (Release 13)," 3GPP, December, 2015.

[176] J. Franks, P. Hallam-Baker, J. Hostetler, S. Lawrence, P. Leach, A. Luotonen,L. Stewart, "HTTP Authentication: Basic and Digest Access Authentication," Network Working Group, June 1999. [Online]. Available: https://www.ietf.org/rfc/rfc2617.txt. [Accessed 19 March 2016].

[177] 3GPP TS 23.246 V13.3.0, "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Multimedia Broadcast/Multicast Service (MBMS); Architecture and functional description (Release 13)," 3GPP, December, 2015.

[178] Muhammad Alam, Du Yang, Jonathan Rodriguez, and Raed A. Abd-Alhameed, "Secure Device-to-Device Communication in LTE-A," *IEEE Journals & Magazines,* vol. 52, no. 4, pp. 66-73, 2014.

[179] Wenlong Shen, Weisheng Hong, Xianghui Cao, Bo Yin, Devu Manikantan Shila and Yu Cheng, "Secure Key Establishment for Device-to-Device Communications," in *IEEE Conference Publications,* 2014.

[180] Christian Gehrmann, Chris J. Mitchell, Kaisa Nyberg, *Manual authentication for wireless devices,* 2004.

[181] F. R. N. Authority, "The Network," FirstNet, [Online]. Available: http://www.firstnet.gov/content/lte-technology#Spectrum Relocation Grant Program. [Accessed 30 March 2016].

[182] 3GPP TS 33.203 V13.1.0 , "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G security; Access security for IP-based services (Release 13)," 3GPP, December, 2015.

[183] 3GPP TS 23.228 V13.5.0 , "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; IP Multimedia Subsystem (IMS); Stage 2 (Release 13)," 3GPP4, March, 2016.

[184] Wikipedia, "OpenID Connect," 09 March 2016. [Online]. Available: https://en.wikipedia.org/wiki/OpenID_Connect. [Accessed 07 April 2016].

[185] Wikipedia, "OAuth," 15 March 2016. [Online]. Available: https://en.wikipedia.org/wiki/OAuth. [Accessed 07 April 2016].

[186] ASTRID, "Press releases," ASTRID, 26 March 2016. [Online]. Available: http://www.astrid.be/templates/content.aspx?id=168. [Accessed 14 April 2016].

[187] M. D. Buyser, "Une journée noire," 07 April 2016. [Online]. Available: http://www.astriddirect.be/fr/nieuws/une-journ%C3%A9e-noire. [Accessed 14 April 2016].

[188] Samsung, "Samsung to Deploy the World’s First 3GPP Standard Based Public Safety LTE Solution in Korea," 11 February 2016. [Online]. Available: http://news.samsung.com/global/samsung-to-deploy-the-worlds-first-3gpp-standard-based-public-safety-lte-solution-in-korea. [Accessed 20 April 2016].

[189] "ETSI Official Web Page," [Online]. Available: http://www.etsi.org/.

[190] R. R. M. C. Communications, "South Korea Plans for Dedicated LTE Public-Safety Network by 2017," 07 October 2014. [Online]. Available: http://www.rrmediagroup.com/Features/FeaturesDetails/FID/482. [Accessed 27 April 2016].

[191] T. M. Association, "TETRA Technology Advantages & Benefits," Macclesfield, England, January, 2006.

[192] Murat Yuksel, Ismail Guvenc, Walid Saad, and Naim Kapucu, "Pervasive Spectrum Sharing for Public Safety Communications," *IEEE Journals & Magazines,* vol. 54, no. 3, pp. 22-29, 2016.

[193] Munawwar M. Sohul, Miao Yao, Xiaofu Ma, Eyosias Y. Imana, Vuk Marojevic, and Jeffrey H. Reed, "Next Generation Public Safety Networks: A Spectrum Sharing Approach," *IEEE Journals & Magazines,* vol. 54, no. 3, pp. 30-36, 2016.

[194] ETSI, "Terrestrial Trunked Radio (TETRA); Direct Mode Operation (DMO); Part 6: Security," ETSI, September, 2012.

[195] 3GPP TR 23.779 V13.0.0, "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Study on application architecture to support Mission Critical Push To Talk over LTE (MCPTT) services (Release 13)," 3GPP, September, 2015.

[196] 3GPP TS 33.310 V13.1.0, "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Network Domain Security (NDS); Authentication Framework (AF) (Release 13)," 3GPP, March, 2016.

Appendix A (LTE Architecture)

Figure A. 1 reviews the high-level architecture of the evolved packet system (EPS). There are three main components, namely the user equipment (UE), the evolved UMTS terrestrial radio access network (E-UTRAN) and the evolved packet core (EPC) [74].

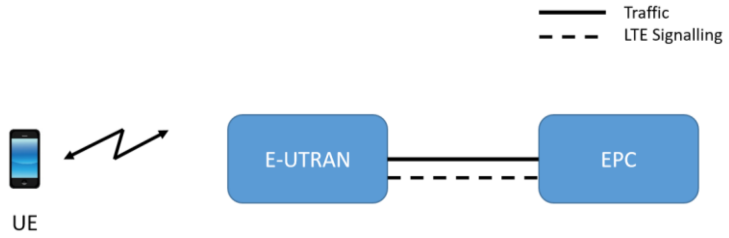

Figure A. 1: High level architecture of LTE

The UE, E-UTRAN and EPC each have their own internal architectures and we will now show internal architecture of EPC while E-UTRAN will only be briefly explained.

The E-UTRAN handles the radio communications between the mobile and the evolved packet core and just has one component, the evolved Node B (eNB). Each eNB is a base station that controls the mobile UEs in one or more cells.

Evolved Packet Core (EPC)

Figure A. 2 shows the main components of the evolved packet core (EPC).

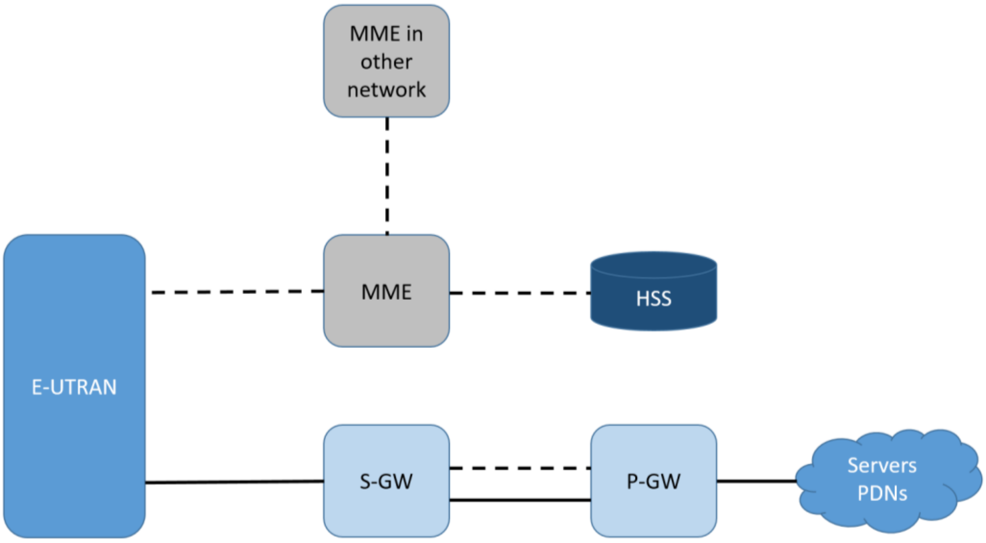

Figure A. 2: Main components of the evolved packet core (EPC)

The home subscriber server (**HSS**), is a central database that contains information about all the network operator’s subscribers.

The packet data network (PDN) gateway (**P-GW**), is the EPC’s point of contact with the outside world.

The serving gateway (**S-GW**) acts as a router, and forwards data between the base station (eNB) and the PDN gateway.

The mobility management entity (**MME**) controls the high-level operation of the mobile UEs, by sending them signalling messages about issues such as security and the management of data streams that are unrelated to radio communications.

The EPC has some other hardware components that were not shown in Figure 2.4. The most important component is the policy and charging rules function (**PCRF**). This authorizes the policy and charging treatment that a service data flow will receive, either by referring to a predefined PCC (Policy and charging control) rule, or by composing a dynamic PCC rule.

Appendix B (MCPTT Functional entities description)

NOTE: Functional entity does not necessarily imply a physical entity.

Application plane

Entities within the application plane provide application control, media control and distribution functions.

Common services core:

Identity management client - This functional entity acts as the application user agent for MC ID (Mission Critical Identity) transactions. It interacts with the identity management server.

Identity management server - The identity management server is a functional entity that is capable of authenticating the MC ID. It contains the knowledge and means to do authentication by verifying the credentials supplied by the user.

The identity management server functional entity may reside in the same domain as the user's MCPTT server.

MCPTT application service:

MCPTT client - The MCPTT client functional entity acts as the user agent for all MCPTT application transactions. MCPTT client is not physical entity but it is located in MCPTT UE, which is its physical representative. In fact, term MCPTT UE will be used throughout our analysis.

MCPTT server - The MCPTT server functional entity provides centralized support for MCPTT services.

The MCPTT server functional entity represents a specific instantiation of the GCS AS described in 3GPP TS 23.468 to control multicast and unicast operations for group communications.

Signalling control plane

SIP entities:

SIP core - The SIP core contains a number of sub-entities responsible for registration, service selection and routing in the signalling control plane.