Security **A**nd Interoperabi**L**ity in Next Generation PPDR Comm**U**nication Infrastructure**S**

Project Number: 313296

Deliverable 6.2

PMR-over-LTE services definition - Intermediate

Scope	Scheduled deliverable
Lead Beneficiary	Rohill
Dissemination level	Public
Document creation date	26/May/2014
Document release date	02/Feb/2015
Contractual Date of Delivery	31/Dec/2014
Version	1.1
Status	Final

***Abstract**: Deliverable 6.2 provides a detailed definition of applicable PMR services that can be delivered over LTE. These PMR services consist of existing PMR functionality, new features found in smartphone apps that support group communications, as well as new data, photo and video capabilities offered by broadband communications. Also addressed are capabilities for interworking with existing PMR systems, including TETRA and TETRAPOL. The definition of PMR services is derived from analysis of the SALUS use cases, analysis of legacy PMR functionality, and analysis of current-state-of-the-art solutions.*

AUTHORS

Name	Organisation	Email
Bert Bouwers	ROH	bert.bouwers@rohill.nl
Jérôme Brouet	ALU-I	jerome.brouet@alcatel-lucent.com

QUALITY ASSURANCE TEAM

Name	Organisation	Email
Hugo Marques	IT	hugo.marques@av.it.pt
David Jelenc	UL	david.jelenc@fri.uni-lj.si
Jernei Kos	UL	jernej.kos@fri.uni-lj.si

EXECUTIVE SUMMARY

The objective of this document is to present the interim version of the PMR-over-LTE services definition. This definition follows the requirements as captured and described within WP2 and WP3.

Following the introductory section, Section 2 provides an overview of functional requirements that are based on the SALUS use cases as described in WP2. In addition, an extensive analysis is made of legacy basic conventional Private Mobile Radio (PMR) and advanced TETRA and TETRAPOL functionality, whereby both generic and unique functionalities, as well as interworking aspects, are being considered. Finally, the early standardisation effort for Mission Critical Push To Talk is analysed as input for the functional requirements.

The non-functional requirements are specified in Section 3. These include performance, scalability, availability (reliability) and security requirements.

Section 4 describes the functionality for the SALUS PMR-over-LTE ecosystem. The D6.2 interim phase of the PMR-over-LTE services definition covers Basic PMR services, PMR supplementary services, Telephony supplementary services and Security services.

Section 5 summarises the interoperability and interworking aspects, required for gradual migration of legacy PMR to PMR-over-LTE solutions. This includes IP integration aspects, as well as interworking aspects with legacy PMR networks that include TETRA and TETRAPOL.

Section 6 provides the concluding remarks. The provided solutions in the D6.2 deliverable (interim) focuses on standard PMR services and interoperability aspects with legacy PMR networks, whereas the D6.5 deliverable (final) will target the additional services that are enabled by mobile broadband, as well as features and capabilities that are offered in state-of-the-art proprietary and standards-based solutions.

TABLE OF CONTENTS

TABLE OF TABLES

1 Introduction

This document provides a detailed specification of Private Mobile Radio (PMR) services that will be delivered over LTE. The selection of applicable PMR services are derived from the following requirements:

- Common requirements for services based on specific use cases that are part of the scenarios defined in WP2 and further analysed in WP3;
- Detailed analysis of functionality provided by legacy PMR systems, and how relevant these are for the definition of PMR services over LTE networks;
- Interoperability aspects that are critical to enhance and expand the services offered by legacy PMR networks.

In addition to the functional requirements, also the non-functional requirements are described in this document that must be taken into account for the design of the PMR-over-LTE system architecture and protocol specifications.

Finally, a detailed functional specification is provided for each of the PMR-over-LTE services. The services are grouped together within the categories: Basic services, PMR supplementary services, Telephony supplementary services and Security services.

2 FUNCTIONAL REQUIREMENTS

2.1 Inputs from WP3

The following table provides an overview of functional requirements with a reference to the capabilities as listed for each of the scenarios described in chapter 4 within D3.1 [2].

The column "Reference" and "Capability" are copied from [2] whereas the content within column "Functionality" refers to the functionalities described in chapter 4 of this document.

Table 1 - Reference to SALUS capabilities

Reference	Capability	Functionality
SC1-C1	Provide interworking between PPDR communication networks based on different radio access technologies	-
SC1-C1.1	Enable communications between PPDR users in different access networks (e.g. TETRA and LTE) for voice applications (e.g. group calls, one to one calls) and advanced features (late entry, dynamic reassignment, prioritisation...)	Interworking aspects Group call Individual call Late entry Dynamic regrouping Priority call
SC1-C1.2	Enable communications between PPDR users in different access networks (e.g. TETRA and LTE) for low data rates applications (e.g. short messages, status messages, location information, pictures...)	Interoperability aspects Text messaging Binary messaging Location reporting Picture transfer
SC1-C1.3	Enable emergency communications between PDDR users in different access networks mixing voice and if possible video information from the emergency device	Interworking aspects
SC1-C1.4	Enable communications for a PPDR user across different access networks (agency's PPDR network, other agency's PPDR network and commercial network).	Interoperability aspects
SC1-C2	Provision of a permanent PPDR system so that it can cope with extra capacity demand in case of major crisis in multiple locations at the same time for the duration to the event (multiple days).	Management and configuration aspects
SC1-C2.1	Quickly and temporarily increase the capacity of the fixed system	N/A - System solution aspect
SC1-C3	Sense the area to improve situational awareness in the command and control centre (CCC) and in the field	Video streaming Picture transfer
SC1-C3.1	Retrieve fixed CCTV footage in the CCC	N/A - Dedicated application
SC1-C3.1.1	Secured access to CCTV flows from the CCTV operator	N/A - Dedicated application

SC1-C3.2	Use of aerial sensing systems (helicopters, fixed wings) to retrieve live video information	N/A - System solution aspect
SC1-C3.3	Use of mobile devices to stream live video from the field to the control room	Video streaming
SC1-C3.4	Dispatching picture/video information to a selected set of PPDR users in the field (could be from different organizations)	Video streaming Picture transfer
SC1-C4	(Ad-hoc) integration of several agencies/organisations in order to manage a major crisis	Interoperability aspect
SC1-C4.1	(Ad-hoc) Inter-agency communications between CCC (bridging)	Interoperability aspect Tactical patch
SC1-C4.2	Inter-agency communications between PPDR users in the field from different organisation and the lead CCC (dynamic grouping, delegation of coordinator role)	Dynamic Regrouping Tactical patch
SC1-C4.3	Means to dispatch / access information to select users (role-based access to information)	Dynamic regrouping
SC1-C4.4	Means to allow closed group communications with controlled access to main CCC	Group call
SC1-C4.5	Means to integrate mobile command posts deployed in the crisis area with the central CCC	Management and configuration aspects
SC1-C5	Advanced scheduling / monitoring of resources in line with mission needs	Location reporting Status messaging
SC1-C5.1	Advanced location of deployed resources (human and vehicles) using tracking systems (outdoor and indoor)	Location reporting
SC1-C5.2	Advanced body sensors to track vital signs, movement, man-down.	Body sensor application
SC1-C6	Transmission and access to broadband information	N/A - Generic broadband IP capability
SC1-C6.1	Means to transmit and receive live video streams between the field and CCC	Video streaming
SC1-C6.2	Means to transmit and receive (high quality pictures) picture between the field and CCC	Picture transfer
SC1-C6.3	Means to access Intranet applications and databases (e.g. criminal records, vehicle structural details...) from the field	N/A - Generic broadband IP capability
SC1-C6.4	Means to (securely) access the Internet (e.g. Google street, augmented reality) from the field	N/A - Generic broadband IP capability
SC1-C6.5	Means to provide controlled (dynamic, tuneable), differentiated and guaranteed access to applications according to their characteristics, priority and pre-emption	Management and provisioning aspects

SC1-C7	Sensing Internet / social media to build intelligence of the situation (note: not is the scope of SALUS project but part of the intelligence / information to meet mission objectives)	N/A - Generic broadband IP capability
SC2-C1	Provide interworking and synchronization between PPDR communication networks based on different access technology	Interoperability aspects
SC2-C1.1	Inter-agency communications between CCCs (bridging)	Interoperability aspects
SC2-C1.2	Inter-agency communications between PPDR users in the field from different organisation and Event Coordination Centre (dynamic grouping, delegation of coordinator role)	Interoperability aspect Dynamic regrouping Tactical patch
SC2-C1.3	Means to dispatch / access information to select users (role-based access to information)	Dynamic regrouping
SC2-C1.4	Enable communications between PPDR users in different access networks (LTE and Wi-Fi) for high data rate applications (e.g. video streaming, database access)	Video streaming
SC2-C1.5	Enable communications between PPDR users in different access networks (TETRA/TETRAPOL, LTE and Wi-Fi) for voice applications.	Interoperability aspects Group call
SC2-C1.6	Enable communications between PPDR users in different access networks (TETRA/TETRAPOL, LTE and Wi-Fi) for low data rate applications (e.g. text based messages)	Interoperability aspects Text messaging Binary messaging
SC2-C1.7	Provide end-to-end secure communications between PDDR users in different access networks	End-to-End Encryption
SC2-C2	ICT infra-structure capable of advanced services	N/A - System solution aspect
SC2-C2.1	Voice and speech recognition system	N/A - Dedicated application
SC2-C2.2	Context related information search	N/A - Dedicated application
SC2-C2.3	Secure Internet access	N/A - Generic broadband IP capability
SC2-C2.4	Video-based behaviour recognition and alerting system	N/A - Dedicated application
SC2-C2.5	CCC hosted application for correlation of multiple data sources and display	N/A - Dedicated application
SC2-C3	Quickly and temporarily increase the capacity of the installed PPDR system by deploying additional Wi-Fi hotspots	N/A - System solution aspect
SC2-C4	Sense the area to improve situational awareness in the CCC and in the field	N/A - Dedicated application
SC2-C4.1	Retrieve CCTV footage in the control room	N/A - Dedicated application
SC2-C4.2	Upstream image/video information to a selected set of PPDR users in the field	Video streaming

SC2-C4.3	Use of secured aerial view (drones/helicopters/balloons) to retrieve live image/video information	Video streaming Picture transfer
SC2-C5	Provide tracking and monitoring technology	Location reporting
SC2-C5.1	Health and environmental status for PPDR users	Body sensor application
SC2-C5.2	Health on injured spectators	Body sensor application
SC2-C5.3	Outdoor and indoor PPDR user location	Location reporting
SC3-C1	Transportable radio solutions with limited time set-up. Similar technologies than the one used for permanent infrastructure	N/A - System solution aspect
SC3-C2	Interconnection of the various transportable and temporary solutions: interconnection between them and also with permanent infrastructures	Interoperability aspects
SC3-C3	PMR group communications voice services	Interoperability aspects Group call Late entry Priority call
SC3-C4	Device to device communications	N/A - System solution aspect
SC3-C5	Non-real time High Speed Data Services	N/A - Generic broadband IP capability
SC3-C6	Real time High Speed Data Services; video quality and latency as parameters of the end-user application	N/A - Generic broadband IP capability
SC3-C7	Connection towards remote equipment as central database servers, HQ and remote control centres	N/A - Generic broadband IP capability
SC3-C8	Needed Capacity for the operation management may be greater than the one designed for routine day-to-day applications.	N/A - System solution aspect

Note that the Not Applicable (N/A) items do not match any existing or future PMR functionality that is subject to standardisation.

2.2 Analysis of legacy PMR functionality

The following table provides an extensive overview of capabilities offered by legacy PMR systems, including TETRA and TETRAPOL.

Table 2 - Legacy PMR functionalities

Functionality (SALUS naming)	TETRA	TETRAPOL	Notes
Group Call	Group call	Talk group	
Group Attachment	Group attachment	Scanning	Scanning is a specific group attachment mode within TETRA
Broadcast Call	Broadcast Call	-	
Individual Call	Individual call	Individual call	TETRA offers capability of both semi-duplex and full duplex calls

Talking Party Identification	Talking Party Identification	Talking party identification	
Call Identification	Call Identification	-	Most likely, TETRAPOL offers comparable functionality
Late Entry	Late Entry	Late Entry	
Priority Call	Priority Call	User & Talk group priority	
Pre-emptive Priority Call	Pre-emptive Priority Call	Pre-emption priority	
Emergency Call	Pre-emptive Priority Call	Pre-emptive emergency call	TETRA considers an Pre-emptive Priority Call with priority level 156 as Emergency Call
Speech Item Priority	Pre-emptive speech item request	-	
Direct Mode Operation	Direct Mode Operation	Direct Mode	Not part of PMR-over-LTE services, while DMO is not yet standardised by the 3GPP
Tactical Patch	-	Talk group merging	Several TETRA vendors offer this as a proprietary feature
Dynamic Regrouping	Dynamic Group Number Assignment	Dynamic Group Number Assignment	
Telephony Call	PSTN interconnect	PABX/PSTN call	
Barring of Incoming Calls	Barring of Incoming Calls	-	
Barring of Outgoing Calls	Barring of Outgoing Calls	-	
Call Authorised by Dispatcher	Call Authorised by Dispatcher	Call authorised by dispatcher	
Include Call	Include Call	Multi-party call	
Call Forwarding	Call Forwarding	Call forwarding	
Call Transfer	Call Transfer	Call transfer	
Ambient Listening	Ambient Listening	Ambient listening	
Discreet Listening	Discreet Listening	-	
Status Messaging	Status message	Status	
Text Messaging	Short Data Service Type 4-TL	Short Message Service	
Binary Messaging	Short Data Service Type 1, 2, 3 and 4	-	
Location Reporting	Location Information Protocol	-	Most likely, TETRAPOL offers comparable functionality
Packet data	Packet data, Single and Multi Slot	Mobile data	Generic functionality of mobile broadband IP
Authentication	Authentication	Authentication	
Mutual authentication	Mutual authentication	Mutual authentication	

Air interface encryption	Air interface encryption	-	Not part of PMR-over-LTE services, while Air Interface Encryption is provided by the LTE network
End to End Encryption	End to End Encryption	End to End Encryption	Includes over-the-air key distribution
Enable disable	Enable disable	Protection against lost terminals	
Permanent disable	Permanent disable	Protection against stolen terminals	

2.3 Analysis of current state-of-the-art

Capability analysis of state-of-the-art proprietary solutions for PMR-over-LTE will be part of the Final version of this deliverable. For reference, the capabilities of the following proprietary solutions will be considered:

- Generic: methods for presence indication as well as closed-group text, picture and video distribution;
- Twisted Pair WAVE® solution (recently acquired by Motorola Solutions);
- Kodiak InstaPoC™ solution;
- Cisco IP Interoperability and Collaboration System (IPICS) solution.

2.4 Analysis of current standardisation effort

It has been recently agreed that 3GPP would take the responsibility for the specifications of the mission critical PTT (MCPTT) over LTE. At the time of writing this deliverable, 3GPP has released a first draft of the requirements of MCPTT [7]. MCPTT is leveraging the Group Communications System Enabler (GCSE) defined in 3GPP Release 12 ([9]) to enhance the efficiency for transmitting the same information to large group of users in the same geographical area and Proximity Services, defined in 3GPP Release 13, for off-network MCPTT communications ([10]).

The 3GPP requirements for MCPTT explicitly target public safety end users, since they are considered as the most demanding in terms of features and performances. The scope of the document covers services requirements such as:

- Support of arbitrated / coordinated group communications within users members of MCPTT group;
- Support of advanced features that are currently supported by legacy PMR systems such as late entry; dynamic group management, priority override, queuing, pre-emption, talker and group identities, location (including privacy);
- Affiliation to multiple groups and reception / transmissions to multiple affiliated groups;
- Support of broadcast calls;
- Support of Emergency Alert calls;
- Support of Imminent Peril calls;
- Support of private calls.

The document also describes high-level security requirements for MCPTT service authentication (a MCPTT user can get MCPTT services from different UEs) and end-to-end confidentiality. MCPTT services and security requirements are provided for both infrastructure and out of coverage (ProSe) transmission modes.

Interworking is also an important aspect addressed by the document. The requirements are going in two directions: interworking with MCPTT users of over LTE systems (includes also roaming), and interworking with narrowband PMR systems such as P25, TETRA and legacy analogue systems.

It is to be noted that interworking with TETRAPOL or Wi-Fi systems are not requirements identified so far by 3GPP community.

The actual specifications for MCPTT will be developed by 3GPP in the following months. The calendar up to now to deliver 3GPP Release 13 is Q1 2016. More information on the actual solution for MCPTT and a gap analysis with the solution being proposed in SALUS will be provided in the final version of the report.

It is also to be noted that in the frame of the early discussions for the definition of the content of the 3GPP Release 14, some contributions are also made in the direction of standardising mission critical multimedia communications. More information will be provided in the final version of the document if available.

3 NON-FUNCTIONAL REQUIREMENTS

This section focuses on non-functional requirements on PMR services on top of LTE.

3.1 Performance

Performance is one of the key requirements to satisfy the usage scenarios of PMR, of which the different aspects are discussed in the next sections.

3.1.1 Call setup delay

The call setup delay for group calls is considered a key performance criterion for public safety applications. In addition, the user experience for less demanding PMR applications is significantly improved when a low call setup delay is offered.

For the design of the TETRA standard, the Public Safety user community has agreed that a 300 ms call setup delay for group calls is acceptable. Most TETRA and TETRAPOL networks meet this user requirement (say within 90% of the cases), also when the call is established over a long distance or over a large number of cells.

Considering the experience on call setup delays within dedicated PMR networks for public safety, SALUS also proposes to use the 300 ms maximum call setup delay for PMR-over-LTE services.

3.1.2 Speech transfer latency

The speech transfer latency is another key performance criterion for public safety applications. Many aspects affect speech transfer latency, including the packet transfer methods, chosen speech vocoder (codec), the performance of speech encoding and decoding, and transport network latency.

For the TETRA standard, the lower limit of speech transfer latency is set to 207,3 ms [3]. This speech transfer latency may be achieved when speech is retransmitted in the same cell, or for Direct Mode Operations (DMO). However, this figure is not feasible for large networks in which transport networks and associated serialisation delays are applicable, which can add up to an addition 50 to 100 ms of delay.

On basis of the above considerations, a maximum speech transfer latency of 300 ms is proposed by SALUS as the requirement that meets both current user experience requirements as well as feasibility for implementation as a PMR-over-LTE service.

3.1.3 Number of calls per second

The number of calls per second is limited by the signalling bandwidth and processing capacity (throughput) of the network.

The signalling bandwidth is severely limited in TETRA due to the slotted Aloha access method with low data rate, allowing fewer than 17 calls per second in the downlink direction (from network to radio) and less than 8 calls per second in the uplink direction (from radio to network) for every control channel on a radio site. Within TETRA, the number of control channels can be increased until four, offering a theoretical maximum of 68 calls per second in the downlink and

32 calls per second in the uplink. However, the multicast functionality of TETRA enables a very efficient call setup procedure for an unacknowledged group call, which is unlike current GSM-R and PTT-over-Cellular standards that require sequential calls to reach multiple radios within a group.

In order to support present and future capabilities of LTE networks, it is therefore suggested to establish two requirements:

- For present LTE networks that do not support broadcast or multicast calls, the requirements for calls per second is established as 900 per second (3 call per second with 300 members each, or 15 calls per second with 60 members each);
- For future LTE networks that support broadcast or multicast calls, the requirements for calls per second is established as 15 per second (same as average for TETRA networks).

3.1.4 Speech quality

Speech quality is expressed in a Mean Opinion Score (MOS). A MOS value of 3,2 is considered appropriate for Private Mobile Radio, whereas a MOS value of 3,5 is most appropriate for telephony services.

The availability of standards based vocoder technology for telephony applications using low bitrates (equal or less than 8 kbps) enables the MOS requirement of 3,5 for all use cases. The only exception is end-to-end transparency with TETRA and TETRAPOL vocoders to enable End-to-End Encryption; in these cases it is preferred to maintain the legacy vocoder.

3.2 Scalability

Scalability can be achieved by adopting the right system architecture whereby the switching and distribution of voice, data and signalling is efficiently arranged throughout the network. From the use cases described in [1] a number of possible solutions can be designed, whereby a mix of distributed (especially for the fast deployable scenario, required for events and disasters) and centralised architectures (for fixed deployment with high capacity requirement) is considered the most appropriate.

Note that for implementation of PMR-over-LTE both the scalability of the LTE network and the PMR services on top of LTE must be considered. These can be implemented separately, or delivered as an integrated solution, for example as part of the Integrated Multimedia Subsystem (IMS) within the reference EUTRAN architecture.

The ideal design for scalability should thus allow a mix of architectures, both for the LTE network design and the PMR services on top of LTE.

3.3 Availability

In PMR networks, the availability is measured in time and place. A common requirement is 99,9% availability, which is not too difficult in terms of equipment and link reliability, but quite demanding in terms of radio coverage.

High availability can thus be achieved by using sufficient radio sites and highly reliable equipment and services combined with automatic failover when link or equipment failures occur.

The solution must be designed with these requirements in mind, whereby the outage must be kept short by means of rapid detection of failures and fast activation of redundant links or equipment.

3.4 Security

Complementing the information provided in SALUS Deliverable 5.1, Table 3 provides an overview of security threats with reference to security services that can be applied as countermeasures.

Table 3 - Analysis of Security Threats

Threat	Description	Countermeasures
Interception - eavesdropping by third party	Reception of communications for curiosity, possible gain or deliberate intent to commit crime	Air Interface Encryption; End to End Encryption
Interception - eavesdropping by other radio user	Reception of communications by another PMR radio user for the purpose of misuse	Air Interface Encryption; End to End Encryption
Interception - reception of user identities for traffic analysis	Gathering and analysis of identities and groups over a period of time to discover patterns of movement	Air Interface Encryption
Interception / Denial of Service – A fake network tries to authenticate legitimate PMR radios	Attack scenario to simulate a network whereby legitimate PMR radio users are denied access to the genuine network, and communication can be intercepted	Mutual Authentication; Intrusion Detection System
Unauthorised access - Use fake PMR radio on legitimate network	Gain illegal access to the network with the intention to commit fraud	Authentication; Intrusion Detection System
Unauthorised access - PMR radio is stolen	Intentional theft and usage of a genuine PMR radio	Disable; Permanent Disable; Intrusion Detection System
Unauthorised access - PMR radio is lost	Genuine PMR radio is misplaced or lost	Disable; Permanent Disable; Intrusion Detection System
Organisation specific - Network operator intercepts traffic	Network operator may have access to components or link that store or carry unprotected communications	End-to-End Encryption

4 FUNCTIONAL DESCRIPTION

The PMR-over-LTE services can be divided in four categories:

- **Basic services**: features that are considered the minimum feature set of a typical PMR network;
- **PMR supplementary services**: features that are considered for more advanced PTT-operated PMR applications;
- **Telephony supplementary services**: features that are required for Public Access Mobile Radio (PAMR) applications;
- **Security services**: features that are critical for security sensitive applications.

There are also the 'PPDR broadband services', but these will be part of the PMR-over-LTE solution to be described in the upcoming SALUS Deliverable 6.5. The above services are considered critical to delivery PPDR users the same capabilities as in legacy PMR networks, as well as offering interworking with these legacy networks while migration to PMR-over-LTE.

4.1 Basic services

The Basic services are considered the minimum feature set of a typical PMR network, which are most relevant for business and industry applications.

4.1.1 Group Call

The group call is the primary mode of operation in a PMR network. The group call allows one-to-many communication, whereby the user requests to talk by pressing the Push-To-Talk (PTT) button. The system confirms the request to talk, after which the user can talk while the PTT remains pressed, and all other members in the group can listen to the talking party. By means of the "request to talk" mechanism the system ensures that only one person can speak at any time.

A group call can involve one or more radios and dispatchers. Each of the radios and dispatchers must be attached to the group in order to be member of this group. In most cases, the radio user can select a group by means of a turn knob or up / down button, after which the group becomes the "selected group".

A radio user can only listen and talk in one group call at a time, whereby the dispatcher can listen and talk in multiple groups simultaneously.

The group call is ended by one of the following conditions:

- Hang timer: if no member of the group is talking during the so-called hang time period (typically 3 seconds);
- Maximum call duration: after exceeding the configured maximum call duration;
- Disconnect: if the radio or dispatcher that started the group call manually ends the call.

4.1.2 Individual call

The individual call allows one-to-one communication between radios as well as radios and dispatchers. The person to call is entered as a number or selected from a phone book, after which the PTT or "hook" button is pressed to establish the individual call.

In semi-duplex mode, the radio or dispatch user requests to talk by pressing the Push-To-Talk (PTT) button. The system confirms the request to talk, after which the user can talk while the PTT remains pressed, and the other user can listen to the talking party. By means of the "request to talk" mechanism the system ensures that only one person can speak at any time.

In duplex mode, both users can simultaneously talk and listen. Operation of the PTT button is thus not necessary.

An individual call is ended by one of the following conditions:

- Hang timer (semi-duplex mode only): if no user is talking during the hang time period (typically 7 seconds);
- Maximum call duration: after exceeding the configured maximum call duration;
- Disconnect: if one of the users ends the call manually.

Another call setup option for individual calls in semi-duplex mode is the so-called "direct setup" feature. This allows the dispatch or radio user to establish the individual call without the need to accept the call by the called person.

4.1.3 Telephony Call

Telephony calls can be made in both directions: either from a telephone set to a PMR radio or dispatcher, or vice-versa. Both the called and calling user can speak and listen simultaneously because of the full duplex capability of PMR-over-LTE.

Telephony related features include Call Identification, DTMF overdial, Telephony Group Call and Direct Dial In.

4.1.4 Broadcast Call

The broadcast call allows the dispatcher to talk to radio users in a group, whereby the radio users cannot talk back. The broadcast call can thus be regarded as an "announcement" call that enables one-direction communication only. The radios provide a clear indication that talk back is not possible.

A broadcast call is ended by inactivity after expiry of the hang time period, or by manual disconnection by the dispatcher.

4.1.5 Status messaging

Status messaging is used to transfer a pre-defined status from the radio to the dispatcher or vice-versa. The pre-defined status message most often represents a frequently used test message (like "arrived at the scene"), but can also control the dispatcher workflow (like speech call requests). Status messages thus offer an efficient method to communicate the status of a person or unit to the dispatcher, or to broadcast a specific assignment to a group of persons.

A PMR-over-LTE status message consists of 5 digits with specific ranges for user and system messages. Due to the compact size, status message transfer is fast with a very small capacity requirement on the IP path.

Within the constraints of the specific ranges of status numbers, the mapping of status numbers to text messages as well as controls is entirely free to define. The description of status messages can be included in the status message in order to display the status text on the

dispatcher station or LTE devices when receiving a status message, and to make the text selectable from the dispatcher station and LTE devices when transmitting a status message.

4.1.6 Text messaging

Text messaging is used to transfer a text message from the radio the dispatcher, from the dispatcher to the radio or between radios. Text messaging can be used to carry instructions, or to exchange information between people, similar to the popular SMS service in mobile telephony networks.

Transfer of an individually addressed text message is confirmed end-to-end by the so-called Transport Layer (TL) protocol. This means that the arrival of the text message on the radio as well as the fact that the message is actually read by the recipient are both confirmed to the transmitter of the text message.

Group addressed text messages are supported as well, allowing the text message to be delivered to all radios that are attached to a group. Although these text messages are transferred by the TL protocol as well, an acknowledgement should not be requested then to prevent the message to be confirmed by all radios simultaneously.

4.1.7 Binary messaging

Binary messaging is used to exchange information between user and server applications. Typical information includes the status of sensors and messages received from beacons.

Binary messages can have an arbitrary length, but should be limited to 140 bytes in order to maintain interoperability with the TETRA standard. The content and formatting of binary messages is not defined. The Transport Later (TL) protocol is not applicable. In SALUS Deliverables 5.2 [5] and 7.1 [6] a message format for exchanging data amongst PPDR terminals and back end applications is proposed.

Group addressed binary messages are supported as well, allowing the message to be delivered to all radios that are attached to a group. This allows for specific applications, like polling of groups of radios.

4.1.8 Registration and de-registration

Registration and de-registration is more or less invisible to the radio user: every time the radio is switched on and off, respectively registers or de-registers itself on the PMR-over-LTE network.

Registration confirms that the radio is switched on, and can be reached via the LTE or Wi-Fi network on which the registration is received. The registration will be rejected when the radio identity is not available in the subscriber database. The registration request is often combined with one or more group attachment requests, either in one combined request or in two separate requests to the network.

De-registration confirms that the radio is switched off or the battery is about to be depleted. After receiving the deregistration request, the PMR-over-LTE solution knows that the radio cannot be reached anymore, resulting in a “Not available” result when trying to call this radio.

4.1.9 Group attachments

Group attachments are executed by the radio to confirm the groups that are selected and / or scanned by the radio, either while registering or after a network change, after selection of a new group or when changing the group scan mode. Because of the group attachments, the network knows which radios need to receive the voice and data messages that are exchanged within the groups.

The basic types of group attachments include the “selected group” and “scanning groups”. The selected group is the group that is selected by the radio user by means of a turn knob or up/down button, and is used by default for transmitting voice when pressing the PTT button. Scanning groups are optional, and can be used to allow the radio user to listen to other groups as well. The selected group has a preference for listening, except when a high priority or emergency call is received on the scanning group.

Scanning groups are often organised in so-called scan lists that can include multiple groups. Permissions to select one or more scan lists and / or to switch on and off group scanning, as well as the content and possibility to edit scan lists, are all configured in the radio programming.

4.2 PMR supplementary services

PMR supplementary services are considered for more advanced PTT-operated PMR applications, like public transport, oil & gas, and public safety.

4.2.1 Late Entry

The Late Entry supplementary service ensures that radios are included in a group call when the user switches on the radio, selects the group or did not receive the call due to signal fading after the group call has started.

4.2.2 Priority Call

The Priority Call (PC) supplementary service allows the user to request for a higher priority voice call. A higher priority voice call results in shorter queue times when traffic channel capacity is exhausted. When a radio channel becomes available, the PMR-over-LTE server will select the highest priority call request first to proceed.

Twelve priority levels are defined, numbered from 0 (no priority) to 11 (priority level #11). The call request priority level can be configured in the PMR radio, or can be assigned on a per subscriber or fleet level in the PMR-over-LTE server. This allows the network operator to assign a priority level that is most appropriate to the user of agency using the network.

4.2.3 Pre-emptive Priority Call

The Pre-emptive Priority Call (SS-PPC) supplementary service allows a dispatch or radio user to establish or continue a speech call when there are no resources available or when the called radio is engaged in another call. The pre-emptive priority call is often related to an “emergency call” that must be completed, regardless of the loading of the system and whether the called party is busy or not.

Two pre-emption methods are applicable:

- Resource pre-emption ensures that capacity is available on the relevant radio sites on which the called radios are present. If no capacity is available, the network will pre-empt

an existing voice or data call that has the lowest priority. When the system can select from multiple calls with the same priority, the call with the longest duration will be pre-empted first.

- Subscriber pre-emption ensures that the called radios are informed on the emergency call, even when the radios are currently engaged in another voice or data call. The radio then ends the existing call and is included in the emergency call automatically.

Resource pre-emption is also applicable in order to continue calls: if a radio decides to choose a fully occupied radio site while engaged in a pre-emptive priority call, also an existing voice or data call must be cleared to allow the call to continue.

Four priority levels are defined for pre-emptive priority, numbered from 12 (pre-emptive priority #1) to 14 (pre-emptive priority #3) and 15 (pre-emptive emergency call). The call request priority level can be configured in the PMR radio, or can be assigned on a per subscriber or fleet level in the network. This allows the network operator to assign a priority level that is most appropriate to the user of agency using the network. Priority level 15 is reserved for operation of emergency calls.

4.2.4 Talking Party Identification

The Talking Party Identification (TPI) supplementary service allows listening parties to see the identity of the talking party. This service is applicable to PTT operated individual calls and group calls.

PMR radios show the Short Subscriber Identity (SSI) number of the talking party by default. If the SSI is included in the phone book of the radio, the corresponding name will be shown instead.

The dispatcher shows both the Short Subscriber Identity (SSI) and the Name alias of the talking party. The information of the Name alias is stored in the PMR-over-LTE server database and can be synchronised also with the Radio User Assignment (RUA) database.

4.2.5 Call Identification

Call Identification (CI) is a supplementary service that allows the called party to see the identity of the calling party. The Call Identification service is applicable to both individual simplex and duplex calls, as well as group calls.

PMR radios show the subscriber number of the calling party by default. If the Name alias is included in the call setup message or the name is available in the phonebook, the corresponding name will be shown instead.

The dispatcher shows both the subscriber number and the Name alias of the calling party. The information of the Name alias is stored in the PMR-over-LTE server database and can be synchronised also with the Radio User Assignment (RUA) database.

4.2.6 Speech Item Priority

Speech Item Priority allows a PMR radio user or dispatcher to interrupt another radio user or dispatcher that is currently talking. This allows a supervisor to override the communication of a team member when an urgent announcement must be made.

The Speech Item Priority feature provides four levels of priority: no priority, low priority, high priority and pre-emptive priority. The low or high priority levels are relevant for speech item queuing, thus the selection of the next party that is allowed to speak; low priority requests take precedence above no priority requests, and high priority requests take precedence above no and low priority requests.

The pre-emptive speech item priority level instructs the PMR-over-LTE server to cut-off communications from the current talking party, and thus overrides the communication immediately. All radio users and dispatchers are informed accordingly, whereby the new talking user identity will be updated and voice can be heard from the party that has requested for the pre-emptive speech item priority. Also the currently talking user will be notified, whereby an “interrupted” message is shown and a tone is heard to notify the user of the interruption.

4.2.7 Dynamic Regrouping

Dynamic Regrouping is a supplementary service that allows remote configuration of groups in a PMR radio. The PMR-over-LTE server supports Dynamic Regrouping for a number of scenarios:

- Add a group without attachment, allowing the radio user to select the new group later;
- Add a group as selected group, forcing the radio user to use the new group for communications;
- Add a group as scanned group, forcing the radio user to monitor activity on the new group while the selected group remains the same;
- Remove an existing group, either a group without attachment, the selected group or a scanning group;
- Execute group-addressed Dynamic Regrouping commands.

Multiple Dynamic Regrouping *add* and *remove* group commands can be combined in a single Dynamic Regrouping command. The Dynamic Regrouping *add* command can include a group name to make it easier for the radio user to choose the correct group for communications. Dynamic Regrouping can be used to remotely reconfigure radios to allow arbitrary users to form a team.

The Chameleon Line Dispatch Station (LDS) provided by Rohill offers a "storm plan" function that allows Dynamic Regrouping regrouping commands to be prepared; these can be executed and rolled back on request later.

4.2.8 Discreet Listening

Discreet Listening (DL) is a supplementary service that allows the dispatcher to monitor voice conversations as well as see text and status messages in which the target radio, dispatcher or telephony extension is included.

The target radio, dispatcher or telephony numbers for Discreet Listening are referred to as “traces” that can be entered, edited and removed in the dispatcher. The dispatcher application allows up to 16 of these trace definitions, whereby communication is heard and messages can be seen when activity of a traced subscriber is detected.

In order to prevent privacy issues, the capability of Discreet Listening can be enabled per dispatcher, and can be made valid for specific fleets only, in order to ensure that Discreet Listening is only used by specific dispatchers according certain rules.

4.2.9 Ambience Listening

Ambience Listening (AL) is a supplementary service that allows the dispatcher to monitor the ambience audio of a radio. The Ambience Listening call feature is available from the dispatcher station.

Ambience Listening is highly valuable to understand what is going on near the radio user when he or she transmits an emergency call. The dispatcher then can determine whether to alert public safety officers, for example when people are threatened. No indication on ambience listening is visible on the radio, so the attacker cannot see that the radio is transmitting.

In order to prevent privacy issues, the capability of Ambience Listening can be enabled per dispatcher, and can be made valid for specific fleets only, in order to ensure that Ambience Listening is only used by specific dispatchers according certain rules.

4.2.10 Location Reporting

Location Reporting is a supplementary service that allows the dispatcher to view and track the location of individual radio users. Both outdoor (GPS) and indoor (Wi-Fi, beacons) location systems must be supported.

Location Reporting is executed periodically by the radio, whereby the reporting is triggered on basis of a time interval and / or distance. The configuration of the time interval and distance parameters can be executed remotely to allow precise control over network load caused by location reports.

The basis for Location Reporting is the TETRA Location Information Protocol (LIP) specification; this specification is widely regarded as the industry standard for PMR location services.

4.3 Telephony supplementary services

Telephony supplementary services include features that are required for Public Access Mobile Radio (PAMR) applications.

4.3.1 Barring of Incoming Calls

Barring of Incoming Calls (BIC) is a supplementary service that allows blocking of certain calls from radio, dispatcher or telephony users on basis of the identity of the calling party. Examples are incoming PSTN telephone calls from telephone extensions that are not identified or trusted, and calls from radios that belong to a different fleet.

4.3.2 Barring of Outgoing Calls

Barring of Outgoing Calls (BOC) is a supplementary service that allows blocking of certain calls to radio, dispatcher or telephony users on basis of the identity of the called party. Examples are outgoing PSTN telephone calls for specific fleets of users, and calls to radios that belong to a different fleet.

4.3.3 Call Authorised by Dispatcher

Call Authorised by Dispatcher (CAD) is a supplementary service that allows the dispatcher to approve or reject calls from radio, telephony or other dispatch users. The dispatcher is informed on the calling user, called user and type of call (simplex, duplex). The called and calling user identity includes the domain (radio, telephone, dispatcher), number (SSI, extension) and name alias (when available).

After interception of a call, the dispatcher is offered three choices to complete the CAD request:

- The dispatcher rejects the call: the call setup is abandoned immediately, whereby the calling user is informed accordingly with reason “call reject”;
- The dispatcher accepts the call: the call setup to the calling party proceeds as requested;
- The dispatcher decides to intervene with the call, allowing the dispatcher to ask the calling user about the reason of the call.

The third choice diverts the call to the dispatcher first, after which the dispatcher can decide either to reject the call, or to allow the call to proceed as requested.

4.3.4 Call Forwarding on Busy

Call Forwarding on Busy (CFU) is a supplementary feature that allows an individual call to a radio or dispatcher to be forwarded to another radio, dispatcher or telephony extension when the original radio is busy in another call. When enabled, calls to a busy radio or dispatcher are redirected to the forward destination.

Automatic rerouting of incoming calls to members of a mobile or dispatcher team is a typical application of the Call Forwarding on Busy feature.

4.3.5 Call Forwarding on No Reply

Call Forwarding on No Reply (CFNRy) is a supplementary feature that allows an individual call to a radio or dispatcher to be forwarded to another radio, dispatcher or telephony extension when the original radio does not answer the call. When enabled, calls to a radio or dispatcher are redirected to the forward destination when the call is not answered within a certain period.

Automatic rerouting of an incoming call to another (backup) destination is a typical application of the Call Forwarding on No Reply feature, for example to divert the call to another team member, or to divert the call to a fixed or mobile telephone number of a person when his or her radio is not answered.

4.3.6 Call Forwarding on Not Reachable

Call Forwarding on Not Reachable (CFNRc) is a supplementary feature that allows an individual call to a radio or dispatcher to be forwarded to another radio, dispatcher or telephony extension when the original radio cannot be reached. When enabled, calls to a radio or dispatcher are redirected to the forward destination when the radio or dispatcher is switched off, or the radio is outside of the coverage area of the network.

Automatic rerouting of an incoming call to another (backup) destination is a typical application of the Call Forwarding on Not Reachable feature, for example to divert the call to another team member, or to divert the call to a fixed or mobile telephone number of a person when his or her radio cannot be reached.

4.3.7 Call Forwarding Unconditional

Call Forwarding Unconditional (CFU) is a supplementary feature that allows an individual call to a radio or dispatcher to be forwarded to another radio, dispatcher or telephony extension. When enabled, calls to this radio or dispatcher are always forwarded to the forward destination, regardless whether the original radio or dispatcher is available or not.

Typical applications for unconditional call forwarding include the ability to temporary use another radio during the time of repair or reprogramming of the original radio, or to use a radio instead of a dispatcher for handling calls when away from the dispatcher workstation.

4.3.8 Call Hold

Call Hold (HOLD) is a supplementary feature to put a voice call “on hold” in order to answer or initiate another voice call. During or after finishing the other call, the voice call may be resumed at any time. Call Hold is applicable to individual voice calls to radio users, telephone users and other dispatchers.

The Call Hold service is available only on dispatcher workstations. A call “on hold” will not be ended on inactivity, although the maximum call duration still applies. The connected user can always disconnect the call.

4.3.9 Include Call

Include Call (IC) is a supplementary feature to include another user in a voice call. The voice call then becomes a “conference call” in which three or more users can communicate to each other. The Include Call feature is applicable only to PTT operated half-duplex individual voice calls. Multiple radio users and dispatchers may be included in the call, but at maximum one telephone user is allowed to be part of the call, while only one user with duplex call capability is permitted in an call with more than two participants.

Every user can disconnect from the call. The call will be ended if less than two users remain in the call. Note that the inactivity period for individual calls also applies for calls that include more than two users.

4.3.10 Call Transfer

Call Transfer (CT) is a supplementary feature to transfer the currently selected voice call to another user. The Call Transfer destination can be a radio user, telephone user or another dispatcher. The Call Transfer feature is applicable to both PTT operated half-duplex and duplex individual voice calls.

While the Call Transfer is in progress, the first user will hear a ringing tone. The called user must accept the call in order to establish the new voice call.

4.4 Security services

Security services include features that are critical for security sensitive applications, like public safety.

Although security features may be considered non-functional services, the implementation does in fact add functionality to the solution in terms of configuration and control. Also, the capabilities are closely following TETRA and TETRAPOL capabilities in order to support interworking capabilities in the SALUS solution.

4.4.1 Authentication

Authentication ensures that only genuine radio users can use the PMR-over-LTE network. Even when the attacker is able to configure a new PMR radio or clone an existing PMR radio, the network will not accept registrations from this radio when the secret keys (referred to as “K” key) in the radio and network do not match.

The authentication algorithm uses a challenge-response mechanism that does not reveal the value of the secret key over the air interface. The mechanism is both efficient and very secure, and also results in a private key needed for Air Interface Encryption (AIE) of individual calls.

When enabled, the network automatically requests for authentication when a radio tries to register itself. In addition, authentication may be requested periodically and / or when the radio performs cell reselection.

4.4.2 Mutual authentication

Mutual authentication allows the radio to validate whether the PMR-over-LTE server is genuine. This is relevant to ensure that radios are not “diverted” to another network or service in order to disrupt or monitor communications by skilled individuals or organisations.

The mutual authentication is requested by the radio as an extension to the standard authentication procedure. After receiving the challenge from the network, the radio will return the response, but also challenge and request a response from the PMR-over-LTE server. This allows both the network and radio to validate each other responses to validate whether the secret keys are matching.

The request for mutual authentication is a configuration item in the PMR radio programming.

4.4.3 Enable - Disable

Enable and Disable is a security service that allows a dispatcher to remotely disable and enable a radio.

Remote Disable allows the responsible person within an agency to disable operation of a radio when the radio is lost or stolen. When disabled, the radio is not able to make or receive voice and data calls, ensuring that communications cannot be heard or disturbed by unauthorised persons. The display is cleared to indicate that the radio is not working, although on the background the radio can still roam to other radio sites, report its position or receive the remote enable command.

Remote Enable allows the radio to be made operational again when the radio is recovered.
The radio can be configured to require authentication and / or encryption to allow Remote Enable and Disable as an additional precaution to prevent false execution of Remote Enable and Disable.

4.4.4 Permanent Disable

Permanent Disable is a security service that allows a dispatcher to remotely “kill” a radio. Permanent Disable ensures that all security sensitive configuration and data is “wiped” from the radio, making it impossible to use the radio. Remote Enable is thus not applicable anymore, and also tracking its position is not possible.

When switching on the radio, the display will either be blank or indicating an invalid configuration. Recovery from a permanent disable state is possible only by the manufacturer or using special tools. Most radios are configured by default to require authentication and encryption in order to perform Permanent Disable as an additional precaution to prevent false execution of Permanent Disable.

4.4.5 End to End Encryption

End-to-End Encryption (E2EE) offers another layer of encryption of voice and data communication, thus separately from the Air Interface Encryption (AIE) capabilities of existing PMR and LTE networks. As the name implies, E2EE encrypts and decrypts voice and data in the radios with no knowledge of keys and algorithms within the network.

E2EE is particular useful for agencies that require the highest level of confidentiality. With no knowledge of keys, it is impossible to intercept the communication, even when full access to the transit and core network can be obtained.

E2EE allows the use of several encryption algorithms, of which the standard Advanced Encryption Standard (AES) with a key length of 128 or 256 bits are the most widely chosen algorithms. AES is adopted by the US government as the standard encryption algorithm to transfer classified information, and can thus be regarded as extremely secure, especially when the 256 bit length option is chosen.

E2EE may be used instead or in addition to Air Interface Encryption (AIE). Obviously, when using E2EE in addition to AIE, the highest level of confidentiality can be reached, whereby AIE also adds the benefit of encrypted signalling.

E2EE requires full transparency of voice and data communication through the network in order to prevent errors in decryption and synchronisation. Decryption is synchronised by so-called synchronisation frames in which the algorithm identity, key index and synchronisation vector is included. This synchronisation frame is sent by the transmitting radio at the beginning of a speech or data fragment, and is repeated during the voice call to overcome lost packets during voice communications and to allow late entry of E2EE group calls. As soon as the synchronisation frame is properly received, the voice and data can be decrypted, even when subsequent synchronisation frames are lost.

E2EE key management is executed from an E2EE Key Management Centre (KMC) by exchanging binary messages with the E2EE encrypted radio. E2EE key management functions include:

- Loading new management and traffic keys in the E2EE equipped radio;
- Query the status of keys;
- Associate E2EE traffic keys with one or more groups;
- Remote stun of a radio (like remote disable and enable);
- Act on an E2EE registration message received on power-up of a radio (query status or load outstanding keys that could not be delivered before).

As described in SALUS Deliverable 5.1 [4], the precondition for remote key management is the programming of a Key Encryption Key (KEK) in the PMR radio. This KEK is used to decrypt the Over-The-Air-Keying (OTAK) messages for transferring new keys and retrieving the status of keys.

A large secure storage area within the radio is reserved for Traffic Encryption Keys (TEKs). Every TEK is associated with one or more groups to provide secure group communications with only those radio users that have received the TEK; all other users can select the group, but cannot listen to the group communication.

Three versions of each TEK are stored; the current version is used by default, the past version is used as backup for radios that have not received the current key, and the future key can be loaded in advance, allowing to switchover to the new key in future.

5 INTEROPERABILITY AND INTERWORKING ASPECTS

SALUS addresses interoperability in two ways. First, the SALUS solution must be agnostic towards the choice of mobile and fixed IP networks to enable both standard PMR and broadband PPDR applications on top of these networks. Secondly, SALUS must support interoperability of PMR functionalities across legacy PMR and PMR-over-LTE networks.

5.1 Interoperability with IP networks

Today, availability of mobile and fixed IP networks is almost ubiquitous. However, constraints are applicable that may affect usability of these IP networks. These constraints must be considered for the design of the SALUS system architecture and protocol for delivering PMR services on top of these IP networks.

5.1.1 Support of IP multicast

IP multicast is an excellent method to distribute group-addressed voice, data and video, while the principle of operation is very similar to the PMR group call concept, allowing the support of hundreds or even thousands of radios in the same group.

IP multicast is widely supported by carrier and enterprise grade fixed and wireless (Wi-Fi) IP switching and routing equipment. IP multicast is also supported in LTE eMBMS architecture [7] but not in unicast service. For LTE two different options exist to support group-addressed voice, data and video services as defined in the Group Communication System Enabler specification [9]:

- Use MBMS bearer service;
- Use unicast bearer service.

In [9], a Group Communication application server maintains two set of interfaces: SGi, Rx for users addressed with unicast and MB2 for PPDR users address via MBMS. To enable this functionality in the interim phase, the gateway to the LTE network must support the mechanisms to route the data to the most appropriate service (user and control plane) that is available for group-addressed voice, data and video transfer.

As a fall-back solution, it is also possible to deliver the data by means of IP unicast streams.

5.1.2 Limited bandwidth

Limited bandwidth is especially a concern when distributing high bandwidth data and video streams over LTE networks, or carrying voice and data over low bandwidth IP networks like satellite links.

A number of options exist to cope with this limitation:

- The appropriate Quality of Service level may be requested or provisioned for the type of service. For example, voice transmission can be assigned the highest priority in order to ensure continuity above file transfer, which is less time critical compared to voice transmission.
- Bandwidth may be reserved for specific purposes. This allows bandwidth management by the application server, enabling resource queuing and pre-emption of calls when bandwidth is not sufficient.

More generally, it is advised that PPDR organisations make use of a managed IP network to interconnect their applications and telecom equipment. An approach based on IP/MPLS usually provides the necessary tool box to manage QoS end-to-end based on services to ensure high level of reliability, resiliency and robustness to multiple network failure events for at least the most critical services.

It is also advised to have consistent setting of QoS between the different domains (IP/MPLS, LTE...) to ensure proper end-to-end behaviour of the services. For instance voice service over LTE (usually QCI = 1) shall be transported on IP packets with Express Forwarding (EF) traffic class.

5.1.3 High delay links

IP links with high delay can be present in various scenarios. Examples include VPN links over low-bandwidth Internet connections to enable secure gateways between networks, and transport of IP over satellite links to interconnect fast deployable PMR systems to national or regional PMR networks.

The PMR-over-LTE services must be able to cope with high delays, providing acceptable user experience in terms of call setup, Push-to-Talk response and voice delay.

5.1.4 Packet drops

Because of the real-time aspect of PMR voice services, the use of TCP is not encouraged since due to its inherent flow control and retransmission techniques, it may result in varying call setup and speech delays, as well as late recognition of failing connections.

The alternative use of UDP is mostly preferred for VoIP, but can also be used for signalling when proper measures are taken to ensure reliable call setup, maintenance and teardown.

5.1.5 Network roaming

One of the key requirements for delivering PMR-over-LTE services is the option to use a mix of both public and private LTE networks. In addition, Wi-Fi hotspots as well as other application specific proprietary wireless IP technologies may be considered.

This requirement can be addressed by allowing the PMR client application to seamlessly switch between different IP networks, whereby the IP address and subnet mask can change at any time.

5.2 Interworking with legacy PMR networks

The following table provides an overview of PMR-over-LTE services, whether or not interoperability is applicable for TETRA and TETRAPOL, and must be considered for the gateway for legacy PMR networks, SALUS solution and the PMR-over-LTE protocol. The five columns in the table are defined as follows:

- The information in the TETRA column specifies whether the functionality is defined by the TETRA standard;
- The information in the TETRAPOL column specifies whether the functionality is defined by the TETRAPOL standard;
- The "Gateway function" refers to the support of the functionality for interworking with legacy PMR networks with the SALUS solution;

- The "Solution function" refers to the support of the functionality for interworking with the SALUS solution as a whole;
- The "Protocol function" refers to the support of the functionality for the definition of the voice, data and signalling protocol used within the SALUS solution.

Table 4 - Interoperability with legacy PMR networks

Functionality (SALUS naming)	TETRA	TETRA-POL	Gateway function	Solution function	Protocol function
Group Call	Yes	Yes	Yes	Yes	Yes
Group Attachment	Yes	Yes	Yes	Yes	Yes
Broadcast Call	Yes	No	Yes	Yes	Yes
Individual Call	Yes	Yes	Yes	Yes	Yes
Talking Party Identification	Yes	Yes	Yes	Yes	Yes
Call Identification	Yes	Yes?	Yes	Yes	Yes
Late Entry	Yes	Yes	No	Yes	Yes
Priority Call	Yes	Yes	Yes	Yes	Yes
Pre-emptive Priority Call	Yes	Yes	Yes	Yes	Yes
Emergency Call	Yes	Yes	Yes	Yes	Yes
Speech Item Priority	Yes	No	Yes	Yes	Yes
Tactical Patch	No	No	No	Yes	No
Dynamic Regrouping	Yes	Yes	Yes	Yes	Yes
Telephony Call	Yes	Yes	Yes	Yes	Yes
Barring of Incoming Calls	Yes	-	No	Yes	No
Barring of Outgoing Calls	Yes	-	No	Yes	No
Call Authorised by Dispatcher	Yes	Yes	No	Yes	No
Include Call	Yes	Yes	Yes	Yes	Yes
Call Forwarding	Yes	Yes	Yes	Yes	Yes
Call Transfer	Yes	Yes	Yes	Yes	Yes
Ambient Listening	Yes	Yes	Yes	Yes	Yes
Discreet Listening	Yes	-	Yes	Yes	No
Status Messaging	Yes	Yes	Yes	Yes	Yes
Text Messaging	Yes	Yes	Yes	Yes	Yes
Binary Messaging	Yes	-	Yes	Yes	Yes
Location Reporting	Yes	-	Yes	Yes	Yes
Authentication	Yes	Yes	No	Yes	Yes
Mutual authentication	Yes	Yes	No	Yes	Yes
End to End Encryption	Yes	Yes	Yes	Yes	Yes
Enable disable	Yes	Yes	Yes	Yes	Yes
Permanent disable	Yes	Yes	Yes	Yes	Yes

6 CONCLUDING REMARKS

An extensive analysis is made of existing PMR services to be provided on top of broadband LTE networks. In this deliverable the legacy PMR services were analysed, including interworking aspects that are required for heterogeneous solutions whereby users can be operating in both legacy PMR networks as well as within public and private LTE networks. Interworking is also critical to support gradual migration from legacy PMR to PMR-on-LTE. The described PMR services are generic enough to support interworking with both TETRA and TETRAPOL networks.

The final PMR-over-LTE services definition will be provided in deliverable D6.5, and will include enhanced PMR functionality that is enabled by the mobile broadband capabilities offered by LTE. This includes the features and capabilities that are offered in state-of-the-art proprietary and standards-based solutions. Where possible, the implementation will follow the definition of the upcoming standards.

BIBLIOGRAPHY

[1] SALUS Deliverable 2.1 “SALUS PPDR use cases – Intermediate”, November 2013.

[2] SALUS Deliverable 3.1 “System requirements, Enterprise Architecture and methodology”, version 1.2, March 2013

[3] ETSI Technical Report ETR-300 1 "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Designers' guide; Part 1: Overview, technical description and radio aspects", May 1997

[4] SALUS Deliverable 5.1, “Security and privacy analysis of TETRA / TETRAPOL, PPDR, LTE and Wi-Fi networks”, August 2014

[5] SALUS Deliverable 5.2, “PPDR Security Architecture, end-to-end security, privacy mechanisms and intrusion detection approach- Intermediate”, January 2015

[6] SALUS Deliverable 7.1, “SALUS PPDR platform – Intermediate”,February 2015

[7] 3GPP TS 22.179 v1.0.0, Mission Critical Push to talk (Release 13), September 2014.

[8] 3GPP TS 23.246, Multimedia Broadcast/Multicast Service (MBMS); Architecture and functional description, v12.4.0, December 2014.

[9] 3GPP TS 23.468, Group Communication System Enablers for LTE (GCSE_LTE); Stage 2, v12.3.0, December 2014.

[10] 3GPP TS 23.303, Proximity Based Services (ProSe), v12.3.0, December 2014.

ACRONYMS

3GPP	3rd Generation Partnership Project
AES	Advanced Encryption Standard
AIE	Air Interface Encryption
AL	Ambience Listening
BAU	Business As Usual
BIC	Barring of Incoming Calls
BOC	Barring of Outgoing Calls
C2	Command and Control
CAD	Call Authorised by Dispatcher
CCC	Command and Control Centre
CCTV	Closed Circuit Television
CFB	Call Forwarding on Busy
CFU	Call Forwarding Unconditional
CFNRc	Call Forwarding on Not Reachable
CFNRy	Call Forwarding on No Reply
CI	Call Identification
CT	Call Transfer
DGNA	Dynamic Group Number Assignment
DL	Discreet Listening
DMO	Direct Mode of Operations
DTMF	Dual Tone Multi Frequency
E2EE	End to End Encryption
eMBMS	Evolved Multimedia Broadcast Multicast Service
ETSI	European Telecommunications Standards Institute
EUTRAN	Evolved Universal Terrestrial Radio Access Network
GPS	Global Positioning System
GCSE	Group Communications System Enabler
IC	Include Call
ICT	Information and Communication Technology
IMS	IP Multimedia Subsystem
IP	Internet Protocol
IT	Information Technology
KEK	Key Encryption Key
KMC	Key Management Centre
LE	Late Entry
LIP	Location Information Protocol
MBMS	Multimedia Broadcast Multicast Service
MCPTT	Mission Critical Push To Talk
MOS	Mean Opinion Score
MPLS	Multiprotocol Label Switching
LTE	Long Term Evolution
OTAK	Over The Air Keying

PAMR	Public Access Mobile Radio
PC	Priority Call
PMR	Private Mobile Radio
PPC	Pre-emptive Priority Call
PPDR	Public Protection and Disaster Relief
ProSe	Proximity Services
PTT	Push To Talk
QCS	QoS Class Identifier
QoS	Quality of Service
RUA	Radio User Assignment
SDS	Short Data Service
SMS	Short Message Service
SS	Supplementary Service
TCP	Transmission Control Protocol
TEK	Traffic Encryption Key
TETRA	Terrestrial Trunked Radio Access
TL	Transport Layer
TPI	Talking Party Identification
UDP	User Datagram Protocol
UE	User Equipment
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
Wi-Fi	Wireless Fidelity