PUBLIC SAFETY NETWORK
TE KUPENGA MARUTAU

Public Safety Network
Appendix 4.3
Services Guidelines
Digital Land Mobile Radio

Contents

1. Introduction 3
2. Document Purpose 3
3. Services Scope 3
4. Services Outline 3
4.1 Public Safety Communication Service 3
4.1.1 Features and Functions 4
4.1.2 Performance Characteristics 9
4.1.3 Multi-Tenancy 10
4.1.4 Management Functions 11
4.1.5 Interworking with MCPTT 11
4.1.6 Communications Centre Voice Control Software 12
4.1.7 Communications Recording 13
4.1.8 Integration 13
4.1.9 Devices and Accessories 14
4.1.10 Service Provisioning and Assurance 15
4.1.11 Voice Quality 15
4.1.12 Coverage 16
4.2 Architectural Principles 17
4.2.1 Single Standardised LMR System 17
4.2.2 Underlying Network Flexibility 18
4.2.3 Application Programming Interface (API) 18
4.2.4 Configuration Management 18
4.2.5 Access Management 18
4.2.6 Compliance 19
4.2.7 Resilience/Redundancy 19
4.2.8 End-to-End Encryption 20
4.2.9 Loose Coupling 20
4.2.10 Continuous Development 20
4.2.11 Batteries and Standby Power 21
Appendix One. Regional/District Autonomy 22
Fire and Emergency Districts 22
Police Districts 23
St John/WFA Districts 23

1. Introduction

The Public Safety Network (PSN) programme is an Emergency Services initiative on behalf of Fire and Emergency New Zealand (Fire and Emergency), New Zealand Police (Police), St John New Zealand (St John), and Wellington Free Ambulance (WFA). The PSN programme is tasked with delivering Mission Critical communication services to the Emergency Services sector.

This document should be read in conjunction with the *Appendix 1. Service Requirements* document.

2. Document Purpose

This document is one of a set of Services Guidelines which outlines the network services required for the successful delivery the PSN and should be read as a guide (except where items are specified) for potential suppliers to propose their own solutions for PSN's requirements.

3. Services Scope

One of the most fundamental communications capabilities to be delivered by the PSN is the Land Mobile Radio (LMR) capability. This will replace existing LMR services for Emergency Services agencies that currently provide one of the primary mechanisms for dispatching and managing frontline resources in the field. The LMR capability will enable voice, messaging and location services for each agency.

The LMR coverage area will exceed cellular coverage, so it will be the primary communications technology outside cellular coverage areas. Inside cellular coverage areas, agencies will be able to make use of either technology. The primary technology can differ per agency and/or per use case and will likely change over time as the services evolve, and as each agency's use of technology evolves.

This document focuses on the LMR capability and includes references to interworking with Mission Critical Push-to-Talk over Cellular (MCPTT) and messaging systems.

As the devices and any accessories used to access the LMR capability are essential to the end-user experience, these are mentioned, but are not an exhaustive discussion on the topic in the entire PSN context. Supporting areas such as SLAs and coverage are all covered in other documents, as is MCPTT itself. The LMR service may include terminals as part of the offering.

4. Services Outline

4.1 Public Safety Communication Service

A public safety communication service is, in its simplest form, a half-duplex voice service where one person speaks at a time while all other members of the group are able to listen in real-time. The 'group' is sometimes referred to as a 'channel' or 'talkgroup' and the words are used interchangeably in this document. LMR applications can also use narrowband data (aka messaging) communications (e.g. status or pre-defined messages, Radio-ID or Alias), and location (i.e. GNSS). LMR applications will also be able to take advantage of location information relating to end-users and end-user devices.

There are a number of features and functions that are often used to enhance the user experience and a non-exhaustive list of these is included in Section 4.1.1 below. Many of these are standard LMR feature sets, however the list may also include PSN specific needs.

Public Safety features as they relate to LMR will follow their respective standard(s) as they apply to the technology (e.g. Telecommunications Industry Association (TIA) and European Telecommunications Standards Institute (ETSI)). These are features that enable access to, and performance of, the LMR service despite the environment in which they are operating. There are also features relating to enhanced capability by devices.

4.1.1 Features and Functions

The following table summarises the set of features expected to be available from the LMR service. These are all features that are of interest to Emergency Services. There is a mixture of talkgroup, device and Communications Centre console features in this table, as well as high-level integration, management, and security functions. This is not an exhaustive list.

Feature	Description
Group Call	Make a one-to-many voice call to all users affiliated to the same talkgroup. Talkgroups can be network connected or off-network. Talkgroups can be agency-specific or cross-agency.
Agency Group Call	Make a voice call to all users within an agency affiliated to the system.
System Call	Make a call (Voice or Data) to all users affiliated to the system.
Multi-Agency Talkgroup	Ability for authorised users to create a talkgroup that spans agencies.
Unit-to-Unit Call	Authorised users make calls directly with another user on the LMR system, irrespective of the current talkgroup, and is not heard on the currently selected talkgroup.
Caller-ID	Sender identification is available to other members of the talkgroup.
Go-Ahead Confirmation	Confirmation (usually via tone) that the channel is free to talk on, and the user who has pressed the PTT button has the right to transmit and will be heard by all others in the group. Any other users (with the exception of the dispatch console) that attempt to gain access will receive a blocked tone and be unable to transmit (a.k.a. floor control).
Call Queuing	Call requests queue when the system is busy and subsequent call-back when system resources become available.
Duress (Emergency) Alert	Sends a priority data message with Global Positioning System (GPS) or other GNSS service, and location co-ordinates advising that the user is under duress. Can be configured to open the channel for a set amount of time.

	Can also send this message to all agency's users within a surrounding area irrespective of channel for increased response from nearby units.
Call-back Messages	Ability to alert a user to contact the sender when available.
Pre-emption for Dispatchers	Dispatchers (or another authorised user) able to pre-empt the user that currently has the channel open (the floor) and the user that was pre-empted is advised (usually via a tone) and returns to listen mode. Several levels of priority that can be set on a per device type or interface level would be of interest. For example, the primary dispatch console always has the highest priority, but a back-up might be higher than a terminal but lower than the primary console.
Narrowband Data and/or Status Messaging	Send messages to nominated devices (fixed) or user selectable (ad hoc) and provide confirmation of successful transmission. Example of this would be to advise of a status update or a request for a voice call. For further details, see 'Messaging' section 4.1.1.1 below.
Packet Data Services	Support low speed data services. Examples of this would be free-form messages (similar to SMS), predefined messages (i.e. status) or standards-based data (i.e. GNSS, distress).
Priority Call Alert	Sends a data message to the relevant talkgroup console notifying the dispatcher of the urgent need to make a voice call if the talkgroup is busy.
Location Services	Ability for LMR terminals to send GNSS location data to all other terminals within an agency (or between agencies) for reporting, tracking, and staff safety.
Geo-fenced Talkgroups	Dynamic group membership based on location which alerts the users and gives the ability for the user to override any automatic changes or make those changes manually.
Remote Change of Talkgroups	Authorised users are able change a terminal's talkgroup affiliation over the air remotely and the user is notified (usually by a tone), and the screen display will adjust accordingly (if applicable)
Remote Monitoring of Terminals	Ability for authorised users to remotely open a user's transmitter. Depending on agencies' requirements this could be surreptitiously or by notification to the user.
Presence	Ability for authorised users to see the status of a terminal via a defined periodic and/or on demand 'poll/ping'. For example, this could be the user status, current talkgroup or location Period or on demand could be terminal or talkgroup specified

Remote monitoring by a Supervisor/Support	Remotely monitor a particular channel from a position outside the coverage area and Communication Centres.
Direct Mode	Ability for devices to communicate directly to each other (device dependent), when the LMR network is unavailable or as part of normal agency operation.
Isolated Operations Fall-back	Similar to Direct Mode, this is the ability to make an LMR call via a base station in an area isolated from any wider network. This relies on support from the base station. This could be a capability of an existing base station/site as a resiliency strategy, as well as a portable deployable base station/site for this specific purpose.
Minimum Capacity	Capacity for normal business operations for each agency and have surge capacity when needed. To ensure that during normal business operation that an agency's Group Call proceeds uncontested and is received by all members subscribed to that talkgroup.
Surge Capacity	Additional capacity above the minimum capacity for unplanned significant events that require additional talkgroups over and above the normal business operations without impacting those normal business activities.
Talkgroup Prioritisation	Talkgroups are able to have a priority level set individually. Talkgroups with a higher priority are able to pre-empt ongoing calls where talkgroups have a lower priority. Pre-emption shall be in the order of lowest priority.
Talkgroup Queuing	Talkgroups of equivalent priority will queue if capacity is insufficient and will notify the user. Talkgroups with higher priority will be front of the queue.
Uncontended Talkgroups	Talkgroups that never queue due to activity on other talkgroups.
Integration	
Dispatch Integration	Integration of LMR into a dispatch environment that utilises an agency's existing radio dispatch capability but may evolve into future technologies to leverage additional features and capability.
CAD Integration	Interfaces to enable access via Computer Aided Dispatch (CAD) tools to exchange information with the LMR system including emergency functionality, meta-data (radio-ID and location) and sending or receiving status messages.
Interworking	Seamless interworking available between nominated cellular and LMR talkgroups where required. Dispatcher selectable interworking available between agency Cellular and LMR talkgroups where required.
Management	

Administration	Real-time administration of talkgroups and terminals including addition, removal, combining and membership additions and deletions.
Inhibit/Un-inhibit	Temporarily disable and re-enable a terminal via a command over the LMR service to meet an agency's security requirements. Confirmations of a successful or unsuccessful message is presented to the user.
Dynamic Talkgroup (linking)	Combine multiple talkgroups in an operational situation to appear as a single talkgroup without detriment to the network, the operation of the network, or user functionality. Dynamic talkgroups can be across multiple agencies as authorised.
Dynamic Talkgroup Coverage	Reduce and increase coverage (sites) available for any given talkgroup in an operational environment without the need to program the terminal.
Over the Air Programming (OTAP)	Program and manage terminals over the air and/or wire. That can be via an Enterprise Network, internet or the LMR service.
Terminal Configuration	Manage non-LMR Service Provider features as required. Can be functionality such as non-network talkgroups and audio interfacing. Service shall be local (directly connected) and/or over the air.
Roles	Different roles need to be defined that include the ability to restrict access to specific talkgroups, listen-only, as well as restricted access to administration functions, and specific sets of administration functions.
Force Terminal Deregistration	Ability for authorised users to remotely force a terminal off the network.
Voice Recording	All communication on a channel with time/date stamping is securely recorded for later review and evidential purposes as required. Caller ID recorded where available.
Recording Review	User-friendly search and playback of recorded communications for authorised users.
Logging	Usage and statistics for LMR transactions. Examples include successful and failed group calls, authentication, site access tracking.
Security	
General	Service must comply with agency-specific information security and system policies and, where appropriate, any relevant New Zealand Information Security Management (NZISM) and Protection Security Requirement (PSR) guidelines and policies.

Multi-Tenancy	All subscribing agencies must be able to administer and use their own LMR services as completely distinct tenancies with complete autonomy and security between them. Any multi-agency functions must be explicitly authorised.
Authentication	All access must be authenticated, with agency-based access.
User Profiles	Different profiles for agencies must be available.
Encryption	End-to-end encryption of all traffic within the talkgroup, all administration traffic, and any data at rest. Encryption standards will align with New Zealand Information Security Manual (NZISM) standards in conjunction with the agency's security level requirement to ensure confidentiality and integrity of transmission. Where talkgroup spans different level requirements, where possible the higher level shall be used.
Key Changes	Ability to use a physical device connected to the terminal to regularly update cryptography keys and option for agencies to hold these.
Over the Air Rekeying (OTAR)	Ability to change/modify the encryption keys in the terminal device over the LMR service.
Managed Service	Service must be actively monitored and managed for service availability, performance, currency as well as proactive security protection. Full change management, incident management and cyber response must be in place for this service. See *Appendix 4.5 Services Guidelines Transparent Network Management.*
Denial of Service	Denial of Service prevention must be in place.
Intrusion Prevention	Intrusion Prevention Service must be in place to detect and prevent unauthorised access.
Security Operations	Security operations must be integrated with agency security operations.
Personnel Security	Service providers must have appropriate joining, moving and leaving processes to limit system access. Authorised support personnel must be appropriately vetted by their employer.

4.1.1.1 Messaging

Human- and machine-readable messages (low bandwidth data) play an important role in Emergency Services operations and have the advantage that they can be sent via (LMR or other) lower bandwidth networks in locations where cellular broadband is not available. Messages are two-way and are as follows:

- Application to person (and vice versa):
    - Human-readable messages from CAD systems to alert and inform field staff and volunteers about an incident.

Currently, Police use broadband applications or SMS for personal messaging. Fire and Emergency, WFA and St John currently use a combination of network paging and SMS for personal messaging. The replacement personal messaging system should have:

- The coverage of the current pager network;
- The resilience afforded by using cellular (e.g. SMS) plus another network; and
- The ability to reply (not currently available via paging).

Fire and Emergency have plans to extend the use of a personal messaging application which works over cellular broadband, Wi-Fi and PSTN, but this is of limited use across beyond areas of cellular coverage. Both Fire and Emergency and St John currently utilise infill paging to supplement network paging, and some form of this (LMR or otherwise) could persist into the future.

- Duress alerts, call requests, predefined messages sent by people in the field to the CAD system.

- Person to person:
  - Human-readable messages sent between emergency services personnel, or between personnel and other operational or administration staff or third parties. Comments above relating to human-readable messages from CAD systems apply here as well.
- Application to application:
  - Remote automation triggered from the CAD system, such as turning on a siren or opening a door; and
  - Information automatically sent to the CAD system, such as vehicle or device location, or station alarms.

4.1.2 Performance Characteristics

Performance-related metrics must fully support or exceed agency requirements, and where possible be standards-based.

Performance characteristics such as the following should be considered:

- Access Time;
- Access Time (during an Emergency);
- End-to-End Access Time;
- Mouth-to-Ear Latency; and
- Late Call Entry Time.

The 3GPP standards TS 22.179 and TS 23.283 should be considered to ensure that the MCPTT and LMR performance characteristics are compatible with the Interworking Function (IWF) as described in Section 4.1.5. Actual measures for performance characteristics will be defined at a later date.

Performance standards shall support or exceed the TIA specifications. In some cases, the agencies' requirements differ from the standards and these figures are addressed in the PSN Service Requirements. Actual measures for performance characteristics are defined in the PSN Service Requirements and will be refined at a later date.

These parameters shall be achieved irrespective of traffic demands from users on any part of the LMR system and irrespective of network backhaul delays.

Traffic modelling shall take into consideration the agency's command and control structure and assume that the mostly heavily used talkgroups will have a dispatcher. For scale of perspective, it should be assumed that all users in a talkgroup area for a particular agency will be communicating with the same dispatcher. Refer PSN Service Requirements Appendix One for 'talkgroup areas'.

For a scale of perspective, any given talkgroup, peaks rarely exceed 40 minutes talk time per hour, with the average for primary talkgroups sitting around 20 minutes talk time per hour. Uncontended talkgroups will allow any level of talk time in a given hour.

Another lens on capacity is the total numbers of operational personnel and vehicles as follows:

Agency	Operational Personnel	Vehicles	Locations
NZ Police	10,000	3,700	380
Fire and Emergency NZ	14,000	2,100	700
St John	5,000	750	300
Wellington Free Ambulance	400	70	30

It shall be noted that operational personnel, vehicles, and locations should be combined to form an overall count as each section may have its own device. For example, two Police officers in a vehicle may have three LMR devices in total.

Operational personnel counts above do not consider individual agency shift patterns, so the theoretical maximum number of officers using the service at any given time will be lower. However, consideration shall be taken into events that require additional personnel in certain circumstances (i.e. natural disaster, terrorism, big planned events).

4.1.3 Multi-Tenancy

Agencies must be able to administer their own terminals and talkgroups including, but not limited to, adding and removing terminals, modifying privileges, adding and removing groups, adding and removing members and geo-fencing. Appropriate administrator roles will be required to allow this capability to be restricted to authorised users only.

Agencies should not be able to view or edit talkgroups from another agency, however there is a use case for multi-agency talkgroups (e.g. 'liaison' talkgroups) and this capability again must be manageable from within each agency (by authorised users). An example is a major road traffic accident or in times of significant disaster (i.e. earthquake, where all Emergency Services are responding and the ability for those located at the scene to access a localised talkgroup may be beneficial.

4.1.4 Management Functions

Management functions for authorised users within an agency are required. Specific authority for dispatchers will be required, including flexibility to assign different functions on a per user basis. Examples of the different types of management functions include:

- Adding/removing terminals;
- 'Polling' terminal status;
- Modifying user talkgroups;
- Changing user privileges;
- Changing features of users in specific groups;
- Combining and splitting talkgroups;
- Adding/removing users in groups; and
- Reviewing recordings of talkgroup activity.

Access mechanisms from agency IT systems include:

- API from service provider into agency systems;
- Web-based Telco provisioning interface;
- VPN-based interfacing; and
- Manual access (phone, email etc.).

4.1.5 Interworking with MCPTT

The Inter Working Function (IWF) is defined in 3GPP Release 16 for connections between MCPTT systems and LMR networks. The IWF must support talkgroups spanning the different technologies including audio transmission, end-to-end floor control, emergency alerts, agency group calls, supported meta-data, secure connectivity and seamless access for all valid users. It must be scaled to meet requirements, which in practice likely means that there should be no limitation to how many talkgroups could be interconnected – the constraint should be on the networks, not the gateway. All IWF gateways should communicate using Internet Protocol (IP) connections native to the MCPTT and LMR standards on both sides of the gateway, unless the LMR network does not support IP as part of the interconnection (i.e. solution may be analogue as part of the transitional period).

The LMR technology solution shall be tested and certified against the 3GPP IWF standard(s).

Connectivity between the networks needs to be in multiple geographically separate locations for resiliency. Given that some LMR talkgroups are in specific regions only, this must also be catered for. Whilst the talkgroups can be trunked back over IP networks, interconnection within a region adds to the resiliency of that region and should be part of the design.

Standards-based interconnection between PSN LMR and MCPTT talkgroups must be considered in the initial design. Specific interconnection to legacy networks (Analogue FM and P25 Trunked) will need to be designed as part of transition.

There are specific use cases for connection to other (non-Emergency Services) networks and the architecture should be extensible to support this.

4.1.6 Communications Centre Voice Control Software

The Communications Centre Voice Control Software is a critical element of the LMR service. The Desktop Voice Control Software (or Console) is described as the system available at a dispatcher's (or other user's) desk to allow them access into the voice capability of an LMR system. The agencies are currently using the Instant Connect (previously Cisco IPICS) platform, but in two different environments (St John/WFA on one, Police/Fire and Emergency on another).

There are two separate approaches, which may both need to be supported during transition to a new LMR system and possibly be ongoing. These are:

1. Integration with the existing Instant Connect (v6.04 or appropriate upgrades) voice console in agency environments.
2. Provision of a new console.

These two approaches are outlined below in sections 4.1.6.1 and 4.1.6.2.

It should be noted that all agencies currently have a form of back-up console directly connected to the LMR system (either via an LMR terminal or 6-wire connection) in addition to a voice console system that resides in the agency network environment at their respective Communications Centres. This provides dispatchers access to voice capability to network talkgroups independently of the primary voice console system and to support local area network communications in the event of a complete console system failure. A similar model is expected to be retained under PSN.

4.1.6.1 Existing Instant Connect Voice Console

Integration with the existing console should include the maximum set of features that can be supported on both the LMR and Instant Connect platforms, including:

- Voice transmission with floor control;
- All required talkgroups;
- Priority override;
- Emergency alert;
- Agency group call;
- Terminal ID; and
- Remote monitoring.

Integrations will need to have appropriate capacity and resiliency to ensure no single point of failure can cause an outage to a Communications Centre.

It should be noted that the current LMR systems while providing dual connections into Instant Connect for backhaul redundancy also provides a redundancy system in the event that the Instant Connect system fails and the architecture will need to support this function.

4.1.6.2 Provisioning a New System/Console

PSN will offer a new voice control system for use in Communications Centres, which agencies may choose to take up. This should support full integration with the LMR and MCPTT systems and support all related features in an appropriate manner for use in the Communications Centre, in conjunction with the IWF in Section 4.1.5. The native support of all features and

functions in Section 4.1.1 above is expected to be delivered without a complex integration requirement. In this model, the console is simply a client of MCPTT system, and the LMR service is presented to the same console by the relevant LMR standards IP-based connection model.

This may be further down the transition path for some agencies as they leverage the richer features available and the MCPTT system itself matures and is expected to be a service capability available as and when needed.

4.1.7 Communications Recording

LMR voice recording is a critical element of the service and all voice communications operating through the service shall be recorded. PSN may choose to integrate into the agency's existing systems or provide a new system.

The current method used by all agencies is via a vendor product called Red Box. While the product is the same, the Police/Fire and Emergency Red Box is a separate system to that of St John/WFA and it is supplied by different vendors.

It is important to note that the current Red Box systems for each agency are integrated into both LMR and telephony systems (e.g PSTN and internal corporate functions).

LMR data (i.e. messaging) recording is of critical importance to the service and shall be made available to authorise agency users.

Voice and data recordings shall meet with the agencies storage and retrieval policies.

4.1.8 Integration

Integration of the LMR system with Computer Aided Dispatch (CAD) and other systems is required and to some extent CAD may need to integrate into either voice control system model above. Currently there are two different CAD software systems depending on the agency.

For all agencies today, processes for dispatchers are that voice is controlled via the Voice Console, and almost all other aspects to managing an incident reside in the CAD system. For example, LMR users often press a button requesting the dispatcher calls them, and in some cases this could be the emergency request. This request appears in CAD, even though it is sent over the radio network. The dispatcher then responds when they are able (prioritising their activities) through the Voice Console. Similarly, all alerting notifications and messages are sent from the CAD interface (by the dispatcher) regardless of how they may be delivered in the field (e.g. paging, cellular text, radio tones).

Therefore secure Application Interfaces, in line with the *Appendix 4.5 Services Guidelines Transparent Network Services* and *Appendix 4.3 Functional Guidelines Integration Current State*, must be made available so that the LMR features (beyond Voice) can be accessed via the CAD application (or any other system) rather than the Voice Console, should this be a requirement from an agency during transition or permanently.

It should be noted that as with the voice control system, agencies may require a form of back-up system directly connected to the LMR service in addition to the connection to the CAD system to allow redundancy in event of a complete loss of CAD function for messaging services.

4.1.9 Devices and Accessories

Given most use cases for LMR are in the field, the end-user experience is not only subject to the performance characteristics, but also the devices and accessories used to access the service. Usability and security are key to a fit-for-purpose service.

The user is required to use their hands, and keep their eyes up, and therefore lapel-mounted speaker-microphones, headsets, or other hands-free devices are critical to being able to access communications. In other circumstances, accessing the device directly may be appropriate.

Devices and their accessories will be expected to operate in a wide variety of situations where exposure to elements such as fire, wind and noise (e.g. machinery and concerts) are commonplace.

Users require the ability to easily and quickly change channels or volume while retaining situational awareness. Specific dedicated devices with physical buttons and knobs and with a simple screen may be appropriate for most cases. There are also devices that can access both cellular and LMR networks which may be appropriate for other use cases.

Where feasible, the device should be able to cover all frequency bands in use by the agency and work anywhere in the agreed coverage areas to limit the number of devices required and offer increased operational flexibility.

The key message is that the device and accessories eco-system for use with LMR is critical to the successful use of the service in the field, and may vary markedly between functional groups within agencies and must be considered at all stages of service design and evolution.

Further consideration will be given to devices in specific requirements and guidelines documents. These documents are not in scope of the network services procurement for the PSN communications capability.

4.1.9.1 Handheld Access

In most cases the device will be a form of ruggedised IP67 (or greater) handheld device attached to a belt or vest. Examples of cases where the device shall be fit-for-purpose include working in and around water (Fire and Emergency high pressure hose) or mud, biohazardous/hazardous environments, running/jumping with a high probability of dropping, and potentially situations where an Intrinsically Safe (or equivalent) device may be required.

Devices shall have the battery capability to last an agency's working shift. Typically, this will be no less than 12 hours operating on a 5-15-80% cycle (i.e. 5% of the time transmitting, 15% of the time receiving and 80% on standby).

4.1.9.2 In-Vehicle Access

A specific use case is in-vehicle access to LMR and a vehicle in this context could be road, air, or water-based. This could take several forms including, but not limited to:

- Hands-free access to the LMR PTT and mic via cable or Bluetooth (or equivalent) using in-car accessories.
- Dedicated hardware appropriate to the agency to be mounted in the vehicle. Includes voice user interface and interfaces for narrowband data consumers (e.g. routers supporting tablets).

- Interfacing to agency specific hardware services – this could be hardware such as Fire and Emergency messaging hardware or vehicle steering wheel controls.
- Interfacing to a safety helmet (motorbike), standards-based headset (helicopter) or audio integration platforms (avionics, specialised vehicles).

4.1.9.3 In-Station Access

Access from stations and other remote locations (i.e. Hospital, Parliament, and Traffic Centres) is a use case for either dedicated hardware (e.g. an LMR terminal on the desk or audio distribution from a server type room) or via other end-user devices such as tablet, laptop, Fire and Emergency/Ambulance turnout console or desktop. Options available should include both privacy capability (i.e. headset) or open speaker (programmable) as these devices could be located at shared desks, open common areas, or other supervisory or administrative locations that require access from time-to-time. This is often listen/read only, but not always. Robust in-station access is important for locations that may not have desktops but require on-station access to LMR from time-to-time.

4.1.10 Service Provisioning and Assurance

It is important for the LMR service to be a complete service with a robust provisioning and assurance processes. The agencies' and the service provider's processes can be integrated for complete end-to-end delivery. The LMR service's processes may also need to integrate with other service provisioning such as a device (e.g. various types of audio interfacing to distribution systems, or interfacing to applications for data capability). A user might also require a specific device type and/or accessory combination that needs to be provisioned and some profiles may require inter-working with the cellular MCPTT service or adopted for communications with allied agencies (non-emergency services).

Examples of personas or profiles include (for each agency, possibly with multiple variants):

- Dispatched frontline emergency services workers;
- Non-dispatched operational staff (i.e. Support Units, Courts);
- Covert or specialist type workers (Armed Offenders, Surveillance, Diplomatic/Witness Protection etc.);
- Dispatchers;
- Agency administrators;
- Vehicles (car, truck, motorcycle, helicopter, boat);
- Agency's internal or contracted service providers (e.g. vehicle maintainers); and
- Limited access for third party or external support staff

4.1.11 Voice Quality

Voice in both directions needs to be readable without repetition, including when high background noise is present around the person transmitting when devices are being used in the normal manner. Examples of normal manner could be in a vehicle with wind and siren noise, a person walking around with high background speech noise or inside a helicopter.

In terms of a Delivered Audio Quality (DAQ) a minimum of 3.4 (out of 5) shall be provided. The following methods shall be used where quantitative measurement of voice quality is required:

- TIA TSB88.1-E;
- TIA TSB88.3-E;
- ITU-T P.862; and
- ITU-T P.863,

4.1.12 Coverage

See separate document *Appendix 5.1 Functional Guidelines Coverage.*

4.2 Architectural Principles

The technical architecture for the LMR service will be defined by the Service Provider delivering the service, however there are some principles that are anticipated to ensure the service delivers appropriately to Emergency Services agencies. Figure 1 below shows an overview of key elements. The remainder of this section discusses the key principles defined to the minimum extent to indicate the intent.

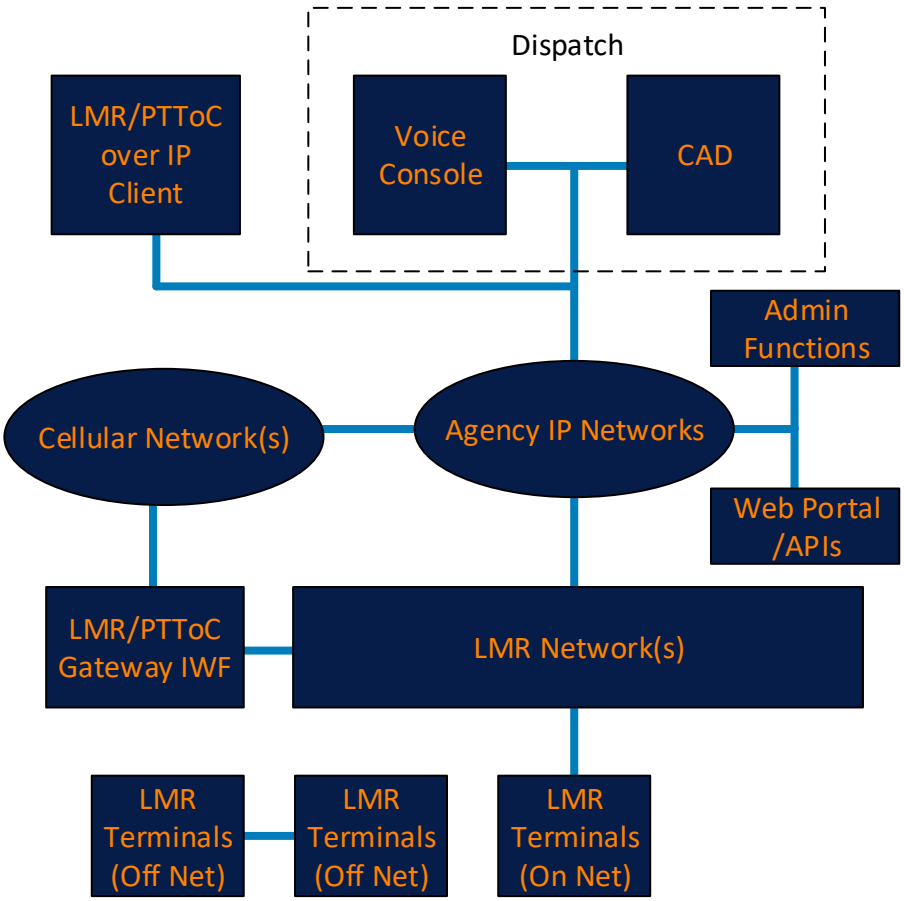

Figure 1: Overview of potential conceptual architecture

4.2.1 Single Standardised LMR System

Whilst it is expected that multiple technology networks will be used as the transport potentially from multiple suppliers, a single standardised LMR system is needed to ensure a seamless experience across all networks and for all agencies to enable inter-operability between users within an agency and between agencies.

The underlying networks (i.e. agency IP network) need to be aware of the LMR technology in use, or at least be aware of the demands on the network from a Quality of Service and other key performance services perspective. It is expected that the service provider will supply technical specifications for agency network and/or system configuration requirements.

A single standardised LMR system is required to ensure interworking between agencies (e.g. common talkgroups for multiple responding agencies at an incident). It is also imperative for

interworking with MCPTT networks, as anything other than a single standardised LMR system would add complexity from a gateway and Communications Centre perspective.

However, the LMR systems shall be broken down into interconnected regional-based systems to maintain capability for region or district autonomy in the event of a major disaster or significant loss of backhaul.

4.2.2 Underlying Network Flexibility

Private IP bearers such as in-station Wi-Fi/LAN/WAN are expected to support QoS and/or equivalent minimum network characteristics to enable a quality LMR experience where devices can use those connections, and these may be LMR-based devices or LMR supporting devices (e.g. Over the Air Programming - OTAP). Where an agency is using their own IP bearer the solution should outline what is required to meet the recommended and minimum requirements.

Where in-vehicle solutions have multiple network backhaul capability (e.g. cellular connections, satellite), and these are available to LMR terminals inside or near the vehicle, again this should support QoS and/or equivalent minimum network characteristics to enable a quality LMR experience. The LMR system shall consider the maximum speed at which an agency vehicle (Land, Sea or Air) may be travelling.

4.2.3 Application Programming Interface (API)

It is expected that the network providers will enable a web portal dashboard to provide agency access to the LMR admin function systems and Application Programming Interface (API) views of network status in real-time so any interruptions to service are understood and operational procedures can be adjusted accordingly. This will include visibility of planned work and associated service impacts. See *Appendix 4.5 Services Guidelines Transparent Network Management* and *Appendix 4.4 Services Guidelines Device and Application Management*.

4.2.4 Configuration Management

Provisioning and management of LMR devices on the network, as well as the management of the device configurations, are all requisite components of the PSN capability. Local management of devices is covered in a separate service guideline document due to the specifics in the device that are abstracted from the network. Remote management of devices shall work in conjunction with any local management. Refer to *Appendix 4.4 Services Guidelines Device and Application Management* for additional guidance regarding:

- Add, modify or remove devices from the network (including stun);
- Modification of the device configuration software and/or firmware;
- Modification of the encryption keys; and
- Monitoring and reporting the current state of the configuration.

4.2.5 Access Management

Remote access management services to LMR functionality and/or application APIs shall have a form of federated identity and access to provide common access policies to any system for simple and straight forward authentication for the agency users. The access management shall be such that changes to existing, adding new or removing exiting users is easily manageable, either internally to the agency or via request to the service supplier.

4.2.6 Compliance

Where required, the LMR system and all its components shall conform to all New Zealand standards and regulations, including but not limited to those outlined under the Radio Communications Act (1989) and the Radio Communications Regulations (2001). This includes but is not limited to the frequencies used and licensing, interference, and type approved terminals.

Where applicable, devices shall be compliant for their respective install. For example, Civil Aviation Authority (CAA) for aircraft and NZ Transport Agency (NZTA) for vehicles.

Agencies currently operate in the ES (Emergency Services) frequency bands as designated by PSRFMG (Public Safety Radio Frequency Management Group) for VHF and UHF, as well as the Commercial F bands for Analogue UHF.

The ES bands (ESA, ESB and ESC) are available to all Public Safety agencies which includes:

- Emergency Services (Police, St John, WFA, Fire and Emergency);
- Department of Conservation (DoC);
- National Emergency Management Agency (NEMA);
- Ministry of Business, Innovation and Employment (MBIE);
- New Zealand Customs Service; and
- New Zealand Defence Force (NZDF).

Any new buildings and towers accommodating the LMR network equipment, are required to comply with the NZ Building Code requirements to meet Importance Level 4 (IL4). This is a Building Code requirement for buildings that are essential to post-disaster recovery or associated hazardous facilities.

4.2.7 Resilience/Redundancy

A Public Safety Communications system needs to be highly resilient to fault, and as such shall have layers of redundancy and the ability to continue to operate in reduced modes of functionality.

Network resiliency shall be such that no device and/or system deemed critical to normal operation of the LMR service is impacted by an equipment or supplementary service failure. In the event this is not achievable any such failure of the service shall have alternative means to access the ‘lost’ functionality.

For example (but not limited to):

- A talkgroup can operate on any available capacity at a base station/site in the event of capacity lost;
- The Communication Centre interface system is geographically redundant with instantaneous failover that is seamless to the user but has alerted them;
- LMR talkgroup access shall be available from any authorised control system so that if a communication centre were to fail an alternative location is able to instantly take over;
- Linking between LMR base stations within districts should be independent of cellular infrastructure; and

- The core (i.e. RFSS) infrastructure and any aggregation nodes (i.e. IWF) are geographically redundant with instantaneous failover.

Additional context to this follows in Appendix One.

4.2.8 End-to-End Encryption

End-to-end encryption (E2EE) is required for all LMR traffic. Whilst this is fairly self-explanatory over an IP network, there are architectural considerations when the network paths traverse networks of different security postures, and more explicitly which endpoints are capable of decrypting the traffic. Examples include end-clients on trusted agency networks, end-clients on public networks, recording interfaces, servers and gateways. Each of these endpoints must be capable of encrypting and decrypting the traffic.

Consideration shall be taken where communications capabilities operate between technology types (i.e. LMR and MCPTT). E2EE is, when utilised, able to operate seamlessly between technologies. More explicitly if E2EE is utilised, encryption/decryption should be carried out in the respective end-clients to avoid the need to transcode within the networks. This is to ensure information integrity and best possible performance.

For any talkgroups that do not require E2EE, codec negotiation between LMR and MCPTT as per 3GPP TS 23.283 is preferred to eliminate any latency and potential call degradation introduced during audio transcoding.

Gateways and servers are particularly important as these will likely sit inside service provider networks and appropriate security controls will be required to ensure any decryption is authorised and necessary. Wherever possible, agencies should maintain control over access to communication.

4.2.9 Loose Coupling

There are multiple integration points including connections between LMR and the underlying networks, the Communications Centre Voice Console, CAD and MCPTT. The ability to separately maintain the lifecycle management of all of these systems is essential for maintainability and upgradeability. This also extends to administration and provisioning/ incident management processes and system interconnections. See document *Appendix 5.1 Functional Guidelines Integration Target State*.

4.2.10 Continuous Development

Continued development to maintain currency, supportability and provide access to modern features will be inherent within the LMR service. As per the previous principle, loose coupling is required to ensure that ongoing application lifecycle development does not impact on the other systems wherever possible. The extensive eco-system of devices and accessories must continue to be supported, but this is not expected to be a static environment, and ongoing development is to be inherent in the service delivery design.

Also important is that equipment and service lives for particular functions of the LMR service are sufficiently long to manage adverse impacts on users and agencies consuming the service. For example, onerous training requirements, vehicles out-of-service for equipment changes, excessive costs due to short lifecycles and having to source sub-optimal devices last-minute due to unplanned loss of support for in-service units. It is expected that regular dialogue is held between agencies, the PSN programme and service providers on the development of the service to allow timely planning and budgeting for future developments.

4.2.11 Batteries and Standby Power

Mains/Standby Power

Power supplies must be sufficient to keep the system operational during prolonged mains power outages and should be supplied from a combination of batteries, UPS units, and standby generators as follows:

1. There shall be a minimum of four (4) hours supply available from batteries at any site that has a standby generator (this allows four (4) hours to get the generator operational or deploy a replacement for the equipment).
2. There shall be a minimum of 10 hours supply available from batteries at a site without a standby generator and which is near to an engineering workshop (viz less than two (2) hours travel by road).
3. There shall be a minimum of 24 hours supply available at main sites without generators and which are further than two (2) hours travelling time from an engineering workshop (by road).
4. There shall be a minimum of 10 days of supply available at solar-powered repeater sites.

Note: It is assumed that 80% of the capacity of the battery calculated at the designed discharge rate of the power supply system is available over a period of 10 years.

Philosophy

The capacity of the batteries will depend upon circumstances, but the following guidelines should be adopted for battery capacities:

1. Battery capacities are calculated based on a discharge from fully charged to 50% charged, within manufacturer recommendations.
2. At mains-fed repeater sites there shall be a minimum of 24 hours of battery capacity.
3. At a solar and/or wind-powered repeater sites the capacity will be based upon local weather conditions.

Appendix One. Regional/District Autonomy

Section 4.2.1 notes the LMR systems shall be broken down into interconnected regional-based systems to maintain capability for region or district autonomy in the event of a major disaster or significant loss of backhaul.

Section 4.2.7 notes architecture principles of resiliency and redundancy, and this Appendix is to provide contextual information on how the agency regions operate.

The intention for using the sub-networks in such occasions would include the agencies setting up co-ordination centres to manage operations and assets in an area still able to use the local radio site(s) to communicate with each other. Traffic levels could be higher than normal during such occasions.

Terminals not in use in these areas prior to the sub-network beginning autonomous operation could be brought into use on the isolated sub-network. The system shall allow such terminals to operate on the isolated infrastructure once in its coverage area.

Access to each channel must be provided from the following locations (shown in the order of importance):

- Communications Centre;
- Alternative Communications Centre;
- District Emergency Room/Operations Centre; and
- Sub-area HQ (via LMR terminal only).

Fire and Emergency Districts

The LMR service shall provide 12* independent radio networks serving the following areas:

Area	Operations Centre Location
Northland	Whangārei
Auckland	Auckland (central city)
Waikato	Hamilton Thames
Bay of Plenty	Tauranga Rotorua
Eastern (Tairawhiti/Hawkes Bay)	Gisborne Hastings
Central (Taranaki, Wanganui, Manawatu)	New Plymouth Whanganui Palmerston Nth
Wellington (inc Hutt-Wairarapa)	Lower Hutt (Avalon) Wellington (central city)

Tasman (Tasman-Marlborough)	Nelson
Canterbury and West Coast	Christchurch Greymouth Timaru
Southern (inc Cen-Nth Otago, East Otago Southland)	Dunedin Queenstown Invercargill

Police Districts

The LMR service shall provide 12* independent radio networks serving the following areas;

District	District Emergency Room Location
Northland	Whangārei
Waitematä	Auckland
Auckland City	Auckland
Counties Manukau	Auckland
Waikato (inc Coromandel)	Hamilton
Bay Of Plenty (Rotorua/Tauranga/Taupō)	Rotorua
Eastern (Gisborne/Hawkes Bay/Napier)	Hawkes Bay
Central (Taranaki, Wanganui, Palmerston North)	Palmerston North
Wellington (inc Kapiti and Wairarapa)	Wellington
Tasman (Marlborough, Nelson and West Coast)	Nelson
Canterbury	Christchurch
Southern (Otago, Invercargill, Stewart Island)	Dunedin
Great Barrier Island*	Auckland

*Great Barrier Island has 2x radio sites (1x Police and 1x DoC) that are shared by all agencies and are only accessible from the Auckland Police Communications Centre via an LMR terminal

St John/WFA Districts

The LMR service shall provide 19 independent radio networks serving the following areas;

District	District Emergency Room Location*
Northland	Whangārei
Auckland North	Mt Wellington (AKL)

Auckland South	Mt Wellington (AKL)
Hauraki / Coromandel	Thames
Waikato	Hamilton
Bay of Plenty	Tauranga
Hawkes Bay	Napier
Taranaki	New Plymouth
Central region	Palmerston North
Wairarapa (WFA)	Masterton
Wellington (WFA)	Wellington
Nelson / Marlborough	Nelson
West Coast	Greymouth
North Canterbury	Christchurch
South Canterbury	Timaru
Dunedin	Dunedin
Invercargill	Invercargill
Central Otago	Queenstown
Auckland PTS	Mt Wellington (AKL)

Note: St John does not currently have a structure where communications fall-back to a single regional centre; locations are indicative of the largest station in the district; fall-back centre for actual deployment would be dependent on location of units being deployed and capability during a failure scenario