PUBLIC SAFETY NETWORK
TE KUPENGA MARUTAU

Public Safety Network Appendix 4.2 Services Guidelines Mission Critical Push-to-Talk (Cellular)

Contents

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 Push-to-Talk (PTT) capability. This will replace the existing Land Mobile Radio (LMR) PTT services operated by the Emergency Services agencies that currently provide one of the primary mechanisms for dispatching and managing frontline resources in the field.

The capability will initially be a mixture of a new, fit-for-purpose, digital LMR and Mission Critical Push-to-Talk (MCPTT) over cellular capability. MCPTT over cellular will potentially work on any IP network, although not necessarily in a Mission Critical manner. The LMR and MCPTT services will combine to provide a resilient service across agreed coverage areas throughout New Zealand. It is expected that 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 paper focuses on the MCPTT over cellular service only, but also includes interworking between MCPTT and LMR.

As the device and any accessories used to access the MCPTT 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 Service Level Agreements, Cellular Services and coverage are all covered in other documents, as is the LMR service.

4. Services Outline

4.1 Mission Critical Group Calling Service

The Mission Critical Group Calling 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. MCPTT applications include the capability to add other media to the communication, (e.g. sending text, links and pictures to the group, or even

escalating from voice to video). MCPTT applications also have the ability to add meta-data to communications, (e.g. timestamps, talker-ID, and location).

For clarity, the MCPTT service largely relies on the Cellular service, so where coverage is acceptable to support a voice service, MCPTT will work, and performance can be assured using the Mission Critical features on the cellular network. It can also work over other IP networks, but will be reliant on the performance of those networks. Deployable (including standalone) cellular capability will support MCPTT, albeit a limited service in the isolated mode.

There are a number of features and functions that are often used to enhance the MCPTT user experience and a non-exhaustive list of these is included in Section 4.1.1 below. Many of these were developed in the LMR domain to solve issues suffered by older deployments, and these have been adopted by providers for their MCPTT applications.

In Section 4.1.6, 3GPP Mission Critical features are discussed as they relate to MCPTT. These are features that enable uncontended access to, and guaranteed performance of, the MCPTT application despite other traffic that may be present on the cellular network. There are also features relating to enhanced location reporting by devices, and Proximity Services (ProSe) where devices can communicate directly with each other when they are in the same localised area.

4.1.1 Features and Functions

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

Feature	Description
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 user that attempts to gain access will receive a blocked tone and be unable to transmit (aka floor control).
Emergency Alert	Sends a priority status 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.
Pre-emption for Dispatchers	Ability for a dispatcher (or another authorised user) to pre-empt the user that currently has the channel open (the floor).
Call Queuing	Ability to queue a call request when the system is busy and subsequent call-back when system resources become available.
Caller-ID	Sender identification is available to other members of the talkgroup.
System Call	Ability to make an announcement to all users subscribed to the system.
Agency Group Call	Ability to make an announcement to all users within an agency subscribed to the system.

Multi-Agency Talkgroup	Ability for authorised users to create a talkgroup that spans agencies.
1-1 Calls	All group capability available in a direct user-to-user or unit-to-unit call.
Location Services	Attaching location data to a group member for reporting or tracking.
Geo-fenced Talkgroups	Dynamic group membership based on location.
Incident-specific Talkgroups	Dynamic group membership set up for users in a particular event, (e.g. a car crash where multiple services are attending).
Presence	Visibility of status of MCPTT client.
Group Send Files	Ability to send files and information such as images, maps, links and videos to all users on a MCPTT channel.
Push to Video	Adding video to a MCPTT channel.
Offline Recording	Ability to record a MCPTT call so an offline user can hear it when they come back online.
Remote Monitoring by a Supervisor/ Support	Agency configurable ability to remotely monitor a particular channel from a position outside the communication centres. This can include authorised users with BYO (Bring Your Own) devices.
Direct Mode	Ability for devices to communicate directly to each other (device dependent), when the terrestrial network is unavailable. This function relates to the application support of this capability (when the underlying device also supports it).
Isolated Operations Fall-back	Similar to Direct Mode, this is the ability to make an MCPTT call via a base station in an area isolated from any wider network. This relies on support from the base station, and likely requires hosting a specific instance of a MCPTT application as part of the base station. This could be a capability of an existing cell site or base station as a resiliency strategy, or it could be a portable 'private cellular' base station for this specific purpose.
Relay Repeated Mode	Ability of a device to relay communications from a device that is out of range of the base station to the base station. This extends the Local Repeated Mode.
Integration	
CAD Integration	Application Programming Interfaces (APIs) to enable access via Computer Aided Dispatch (CAD) tools to exchange information with the MCPTT system. Examples include meta-data (talker-ID and location) and sending or receiving status messages, but this could be taken further to exchange of files, maps images, or even presenting voice or video through the CAD interface.
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 including addition, removal, combining and membership adds and deletions.
Dynamic Talkgroup (linking)	Ability to 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.
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 Talkgroup	Ability to remotely force a user into the correct talkgroup.
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.
Review	User-friendly search and playback of recorded communications for authorised users.
Logging	Usage and statistics for successful and failed group calls.
Security	
Multi-Tenancy	All subscribing agencies must be able to administer and use their own MCPTT 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 role-based access control.
User Profiles	Different profiles for users must be available.
Encryption	End-to-end encryption of all traffic within the group, and all administration traffic. Where sessions may need to be decrypted/re-encrypted such as gateways, appropriate security controls will be needed. Encryption standards will align with New Zealand Information Security Manual (NZISM) standards to ensure confidentiality and integrity of transmission.
Key Changes	Ability to regularly update cryptography keys and option for agencies to hold these.
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.

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.

4.1.2 Performance Characteristics

Performance-related standards must fully support or exceed agency requirements, and where possible be standards-based, including the 3GPP TS 22.179 specifications regarding Key Performance Indicators (KPIs) for MCPTT as per the list below. The 3GPP standard is chosen to ensure that the MCPTT and LMR specifications are compatible with the Interworking Function (IWF) as described in Section 4.1.7. Performance standards not relating to these KPIs shall support or exceed the relevant 3GPP standards.

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

Where a standard exceeds the agencies' requirements, the standard will be the default. In some cases the agencies requirement may exceed the standard and these figures are addressed in the PSN Service Requirements.

Performance parameters shall be achieved irrespective of traffic demands from users on any part of the cellular system not subscribing to Mission Critical services and irrespective of network backhaul delays.

Note that the definition in section 6.15.3.1 of TS 22.179 does not completely capture agencies requirements. PSN requires KPI 2 to include all receiving users in a group[1] being connected and receiving the call.

Also note that 6.15.3-001 expresses the KPI measurements in scenarios "where there is negligible backhaul delay". PSN anticipates QoS to address any issues with backhaul in the New Zealand context.

For a scale perspective, it should be assumed that three to four primary talkgroups are required in each geographic area (areas not overlapping and typically aligning with 12-14 districts around New Zealand) for each service (Police, Fire and Emergency, St John or WFA In addition, special-purpose or ad-hoc talkgroups could be at any time up to 60 in each region.

[1] While operating within the network coverage area.

For 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.

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	14,000	2,100	700
St John	11,000	700	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 MCPTT devices in total.

Operational personnel above do not consider individual agency shift patterns, so the theoretical maximum number of personnel using the service at any given time will be much 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 Identity and Access Management

Identity and Access Management (IDAM) is the capability for authenticating who has access to MCPTT services, and what they are authorised to do. Authorisation is likely to be within the administration capability of the MCPTT service, so this section focuses on authentication.

There will likely be different identity types relating to the different types of access. The following types of identity have been identified:

- Person (individual identity);
- Role (e.g. shift manager);
- Vehicle (always associated with a specific vehicle ID); and
- Location (e.g. a station or hospital).

The identity store could be one of the following:

- Enterprise Directory and Policy (i.e. same sign-on as LAN access using technologies such as SAML or OAuth);
- Direct;
- Federated;
- Federated through an access provider;
- Non enterprise data store (e.g. Apple ID, Google ID);
- Dedicated MCPTT identity store; and
- SIM card.

In some circumstances (e.g. handheld devices), device access will most likely need to be handled separately from the application access. However, the two may be interrelated, for instance, once the application has been logged on at the start of a shift, accessing the device (e.g. through a PIN code, or proximity token/wearable) may be considered enough to access the application until it is logged out (or timed out) at the end of the shift.

In other circumstances (e.g. in-vehicle devices), the device access itself will imply access to the application.

Two-factor authentication will need to be supported for many use cases.

4.1.4 Multi-Tenancy

Agencies must be able to administer their own users and talkgroups including, but not limited to, adding and removing users, 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. Talkgroup names should be unique to each agency. Each agency can have a talkgroup that has the same name as a talkgroup in another agency, but the talkgroup is unique to their agency and not connected or conflicting with any other agency with a talkgroup of the same name.

Agencies should not be able to view or edit talkgroups from another agency, however there is a use-case for multi-agency talkgroups and this capability again must be manageable from within each agency (by authorised users). An example is a major road traffic accident where all emergency services are responding and the ability for those located at the scene to access a localised talkgroup is valuable.

4.1.5 Management Functions

Management functions for authorised users within an agency are required. Specific authority for dispatchers will be required, as well as the flexibility to assign different rights to different roles for administration functions. Examples of the different types of management functions include:

- Adding/removing users;
- Changing user privileges;
- Changing features of users in specific groups;
- Adding, modifying, combining, splitting and removing groups;
- Adding/removing users in groups; and
- Reviewing recordings of talkgroup activity.

Access mechanisms from agency IT systems include:

- VPN-based API from Service Provider into agency systems;
- Web-based Telco Provisioning Interface; and
- Manual access (phone, email etc.)

4.1.6 3GPP Mission Critical Standards

MC PTT over cellular broadband will be integrated with the network to fully support Mission Critical features. The primary examples are described below. See *Appendix 4.1 Services Guidelines Cellular.*

4.1.6.1 QPP

Quality of Service, Priority and Pre-emption (QPP) are capabilities provided by the underlying network and must be able to be leveraged appropriately for the MCPTT traffic flowing over the network. These functions are described in more detail in the Services Guideline: Cellular, but at a high level ensure access to the network when it is required, and ensure that the traffic is transported with appropriate latency, jitter and packet loss characteristics to ensure the application is usable in a high quality manner at all times. 3GPP Release 14 for cellular technologies is generally considered the minimum specification for these features from a standards perspective.

For the avoidance of doubt, effective QPP is essential for significant operational uptake of MCPTT services within Emergency Services, and is fundamentally a pre-requisite for agencies considering using MCPTT as their preferred voice dispatch tool for primary emergency response missions.

4.1.6.2 Enhanced Location

Enhanced location relates to specific features such as a higher regularity of updates for the GPS location of the end-device, and remote activation or retrieval of a device location.

4.1.6.3 Proximity Services

Proximity Services (ProSe) relates to the ability for the end-devices to:

- have a direct connection with each other for a MCPTT session if the terrestrial connection is not available, assuming they are close enough to form a connection and the devices both support this mode of operation – this can deliver voice/MCPTT, video and data; and
- share access to the terrestrial network (relay the session) if one device is within range and the other is not (but they can reach each other), again including voice/MCPTT, video and data.

4.1.7 Interworking with LMR

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 native IP connections on both sides of the gateway, unless the LMR network does not support IP backhaul (i.e. it is analogue).

The IWF gateway facilitates migration from existing LMR systems, as well as providing a fundamental element in the target state for PSN. Connectivity between the networks needs to be in multiple geographically separate locations for resiliency. Given that some LMR talkgroups

are in specific geographic areas only, this must also be catered for. Whilst the talkgroups can be trunked back over IP networks, interconnection within an area adds to the resiliency of that area 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 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.

The operational requirements for the gateway need to allow integration and automation with the primary provisioning of PTT Groups, number plans, etc. in order to avoid configuration errors and reduce reliance on manual provisioning overheads.

4.1.8 Communications Centre Voice Control Software (Console)

The desktop voice control software (or console) is the system available at a dispatcher's (or other user's) desk to allow them access into the voice capability of the MCPTT system, and how the Communications Centre uses this is a critical aspect for the overall MCPTT system. There are two separate approaches, which may both need to be supported during transition and possibly be ongoing. These are:

1. Integration with the existing voice control software in agency environments.
2. Provision of new voice control software as a part of PSN.

4.1.8.1 Existing Instant Connect Voice Control Software

Integration with the existing console voice control software should include the maximum set of features that can be supported on both the new MCPTT and the existing platforms (currently Instant Connect v6.04) that are used as two completely separate implementations (St John/WFA and Police/Fire and Emergency) including:

- Voice transmission with floor control;
- All required talkgroups;
- Priority override;
- Emergency alert;
- Agency group call;
- Caller 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. Integration must also consider the IWF function described in Section 4.1.7 to ensure a seamless end-user experience incorporating usability and resiliency.

4.1.8.2 Provisioning New MCPTT Voice Control Software

PSN will offer a new service for voice control software (console) for use in Communications Centres, which agencies may choose to take up. This should support full integration with the MCPTT system and support all related features in an appropriate manner for use in the Communications Centre, including chat, video, file attachment and other collaboration

functions common in modern MCPTT systems. The voice control software must also fully support integration with the PSN LMR system in conjunction with the IWF described in Section 4.1.7. 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 voice control software is simply a client of MCPTT system, and the LMR service is presented to the same voice control software 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.

4.1.9 Voice Recording

Voice recording is a critical element of the service. PSN may choose to integrate into the agency's existing systems or provide a new system, especially as there are many aspects in addition to voice (including meta-data and media) which MCPTT can support, and all of this will need to be recorded.

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 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 (e.g. 111, Service Desks) systems for multiple aspects of the organisation and it is recorded at an IP layer.

4.1.10 Integration

Integration with Computer Aided Dispatch (CAD) systems is likely to be required to some extent for either voice control software model above.

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, operational personnel often press a button requesting the dispatcher calls them. 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 Programming Interfaces (APIs) must be made available so that the MCPTT features (beyond voice) can be accessed via the CAD application rather than the voice control software, should this be a requirement of an agency during transition or permanently.

4.1.11 Devices and Accessories

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

In many cases, the interface will be an application that runs on a smart mobile device (with optional accessories) leveraging the network, application and a device's support of Mission Critical features to ensure end-to-end service quality. Where the user is required to use their hands, and keep their eyes up, lapel-mounted speaker-microphones or headsets are critical

to being able to access communications. In other circumstances, accessing the screen 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 an embedded app and a simple screen (or even no screen) may be appropriate for some use cases also. There are also devices that can access both cellular and LMR networks which may be appropriate for other use cases.

The key message is that the device and accessories eco-system for use with MCPTT apps is critical to the successful use of the service in the field 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.

4.1.11.1 Handheld Access

In most cases the device will be a form of ruggedised handheld device (or standard device in a ruggedised case) 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 other potentially dangerous environments.

Devices shall have the battery capacity to last an agency's working shift. Typically, this will be 8-14 hours of operation. There may be the opportunity to recharge in a vehicle or on-station, but this is by no means guaranteed, so a way to maintain battery life for this length of time while on duty is imperative.

4.1.11.2 In-Vehicle Access

A specific use case is in-vehicle access to MCPTT (both stationary and when moving). This could take several forms including, but not limited to:

- Hands-free access to the application on a cell phone via cable or Bluetooth (or equivalent) using in-car accessories;
- Use of a Mobile Data Terminal (MDT) with the application installed and using either the screen or other dedicated buttons (e.g. on the steering wheel), or voice prompts to control the communications;
- Dedicated hardware appropriate to be mounted in the vehicle;
- 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);

4.1.11.3 In-Station Access

Access from stations and other remote locations is a use case for either dedicated hardware (e.g. kiosk-style) or via other end-user devices such as tablet, laptop, or desktop. These could

be located at shared desks, 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 MCPTT from time-to-time.

The usability may be as simple as installing an application on an end-user device that can be used with a headset, but consideration of the usability under different scenarios needs to be made as part of the MCPTT service design and evolution.

4.1.12 Service Provisioning and Assurance

For the avoidance of doubt, it is important for the MCPTT service to be a complete service with robust provisioning and assurance processes. The agencies' and the Service Provider's processes can be integrated for complete end-to-end delivery. The MCPTT service's processes may also need to integrate with other service provisioning (such as a device), for instance, adding and remove users of different types, as well as for other profile types such as a vehicle deployment (e.g. with a tablet or specific in-vehicle device). A profile might also involve a specific device type and/or accessory combination that needs to be provisioned, or other requirements such as checking the connection/device for a user on their own device. Some profiles may require inter-working with LMR, some may not.

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

- Frontline emergency services workers;
- Volunteers (depending on role, may be the same as frontline);
- Dispatchers;
- Agency administrators;
- Vehicles;
- Other sub-contracted users (e.g. helicopter crews); and
- Service agents.

4.1.13 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 mean opinion score (MOS), a minimum of 3.5 (out of 5) shall be provided. The method described in the ITU-T P-863 shall be used where quantitative measurement of voice quality is required.

4.1.14 Other Users

There are use cases for other users needing access to Emergency Services talkgroups either permanently or on an ad-hoc basis. Examples include hospitals, Civil Defence, Community Patrol, Maori Wardens, airport groups, Search and Rescue, and other government agencies such as Department of Conservation and the Ministry of Foreign Affairs and Trade. These use cases will need to be considered in the overall solution allowing for specific access to users who are not necessarily Emergency Services staff or volunteers.

4.2 Architectural Principles

The technical architecture for the MCPTT 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.

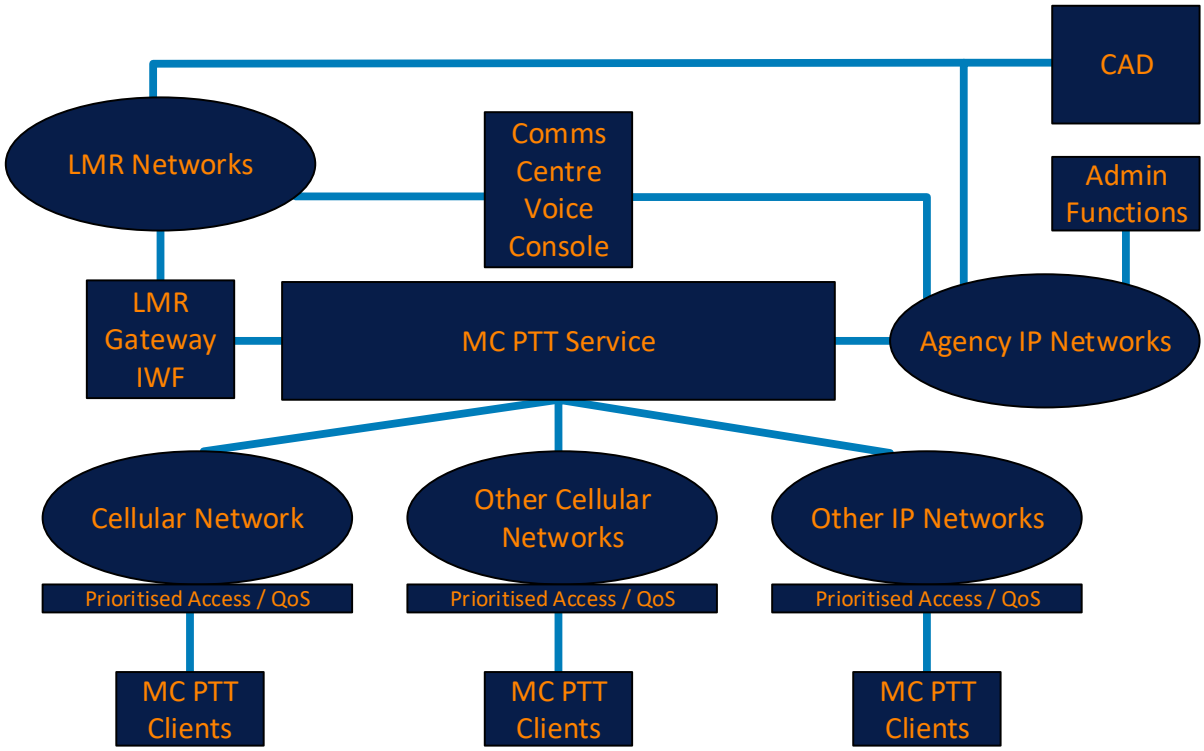

Figure 1: Overview of potential conceptual architecture

4.2.1 Single MCPTT Service

Whilst it is expected that multiple cellular (and other IP) networks will be used as the transport, potentially from multiple suppliers, a single MCPTT application and system is needed to ensure a seamless experience across all networks and for all agencies. This will require the underlying networks to be aware of the application, or at least be aware of the demands on the network from a Quality of Service perspective.

A single system (i.e. national 'numbering plan') 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 LMR networks, anything other than a single MCPTT application and system would add complexity from a gateway and Communications Centre perspective.

A Mobile Network Operator (MNO) utilising existing commercial infrastructure, rather than a virtual operator (MVNO), is the preferred architecture for cellular Mission Critical Services, however it is expected that the MCPTT platform infrastructure is dedicated to the PSN.

4.2.2 Underlying Network Flexibility

Whilst the primary use case is connectivity over cellular networks leveraging Quality of Service, Priority and Pre-emption capabilities (QPP), the application needs to be accessible by any authorised user across any network. Wherever possible, networks with an equivalent QPP capability should be preferred. However, as a general rule, any connection is better than no connection, with the exception of severely degraded audio, which should be excluded to avoid undermining the usability of the talkgroup for other members.

Private IP bearers such as in-station Wi-Fi/LAN/WAN are expected to support QPP and/or equivalent minimum network characteristics to enable a quality MCPTT experience where devices can use those connections.

Where in-vehicle routers have multiple network connections (e.g. multiple cellular connections, satellite), and they are available to devices inside or near the vehicle, the network connections should support QPP and/or equivalent minimum network characteristic, to enable a quality MCPTT experience.

Untrusted connections (e.g. internet) will be a network of last resort. However, it is still a viable access mechanism and appropriate security controls (IDAM, permissions, encryption, etc.) need to be in place for this type of access by authorised users (e.g. an on-call supervisor at their home listening on a talkgroup before responding to an escalated incident).

4.2.3 End-to-End Encryption

As previously mentioned, end-to-end encryption (E2EE) is required for MCPTT 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, MCPTT 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 done in the respective end-clients to avoid the need to transcode within the networks. This is to ensure information integrity and best possible performance.

Gateways and servers are particularly important as these may 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.

4.2.4 Loose Coupling

There are multiple Integration Points including connections between MCPTT and the underlying networks, the Communications Centre voice control software, CAD and LMR. Loosely coupling the Integration Points provides the ability to separately maintain the lifecycle management of all these systems, which is essential for maintainability and upgradeability. This also extends to administration and provisioning/incident management processes and system interconnections. See document *Appendix 5.4 Functional Guidelines Integration Target State.*

4.2.5 Continuous Development

Continued development to maintain currency, supportability and provide access to modern features will be inherent within the MCPTT 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.