Next Generation Critical Communications

Proposed Reference Architecture

Candidate Release: Version 1.0 - September 2019

Contents

Introduction **3**

Purpose 3

Audience 3

Overview 3

Services **5**

Mission Critical Mobile Service 5

Mission Critical Group Calling Service 6

Mission Critical Messaging Service 9

Standard Mobile Service 10

NGCC Certified Devices and Accessories 10

Device and Application Management 12

Non-NGCC Agency Specific Device 12

Coverage Enhancement 13

Transparent Network Management 14

Satellite Communication 14

Architecture **15**

Overview 15

Cellular – Long Term Evolution (LTE) 15

Land Mobile Radio (LMR) 19

Integration and Interworking 20

Security 24

Operational Management and Service Levels **26**

Overview 26

Service Management 26

Business and Operational Support Systems 26

During a disaster or extreme event 26

Technical Measures: Coverage, Performance and Availability 27

Appendix A – Glossary **28**

Introduction

The Next Generation Critical Communications (NGCC) programme is a joint initiative across the Emergency Services sector which consists of four independent agencies: NZ Police, Fire and Emergency NZ (FENZ), St John, and Wellington Free Ambulance.

This document should be read in conjunction with the Next Generation Critical Communications (NGCC) Concept Brief available from the programme web site: https://www.police.govt.nz/about-us/programmes-and-initiatives/next-generation-critical-communications-ngcc.

Purpose

The purpose of this document is to describe a proposed overarching reference architecture for the NGCC capabilities. This document will continue to evolve, with a baseline version being finalised as part of a formal procurement exercise.

This reference architecture, together with agency business requirements, will inform the Solution Architecture documents that will define the specific technical deliverables and services for future NGCC procurement activities.

Audience

This document is targeted at Service Providers who may deliver specific components of the NGCC capability to ensure they understand the end-to-end architecture view.

It is also intended to provide this perspective to stakeholders within the NGCC Programme itself and the Emergency Services agencies who will make use of the services.

Overview

The NGCC programme is tasked with delivering Mission Critical communication services to the Emergency Services sector. Emergency Services must be able to respond at any time, and in any place. To do this, they rely heavily on radio and mobile communications to coordinate, manage, protect and direct their geographically-dispersed staff, volunteers and resources. To provide appropriate emergency services, first responders need the right information, at the right time, in the right place.

Land Mobile Radio (LMR) is used to deliver mission critical voice and messaging services today, with a mixture of networks either owned and operated by Emergency Services, or supplied by a service provider. Commercial cellular services are also in use today.

The programme needs to address both end-of-life issues and capability gaps in current technology. Significant elements of the LMR system infrastructure are approaching or have reached end-of-life, and commercial cellular networks are not reliable enough and lack coverage and capability to deliver Mission Critical services.

A nationwide, common and consistent set of capabilities will be established that meets the needs of the Emergency Services sector. These capabilities will be presented as services in a catalogue from one or more commercial service providers that agencies can procure.

Communications services are Mission Critical when they may be used in operations relating to urgent, time-critical incidents, or when their performance is a significant contributing factor to the success or failure of work carried out by Emergency Services. This directly drives a requirement for a higher level of availability and guarantee of performance and security over and above that required for day-to-day use. Due to the nature of the operational functions within Emergency Services, it is unpredictable when this may occur, and therefore the communications services must always be maintained at a Mission Critical quality.

Services

Emergency Services agencies will procure services established by the NGCC programme to support their operational functions. This section presents an early high level draft of a proposed service catalogue.

Proposed services include:

1. Mission Critical Mobile Service
2. Mission Critical Group Calling Service
3. Mission Critical Messaging Service
4. Standard Mobile Service
5. NGCC Certified Device and Accessories
6. Device and Application Management
7. Agency Specific Devices
8. Coverage Enhancement
9. Transparent Network Management
10. Satellite Communication

In the tables below, the description and features section describe potential service types. The dependencies section describes major dependencies between services or on other related elements. The variations section anticipates options within the overall service that are likely to be needed to meet different use cases.

Services are expected to evolve over time as the underlying technology evolves.

Mission Critical Mobile Service	
Description	Connection to the LTE network with standards-based (3GPP) Mission Critical uplifts enabling voice, text and data services. The Mission Critical uplifts will ensure voice, video and data applications operate at a highly reliable level of performance appropriate for Mission Critical operational functions, potentially at the expense of other traffic on the network.
Features	The Mission Critical uplifts applicable to this service are: • priority access to the network including capacity and capability (jumping to the front of the queue) when first responders need to access communications; • pre-emption – first responders having the first call on network access and, when necessary, being able to displace non-emergency services users already on the network;

	• QoS (quality of service) ensuring that communications work appropriately ‘end-to-end’ across the network; and • Access to enhanced location-based services (remote activation, decreased polling interval).
Dependencies	Mission Critical capable devices and accessories. End-to-end Mission Critical connections depend on all parties supporting the features (e.g. Mission Critical voice calling or texting, agency gateways and connections to Mission Critical application servers). Applications must support Mission Critical access (e.g. configured to use the MC-Data bearer, set QoS markings correctly, configured to access location-based services).
Variations	Private network (APN) or Internet based. Internet of Things (IOT) connections. Access to this service for an authorised user at their own expense, or at a subsidised cost (e.g. devices for approved volunteers and/or first responders). Integration to Mission Critical voice services (e.g. SIP trunk for priority calling between communications centre staff and frontline offices). Data only options, low usage, high usage options.

Mission Critical Group Calling Service

Description	MC PTT (Mission Critical Push to Talk) service delivering half-duplex voice services (i.e. one person speaks at a time while all other members of the group are able to listen in real time).
Features	**LTE** MC PTT over LTE will be integrated with the network to fully support Mission Critical features. The interface will likely be an application that runs on a smart mobile device (with optional accessories) leveraging both the network and the device’s support of Mission Critical features to ensure end-to-end service quality. Dedicated LTE handsets and/or accessories for MC PTT only may also be appropriate. **LMR**

LMR PTT services are not really separable from the network connection itself, so the LMR variation of the Mission Critical Group Calling service will include the LMR network connection. LMR mobile and portable terminals will be used to access this service.

LTE and LMR

Should agencies procure PTT services using both LMR and Mission Critical LTE, a subset of their talk-groups can be configured to span both technologies.

The following table shows the likely features of a Mission Critical Push To Talk (MC PTT) service.

Feature	**Description**
Floor Control	Confirmation (usually via tone) that the channel is free to talk on, and the user who has pressed the PTT button has the “floor”. Any other user that attempts to gain access will receive a blocked tone and be unable to transmit.
Emergency Alert	Sends a priority status message with Global Positioning System (GPS) location co-ordinates advising that the user is under duress. Can be configured to open the channel for a set amount of time as part of this.
Priority Over-ride for Dispatchers	Ability for a dispatcher (or another authorised user) to override the user that currently has the channel open.
CAD Integration	Application Programming Interfaces (APIs) to enable access via Computer Aided Dispatch (CAD) tools to exchange information with the MC PTT system. Examples include meta-data (talker-ID and location) and sending or receiving status messages.
Remote monitoring by a supervisor / support	Ability to remotely monitor a particular channel from a position outside the communication centres.
Location Services	Attaching location data to a group member for reporting or tracking.
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.
	Logging	Usage and statistics for successful and failed group calls.
	Security	End to end encryption of all voice traffic will be available.
	Interworking	Seamless interworking available between nominated LTE and LMR talkgroups where required. Dispatcher selectable interworking available between agency LTE and LMR talkgroups where required.
	Administration	Ability to manage talk-groups.
	Geo-fenced talk-groups	Dynamic group membership based on location.
	Incident-specific talkgroups	Dynamic group membership set up for users in a particular event.
	Presence	Visibility of status of PTT client.
	Group send files	Ability to send files and information such as images, maps, links and videos to all users on a PTT channel.
	Push to Video	Adding video to a PTT channel (LTE only).
	Voice Message Fallback	Ability to record a PTT call so an offline user can hear it when they come back online (LTE only).
	Advanced Administration	Real-time administration capability to control group membership based on user, and to create ad-hoc talk-groups and add and remove members.
	Direct Mode	Ability for devices to talk directly to each other (device dependent).
	Local Repeated Mode	Ability to make a PTT call via a repeater in area isolated from any wider network.
Dependencies	Mission Critical mobile service (LTE only).	

	Mission Critical capable device and accessories, appropriate for LTE, LMR, or both. Inter-working with legacy half-duplex voice services e.g. analogue radio for transition and potentially other third party networks.
Variations	LMR or LTE only. Communications Centre (PTT console) interface. Applications for desktops and tablets suitable for in-station or in-vehicle deployment. Off-network capability only (device dependent).

Mission Critical Messaging Service	
Description	Mission Critical messaging service capable of delivering one-way and two-way text-based messages to and from an end-user device. It can also be used as the communications technology for an automation function such as remote response activation, or status messaging such as standard and priority callback requests.
Features	Indicative features of this service are as follows: • One-to-one and one-to-many text messaging; • 2-way communication (if terminals and network support it). May be constrained to pre-defined messages or functions; • Ability to integrate with automation functions such as remote response activation; • Ability to integrate with status messaging systems such as those provided within CAD applications; and • Ability to tag messages with GPS co-ordinates. Note: Messaging may be delivered as part of an agency's operational application-set in which case it will use the Mission Critical Mobile service to leverage a Mission Critical data bearer for this communication, rather than using this Mission Critical Messaging service.
Dependencies	Mission Critical mobile service (LTE only). Mission Critical PTT service (LMR only). Mission Critical capable device and accessories.

	Integration with critical and non-critical dispatch and staff communications systems.
Variations	This service will be very dependent on the networks that are transporting the message and the terminals used to display it, so there will be a number of variations available with specific features and constraints. LMR status and remote response activation messaging. Cellular text messaging (Short Message Service). NB-IOT (Narrow Band - Internet of Things) networks that provide low-power, long-range, low-capacity data services. Legacy one-way, non-guaranteed paging services.

Standard Mobile Service

Description	Common, commercial mobile services for non-Mission Critical users.
Features	Voice, data and text services as per common commercial services.
Dependencies	Compatible device and accessories.
Variations	IOT connections. Data only options, low usage, high usage options. Access to this service for other authorised users at their own expense, or at a subsidised cost (e.g. devices for approved non-operational volunteers or a friends-and-family scheme).

NGCC Certified Devices and Accessories

Description	Handheld, tablet, in-vehicle and in-station (fixed) devices and accessories appropriate for accessing services provided in this catalogue and other mobile applications.
Features	Devices available as-a-service meaning they are leased and: • managed and maintained including replacement when lost, broken or end of life; • meet the minimum specifications for their intended purpose through a certification programme (including support of Mission Critical features if required); and

	• enable access to a full range of accessories appropriate for agencies' varied use cases.
Dependencies	Device and accessories may have technical interdependencies in order to work together. Certification (to support Mission Critical services) Connection to the network – either standard or Mission Critical Mobile service Mission Critical PTT (for Mission Critical PTT capability – LTE and/or LMR depending on the device and use case)
Variations	Different options to meet the variety of use cases, see below for more detail of the most common types of devices and accessories that will be available through the catalogue. Note that specialist devices (e.g. connected medical equipment) will still be able to access NGCC services, but as non-NGCC agency-specific devices, as opposed to procuring the hardware through this catalogue. **Personal/Handheld Devices** Personal devices and accessories will have options for specific networks (LMR or LTE), and multiple networks (LMR and LTE), including mixed options through the use of advanced accessories such as remote speakers, microphones, and cameras which may have network connections of their own. A full range of devices will be available to meet agency needs, based on the technology options available. Note that some devices and accessories (especially low-cost items) may be more appropriate to be purchased outright with limited asset management. **In-Vehicle Devices** For the user interface, hands-free and/or mobile radio-style interfaces will be available for use with PTT services in vehicles, similar to a mobile LMR unit today, or a cellular car kit / integration to in-vehicle console or steering-wheel buttons. Permanently-mounted tablets (or portable tablets with docking stations) for use as Mobile Data Terminals installed in vehicles. Equipment options will be available for specialist vehicles such as helicopters and boats, however these will be subject to the regulations that govern those types of vehicles and may require specialist and/or customised equipment and installation. **In-Station Devices** Console-mounted terminals to meet requirements, noting that PTT clients can also be run on standard desktop and laptop terminals. This is likely to be separate from dedicated console software that will continue to be used

	in communications centres, alongside console-mounted equipment for resilience and Business Continuity Plan (BCP) operation.

Device and Application Management

Description	Capability to remotely manage and set policy on mobile devices.
Features	Mobile Device Management available as a service for agencies to set policies that can: • control on-boarding and initial configuration; • set security and other policies; • push applications and software updates; • manage asset inventory; and • remote lock and wipe. An App Store or equivalent way to present a list of certified applications to mobile devices will allow agencies to safely select from a white-list of applications for particular common functions.
Dependencies	Application and device certification
Variations	LTE device management. Secure containers for corporate information and applications for shared or personal devices including for agency-specific devices. LMR device management. Fixed console-type device management.

Non-NGCC Agency Specific Device

Description	This service is a variation on other services (as required) to support non-NGCC catalogue devices. This is to support specialist or other devices held by Emergency Services and/or people working or volunteering for Emergency Services using their own devices.

	The most likely services that will be offered in this manner are the Mission Critical Mobile Service and Mission Critical Push to Talk, but the catalogue will offer others to meet requirements.
Features	Service-dependent.
Dependencies	For Mission Critical services, devices will need to be certified to guarantee the support of the features. Authorised users only.
Variations	Temporary connections for international emergency services personnel serving in New Zealand. Appropriate commercial packages for different use cases, e.g. telemetry devices with low data volumes, streaming video cameras with high data volumes.

Coverage Enhancement

Description	Services to improve coverage including vehicle based solutions, temporary deployable solutions and permanent fixed solutions.
Features	In-vehicle coverage enhancement systems will use a combination of vehicle-mounted antenna and high power equipment to improve or extend the coverage achievable with a handheld device. This can then provide connectivity to devices inside or in close proximity to the vehicle. Vehicle communications solutions will be fully integrated into the vehicle allowing for power management, operational use of vehicle, space and equipment location. Deployables are portable LTE or LMR base stations that are mounted on trailers or vehicles, or transportable in a backpack or vehicle. These will provide an area of coverage that can be established anywhere that the infrastructure can be transported to. This can use satellite, microwave, or other technologies to provide backhaul to the main network, or be set up to deliver a standalone service in the local area only. It is expected that there will be a mixture of deployables held by Emergency Services and the service providers, with Emergency Services providing the initial response at an incident (first few hours) and Service Providers establishing deployables for planned or longer-term requirement (multi-day or longer). It is expected that Service Providers will liaise with Emergency Services for all planned or long term (multi-day or longer) deployables.

	Permanent coverage extension requests can be made through the catalogue.
Dependencies	
Variations	Vehicle-integrated Transportable – backpack Transportable – by vehicle Backhaul and standalone options LTE and LMR options Permanent deployment

Transparent Network Management

Description	Transparent visibility of the network status provided to authorised parties within the Emergency Services agencies.
Features	A dashboard view of network status in real-time so any interruptions to service are understood and can be operationally worked around. This will include visibility of planned work and associated impact.
Dependencies	Authorised user access only – e.g. communications centre, portable command centre
Variations	

Satellite Communication

Description	Satellite communication network connections and devices providing voice, messaging and/or data services.
Features	Provides communication beyond the reach of terrestrial networks. Specific features will depend on the service and device.
Dependencies	Appropriate user equipment – may be included as part of the service.
Variations	Satellite phones, data terminals or routers.

Architecture

Overview

Critical communications performs a vital role in the overall service delivery of Emergency Services in order to dispatch and manage a distributed frontline workforce. Figure 1 below shows where critical communications sit within a reference enterprise architecture view.

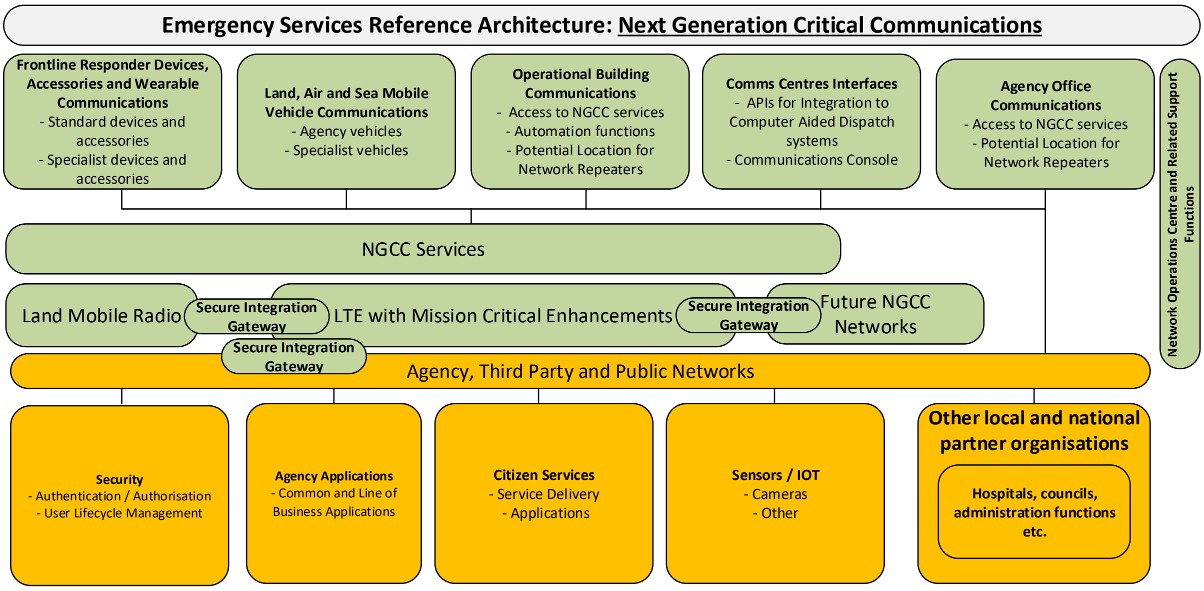
Emergency Services Reference Architecture: Next Generation Critical Communications
Frontline Responder Devices, Accessories and Wearable Communications
- Standard devices and accessories
- Specialist devices and accessories
Land, Air and Sea Mobile Vehicle Communications
- Agency vehicles
- Specialist vehicles
Operational Building Communications
- Access to NGCC services
- Automation functions
- Potential Location for Network Repeaters
Comms Centres Interfaces
- APIs for Integration to Computer Aided Dispatch systems
- Communications Console
Agency Office Communications
- Access to NGCC services
- Potential Location for Network Repeaters
Network Operations Centre and Related Support Functions
NGCC Services
Land Mobile Radio
Secure Integration Gateway
LTE with Mission Critical Enhancements
Secure Integration Gateway
Future NGCC Networks
Secure Integration Gateway
Agency, Third Party and Public Networks
Security
- Authentication / Authorisation
- User Lifecycle Management
Agency Applications
- Common and Line of Business Applications
Citizen Services
- Service Delivery
- Applications
Sensors / IOT
- Cameras
- Other
Other local and national partner organisations
Hospitals, councils, administration functions etc.

Figure 1 – Reference Architecture View

In order to meet the high availability and resilience requirements of Emergency Services, it is expected that a hybrid approach will need to be taken in the majority of areas. This will ensure a primary and at least one alternative communications network technology in the majority of locations. Communications network technologies are expected evolve over time.

The remainder of this section breaks the technologies into the two major communications network types that will be used initially, and also outlines key principles for integration, interworking and security.

Cellular – Long Term Evolution (LTE)

Overview

For over a decade, the industry has been exploring the options to deliver public safety radio-style services across a cellular network including the key features that make these "Mission Critical". This is seen as the next generation beyond standards-based LMR networks including P25 and TETRA. As well as voice-based services, LTE, also known as 4G, enables the use of applications that require broadband data such as video-streaming, mapping, location imaging and other intelligence information. From an economic perspective, it allows the network costs to be shared across a broad customer base, and similarly enables the use of common end devices and leverages the associated innovation and cost base. Furthermore, the 3GPP standards associated with LTE/4G are continually evolving to 5G and beyond, and this helps ensure the long term viability of Mission Critical services.

Existing commercial cellular networks in New Zealand are limited in their coverage, resilience and congestion-management capabilities which restricts the ability to rely on these networks for Mission Critical applications today. In order to remedy these limitations, this reference architecture describes the following key areas:

- Deployment model including possible use of multiple commercial cellular networks;
- Enhanced features on LTE networks covering 3GPP Mission Critical Open Platform standards-based features for QPP (Quality of service, Priority and Pre-emption);
- Mission Critical Push to Talk application to provide group communications;
- Coverage and/or capacity expansion including the use of vehicles to improve usability, and the use of deployables to establish temporary coverage or capacity in areas with limited or no coverage or capacity; and
- Added network resilience.

Deployment Model

The deployment model as shown below in Figure 2 defines a potential architecture for making use of multiple LTE networks with seamless access to all services, regardless of the actual network being used.

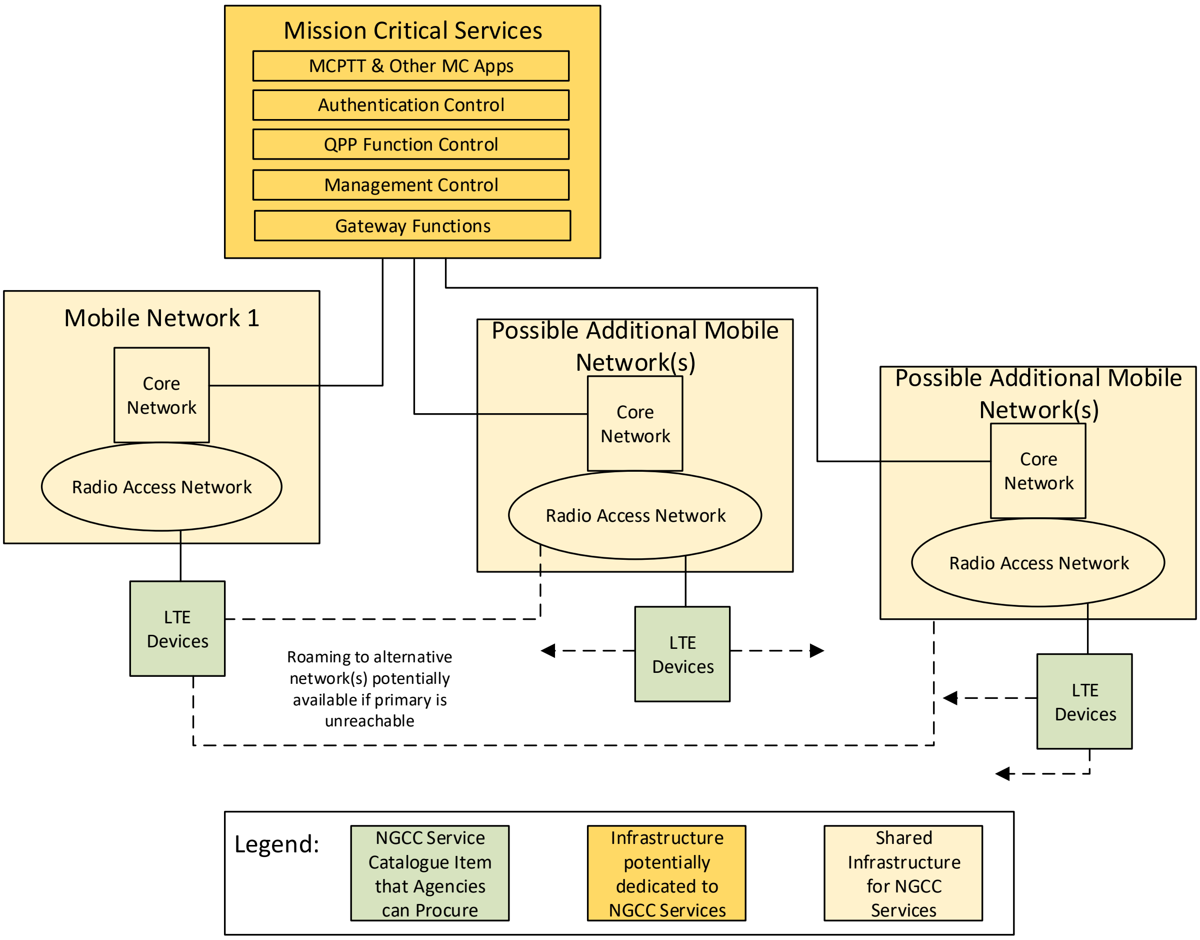
Mission Critical Services
MCPTT & Other MC Apps
Authentication Control
QPP Function Control
Management Control
Gateway Functions
Mobile Network 1
Core Network
Radio Access Network
Possible Additional Mobile Network(s)
Core Network
Radio Access Network
Possible Additional Mobile Network(s)
Core Network
Radio Access Network
LTE Devices
LTE Devices
LTE Devices
Roaming to alternative network(s) potentially available if primary is unreachable
Legend:
NGCC Service Catalogue Item that Agencies can Procure
Infrastructure potentially dedicated to NGCC Services
Shared Infrastructure for NGCC Services

Figure 2 – Potential LTE Deployment Model

In Figure 2, the orange shaded components are ideally dedicated instances (or tenancies) for Emergency Services, whereas the other elements are likely to be fully leveraged. The particular model for enabling one or more mobile networks that will be used in practice, and which specific elements sit in the Mission Critical Services layer versus the individual mobile operator networks, will be dependent on the market's response to the relevant procurement exercises, as long as the primary outcomes are met:

1. Single administration and service management interface/portal for an agency, with ability to manage their devices, USIMs, and service provider services, regardless of which network their devices are connecting to;

2. Common end-user experience and access to applications across all LTE services; and

3. Common baseline security levels.

The rationale for the type of deployment model illustrated in Figure 2 is:

- Ability to leverage one or more providers' commercial networks (for coverage, capacity and resilience) sharing their RANs (Radio Access Networks) with their corporate and consumer customers and leveraging their commercial spectrum;

- QPP will be enabled on each network to ensure Mission Critical access, but a common point of control for policy will ensure a consistent user experience and approach to security;

- Dedicated instances of infrastructure in the Mission Critical Services layer allows for:

    - Control of user, device and connection management independent of mobile operator networks;

    - Core network management independent of mobile operator networks – this allows for step-in rights and other commercial controls unlikely to be available directly on an operators' network;

    - Complete control of the most important integration points (e.g. access to communications centre, business applications, identity store);

    - Simple demarcation between the dedicated Mission Critical Services layer and the mobile networks using a 3GPP standards-based approach;

    - Increased reliability, resilience and security for Mission Critical Services; and

    - Greater control of feature and enhancement upgrades and/or remediation.

The Mission Critical Services layer holds the subscriber database, and defines who has access to which services (including access to one or more mobile operator networks). This is also where the application servers are located so these services can be accessed across any mobile network. User and service management will be via this layer to ensure a common, consistent point for all administration of NGCC services.

Access into each agency's environment will be via secure gateways. These will be replicated for resilience, likely in 3 separate locations to mirror the availability built today into each agency where 3 separate communications centres are operated for each of the Emergency Services (Police, FENZ, plus combined St John and Wellington Free Ambulance). The gateways will be configured to ensure appropriate security and to translate QoS parameters between the networks as appropriate to ensure end-to-end performance.

Standards

Cellular networks interoperate with each other and devices due to open standards maintained and developed by 3GPP (Third Generation Partnership Program) which is a partnership between seven major international standards bodies. Over recent years, the development of Mission Critical features using LTE have been a priority for 3GPP. The standards are defined in Releases, and Release 14 (finalised in 2017) is deemed to be the minimum to support Mission Critical Data and Mission Critical Push to Talk services. LMR interworking standards are expected to be defined in Release 15, however this has not been finalised at the time of writing.

International jurisdictions, particularly the United Kingdom (ESN – Emergency Services Network) and United States of America (FirstNet) are driving the continued development of the Mission Critical 3GPP standards, and the corresponding manufacturer implementation of associated features.

This reference architecture aligns to the 3GPP standards wherever they are applicable, and the expectation is to evolve with the standards over time ensuring an ongoing modern, supportable service.

QPP – QoS, Priority and Pre-emption

The most fundamental elements defined in the standards to enable the delivery of Mission Critical services (including Push to Talk) over cellular, are known as QPP – QoS, Priority and Pre-Emption. Each of these serves a different function:

- QoS – Quality of Service defines the end-to-end performance characteristics of a traffic flow in terms of latency, jitter and packet loss. This is important for a predictable, reliable user experience, especially for voice and video applications;

- Priority – this means that Mission Critical applications and services get preferred access to the network over other connections when there is contention; and

- Pre-emption – this means that where there are capacity constraints, other users are disconnected in favour of Mission Critical applications and services.

These features will be enabled in the mobile operators' LTE network(s), and orchestrated from the Mission Critical Services layer shown in Figure 2.

Coverage

The usable coverage area for LTE services will include the combined footprints of one or more commercial mobile operator networks, enhanced by the existing government investment with RCG (Rural Connectivity Group) to expand rural coverage via the Rural Broadband Initiative 2 and the Mobile Black Spots Fund. This extra coverage is available through all of the commercial mobile networks in New Zealand, and will be transparently available through NGCC.

The Emergency Services' coverage requirements extend beyond this, and this will be addressed as follows:

1. Using vehicle-based technology with aerials and higher-power equipment to extend the range of the existing network. Devices will then connect transparently via the vehicle which acts like a portable cell site. This helps areas on the fringe of coverage, and inside buildings.

2. Additional investment in coverage for areas Emergency Services access often and there is no existing coverage. This includes mobile black spots on state highways, locations of interest, and areas between good coverage where specific in-fill investment would create a larger usable area of continuous coverage.

3. Use alternative technology (where there is no LTE coverage) through partners such as Wireless ISPs (WISPs) and/or satellite services providers.

4. Use of deployable capability.

Resilience

Cellular service outages usually occur because of power failure to an individual cell site, or an outage in the transmission network that serves a particular cell site.

In cities, neighbouring cell sites can usually pick up the traffic as overlapping coverage is in place for capacity reasons, and with QPP, Emergency Services can still reliably access Mission Critical services. Should an individual mobile operator not have overlapping coverage, another mobile operator could potentially be used by Emergency Services under the roaming-style of arrangement shown in Figure 2.

Outside cities, outages are more common as there tends note to be overlapping coverage, and mobile operators often share infrastructure. This is certainly the case for all access provided as part of the RCG investments. NGCC will work with the mobile operators to “harden” key sites to decrease the likelihood of power and transmission issues causing service outages. The areas selected will depend on the demand, risk profile, and cost.

Deployable LTE and/or LMR capability will be used to provide access during service-impacting outages in the LTE network.

Variations

Cellular networks can be used to deliver narrow-band services, potentially over a wider area, and using less power than standard LTE services by using technologies such as NB-IoT and LTE-M. This type of service is targeted at IOT (Internet of Things) devices, and may provide a useful option for a 2-way messaging service. Integration would be via the cellular gateway into agency networks for use with CAD or other turnout systems. End user device support for these technologies is not currently common.

Land Mobile Radio (LMR)

Overview

LMR networks are currently used for operational communications in all of the Emergency Services agencies. The networks are disparate across the agencies, and many components are end of life and require replacement.

LMR’s role in this reference architecture is as an alternative network and resilience option limited to Mission Critical Group Calling (PTT) and Mission Critical Messaging (status update and remote response activation messaging). LMR network capability will be established that is owned and managed by a commercial service provider, delivered as a service and consistent across all Emergency Services agencies.

Deployment Model

This section will be updated once the investigation work is complete – expected late 2019.

The current state is a mixture of Police-owned, and service-provider owned analogue networks and a Police-owned P25 Phase 1 trunked network. There is a mixture of spectrum used, primarily in ESA, ESB, F and ESC bands for these networks. The most current deployment is the P25 trunked network in Auckland, Wellington and Canterbury which is used by NZ Police and Wellington Free Ambulance. This network was established as part of the WGRN (Whole of Government Radio Network) initiative and is also used by a small number of other users.

The future state is being developed, but the working assumption is it will be P25 to leverage the most recent radio investment within NZ (via the WGRN).

Investment in resilience (backhaul and/or batteries/generators) will focus on areas where LMR is the primary access mechanism.

Coverage

Coverage requirements for LMR will be based on agency requirements, with the focus being on covering the same areas as LTE (for backup) and also rural areas that are not in the LTE coverage footprint. Coverage in remote areas (where there is no road access) will be fortuitous only, with the design being to use deployable coverage.

Resilience

LMR service outages usually occur because of power failure to an individual base station, or an outage in the transmission network that serves a particular base station. Therefore investment in power and backhaul resilience will be appropriate to meet service levels.

Additionally (unlike LTE), base stations will continue to work in a localised manner without backhaul, so local users can still communicate with each other. Devices can communicate directly with each other over short distances should there be a total outage of a base station.

It is expected that LMR and LTE technology deployments will not leverage common infrastructure such as power and backhaul to ensure maximum service diversity and resilience. Where this is not practical in an area, specific design work will be required to ensure at least one network will be available (e.g. through extended battery capacity, generator backup, alternative backhaul mechanisms, or higher service levels for time to repair) to meet agreed service up-time requirements in the event of the shared power or backhaul failing.

Integration and Interworking

NGCC services will integrate and interwork with each other, and with other systems within Emergency Services.

The key business integration points include the Communications Centres with their CAD (Computer Aided Dispatch) and voice console and control tools as well as back office systems supporting service activation, application and device management, and automation functions. All must work seamlessly with the NGCC capability.

Interworking between NGCC services based on LMR and LTE is essential to meeting resilience and coverage needs where agencies have chosen to procure both. This includes both the remote user perspective, and the Communications Centre and related applications interfaces.

All networks will come together using IP, and end-to-end service security (encryption), availability and performance will be key to a reliable capability supporting the operational use of NGCC services and business applications.

Other integration points relate to support functions such as Identity Management and User/Device Lifecycle Management. These interfaces will use the same interconnection points into agency networks to allow enterprise applications to be accessed. IP-based gateway connections with appropriate resilience (multiple independent connections) and QoS standards are required to allow for end-to-end performance predictability for application traffic flows.

Communications Centre

From a dispatcher's perspective, the following elements will interface into the critical communications environment:

- A single Push to Talk interface or console (voice control);
- CAD interface for messaging and application-based mobile dispatch tools, as well as presentation of location-based information on vehicles or other resources;
- Voice Recording; and
- Integration with legacy systems to enable transition from current state to end state.

Figure 3 below shows the different interface points including the responsibility for each piece.

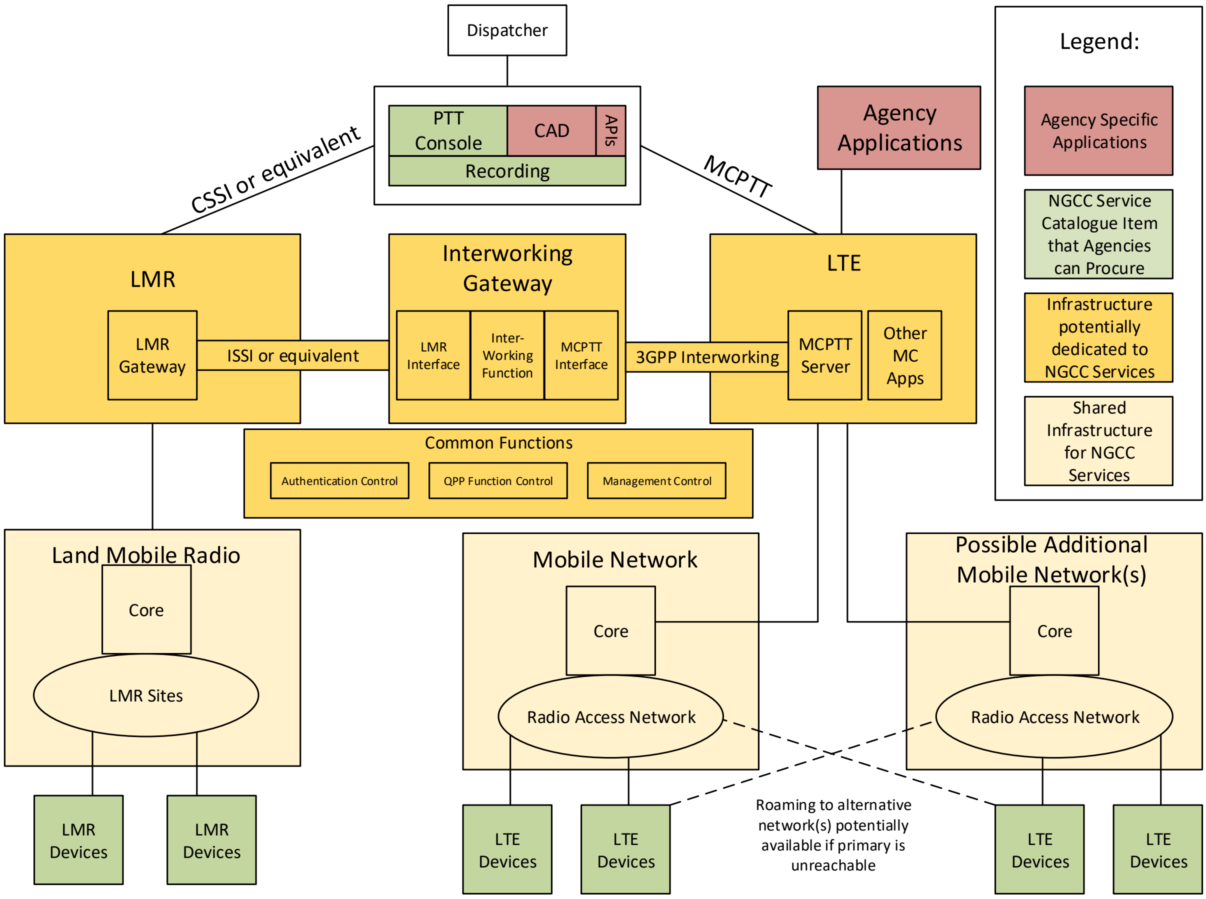

Figure 3 – Integration View

MC PTT consoles can provide a lot more than a voice interface, however the current mode of operations in all agencies is that the majority of non-voice communication is handled through a their CAD interfaces. At a reference architecture level, NGCC will enable agencies to choose any of the following three approaches to be taken:

1. Use existing PTT console system for NGCC voice communications, integrate existing CAD and NGCC services for non-voice communications;

2. Establish a new PTT console system as a service for NGCC voice communications, integrate existing CAD and NGCC services for non-voice communications; or

3. Establish a new PTT console system as a service from NGCC with enhanced functionality to include additional (non-voice) elements within the PTT console itself, integrate existing CAD natively and/or through the PTT console system as required.

This will be achieved through a modular approach, and whilst it is likely that agencies will adopt a consistent approach, this is not dictated by the reference architecture and this level of flexibility will ensure business processes can be enabled by the most appropriate integration approach, which may change over time.

The options in how to enable recording are similar to those described above for the console, there is the option to use existing (if it meets requirements) or to replace it with a service from NGCC. As more non-voice communications are used, it becomes essential to record these in addition to voice communications.

All integration will be standards-based leveraging IP connectivity, allowing multiple interfaces for resiliency, and allowing communications centres to be virtualised to the extent preferred operationally by each agency.

LTE and LMR Push-to-Talk Interworking

Interworking between legacy PTT systems is a critical tool for transition to new services, as well as for enabling talk-groups to span NGCC LTE and LMR networks, where an agency's target state is a hybrid approach.

The interworking approach is shown in Figure 3. This will align with Release 15 of the 3GPP standards, and is expected to fully support ISSI (InterRF Sub-System Interface) and CSSI (Console Sub-System Interface) or equivalent functions for LMR systems and define how the meta-data will be transferred between the networks.

The PTT console will connect to both LMR and LTE networks for resiliency and efficient traffic paths. Dispatchers will be able to manage talk-groups in all networks.

IP Networking

Services that run over NGCC will likely traverse multiple types of networks with multiple types of connections using different vendors equipment managed by different providers, including the agencies themselves. An end-to-end view will be important to maintain throughout the design phase and for ongoing operations. This architecture recognises that IP will be the protocol used end-to-end and appropriate QoS mechanisms with well-defined, standards-based demarcation points to maintain service end-to-end. Firewalls will be used between networks and must be specified appropriately to maintain throughput, availability and QoS as well as providing a security border for each network.

Mission Critical Telephony

Phone calls between communications centres, first responders, and any others involved in operational response would benefit from the Mission Critical uplifts defined in the 3GPP standards. To the extent practical, common users (such as communication centres) will be able to call frontline officers in a priority manner leveraging SIP-based connections to the mobile networks with QPP enabled end-to-end.

Other Networks

Future NGCC capability such as satellite, trusted and untrusted WiFi, and other communications networks are expected to be IP-based, and therefore relatively simple to integrate and offer "over the top" access to NGCC applications including PTT. To make this Mission Critical, integrated QPP capabilities will be required, with 3GPP standards defining the interworking.

Identity Management

PTT applications will use identity sources from within agencies, allowing agencies to undertake their own user and device management in line with their HR and asset management processes. This type of integration will be required for device management and user access to specific applications also. User and device identity is key for all applications, and for tagging information such as video files being stored from body-worn cameras. These types of applications, including device management will be the responsibility of the agency, but potentially available through the NGCC service catalogue.

Enterprise Applications (using Mission Critical Data)

Access to enterprise applications will be supported as per current and future mobility initiatives with the following enhancements:

- Ability to leverage mission critical data (with or without the use of agency APNs);
- End-to-end Quality of Service can be configured by aligning QoS schemas between agency networks and the mobile network; and
- Multiple gateways to ensure resilient access between agency networks and the mobile network.

Agency policies controlling access to any particular app can be controlled using Mobile Device Management and/or App Store functionality as appropriate.

Automation

As part of the dispatch process, some agencies use automation to perform operations such as opening the station public address system, turning off appliances and opening doors, and this type of automation will be supported by NGCC services over IP allowing it to be carried by a private network or LTE, and also over LMR (if required).

Security

Threat Protection

To protect against rapidly changing threats, security will be applied at all layers of NGCC services including the cellular access network, other access networks, core network and devices. Security monitoring and incident response will be provided to ensure secure and reliable delivery of services.

Relevant standards and best practice guidelines (including Protective Security Requirements, PSR) will be referenced to ensure commercial providers are delivering appropriately secure services, and following required staff vetting processes. Best practice guidelines for network security will be applied to protect against threats such as denial of service and unauthorised access to systems and services.

Network Security

Best practice guidelines for network security will be applied to protect against threats such as denial of service and service disruption. Service Providers and agencies will be responsible for the border security between their environments, and for following best practice in the configuration and management of their infrastructure.

Where gateways are used to interconnect different types of connections, especially when traffic is decrypted and re-encrypted, it is important to apply appropriate security controls to ensure these are not weak points that can be exploited.

Device Security

Mobile, hand held and portable devices need to be regarded as inherently insecure, therefore individual agencies will need to apply an appropriate level of security using a combination of:

1. **Access controls** - e.g. passcode access and/or biometrics, balanced against the usability needs of a frontline staff member in stressful situations;

2. **Device hardening** – e.g. disabling unused services;

3. **Security applications and settings** – e.g. end-point protection; and

4. **Centralised configuration management and over-the-air control** – e.g. standardised build and application set, remote disable and wipe capability.

An appropriate balance of usability and security will need to be struck as part of operationally on-boarding any particular service, with NGCC services being configurable to meet each agency's security requirements.

Security of Communications Traffic

NGCC services will allow agencies to apply their own end-to-end encryption to the level they deem appropriate for the applications they are running if a higher degree of protection is required.

Some access, integrity and confidentiality controls will be in place through the inherent design of LTE networks, and equivalent for other telecommunications bearers:

- Mutual authentication between the network and the user device (authorisation);

- Encryption of Control Plane traffic (integrity); and

- Encryption of User Plane traffic (confidentiality and integrity).

For applications that run over NGCC (including PTT), these will need to be encrypted end-to-end to ensure security as the specific bearers could change under the various coverage and availability scenarios. Therefore, even if the inherent LTE security is deemed sufficient for the particular application, there is the possibility in the hybrid architecture that the traffic will traverse another bearer with different security characteristics.

Physical Security

The working assumption is that current commercial operator base station / site practices are sufficient to meet Emergency Services availability needs. This will need to be validated through requirements and commercial discussions to ensure Emergency Services do not expose themselves to undue communications availability and security risks.

Operational Management and Service Levels

Overview

NGCC services will be provided by commercial Service Providers, and therefore operational management and service levels become crucial to the successful ongoing delivery of services in an acceptable manner to Emergency Services.

Day-to-day service management will be directly between the agencies using the services, and providers that are delivering them. This will be primarily via a self-service portal for fulfil and assure, incident management, and service reporting, supported by appropriate escalation and governance structures.

Service Management

Service management from service providers will need to be appropriate to meet the Emergency Services' requirements for critical services. This will likely include a higher level of response to incidents and requests for moves, adds and changes building on existing service management frameworks.

From a network management perspective, availability of services will need to be presented to communications centres' operational management in real-time, ideally via API, including both planned and unplanned outages. The ability to inform frontline staff and manage around planned and unplanned outages is imperative to the delivery of critical communications. Escalation paths to negotiate and notify timing of planned outages if they will have a major operational impact will be needed.

Business and Operational Support Systems

BSS (Business Support Systems) and OSS (Operational Support Systems) are used by network operators to manage their networks and the users of those networks. These tend to be complex and highly integrated to the individual networks. This architecture describes multiple networks and the systems that provision services across these networks will need to be integrated with the Mission Critical layer (as per Figure 2) that defines the identities of Mission Critical users. This is non-trivial and will be a key requirement of the solution to be envisioned from the outset across all networks (including both LTE and LMR).

For LTE, all aspects of provisioning and assurance with each MNO will need to be considered to ensure end-to-end service can be established and managed. This will also include billing, business analysis and reporting systems.

Provisioning security (how to ensure connections are restricted to valid Emergency Services users only) will also be a key function of the BSS.

During a disaster or extreme event

No amount of design and procedural planning will prepare for every eventuality, and the unpredictability of natural disasters and extreme events requires resilience in the approach. For service providers, this will include what to do in disaster scenarios such as the establishment of temporary access through deployables and re-establishing communications as quickly as possible. Procedures will need to be agreed in advance and work in lock-step with Emergency Services and other Civil Defence authorities so they can be effectively followed in these situations. This will be an improvement on the arrangements that already exist today, as Emergency Services will be more heavily reliant on service provider networks for communications under NGCC than they are today.

Technical Measures: Coverage, Performance and Availability

LTE

The business requirements for LTE services will be used to define how coverage and performance are modelled by the service providers (what we should expect), and also how we measure that performance. The three key measurement areas for LTE are coverage, performance and availability. All three will need to be addressed in terms of design inputs for service providers, and also measurable performance metrics that can be used for SLA (Service Level Agreements). It is anticipated that there will be a need for multiple levels of definition including at least a minimum (SLA) and a target (design parameter).

LTE is capable of delivering very high bandwidth, but depending on where the cell-edge is defined, the performance there will be much lower than the theoretical maximum, and NGCC will have to clearly define a minimum working performance specification to negotiate with service providers. This specification will also need to include a maximum number of devices concentrated in close proximity of each other so the model to cater for a localised “surge” event.

Performance and coverage are intrinsically linked. Voice only communications (<1Mbps symmetrical) will show a different coverage picture to video which requires 2Mbps+ downlink for streaming to a mobile device and 2Mbps+ uplink for streaming from a mobile device in high definition.

Measurement of coverage and performance is best achieved through a combination of telemetry information from the network and devices. An application that reports from mobile devices will deliver an objective view of real-world performance and the information gleaned will allow service levels to be measured, and future investment in coverage to be prioritised.

Network statistics will prove the effectiveness of QoS, Priority and Pre-emption in the network.

Availability will be measured in terms of network element availability, as well as a client’s accessibility and retainability. The definition of availability will have a minimum performance level – if it is below this, Emergency services will deem it unavailable.

LMR

The three key measurement areas for LMR are coverage, capacity, and availability. For LMR, coverage (at an appropriate minimum field signal strength and signal to noise ratio) will be the key measure of effective, usable access to the network. Capacity will need to be appropriately designed to meet requirements, and if the solution is trunked, queuing measured to ensure an effective, operational service is available. Targets will be agreed for availability and the solution will be designed and measured against these.

Appendix A – Glossary

The following table identifies the abbreviations and terms used in this document:

Abbreviation or Term	Full Abbreviation / Description
3GPP	**3rd Generation Partnership Program** –the main standards organisation responsible for the development of mobile broadband communication networks, services and capabilities.
API	**Application Programming Interface** - a set of clearly defined methods of communication between various software components.
APN	**Access Point Name –** identifies the data network that a mobile data connection is made to. Standard commercial users access the Internet but this can be used to connect an enterprise user to a private network.
BSS	**Business Support System** – systems used by a telecommunications service provider to manage its customer-facing activities.
CAD	**Computer Aided Dispatch** – software systems consisting of several modules that provide services at multiple levels in a communications centre and in the field of public safety. These services include call input, call dispatching, call status maintenance, event notes, field unit status and tracking, and call resolution and disposition.
Emergency Services Agencies	This term refers to the four primary Emergency Services agencies NZ Police, Fire and Emergency NZ, St John and Wellington Free Ambulance.
First Responder	This term is used in this document to refer to any paid or volunteer personnel within the Emergency Services Agencies who is involved in delivering Emergency Services' operational functions.
HSS	**Home Subscriber Server** – database that contains the user identification, addressing, profile information, mutual network-terminal authentication and radio-path encryption.
IP	**Internet Protocol** - the principal communications protocol in the Internet protocol suite for relaying packets across network boundaries. Its routing function enables internetworking, and essentially establishes the Internet.
LMR	**Land Mobile Radio** – analogue or digital "private" radio services such as the existing P25 digital and the analogue radio networks

Abbreviation or Term	Full Abbreviation / Description
	owned and operated by NZ Police (and used by multiple Emergency Services agencies), and the commercial radio networks, such as those used by St John Ambulance.
LTE	**Long Term Evolution** – A 3GPP standard for cellular communication networks. Also commonly referred to as 4G.
Mission Critical (MCx)	**Mission Critical services** – the communications services required for Emergency Services agencies to undertake operations relating to the safety of people or property.
MC PTT	**Mission Critical Push To Talk** – Mission Critical version of PTT. This is generally used in the context of the 3GPP definition.
NB-IOT	**Narrow Band - Internet of Things** - is a Low Power Wide Area Network (LPWAN) radio technology standard developed to enable a wide range of devices and services to be connected using cellular telecommunications bands
NGCC	**Next Generation Critical Communications** – the next generation of mobile communication services to be offered to Emergency Services agencies in New Zealand.
OSS	**Operational Support System** – systems used by a telecommunications service provider to manage their network(s).
P25	**Project 25** - a suite of standards for digital mobile radio communications designed for use by public safety organisations in North America and has been widely adopted there as well as in Australia and by NZ Police in Auckland, Wellington and Canterbury.
PCRF	**Policy and Charging Rules Function** – real-time determination and enforcement of policy rules in a multimedia network. This is an important part of establishing appropriate network resources for MCPTT services.
PSR	**Protective Security Requirements** - PSR outlines the Government's expectations for managing personnel, physical and information security. https://protectivesecurity.govt.nz/
PTT	**Push To Talk** – half-duplex voice communication services, often with floor control, group and user management capabilities.
QoS	**Quality of Service** – a network’s ability to deliver specific characteristics as required by an application to function correctly.

Abbreviation or Term	Full Abbreviation / Description
	This specifies minimum acceptable bandwidth, latency, jitter and packet loss levels.
RF	**Radio Frequency** - is any of the electromagnetic wave frequencies that lie in the range extending from around 20 kHz to 300 GHz, which roughly equates to the frequencies used in radio communications.
SIP	**Session Initiation Protocol** - signalling protocol used for initiating, maintaining, and terminating real-time sessions that include voice, video and messaging applications. SIP is used for signalling and controlling multimedia communication sessions in applications of Internet telephony for voice and video calls, in private IP telephone systems, in instant messaging over IP networks as well as mobile phone calling over LTE (VoLTE).
SLA	**Service Level Agreement** – operational performance terms in place between consumers and providers.
TETRA	**Terrestrial Trunked Radio** – a European standard for a trunked radio system. TETRA was specifically designed for use by government agencies, emergency services for public safety networks, rail transport staff for train radios, transport services and the military. TETRA is the European version of trunked radio similar to P25.
USIM	**Universal Subscriber Identity Module** – microprocessor chip used to identify subscribers on a mobile network. USIM cards store subscriber information and authentication information as well as providing storage space for data and applications.