

# **Public Safety Network**

## **Appendix 5.4**

### **Functional Guidelines**

### **Integration Target State**

## Contents

|  |    |
|--|----|
| 1. Introduction .....  | 3  |
| 2. Document Purpose .....  | 3  |
| 3. Integration Approach.....   | 3  |
| 4. Integration Governance .....  | 3  |
| 5. PSN Target State Integration High-Level Technical Specification ..... | 4  |
| 5.1 Transport/Network Connection .....                                   | 4  |
| 5.2 PSN Services .....   | 8  |
| 5.2.1 Functional Categories .....  | 9  |
| 5.2.2 Interfaces.....  | 10 |
| 6. Common Agency Integration Enablers.....                               | 26 |
| 6.1 Federated Identity and Access Management .....                       | 27 |
| 6.2 Messaging .....  | 27 |
| 6.3 Location.....  | 27 |
| 6.4 Voice .....  | 27 |
| 6.5 Recording .....  | 27 |
| 6.6 Security Testing and Certification .....                             | 27 |
| 6.7 Device Testing & Certification .....                                 | 28 |
| 6.8 Transparent Network Management .....                                 | 28 |
| 6.9 Other .....  | 28 |
| 7. Agency Application Usage of PSN Capabilities.....                     | 28 |
| 8. Test and Integration Lab .....  | 29 |

## 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* and *Appendices 4.1 to 4.5 Services Guidelines* documents.

## 2. Document Purpose

This document describes the target state from an integration perspective. It is intended to provide agencies, potential Service Providers, and other stakeholders with a high-level view of the interfaces between agencies and services, and between services including:

- the type of interface it is;
- what type of traffic it will carry;
- endpoints;
- standards and/or specifications where known;
- agency considerations; and
- transition considerations.

It is not intended to fully define the PSN interface specifications but is rather a guide as to what the likely interfaces are to assist Service Providers with their design and planning ahead of detailed service and transition design.

The current state integration view is described in *Appendix 5.3 Functional Guidelines Integration Current State* document.

Common agency integration enablers must be established to achieve programme goals. Service Providers are expected to provide capabilities that are aligned with the integration goals of the programme.

## 3. Integration Approach

The approach to performing transition from the current state to the target state is addressed in the *Appendix 5.6 Functional Guidelines Transition Delivery Framework* document.

## 4. Integration Governance

The PSN Programme will provide governance over integration and transition activities. See *Appendix 5.6 Functional Guidelines Transition Delivery Framework* for more information.

## 5. PSN Target State Integration High-Level Technical Specification

This section lists and describes the interfaces between PSN services and agencies, as well as between the services themselves.

### 5.1 Transport/Network Connection

The network connections between each agency and the Service Providers, and between the Service Providers that deliver the core transport function to connect agencies to services, are the primary enablers for access to and usage of PSN services.

The network connection and fundamentals of the transport layer are specific to the network technology (LMR, cellular and others such as Satellite), however the interconnection itself will likely be IP in both cases. Figure 1 below shows where the interface descriptions fit.

Transport / Network Interconnections

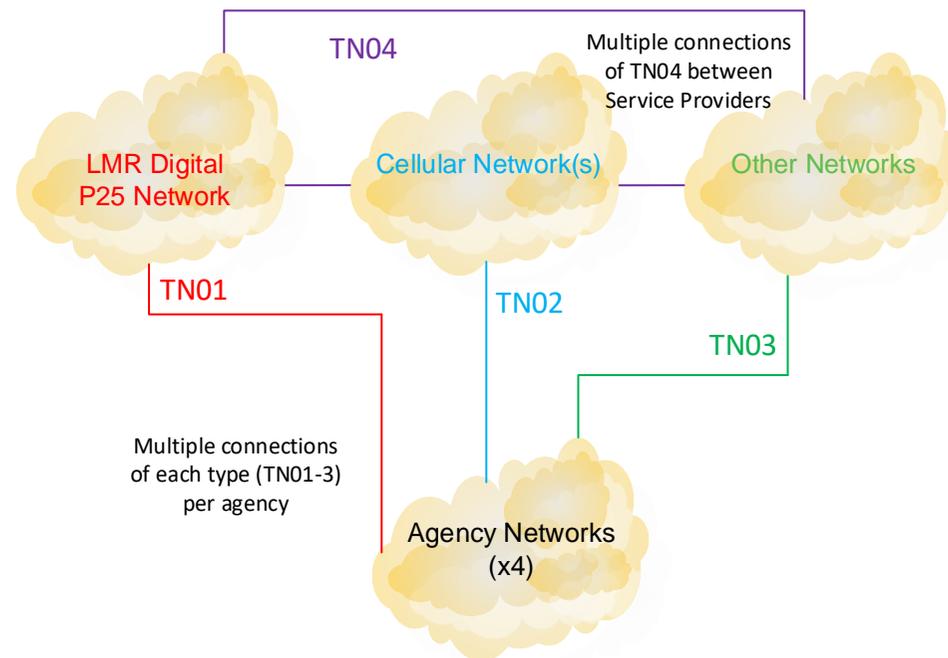


Figure 1: Transport / Network Connections

The table below provides a description for each of the interfaces shown in Figure 1.

| ID   | Interface Type | Function  | Endpoints   | Standards/Applicable Specifications  | Agency Specific Information  | Transition Considerations   |
|------|----------------|---|---|--|--|---|
| TN01 | IP trunks.     | Carry P25 CSSI/ISSI (or other relevant protocol)<br>Will include <ul style="list-style-type: none"> <li>• voice and messaging traffic;</li> <li>• related signalling and meta-data; and</li> <li>• any packet data services.</li> </ul> | LMR Service Provider firewalls and/or SBCs (Session Border Controllers) depending on the service architecture.<br><br>Agency firewalls and/or SBCs depending on the service architecture. | IP connections with automatic failover.<br><br>Must have sufficient capacity, scalability and resilience to meet service levels.<br><br>Network-level encryption optional – the applications using the IP interconnections will encrypt the traffic. | In addition to centralised connections, de-centralised connections directly into Communications Centres are required for resiliency that align with agency operating procedures. Each region should have stand-alone infrastructure without reliance on infrastructure in another region. For example, all agencies have Auckland (North), Wellington (Central) and Christchurch (South) Communications Centres. The southern Communications Centre should be able to communicate with southern LMR networks without a dependency on infrastructure in another island. | Installation and commissioning – today’s circuits are E1s or E&M, moving to all IP.<br><br>Traffic model.<br><br>Firewall and network capacity.<br><br>IP addressing.<br><br>Routing and failover.<br><br>Quality of Service. |

| ID   | Interface Type | Function   | Endpoints   | Standards/Applicable Specifications  | Agency Specific Information   | Transition Considerations  |
|------|----------------|--|---|--|---|--|
| TN02 | IP trunks.     | Carry MCPTT SIP and configuration management traffic, as well as messaging and data traffic. | Cellular Service Provider firewalls and/or SBCs (Session Border Controllers) depending on the service architecture.<br><br>Agency firewalls and/or SBCs depending on the service architecture.                | IP connections with automatic failover.<br><br>Must have sufficient capacity, scalability and resilience to meet service levels.<br><br>Network-level encryption optional – the applications using the IP interconnections will encrypt the traffic. | Primary connections will be into Data Centres to carry the bulk of application traffic.<br><br>Similar to TN01, there will likely be a requirement to enable Communications Centres to connect directly (using SIP) to the MCPTT servers. | Installation and commissioning.<br><br>Traffic model.<br><br>Firewall and network capacity.<br><br>IP addressing.<br><br>Routing and failover.<br><br>Quality of Service.<br><br>Recording capability  |
| TN03 | IP trunks.     | Carry MCPTT SIP as well as messaging and data traffic.                                       | Other Service Providers (e.g. satellite) firewalls and/or SBCs (Session Border Controllers) depending on the service architecture.<br><br>Agency firewalls and/or SBCs depending on the service architecture. | IP connections with automatic failover.<br><br>Must have sufficient capacity, scalability and resilience to meet service levels.<br><br>Network-level encryption optional – the applications using the IP interconnections will encrypt the traffic. | Primary connections will be into Data Centres to carry the bulk of application traffic.   | Installation and commissioning.<br><br>Traffic model.<br><br>Firewall and network capacity.<br><br>IP addressing.<br><br>Routing and failover.<br><br>Quality of Service.<br><br>Recording capability. |

| ID   | Interface Type | Function   | Endpoints   | Standards/Applicable Specifications  | Agency Specific Information | Transition Considerations |
|------|----------------|--|---|--|-----------------------------|---------------------------|
| TN04 | IP trunks.     | Carry interworking traffic (control and data) between Service Providers. | Other Service Providers (e.g. satellite, LMR and cellular) firewalls and/or SBCs (Session Border Controllers) depending on the service architecture.<br><br>Agency firewalls and/or SBCs depending on the service architecture. | IP connections with automatic failover.<br><br>Must have sufficient capacity, scalability and resilience to meet service levels.<br><br>Network-level encryption optional – the applications using the IP interconnections will encrypt the traffic. | N/A                         | N/A                       |

Notes:

1. Performance standards must fully support agency requirements and, where possible, be standards-based. Where a standard exceeds the agencies requirements, the standard will be the default.

## 5.2 PSN Services

The PSN services that will use the trunks and network connections described in the previous section are described in this section. Figure 2 below identifies the anticipated interfaces between agencies and the services and, where relevant, interfaces between the services themselves.

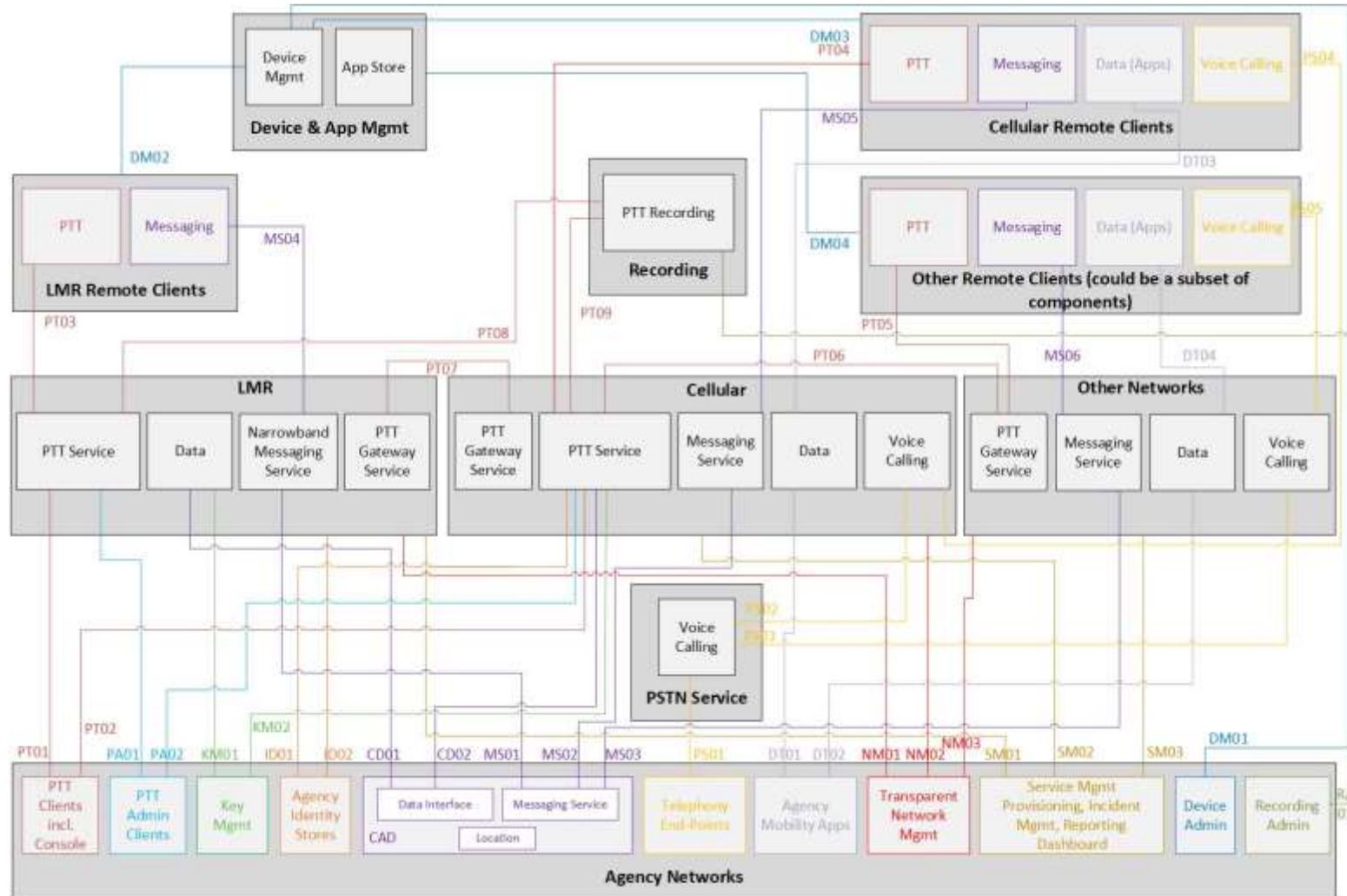


Figure 2: PTT and Related Services - Connections

### 5.2.1 Functional Categories

| Category                | Description  |
|-------------------------|--|
| Device & App Mgmt.      | Systems for device and application management hosted by a Service Provider or other third party                              |
| Cellular Remote Clients | All cellular devices whether portable, mobile or fixed providing cellular services to Emergency Services personnel           |
| LMR Remote Clients      | All LMR devices whether portable, mobile or fixed providing digital radio services to Emergency Services personnel           |
| Recording               | Systems for recording of MCPTT over cellular and LMR calls hosted by an agency, Service Provider or third party              |
| Other Remote Clients    | All satellite or other services devices whether portable, mobile or fixed providing services to Emergency Services personnel |
| LMR                     | Land Mobile Radio network systems  |
| Cellular                | Cellular network systems   |
| Other Networks          | Satellite, Personal Alerting or other network systems  |
| PSTN Service            | Public Switch Telephone Network systems  |
| Agency Networks         | All systems that are hosted within agency networks either on premise or cloud-based  |

## 5.2.2 Interfaces

| ID   | Interface Type     | Function  | Endpoints  | Standards/Applicable Specifications   | Agency Specific Information  | Transition Considerations   |
|------|--------------------|---|--|---|--|---|
| PT01 | LMR IP interface   | Carry LMR PTT console traffic – media and signalling. | Agency voice console and other clients to LMR service.   | P25 (standardised by TIA).<br><br>Must work complementary with PT02 and PT07.                                     | Must function across multiple levels of resilience appropriate for highly available Communications Centres with out-of-band access to local LMR channel. | Resilient network connections of sufficient capacity to be in place.<br><br>Use of existing console.<br><br>Communications Centre desktop/application suite.<br><br>Use of station consoles (directly patched to radios) as part of resilience. |
| PT02 | MCPTT IP interface | Carry MCPTT console traffic – media and signalling.   | Agency voice console and other clients to MCPTT service. | Mission Critical Voice standards by 3GPP (minimum Release 14).<br><br>Must work complementary with PT01 and PT07. | Must function across multiple levels of resilience appropriate for highly available Communications Centres.  | Resilient network connections of sufficient capacity to be in place.<br><br>Use of existing console.<br><br>Communications Centre desktop/application suite.  |

| ID   | Interface Type  | Function  | Endpoints  | Standards/Applicable Specifications                            | Agency Specific Information  | Transition Considerations   |
|------|---|---|--|--|--|---|
| PT03 | LMR Air interface                                       | Carry remote PTT traffic over the LMR network – media and signalling. | Agency LMR devices to LMR PTT service.               | P25 (standardised by TIA).                                     | Primary or secondary service for frontline voice communications depending on network availability. | Transition from existing network with handheld, in-vehicle, in-station and Communications Centre console operational environment.<br><br>Core aspects must be complete before transitioning any remote users. |
| PT04 | MCPTT IP interface over Cellular                        | Carry remote MCPTT traffic – media and signalling.                    | Agency MCPTT clients to MCPTT service.               | Mission Critical Voice standards by 3GPP (minimum Release 14). | Primary or secondary service for frontline voice communications depending on network availability. | Resilient network connections of sufficient capacity to be in place.<br><br>Core aspects must be complete before transitioning any remote users.  |
| PT05 | MCPTT IP interface over other networks (e.g. satellite) | Carry remote MCPTT traffic – media and signalling.                    | Agency MCPTT clients to MCPTT service (via gateway). | Mission Critical Voice standards by 3GPP (minimum Release 14). | Tertiary service for frontline voice communications depending on network availability.             | Resilient network connections of sufficient capacity to be in place.<br><br>Core MCPTT aspects and inter-working must be complete before transition.  |

| ID   | Interface Type  | Function  | Endpoints  | Standards/Applicable Specifications   | Agency Specific Information  | Transition Considerations  |
|------|---|---|--|---|--|--|
| PT06 | MCPTT IP interface between IP networks                | Carry remote MCPTT traffic – media and signalling.      | Agency MCPTT clients to MCPTT service (via gateway). | Mission Critical Voice standards by 3GPP (minimum Release 14).                        | Connectivity between other networks through to MCPTT service.  | N/A  |
| PT07 | IP IWF (Inter Working Function) between LMR and MCPTT | Carry remote PTT traffic – media and signalling.        | LMR gateway to MCPTT gateway.                        | Mission Critical Voice Inter Working Function standards by 3GPP (minimum Release 16). | Requested talk-groups must be spanned across MCPTT and LMR environments.   | Must be in place before MCPTT and LMR services are used in production together for requested talkgroups.<br><br>Console and CAD integration must be in place alongside current set-up. |
| PT08 | LMR IP Interface                                      | Carry LMR IP media and meta-data to Recording server.   | LMR service to Recording server.                     | P25 (standardised by TIA).  | Security considerations for recorded media are paramount.<br><br>Administrative rights as to who can access what content is important. | Agencies may elect to use their existing Red Box systems or migrate partially or wholly to a PSN service.  |
| PT09 | MCPTT interface                                       | Carry MCPTT IP media and meta-data to Recording server. | MCPTT service to Recording server.                   | Mission Critical Voice standards by 3GPP (minimum Release 14).                        | Security considerations for recorded media are paramount.<br><br>Administrative rights as to who can access what content is important. | Agencies may elect to use their existing Red Box systems or migrate partially or wholly to a PSN service.  |

| ID   | Interface Type                        | Function                                      | Endpoints  | Standards/Applicable Specifications   | Agency Specific Information  | Transition Considerations                   |
|------|---------------------------------------|---|--|---|--|---|
| PA01 | IP Interface to LMR admin portal      | Carry secure web and/or secure API traffic.   | Configuration and group management clients (agency) to configuration and group management server (Service Provider). | Secure web connection.  | Different roles are required to allow appropriate administrative access.                           | IDAM integration for access.                |
| PA02 | IP Interface to MCPTT admin portal    | Carry secure web and/or API traffic.          | Configuration and group management clients (agency) to configuration and group management server (Service Provider). | Secure web connection.  | Different roles are required to allow appropriate administrative access.                           | IDAM integration for access.                |
| KM01 | IP Interface to Key Management Server | Carry key management traffic P25 Network.     | Key management client (agency) to key management server (Service Provider).  | P25 (standardised by TIA)   | Agencies require control over access to encryption keys.   | Appropriate controls for key management.    |
| KM02 | IP Interface to Key Management Server | Carry key management traffic over secure API. | Key management client (agency) to key management server (Service Provider).  | Secure web connection.  | Agencies require control over access to encryption keys.   | Appropriate controls for key management.    |
| ID01 | IP Interface for Identity Management  | Carry authentication requests and responses.  | Service Provider interface to agency identity store. Optional federation function to abstract this.                  | Federated Identity management using standards-based technologies such as OAUTH, SAMLv2. | Single sign-on and user lifecycle management are important to the integrity of access to services. | Design for how to securely federate access. |

| ID   | Interface Type                       | Function                                     | Endpoints   | Standards/Applicable Specifications   | Agency Specific Information  | Transition Considerations   |
|------|--------------------------------------|--|---|---|--|---|
| ID02 | IP Interface for Identity Management | Carry authentication requests and responses. | Service Provider interface to agency identity store. Optional federation function to abstract this. | Federated Identity management using standards-based technologies such as OAUTH, SAMLv2. | Single sign-on and user lifecycle management are important to the integrity of access to services. | Design for how to securely federate access.   |
| CD01 | IP LMR interface for CAD             | Carry packet data services.                  | CAD and LMR system.   | P25 (standardised by TIA) or in format supported by CAD systems.                        | Business process integration is essential.   | <p>Resilient network connections of sufficient capacity to be in place.</p> <p>Co-existence with existing integration and processes.</p> <p>Managing alongside ongoing lifecycle management of CAD system.</p> <p>Possible development within CAD required.</p> |

| ID   | Interface Type                     | Function  | Endpoints  | Standards/Applicable Specifications                              | Agency Specific Information   | Transition Considerations   |
|------|------------------------------------|---|--|--|---|---|
| CD02 | IP MCPTT interface for CAD         | Carry incident information and remote user meta-data. | CAD and MCPTT application.                       | Secure connection via API or in format supported by CAD systems. | Business process integration is essential.  | <p>Resilient network connections of sufficient capacity to be in place.</p> <p>Co-existence with existing integration and processes.</p> <p>Managing alongside ongoing lifecycle management of CAD system.</p> <p>Possible development within CAD required.</p>                         |
| MS01 | IP LMR Messaging interface for CAD | Carry two-way messaging information.                  | CAD Messaging service and LMR Messaging gateway. | P25 (standardised by TIA).                                       | <p>Pre-defined status messages (including priority and duress) will need to be designed and agreed.</p> <p>Business process integration is essential.</p> | <p>Resilient network connections of sufficient capacity to be in place.</p> <p>Co-existence with existing integration and processes.</p> <p>Managing alongside ongoing lifecycle management of CAD system.</p> <p>CAD integration.</p> <p>Possible development within CAD required.</p> |

| ID   | Interface Type                         | Function                             | Endpoints  | Standards/Applicable Specifications   | Agency Specific Information  | Transition Considerations   |
|------|--|--------------------------------------|--|---|--|---|
| MS02 | IP Cellular (Text/SMS) Message for CAD | Carry two-way messaging information. | CAD Messaging service and Cellular SMS Messaging gateway.                            | Leverage Mission Critical standards for Quality of Service, Priority and Pre-emption (QPP). Needs to extend end-to-end ensuring all aspects implement this including the network, gateways and servers. |  | <p>Resilient network connections of sufficient capacity to be in place.</p> <p>Co-existence with existing integration and processes.</p> <p>Managing alongside ongoing lifecycle management of CAD system.</p> <p>CAD integration.</p> <p>Possible development within CAD required.</p> |
| MS03 | IP 'Other' Messaging interface for CAD | Carry two-way messaging information. | CAD Messaging service and remote Messaging gateway (e.g. Personal Alerting Service). | As relevant to the specific network (e.g. Personal Alerting Service).   | Business process on how to associate different connection types to individuals, vehicles or stations as appropriate. | <p>Resilient network connections of sufficient capacity to be in place.</p> <p>Co-existence with existing integration and processes.</p> <p>Managing alongside ongoing lifecycle management of CAD system.</p> <p>CAD integration.</p> <p>Possible development within CAD required.</p> |

| ID   | Interface Type                            | Function                             | Endpoints   | Standards/Applicable Specifications                                   | Agency Specific Information  | Transition Considerations   |
|------|---|--------------------------------------|---|---|--|---|
| MS04 | LMR Messaging Air interface               | Carry two-way messaging information. | LMR Messaging service and LMR remote devices.   | P25 (standardised by TIA).  | Specific use of LMR messaging varies by agencies and end-to-end processes are essential to understand for detailed design.                           | Transition from existing network with handheld, in-vehicle, in-station and Communications Centre console operational environment.<br><br>Core aspects must be complete before transitioning any remote users. |
| MS05 | Text / SMS Cellular interface             | Carry two-way messaging information. | Cellular SMS server and cellular remote devices.  | 3GPP standards including QPP.   | Specific use of SMS varies by agencies and end-to-end processes are essential to understand for detailed design.                                     | Core aspects must be complete before transitioning any remote users.  |
| MS06 | Messaging interface(s) for other networks | Carry two-way messaging information. | Messaging service to remote devices over specific networks (e.g. Personal Alerting Service) | As relevant to the specific network (e.g. Personal Alerting Service). | Specific use of the other types of messaging varies by agencies and region, so end-to-end processes are essential to understand for detailed design. | Core aspects must be complete before transitioning any remote users.  |

| ID   | Interface Type                       | Function                          | Endpoints   | Standards/Applicable Specifications   | Agency Specific Information                                    | Transition Considerations  |
|------|--------------------------------------|-----------------------------------|---|---|--|--|
| PS01 | Agency PSTN trunks                   | Carry voice calls and signalling. | Agency VoIP or PBX gateway to telecommunications gateway. | Currently ISDN (generally) but planned to migrate to SIP.<br>Provide QPP end-to-end for calling to Emergency Services remote devices.   | Typically shared with agency-wide organisational use.          | Capacity and ability to apply QPP end-to-end.                        |
| PS02 | Telco Interconnect                   | Carry voice calls and signalling. | Telco gateway to telco gateway.                           | Relevant interconnect agreement.  | N/A.   | Capacity.  |
| PS03 | Telco Interconnect                   | Carry voice calls and signalling. | Telco gateway to telco gateway.                           | Relevant interconnect agreement.  | N/A.   | Capacity.  |
| PS04 | Voice interface for Cellular calling | Carry voice calls and signalling. | Cellular Voice server to remote cellular device.          | Leverage Mission Critical standards for Quality of Service, Priority and Pre-emption (QPP). Needs to extend end-to-end ensuring all aspects implement this including the network, gateways and servers. | Device behaviour for devices that also run MCPTT to be agreed. | Core aspects must be complete before transitioning any remote users. |

| ID   | Interface Type                            | Function                          | Endpoints  | Standards/Applicable Specifications   | Agency Specific Information   | Transition Considerations   |
|------|---|-----------------------------------|--|---|---|---|
| PS05 | Voice interface for Other network calling | Carry voice calls and signalling. | Voice server to remote device (e.g. satellite).                | Provide QPP-equivalent capability to ensure calls can always get through.<br><br>3GPP specified standards for other networks are to be used where applicable.   | Processes for when to use the device (e.g. if it is via a different phone number, how does a user know when to use that contact method?).   | Core aspects must be complete before transitioning any remote users.<br><br>Specific equipment that may be required either handheld, accessories, in-vehicle or on-station. |
| DT01 | IP interface to Cellular data network     | Carry mobility application data.  | Agency firewall to Cellular network Points of Presence (POPs). | 3GPP standards for Mission Critical Data (Release 14 minimum) and end-to-end application of QPP for all aspects of the connection.<br><br>Applications are expected to use their own encryption or use an agency VPN to appropriately secure their applications for carriage across a public network. | Mobility applications vary greatly in their demand for the network and how they can be identified. This will need to be baselined and understood for detailed design along with guidance for how new apps are to be deployed and guaranteed appropriate QPP.<br><br>Some agencies will require an APN, others will not. | Resilient network connections of sufficient capacity to be in place.<br><br>Co-existence with existing integration and processes.   |

| ID   | Interface Type                      | Function  | Endpoints   | Standards/Applicable Specifications  | Agency Specific Information   | Transition Considerations  |
|------|-------------------------------------|---|---|--|---|--|
| DT02 | IP interface to Other data networks | Carry mobility application data (e.g. dispatch turnout messaging data). | Agency firewall to remote network POPs (e.g. internet, satellite, IOT). | <p>IP interconnect.</p> <p>QPP-equivalent guarantees of service are required.</p> <p>Applications are expected to use their own encryption or use an agency VPN to appropriately secure their applications for carriage across a public network.</p> | <p>Mobility applications vary greatly in their demand for the network and how they can be identified. This will need to be baselined and understood for detailed design along with guidance for how new apps are to be deployed and guaranteed appropriate QPP.</p> | <p>Resilient network connections of sufficient capacity to be in place.</p> <p>Co-existence with existing integration and processes.</p> |

| ID   | Interface Type             | Function  | Endpoints  | Standards/Applicable Specifications  | Agency Specific Information  | Transition Considerations  |
|------|----------------------------|---|--|--|--|--|
| DT03 | Cellular IP MC Data bearer | Carry mobility application data (e.g. dispatch turnout messaging data). | Cellular data service to remote cellular device.                             | <p>3GPP standards for Mission Critical Data (Release 14 minimum) and end-to-end application of QPP for all aspects of the connection.</p> <p>Applications are expected to use their own encryption or use an agency VPN to appropriately secure their applications for carriage across a public network.</p> | <p>Mobility applications vary greatly in their demand for the network and how they can be identified. This will need to be baselined and understood for detailed design along with guidance for how new apps are to be deployed and guaranteed appropriate QPP.</p> <p>Some agencies will require an APN, others will not.</p> | Core aspects must be complete before transitioning any remote users. |
| DT04 | IP Data bearer             | Carry mobility application data (e.g. dispatch turnout messaging data). | Other network data service to remote device (e.g. internet, satellite, IOT). | <p>As relevant to the specific network technology.</p> <p>QPP-equivalent guarantees of service are required.</p> <p>Applications are expected to use their own encryption or use an agency VPN to appropriately secure their applications for carriage across a public network.</p>                          | Use cases need to be clearly understood, and technology only used when/where required (especially if high cost).   | Core aspects must be complete before transitioning any remote users. |

| ID   | Interface Type                                  | Function                                    | Endpoints   | Standards/Applicable Specifications  | Agency Specific Information   | Transition Considerations  |
|------|---|---|---|--|---|--|
| NM01 | IP interface for transparent network management | Carry secure web and/or secure API traffic. | Transparent network management client (agency) to transparent network management server (Service Provider). | Secure web connection.   | View required in Communications Centres so dispatchers can see what network service is available to crews on their way to an incident, and at the incident. | Information to be displayed in a convenient and intuitive manner for the dispatcher, commander or other authorised user. |
| NM02 | IP interface for transparent network management | Carry secure web and/or secure API traffic. | Transparent network management client (agency) to transparent network management server (Service Provider). | Secure web connection.   | View required in Communications Centres so dispatchers can see what network service is available to crews on their way to an incident, and at the incident. | Information to be displayed in a convenient and intuitive manner for the dispatcher, commander or other authorised user. |
| NM03 | IP interface for transparent network management | Carry secure web and/or secure API traffic. | Transparent network management client (agency) to transparent network management server (Service Provider). | Secure web connection.   | View required in Communications Centres so dispatchers can see what network service is available to crews on their way to an incident, and at the incident. | How will this information be displayed in a useful manner for the dispatcher?  |
| SM01 | IP interface for service management             | Carry secure web and/or secure API traffic. | Service management client (agency) to Service management server (Service Provider).                         | Secure web connection. Where applicable open APIs such as those from TM Forum to be leveraged. | Agency-specific portal. PSN view across the service for overall KPIs.   | Integration with existing processes, configuration management databases and asset management systems.                    |

| ID   | Interface Type  | Function                                    | Endpoints   | Standards/Applicable Specifications   | Agency Specific Information  | Transition Considerations  |
|------|---|---|---|---|--|--|
| SM02 | IP interface for service management                       | Carry secure web and/or secure API traffic. | Service management client (agency) to Service management server (Service Provider).     | Secure web connection. Where applicable, open APIs such as those from TM Forum to be leveraged. | Agency specific portal. PSN view across the service for overall KPIs.  | Integration with existing processes, configuration management databases and asset management systems.  |
| SM03 | IP interface for service management                       | Carry secure web and/or secure API traffic. | Service management client (agency) to Service management server (Service Provider).     | Secure web connection. Where applicable, open APIs such as those from TM Forum to be leveraged  | Agency specific portal. PSN view across the service for overall KPIs.  | Integration with existing processes, configuration management databases and asset management systems.  |
| DM01 | IP interface for device management admin                  | Carry secure web and/or secure API traffic. | Device management admin client (agency) to Device management server (Service Provider). | Secure web connection.  | Processes for enrolling devices as an element of overall service deployment.   | Agencies may prefer to use existing device management capability.<br><br>Integration into provisioning and support processes.<br><br>IDAM integration. |
| DM02 | LMR over the air interface and/or corporate LAN/WAN/Wi-Fi | Carry LMR device management information.    | Device management server to LMR device.   | P25 (standardised by TIA).  | Processes for enrolling devices as an element of overall service deployment.<br><br>Agency specific processes including local configuration from a laptop for specific use cases are required. | Integration into provisioning and support processes.<br><br>IDAM integration.  |

| ID   | Interface Type   | Function  | Endpoints  | Standards/Applicable Specifications | Agency Specific Information  | Transition Considerations  |
|------|--|---|--|-------------------------------------|--|--|
| DM03 | IP interface for cellular device management                              | Carry cellular device management information.                 | Device management server to cellular device.                                       | Secure IP connection.               | Processes for enrolling devices as an element of overall service deployment.   | Agencies may prefer to use existing device management capability.<br><br>Integration into provisioning and support processes.<br><br>IDAM integration. |
| DM04 | IP interface for other device management                                 | Carry other device management information.                    | Device management server to other device.  | Secure IP connection.               | Processes for enrolling devices as an element of overall service deployment.   | Agencies may prefer to use existing device management capability.<br><br>Integration into provisioning and support processes.<br><br>IDAM integration. |
| RA01 | IP interface for admin and review of recording system and stored content | Carry web, media traffic, securely over web or API interface. | Recording admin and review client (agency) to Recording server (Service Provider). | Secure web connection.              | Security considerations for recorded media are paramount.<br><br>Administrative rights as to who can access what content is important. | Agencies may elect to use their existing Red Box systems or migrate partially or wholly to a PSN service.  |

Notes:

1. For architectural purposes, Push-to-Video is viewed as being an escalation of MCPTT, and therefore is implicit in Figure 2 and the above table wherever MCPTT is shown, and the endpoints support video.

2. Where cellular network(s) are mentioned, it is expected that all available networks can be used transparently by any authorised connection. This aspect of the architecture is 'in the cloud' from the perspective of the PSN programme but will be fundamental to the Service Provider's method of delivery.
3. Cellular services will be LTE or above including VoLTE whenever possible. Fall-back to 3G Voice and data should be a last resort only but supported transparently to the end user.
4. Presentation of talkgroups that are present in both the MCPTT over cellular and LMR domains (and potentially other domains as well) will need to be consistent across PT01 and PT02 in conjunction with the Interworking gateways in those services. An appropriate architecture will be required to enable full functionality as well as technology domain resilience.
5. Performance standards must fully support agency requirements and, where possible, be standards-based. Where a standard exceeds the agencies requirements, the standard will be the default.

## 6. Common Agency Integration Enablers

The integration of systems in the PSN programme is between multiple agencies, multiple Service Providers and multiple supporting partners. Over time, the integration of new systems and capabilities has created many point-to-point integrations between tightly coupled systems in today's environment. High cost and risk change can be a result of this. During the transition to PSN capabilities, the integration points will be rationalised to achieve the following goals:

- Common and consistent integration across agencies including new agencies in addition to the first four in the future;
- Loose coupling of services to ensure more independent release lifecycles;
- Low marginal cost and effort to integrate new systems with existing capabilities; and
- Minimise or eliminate lock step changes on capability releases.

Integration patterns will be chosen that are aligned with the goals above. Integration patterns include:

- Common interface standards used by all agencies and Service Providers (e.g. cellular and LMR standards);
- Common systems shared by all agencies (e.g. app store);
- Common interface specifications implemented by all agencies and Service Providers (e.g. messaging, location or recording APIs);
- A common interface provided by a single Service Provider to access capabilities of multiple Service Providers (e.g. PSTN); and
- Concurrent support for multiple interface versions to provide agencies with reasonable windows for adoption and transition.

Agencies and Service Providers will likely benefit from common integration components, tools, and documentation, and a lab environment for integration activities.

The integration of PSN capabilities will be inhibited by a piecemeal approach where each Service Provider provides different interfaces for Identity and Access Management (IDAM), messaging, location, service/user provisioning and other systems. Each Service Provider must provide an approach to integration that supports:

- Service Provider integration with interfaces offered by agencies or other parties' systems (e.g. common messaging, location, IDAM);
- Hosting of systems that support capabilities offered by multiple Service Providers (e.g. common messaging, voice calling services); and
- Support multiple interface versions concurrently.

To achieve the PSN programme's goals of loose coupling and avoiding lock step change, agencies will benefit from preparation of existing systems prior to PSN capability releases being available for transition. For example, adopting common architecture for messaging, location and identity will reduce the time, complexity and transition risk.

The Service Providers will provide a compelling multi-agency common integration approach for the following:

- Federated Identity and Access Management;
- Messaging;
- Location;
- Voice;

- Recording;
- Security testing and certification;
- Device testing and certification;
- Transparent Network Management services; and
- Other.

Taking a common approach to all the items above will:

- Simplify transition;
- Minimise agency effort to integrate or access separate Service Provider systems;
- Improve lifecycle management through decoupling of agency and Service Provider systems;
- Improve security and access control;
- Avoid every agency integrating with every Service Provider in a custom manner; and
- Incur only marginal cost adding additional agencies beyond the first four.

### 6.1 Federated Identity and Access Management

A common approach will also:

- Simplify the on-boarding and off-boarding of agency users;
- Provide Single Sign On for all administrative functions within PSN; and
- Improve security and access control.

### 6.2 Messaging

A common approach will also:

- Separate message from medium: a message could be delivered to a user as an SMS, via LMR or on an over-the-top messaging service.

### 6.3 Location

A common approach will also:

- Simplify the creation of new location-based services such as those for situational awareness.

### 6.4 Voice

A common approach will also:

- Ensure end-to-end QPP; and
- Provide greater resilience.

### 6.5 Recording

A common approach will also:

- Ensure consistency across multiple domains (i.e. cellular, LMR, satellite).

### 6.6 Security Testing and Certification

Common integration services for security testing and certification will reduce the overhead of individual agencies.

## 6.7 Device Testing & Certification

Efficient capability for device testing and certification is necessary for the integration of PSN capabilities and agency transition activities.

## 6.8 Transparent Network Management

Transparent network management will only be possible with the application of common interfaces and data transfer formats. These formats will need to be agreed and Service Providers will be expected to align with PSN specifications and integration governance.

## 6.9 Other

During the integration activities undertaken during transition other common areas will be identified and Service Providers will be expected to align with PSN common specifications and integration governance.

## 7. Agency Application Usage of PSN Capabilities

PSN services, as shown in the previous section, are enablers beyond PTT and other voice capability for agencies. The most obvious example is Mission Critical Data. Putting mobility applications across a reliable bearer means that business processes that rely on them can shift from best efforts availability to an operationally reliable service with availability, performance and coverage service levels underpinning them.

This section highlights a number of areas where agencies can leverage the PSN capabilities further and integrate these into their systems and processes to deliver value to their organisations beyond the initial scope of PSN deliverables.

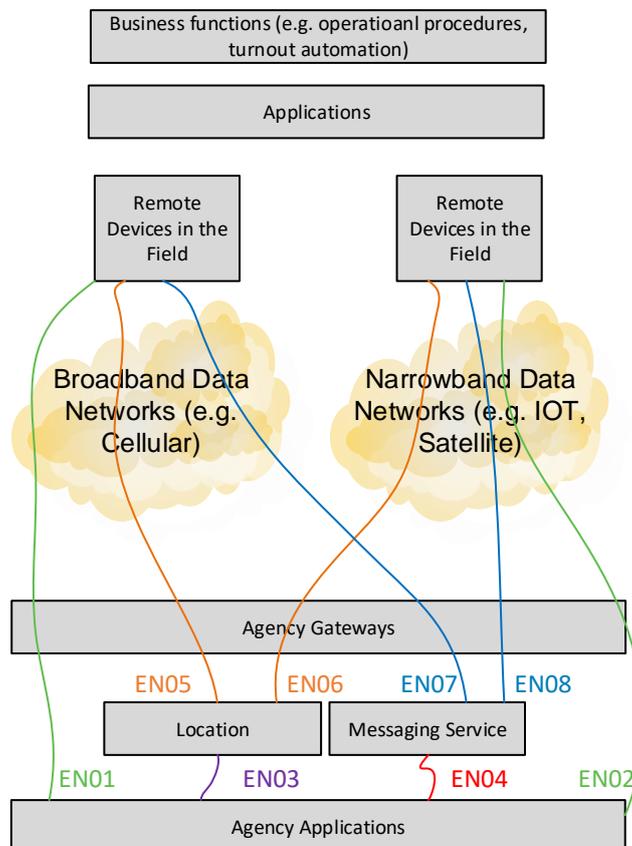


Figure 3: Agency Enablers

| ID   | Description  | Examples  |
|------|--|---|
| EN01 | IP connectivity out to mobile broadband clients over a Mission Critical data bearer.                           | Mobility applications such as dispatch, situational awareness, etc.   |
| EN02 | IP connectivity out to mobile narrowband clients over a Mission Critical data bearer.                          | Lightweight mobility applications (e.g. turnout automation functions such as sounding an alert and opening a door etc). |
| EN03 | IP connectivity to Location service(s) that shows where agency resources are geographically in near real-time. | Situation awareness applications, CAD, etc.   |
| EN04 | IP connectivity to 'Messaging' service(s) that will then have connections out to the various networks.         | Dispatch applications, or other alerting or notification systems.   |
| EN05 | Connectivity to broadband networks where remote resources can report their GPS location.                       | Automatic Vehicle Location (AVL) over cellular, cellular devices, tablets, wearables, etc.                              |
| EN06 | Connectivity to narrowband networks where remote resources can report their GPS location.                      | AVL (over satellite), IOT devices, etc.   |
| EN07 | Connectivity to remote messaging clients over broadband networks.  | Cellular SMS, in-app messaging (e.g. PTT or other dispatch application), etc.   |
| EN08 | Connectivity to remote messaging clients over narrowband networks.   | LMR status messaging, IOT devices, paging, satellite text messaging, etc.   |

## 8. Test and Integration Lab

The agencies and Service Providers may jointly establish a test and integration lab(s) for the purposes of integration and testing activities.