Key user selection criteria driving public safety mobile broadband core networks

26 October 2026

Advancing global critical communications for a safer, more connected world

Background to this study

In the Public Safety market, government authorities in more than 11 countries have deployed or are deploying **mission critical mobile broadband** services, beginning with the implementation of a **dedicated core network**, with many more countries evaluating or planning to procure such equipment and services.

Following requests from several members, TCCA were asked to provide a succinct, **high-level description** of the various **3GPP core network architecture options** that are deployed or being deployed in the market – importantly via government procurement - and **key user criteria** that were used to select these, as part of the decision-making process. Whilst the criteria identified is not exhaustive, it was common across the examples cited in this analysis.

This work was undertaken by the **Core Architecture Options Task Force**. The majority of input for this work was provided by government authorities involved in the procurement of public safety networks.

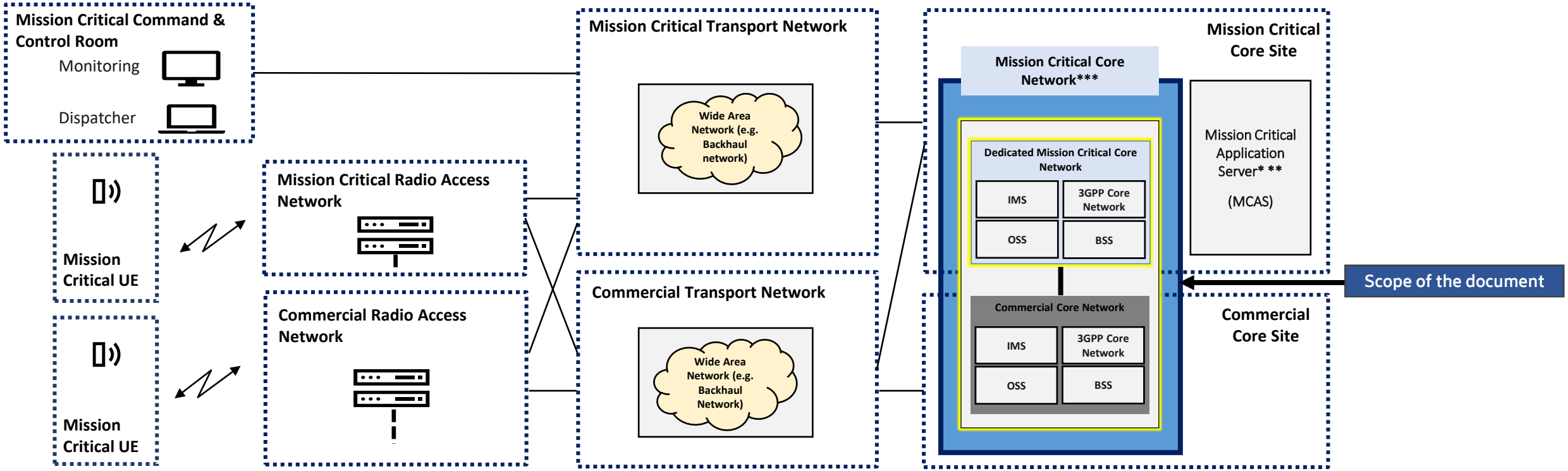
Contents

1. Mission Critical High-Level Network Architecture
2. Mission Critical Core Network - Detailed View
3. Public Safety Broadband Deployment Models
    1. Considerations
    2. High-Level Overview
    3. Examples of Combination Models
    4. MVNO Deployment Models
    5. Definitions
4. Key User Selection Criteria Definition
5. Comparison of Public Safety Broadband Deployment Models
    1. High-Level Considerations
    2. Models currently deployed/being deployed in the market for broadband services
6. Abbreviations
7. Core Architecture Options (CAO) Task Force Members
8. Appendix - Overview on RAN Sharing Public Safety Broadband Deployment Models

Mission Critical High-Level Network Architecture

The primary objective of this task force was to capture the range of **core network architectures** that have been **deployed or are being deployed**, driven by **government procurements**. And, furthermore, capture the key user criteria driving the implementation of the **Mission Critical Core Network** architecture as shown below.

Note: Although not the focus of this task force, the Mission Critical Application Server (MCAS) – enabling 3GPP Mission Critical Services (MCX), including Mission Critical Push-to-Talk - may be co-located at the same **Mission Critical Core Site**.



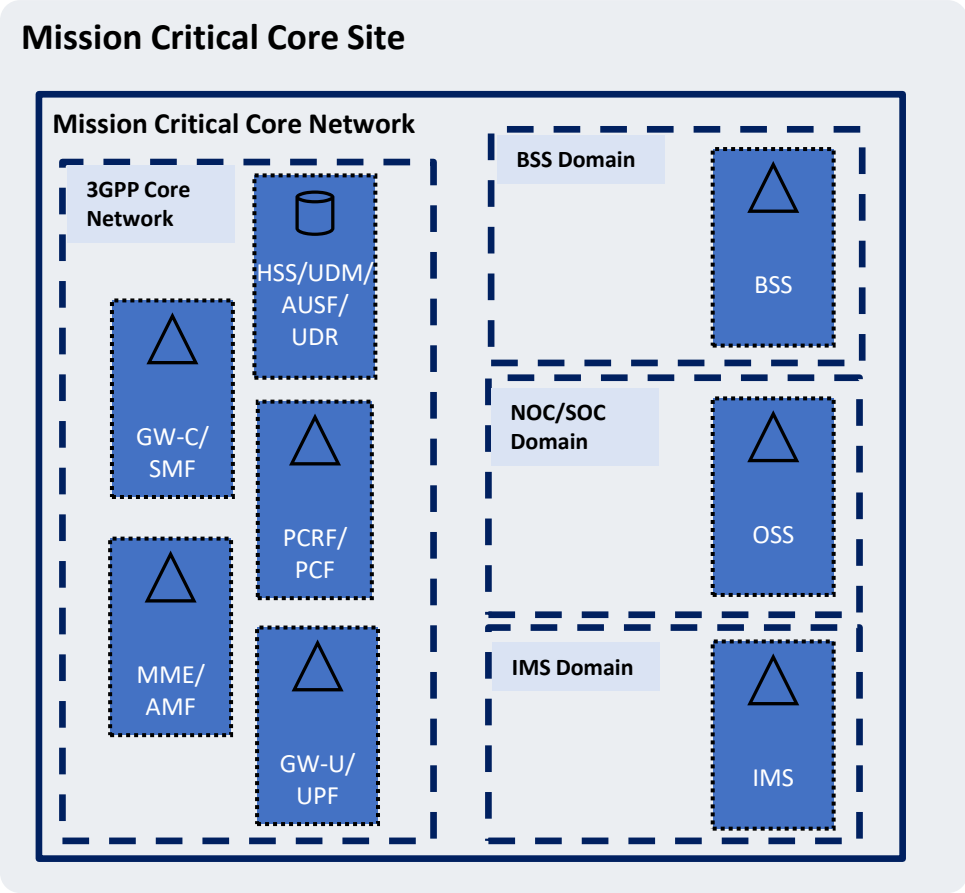
* The MCAS may be implemented one of two ways, subject to Mission Critical Application vendor support i.e. either using an IMS SIP Core versus embedded SIP Core. The evaluation of SIP core implementations will be considered under Phase 2 task force work.

** The MCAS is operated by the Public Safety Operator (PSO).

*** The Mission Critical Core Network can leverage commercial network assets with different levels of sharing, please refer to slide 7 and 8 for more details.

Mission Critical Core Network
Detailed View

- This slide is detailing the Mission Critical Core Network components including the 3GPP core network, IMS, OSS and BSS.
- In the Mission Critical Core Network, the IMS can play two roles either acting as a SIP core - responsible for the SIP registration, service selection, and routing in the signaling control plane - and/or it can be used for VoLTE/VoNR services. The Public Safety Operator (PSO) can also leverage the Mobile Network Operator's (MNO) IMS for non-critical services (VoLTE/VoNR).
- The MCAS (not shown here) may be co-located with the Mission Critical Core Site or distributed elsewhere.
- Furthermore, the MCAS may be implemented one of two ways, subject to Mission Critical Application vendor support i.e. either using IMS SIP Core versus embedded SIP Core. The evaluation of SIP core implementations will be considered under Phase 2 task force work.
- Note: The 3GPP Core Network functions shown (as part of the 3GPP core network) are not exhaustive.



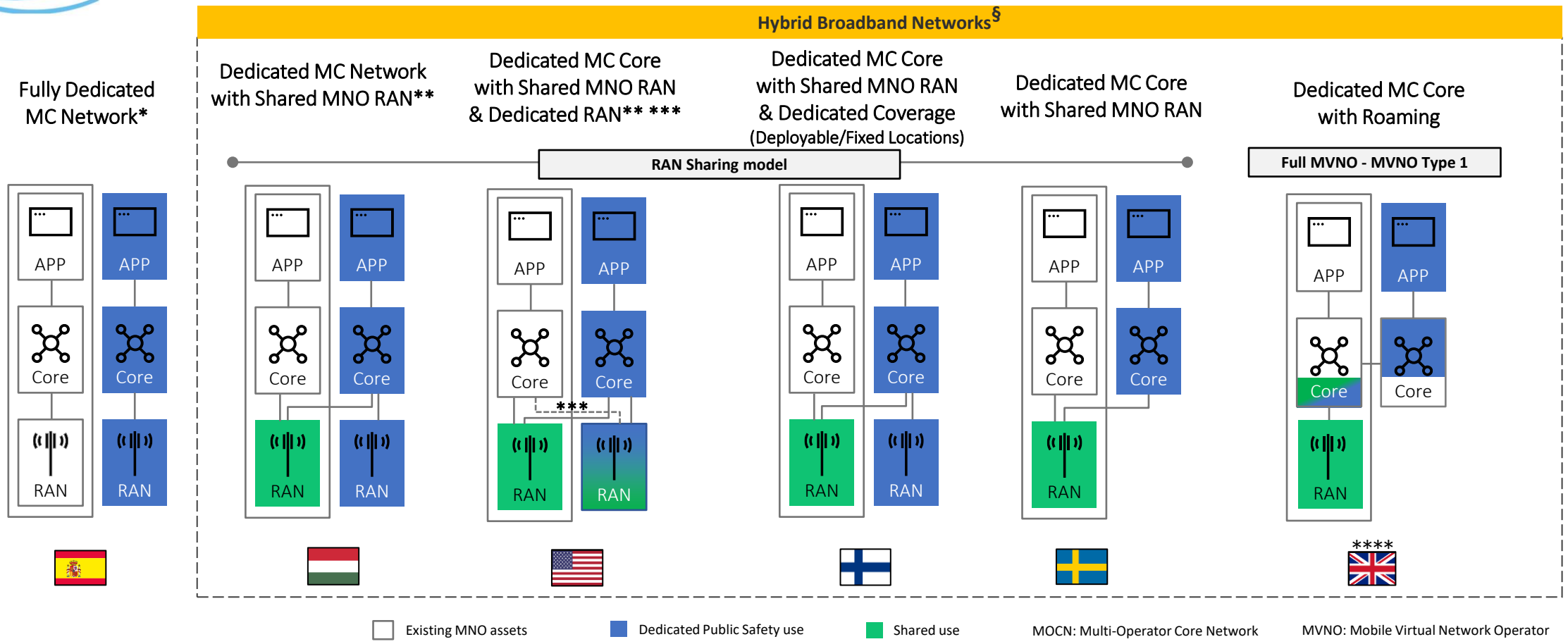
Public Safety Broadband Deployment Models
Considerations

- In the following slides, the Public Safety broadband deployment models of various countries are shown, and which have been or are being **delivered under government procurement**.
- The Public Safety broadband deployment models reflected in this presentation may not be the end state; it is **likely that these will evolve**, particularly **adding more resilience** over time. The latter may include but are not limited to integrating additional MNOs, potentially adding dedicated RAN using dedicated Public Safety spectrum, etc.

Public Safety Broadband Deployment Models

High-Level Overview (currently deployed/being deployed)

Note:
In practice, the APP box shown for all these deployment models will typically include a range of public safety-related applications, including the MCAS; the latter operated by the PSO.



* Assumes national coverage using dedicated RAN, including possible sharing of physical MNO sites and/or backhaul network.

** Assumes national (or near-national) coverage through use of a dedicated MC network (Core & RAN), combined with access to MNO RAN for additional capacity and coverage.

*** When not in use by mission critical users dedicated spectrum may be accessible to commercial users on a secondary basis; note QPP will be enabled in such cases to prioritize mission critical users.

**** ESN UK is delivered using a national roaming architecture, whereby the dedicated core network is split across PSO and MNO premises.

§ For all hybrid models here, it's assumed that the RAN (inc. transmission) is hardened sufficiently to meet end operational needs and supports QPP.

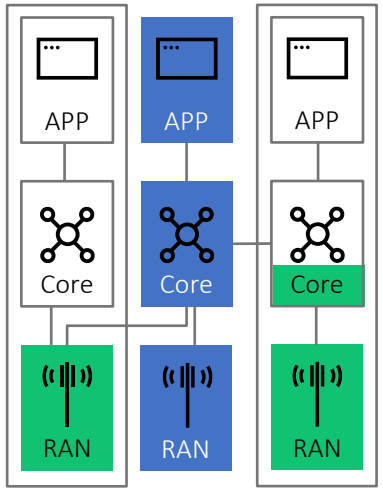
Public Safety Broadband Deployment Models

Examples of Combination Models (deployed/being deployed)

Note:
In practice, the APP box shown for all these deployment models will typically include a range of public safety-related applications, including the MCAS; the latter operated by the PSO.

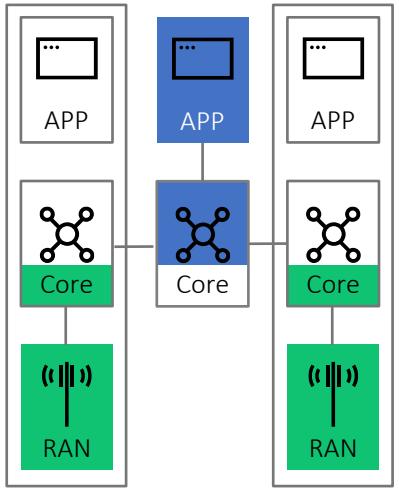
Hybrid Broadband Networks§

Dedicated MC Core
with Shared MNO RAN & Dedicated Coverage*
+ National Roaming (MNO2 and/or MNO3)**

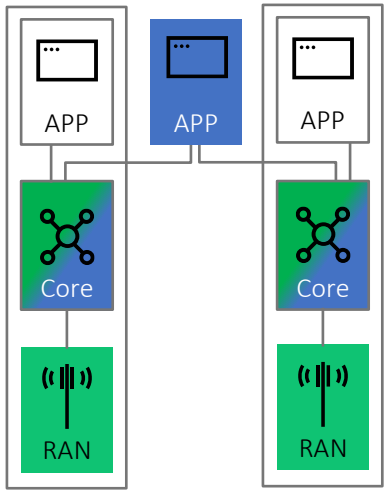


Being deployed

Dedicated MC Core
with Roaming
Full MVNO - MVNO Type 1
with multiple MNOs



Shared MNO Network with
Dedicated Core Elements
Light MVNO - MVNO Type 3
with two MNOs



***

Existing MNO assets | Dedicated Public Safety use | Shared use | MOCN: Multi-Operator Core Network | MVNO: Mobile Virtual Network Operator

Presentation on behalf of TCCA

* Dedicated Coverage includes use of dedicated RAN in deployable coverage solutions as well as at fixed locations.

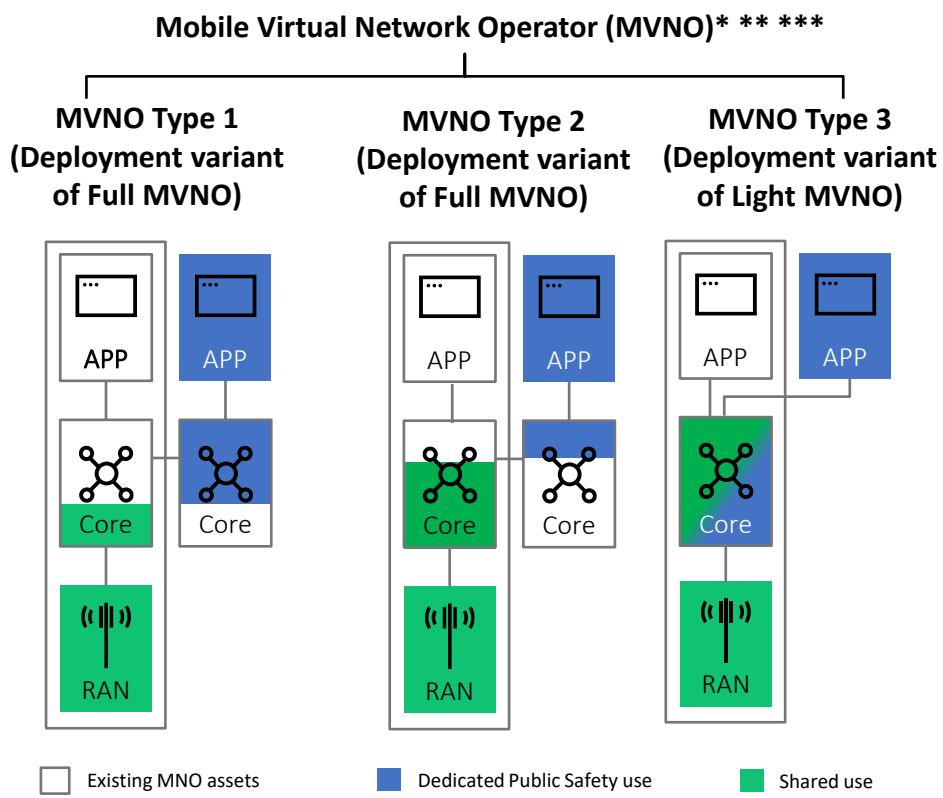
** Represents roaming to one (or more) MNOs, which may include QPP.

*** New Zealand's Public Safety Broadband Network currently does not include an MCAS. Other Public Safety-related applications are however in use.

§ For all hybrid models here, it's assumed that the RAN (inc. transmission) is hardened sufficiently to meet end operational needs and supports QPP.

Public Safety Broadband Deployment Models
MVNO Deployment Models (Deployed and Considered)

Note:
In practice, the APP box shown for all these deployment models will typically include a range of public safety-related applications, including the MCAS; the latter operated by the PSO.



MVNO deployment types are neither standardized in 3GPP, nor strictly defined in GSMA, even though there are MVNO references used throughout. **In practice, different variants of MVNO deployment types (and corresponding business models) exist in the market (both for LTE and NR).**

For this analysis, three possible variants of MVNO are described herein:

- **MVNO Type 1**: The Public Safety broadband network has dedicated PCRF/PCF, PGW-C/H-SMF, PGW-U/H-UPF, HSS/UDM/AUSF/UDR and may have dedicated IMS. The Public Safety broadband network has dedicated BSS and OSS. The PSO receives OSS metrics related to the shared use of the MNO's network assets. MVNO Type 1 is a roaming-based deployment where the Public Safety broadband network has its own PLMN ID.
- **MVNO Type 2**: The Public Safety broadband network has dedicated HSS/UDM/AUSF/UDR only and has its own PLMN ID. The Public Safety broadband network has dedicated BSS and OSS. The PSO receives OSS metrics related to the shared use of the MNO's network assets.
- **MVNO Type 3**: The Public Safety broadband network may not have any dedicated network assets except for the MCAS (if present). The PSO relies entirely on the MNO's BSS and OSS. There is also no dedicated PLMN ID for the Public Safety broadband network.

* In all MVNO types, the Public Safety broadband network does not have its own RAN nor the MME/AMF; instead, it shares the commercial MNO's RAN and MME/AMF.

** In all MVNO Types, the Public Safety broadband network may have some dedicated core network elements hosted at the MNO premises.
*** In all MVNO Types, the Public Safety broadband network shares core network elements with the commercial network to varying degrees.

Public Safety Broadband Deployment Models
Definitions (1/3)

- **Fully dedicated mission critical network**: The Mission Critical broadband network consists of end-to-end network assets including the RAN (and dedicated spectrum), the transport network, the core network (with IMS), the OSS/BSS and the MCAS. It's assumed to provide nationwide coverage using low band spectrum (up to 2x10 MHz), and possibly mid-band spectrum in high-risk or major operational areas with higher capacity needs, supported by a fleet of deployable coverage solutions. The backhaul and/or RAN sites may be shared with the MNO(s).
- **Dedicated mission critical network with shared MNO RAN:** The Mission Critical broadband network consists of end-to-end network assets providing national (or near-national) coverage, augmented with shared use of MNO RAN. Sharing agreements will typically include spectrum, towers, antennas, radios and baseband. Multiple levels of RAN sharing between the PSO and the MNO can be achieved as depicted in slide 24 (appendix). When shared MNO RAN (via MOCN) is used, it's assumed the RAN (inc. transmission) is hardened sufficiently, and supports QPP mechanisms, to meet public safety end user operational requirements, including prioritizing these users during major events / high-load situations.
- **Shared spectrum:** MNO spectrum is shared with the PSO and accessible to public safety users. It's assumed that QPP is configured in the MNO RAN to prioritize public safety users during major events / high-load situations.
- **Dedicated spectrum:** The spectrum is allocated to Public Safety use and, in some cases, may be accessible (subject to agreement) by MNO users when not in use by public safety users. QPP enables prioritization of public safety users during high-load situations, and band clearing techniques may also be used to reserve the spectrum exclusively for public safety users. The dedicated spectrum may be deployed nationwide or covering key operational areas.

Public Safety Broadband Deployment Models
Definitions (2/3)

- **Multi-Operator Core Network (MOCN) :** Defined in 3GPP TS 23.251/23.501. The Mission Critical broadband network shares the baseband, radio, and spectrum with the MNO, while operating a dedicated mission critical core network and the MCAS. The transport network can either be owned by the Mission Critical broadband network or by the MNO.
- **Multi-Operator Radio Access Network (MORAN) :** This concept is not explicitly defined in 3GPP and therefore subject to vendor-specific implementations. Please refer to the appendix slide 24 for more details about MORAN deployment variants.
- **Mobile Virtual Network Operator (MVNO) :** Various MVNO types exist in the market. As per 3GPP TS 22.101, MVNO do not have their own RAN, instead they rent RAN from one (or more) MNOs and offer mobile services re-using the network infrastructure of the MNO(s), i.e. the host Public Land Mobile Network (PLMN). The 3GPP standard does not define MVNO deployment models. Different MVNO deployment models exist in the market based on the level of sharing between the PSO and MNO.
  - **Full MVNO**: The Mission Critical broadband network consists of some dedicated core network assets and uses its own PLMN Identifier (PLMN ID). Several full MVNO variants exist in the market. One full MVNO variant (MVNO Type 1) operates on the basis that the public safety end user is accessing the MNO network as a roaming user, leveraging the MNO assets to access the MCX that are deployed in the Mission Critical Core Site or distributed outside the Mission Critical Core Site.
  - **Light MVNO:** The Public Safety broadband network may have dedicated core network functions, while leveraging the MNO network assets. The PSO may lease an IMSI series from the MNO's HSS/UDM. (No dedicated PLMN ID is allocated for the Public Safety network).

Public Safety Broadband Deployment Models
Definitions (3/3)

Secure MVNO: This is a full MVNO deployment model type that incorporates various security aspects to protect user data, communications, and privacy. These include but not limited to:

- IPSec VPNs between the Mission Critical Core Network and the MNO Core Network;
- End-to-End Encryption;
- Subscriber Database, controlled by the PSO;
- Topology hiding.

Key User Selection Criteria Definition (1/5)

Resiliency | **Control** | **Security** | **Operational** | **Affordability**

The requirements listed on this and the following slides are illustrative examples only. In practice, the list of requirements will be longer and far more extensive.

Resiliency

- Ability of the network to continuously deliver its intended services and functions in the face of challenges such as failures, attacks, natural disasters, or other unexpected disruptions.
- Network resilience also encompasses the network's ability to handle failures or disturbances gracefully, maintaining the highest possible level of performance in any given situation, even when parts of the system are compromised or under stress.
- A resilient network is designed to recover quickly from failures or outages, maximizing overall service availability and ensuring continuity of public safety user operations wherever possible.

Example of questions:

Q1 – Does the deployment model involve multiple commercial MNOs to increase resiliency (such as roaming to other operators to provide coverage extension, or as a fallback service) ?

Q2 – Does the deployment model involve use of dedicated spectrum, in some way, to address for example specific use cases, public safety user operational scenarios or restricted areas ?

Q3 – Does the deployment model involve additional redundancy layers by design ?

Key User Selection Criteria Definition (2/5)

Resiliency | **Control** | Security | Operational | Affordability

The requirements listed on this and the following slides are illustrative examples only. In practice, the list of requirements will be longer and far more extensive.

Control

- Ability for the PSO to operate and maintain the core network independently of the MNO(s), or as far as reasonably possible.
- Ability for the PSO to control and manage the network and the network services it provides, including configuration, access management, policy enforcement, QPP configuration, etc.
- Ability for the PSO to deploy, control, manage and maintain the MCX.

Example of questions:

Q1 – To what degree does the deployment model minimize coupling with commercial MNOs infrastructure ?

Q2 – Is the deployment model based on a Dedicated Core (full or partial) operated by the PSO ?

Q3 – Does the PSO operate the BSS and OSS ?

Q4 – Does the PSO have change management control over the network functions related to the deployment model ?

Key User Selection Criteria Definition (3/5)

Resiliency | Control | **Security** | Operational | Affordability

The requirements listed on this and the following slides are illustrative examples only. In practice, the list of requirements will be longer and far more extensive.

Security

- Ability of the Public Safety broadband network to meet CIA (Confidentiality, Integrity and Availability) requirements, including but not limited to protection of sensitive data (end user identities and organization, user-to-device mapping, service subscription, subscriber location information and the security keys).
- Ability of the Public Safety broadband network to detect, protect and mitigate attacks.

Example of questions:

Q1 – Does the network architecture provide a dedicated Security Operations Center (SOC) for the PSO ?

Q2 – Does the network architecture provide service layer separation for the PSO ?

Q3 – Does the PSO's network include the subscription data and the subscription management core functions ?

Q4 – Does the PSO have control over the lifecycle management of USIM profiles on the SIM/eSIMs used in the Public Safety broadband network ?

Q5 – Is the deployment model heavily dependent on the commercial MNO(s) from a security perspective ?

Key User Selection Criteria Definition (4/5)

Resiliency | Control | Security | **Operational** | Affordability

The requirements listed on this and the following slides are illustrative examples only. In practice, the list of requirements will be longer and far more extensive.

Operational

- Ability of the Public Safety broadband network to respond to the evolving communication and operational needs of the public safety end users, including increased performance, capacity and required functionality.
- Ability of the Public Safety broadband network to provide suitable means to the PSO and/or end user agencies for monitoring the functioning of the network and services (often referred to as network visibility, observability that includes Performance Management and Fault Management).
- Ability of the Public Safety broadband network to support the rollback of software releases, e.g. should latent issues be discovered that impact public safety end user operations.

Example of questions:

Q1 – How effective is the deployment model at allowing the PSO and end users agencies to monitor the network and services ?

Q2 – How effective is the deployment model at supporting the end user agencies' needs throughout the lifecycle of the network ?

Q3 – How effective is the deployment model at coping with day-to-day as well as major events/incidents, and the relationships needed between different parties including public safety end users, MNO(s) and the PSO ?

Key Selection Criteria Definition (5/5)

Resiliency | Control | Security | Operational | **Affordability**

The requirements listed on this and the following slides are illustrative examples only. In practice, the list of requirements will be longer and far more extensive.

Affordability

- Ability of the solution to fall within an average country's expenditure budgets (CAPEX & OPEX) of the PSO. Unless stated otherwise, it's assumed the PSO does not have the option to monetize dedicated spectrum.

Comparison of Public Safety Broadband Deployment Models

High-Level Considerations

- The following table highlights **key selection criteria identified as common** across the projects studied, supported by feedback gathered from discussions with government authorities. In addition to the identified criteria, various assumptions were made for each model - the main ones are stated as footnotes.
- **Each authorities' situation is unique** to a greater or lesser extent. As can be seen by the plethora of models deployed in the market today (the majority of which are 'hybrid' (see slides 7 and 8)), there is **no one size fits all**.
- From all the options theoretically possible, the actual number of options available to any given authority will be **affected by many 'local' factors**, such as the willingness and feasibility of one (or more) MNO to partner with authorities to provide fit-for-purpose mission critical communications; availability of dedicated spectrum; project investment profile, etc.
- Local factors are also likely to change over time, and therefore both short and long-term objectives need to be considered. From this study, it's apparent that a model an authority starts with is likely to evolve, **enhancing levels of resilience over time**.

Comparison of Public Safety Broadband Deployment Models

Representing models currently deployed/being deployed

		Hybrid Broadband Networks§						
	Fully Dedicated MC Network*	***Single MNO*** **Dedicated MC Network (Core/RAN) with shared MNO RAN (using MOCN)**	***Single MNO*** **Dedicated MC Core with shared MNO RAN (using MOCN) + Dedicated Coverage*** **	***Single MNO*** **Dedicated MC Core with shared MNO RAN (using MOCN)**	***Single MNO*** **Dedicated MC Core with Roaming, Full MVNO - MVNO Type 1**	***Combination*** **Dedicated MC Core with shared MNO1 RAN (using MOCN) + Dedicated Coverage*** ** **+ National Roaming to MNO2 and/or MNO3**	***Combination*** **Dedicated MC Core with Roaming, Full MVNO - MVNO Type 1 with multiple MNOs**	***Combination*** **Shared MNO Network with Dedicated Core Elements, Light MVNO - MVNO Type 3 with 2x MNOs**
	Model 1	**Model 2**	**Model 3**	**Model 4**	**Model 5**	**Model 6**	**Model 7**	**Model 8**
Resiliency	High	Highest	High-Medium	Medium	Medium	High	High	Medium-Low
Control	Highest	High	High	High	Medium	High-Medium	Medium	Low
Security	Highest	High	High	High	High-Medium‡	High‡	High-Medium‡	Low
Operational	Medium	Highest	High	High	Medium	High	Medium	Low
Affordability	Low	Low**	Medium	High-Medium	High	Medium	High	Highest

Note: MC = Mission Critical

* Assumes national deployment using low band spectrum, combined with use of mid-band spectrum for higher-risk operational areas and deployable coverage solutions.

** In the US deployment, the measure of Affordability will be significantly higher given the ability to have secondary use of dedicated public safety spectrum for consumers, during periods of inactivity by mission critical users; note QPP will be enabled in such cases to prioritize mission critical users.

*** Dedicated Coverage includes use of dedicated RAN in deployable coverage solutions as well as at fixed locations.

‡ Assumes a form of secure roaming is implemented (inc. topology hiding, IPSec, etc.).

§ For all hybrid models here, it's assumed that the RAN (inc. transmission) is hardened sufficiently to meet end operational needs and supports QPP.

Abbreviations (1/3)

Abbreviations	Definitions
APP	Suite of Public Safety applications including the Mission Critical Application Server
AMF	Access and Mobility management Function
AUSF	Authentication Server Function
BSS	Business Support Systems
CAO	Core Architecture Options
CIA	Confidentiality, Integrity and Availability
eSIM	Embedded Subscriber Identity Module
GW-C	PDN Gateway/Serving Gateway Control Plane
GW-U	PDN Gateway/Serving Gateway User Plane
HSS	Home Subscriber Server
IMS	IP Multimedia Subsystem
MC	Mission Critical
MCAS	Mission Critical Application Server

Abbreviations (2/3)

Abbreviations	Definitions
MCX	Mission Critical Services
MME	Mobility Management Entity
MNO	Mobile Network Operator
MOCN	Multi-Operator Core Network
MORAN	Multi-Operator Radio Access Network
MVNO	Mobile Virtual Network Operator
NOC	Network Operations Center
OSS	Operations Support Systems
PCF	Policy Control Function
PCRF	Policy and Charging Rules Function
PLMN	Public Land Mobile Network
PLMN ID	Public Land Mobile Network Identifier
PSO	Public Safety Operator

Abbreviations (3/3)

Abbreviations	Definitions
QPP	QoS, Priority and Pre-emption
RAN	Radio Access Network
SIM	Subscriber Identity Module
SMF	Session Management Function
SOC	Security Operations Center
TF	Task Force
UDM	Unified Data Management
UDR	Unified Data Repository
UE	User Equipment
UPF	User Plane Function
USIM	Universal Subscriber Identity Module
VoLTE	Voice over Long Term Evolution
VoNR	Voice over New Radio
3GPP	3rd Generation Partnership Project

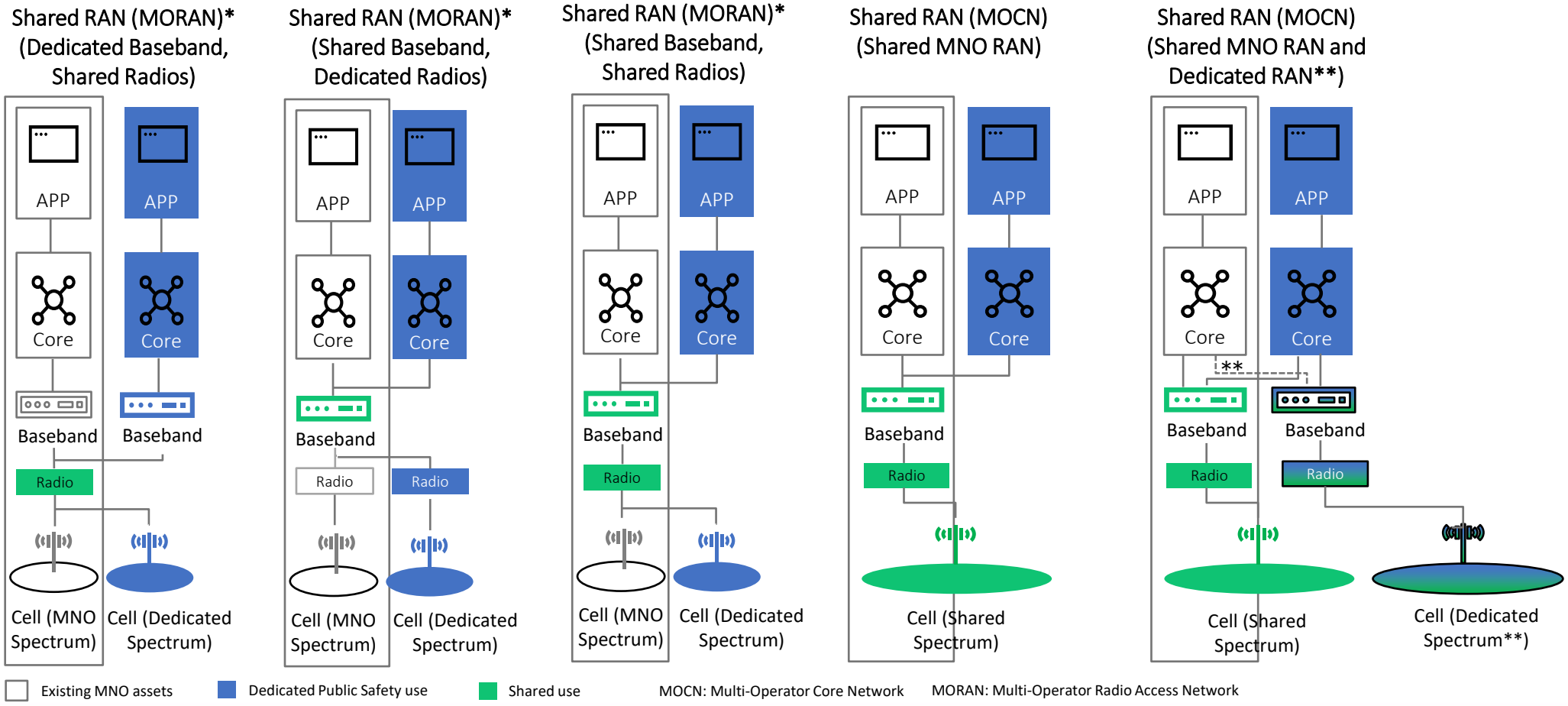
Core Architecture Options (CAO) Task Force Members

Jason Johur, TCCA, Ericsson (Task Force Co-Lead)
Zeineb Makni, Ericsson (Task Force Co-Lead)

Anatoli Levine, Softil
Guilherme Pizzato, Nokia
Harald Ludwig, TCCA
Itsik Fisher, Nokia
Jahid Masud, Lyse
Janne Ahava, Erillisverkot
Kevin Graham, TCCA
Matt Schiller, FirstNet Authority
Neal Richardson, Otarise Services
Nihal Samaraweera, UK Home Office
Prashant Raghuvanshi, AT&T FirstNet
Renauld Mellies, ACMOSS
Stefano Faccin, Qualcomm
Tero Pesonen, TCCA
'Winter' Chaunchuan Leng, Hytera

Appendix
Overview on RAN Sharing Public Safety Broadband Deployment Models

Note:
In practice, the APP box shown for all these deployment models will typically include a range of public safety-related applications, including the MCAS; the latter operated by the PSO.



*In MORAN, the spectrum is dedicated to each operator.

** When not in use by mission critical users, dedicated spectrum may be accessible to commercial traffic on a secondary basis (via MOCN), while QPP is always on for mission critical users across both shared and dedicated spectrum.

Note - When shared MNO RAN is used, it's assumed that the RAN (inc. transmission) is hardened sufficiently and supports QPP in case of shared spectrum.



www.tcca.info | Follow us on tcca-critical-communications

Advancing global critical communications for a safer, more connected world