SUMMUM

The ultimate goal of public safety communications

ROHILL

1 SUMMUM – Rohill's vision for the future of European public safety communications

Rohill is convinced of the need for a radically new, totally open communications model for European public safety. This model must be implemented by a specific, specialised, independent consulting firm working closely with Governments and agencies. This firm would understand the current situation in each market, capturing requirements from a diverse range of national security and public safety agencies and institutions, as well as maintaining a razor-sharp focus on continually evolving open platforms, by selecting and integrating best-in-class solutions from multiple vendors.

This new trusted solutions provider would advise Governments and agencies with total independence from all existing and future suppliers as well as mobile network operators (MNOs). National security and public safety organisations must be fully independent of shareholder-driven companies so the new entity must be structured as a public-private partnership, perhaps majority Government-owned and controlled, operating similar to a critical national infrastructure model, such as that used for power companies, railways or airports.

TETRA will remain a critical solution for European public safety agencies for many years to come, so TETRA network upgrades and new deployments must be truly open, based on open interfaces, with fully transparent voice at the core, so that broadband services can be easily integrated in a common, fully virtualised platform. SMVNOs (secure mobile virtual network operators) created for public safety must not be based on existing TETRA networks with limited proprietary interfaces. The independent advisory firm must have access to open interfaces to integrate legacy and complementary technologies such as analogue, DMR, but also satellite and paging, as well as broadband services from MNOs, together with future private regional networks and rapidly deployable solutions.

Unfortunately, the European public safety broadband market has been struggling to gain momentum due to global LTE vendors still not able to deliver complete solutions due to the lack of specialised terminals and key applications. Over 50 PTT applications are now available, but none of these, with the exception of Rohill's TeamLink, appears to be ready for full integration into existing public safety TETRA networks, and many of them are vendor specific. Even current Internet protocols mean that basic voice is slow, delayed and unpredictable, when compared to existing TETRA solutions.

The switchover to broadband must therefore be gradual and built on top of mission-critical voice. Public safety requires a non-vendor specific, 100% proven, open PTT ecosystem as good as TETRA today. Rohill's TeamLink is the right choice offering a robust voice-based application for Android and iOS. There will be huge benefits from an optimised broadband solution for national security that is open, secure and best-

in-class. The addition of specialised broadband data and applications for specific tasks will increase efficiency, control and of course, security.

Although TETRA is a global ETSI standard and has been highly successful in the public safety arena over the past 20 years, only its air interface is truly open. There is a need for truly open, unlimited interworking, that can be extended to hybrid TETRA + LTE solutions. The practice of certain core TETRA suppliers adding proprietary interfaces and bundling applications platforms is no longer acceptable.

Future public safety broadband solutions must be built on open, virtualised platforms offering a full range of standard terminals and applications. Proprietary solutions are difficult to be inspected for backdoors or to prevent cybercrime. Public safety also demands specialised applications that can be customised and easily added and removed in a plug-and-play fashion.

The missing link is a newly designed entity - a Secure Multiple Mobile Virtual Network Enabler (SM^{2}VNE) - specific to each country, that manages all legacy networks, negotiates on public safety's behalf and manages all relationships with vendors, system integrators, MNOs, MVNOs etc. and is responsible for all security and data management. There will also potentially be the need to integrate multiple MNOs – taking the best key performance indicators (KPIs) from each to guarantee public safety a superior service – in addition to private, regional broadband networks and rapid deployment solutions. Different agencies such as Defence, Police or Fire will also require their own SMVNO.

Only a fully independent body will be able to bring all these pieces of the security jigsaw puzzle together in a fully virtualised, standards-based, interoperable solution, liaising with similar bodies in neighbouring countries to facilitate cross-border operations.

Rohill will play a central role in helping these trusted SM^{2}VNEs create and drive forward this new mission-critical communications paradigm. Its open standards-based solutions guarantee software source code inspection, national standards and production for cost control and security; overnight switchover of TETRA, if required; the maintenance, integration and migration of all legacy networks; a totally agnostic approach to LTE and future 5G solutions; and of course, perhaps most importantly, the TeamLink application ecosystem running over a generic platform for the full integration of all specialised applications.

A poor implementation of public safety broadband by Governments and their agencies will lead to an increase in system-wide cyberattacks threatening national security. A successful, optimised deployment based on full virtualisation of fixed, mobile and IP communications will provide huge societal and economic benefits.

The days of multinational companies building complete, bespoke solutions for national security and public safety agencies are over. Existing TETRA solutions with

proprietary interfaces should not be allowed to tie in agencies or limit their future development as we move into the broadband era. Rohill believes in a fully competitive environment for public safety communications based on open, integrated, best-in-class COTS solutions allowing full customisation and specialisation to fit local, national and individual agency requirements. This is the SUMMUM – the highest possible aspiration for public safety - that will be explained in greater detail in the pages that follow.

Public safety agencies in Europe and around the world deserve the very best communications solutions. Do not accept anything less than the SUMMUM!

2 IN SEARCH OF A NEW PUBLIC SAFETY MODEL

Across Europe, and around the world, increasingly interconnected societies and economies are undergoing dramatic generational change. Traditional ways of life are disrupted, and the authority of Government, public institutions and big business is being challenged. Absolutely nothing is immune to change in today's world.

It is therefore no surprise that public safety and national security are now most definitely and rightly back at the top of Government agendas in the European Union and beyond its borders.

For decades, public safety and emergency services have implemented the same tried-and-tested practices and procedures within their respective organisations. The lives and well-being of police officers, paramedics, fire-fighters and the public they serve continue to depend on robust, wide-area coverage private mobile radio communications networks optimised for group calls, emergency calls, short status messages and instant push-to-talk (PTT).

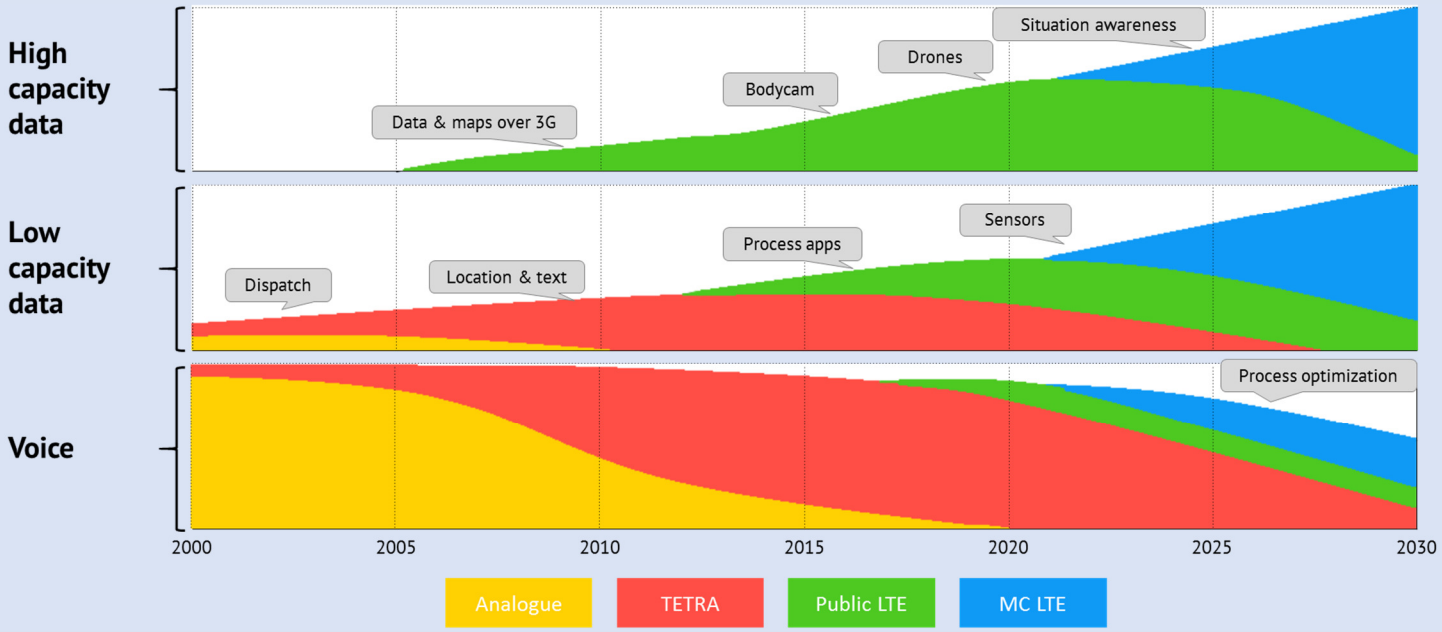
Meanwhile, the amount of mobile data running over increasingly sophisticated public mobile networks has continued to grow exponentially over the past decade since the launch of the iPhone and the global adoption of the Android mobile OS platform.

Cost-conscious Governments are finding it harder to justify running expensive, closed mission-critical communications platforms, often still with proprietary features, totally separate from the public mobile networks. At the same time, the cost of building brand-new, purpose-built, private, dedicated public safety broadband networks continues to grow. Difficult trade-offs must therefore be made regarding spectrum allocation, security, functionality and performance as public safety users potentially move from private to public networks for mission-critical services.

As of today, TETRA remains the global gold standard for mission-critical voice communications. Higher-speed data transmission may be able to provide increased operational efficiencies for public safety, but instant voice communications will remain at the heart of these operations for many years to come due to the need for these organisations to guarantee fundamental officer safety.

TETRA is a narrowband solution, and therefore needs to be complemented with broadband solutions to fulfil public safety organisations' complete communications needs. The global standards body, 3GPP has developed the fourth-generation solution, LTE, and is now in the process of defining the fifth generation, 5G, that will initially co-exist with LTE. Mission critical features are part of the release planning of 3GPP but full deployments including these features will take several more years.

Expected evolution European mission-critical communications market



Mission-critical communications is much, much more than any single technology or set of special applications. End-to-end mission-critical solutions are a comprehensive combination of practices, procedures and technologies designed to maintain operations during worst case scenarios when all other solutions fail, providing guaranteed coverage, capacity, security, availability, as well as taking into account complex human factors.

A fundamentally new model is needed that provides the right tools for public safety personnel working under enormous pressure and stress in a rapidly changing, complex, dangerous modern world. This model must preserve the best from the past and allow us to take advantage of new, evolving functionality and capabilities, based on open standards, open interfaces, open APIs and open minds. This document sets out the case for one such model.

3 A NEW USER-FOCUSED PARADIGM

The rise of the global TETRA critical communications standard encouraged the creation of a strong and varied ecosystem of manufacturers of infrastructure, terminals and applications. However, nationwide public safety system and terminal procurements could only truly be managed and delivered by a very small number of suppliers. Although TETRA is a highly robust, secure solution, this lack of true competition denied Governments the economies of scale and many advanced features available in the wider communications market.

The global mobile communications market has been evolving rapidly towards radically new, virtualised, increasingly automated, all-IP service-based, 3GPP LTE architectures. The rise of cloud-based services, fixed-mobile convergence, open source development and the rapid rise of OTT/Internet players entering the telecommunications space has empowered many end-users to take control of their communications. As well as basic commercial mobile broadband services, national public safety organisations looking to regain control over their critical communications will also require:

Guaranteed access to fully integrated, always available, end-to-end mission-critical applications.

Public safety and national security to be prioritised during emergencies.

Fully open, standardised, backward and forward compatible solutions from multiple suppliers.

Consistent, visible and manageable long-term costs.

Service level agreements (SLAs) that allow continuous updates and migration to best-in-class solutions.

Availability of new hardware, such as drones, robots, autonomous vehicles, IoT sensors and other edge devices, running on secure platforms.

Availability of open software that can be inspected by the relevant authorities.

Availability of new applications, such as AI (artificial intelligence), AR (augmented reality) and live stream video, that improve network operations and situational awareness in control rooms.

4 DECISION TIME FOR NATIONAL GOVERNMENTS

Governments have both a statutory and moral duty to provide the best possible public safety and national security communications solutions for emergency services response personnel, so that they can protect the public and maintain law and order.

TETRA will remain the standard of choice for mission-critical voice services. Lower-capacity data services are also likely to follow a gradual migration path from TETRA to LTE. Higher-capacity data is simply not possible over narrowband technologies, so 3GPP mission-critical standards promise to open up exciting new opportunities for public safety organizations.

Key decisions need to be taken today that will shape the public safety environment for the next 20 years. Governments must choose the best possible, future-proof model at a time of rapid technological change, when faced with so many different options.

The following decisions need to be taken today by authorities:

A suitable hybrid TETRA + LTE model must be chosen according to the current national situation.

The right mix of public and private networks must be built, taking account of current and future legislation, regulation and SLAs, as required.

Public-private partnerships must be set up to manage these networks.

Fully open and standards-based future networks may still require specific, special features adapted to public safety needs.

National Governments must retain ultimate control over all solutions in the interests of national security.

All mission-critical narrowband and commercial broadband solutions must be truly mission-critical grade.

Enough radio spectrum must be available to allow public safety networks to function properly at all times.

5 SUMMUM: AN OPTIMISED SECURE COMMUNICATIONS EXPERIENCE

Although it's hard for any of us to imagine what the global critical communications market might look like in a decade, we can be sure the perfect solution will need to be:

SECURE:

All aspects of security, including cybersecurity, must be taken seriously within a mission-critical system. End-to-end encryption together with proper authentication and authorisation mechanisms, and perhaps even national algorithms, are becoming a necessity to protect sensitive data running over IP links. Carrier-grade, hardened operating systems and secure key management are critical for securing both networks and devices.

UNIFORM:

All advanced communications systems are founded upon fully open, end-to-end, IP-based architectures for core, transport, management and dispatch solutions. Soft switch architectures provide the most simple, consistent, scalable performance. A single, fully integrated hardware and software platform for both TETRA and LTE, allows smoother, gradual, seamless migration from existing technologies to more advanced, future, uniform solutions.

MISSION-CRITICAL:

Mission-critical systems must be user-friendly, intuitive, and therefore simple to use in times of crisis. They incorporate multiple, redundant networks, technologies and services designed to guarantee operations when individual solutions fail. Public safety organisations must only consider mission-critical standards such as TETRA and LTE MCPTT (3GPP Release 13 and beyond), with a call set-up times of max. 350ms and at least five nines (99.999%) availability (5 minutes downtime annually).

MODIFIABLE:

It is increasingly vital for communications solutions to be more flexible and customisable to satisfy customers' dynamic and diverse requirements. Configuration of networks and subscribers must be both easy and fast, allowing user interfaces, i.e. for dispatch and network management, to adapt to each agency and user group. The perfect future solution must guarantee seamless migration from legacy TETRA networks enabling all its critical features.

UNIFIED:

Any complete mission-critical solution must guarantee full integration and interoperability between diverse systems, beginning by integrating existing

narrowband technologies such as analogue, DMR, TETRA and Tetrapol into a common platform. New standards-based mission-critical LTE features should be compatible with all those deployed for existing users. In an increasingly service-based, app-driven world, open APIs must be developed and implemented to optimise network operations.

MOBILE:

Fully mobile public safety organisations need 100% geographical coverage all the time with finite operational budgets. Public and private LTE networks can extend and supplement wide-area TETRA coverage in indoor environments. Complementary solutions such as satellite, HF and VHF radio can be added for long-range communications in difficult terrain. Additional solutions include Rohill's TeamLink MCPTT functionality and optimised CVDP protocol for multi-bearer support over 4G, 5G and even WiFi for voice call continuity.

SUMMUM is the final goal for public safety organisations across Europe and around the world. A unique operating model has been conceived by the internationally-acclaimed mission-critical solutions provider Rohill that will allow agencies to reach the SUMMUM of mission-critical communications.

6 THE "MISSING LINK" SM²VNE[1] MODEL FOR OPTIMISED SECURE COMMUNICATIONS

New network architectures and business models developed by globally dominant Internet companies such as Google, Facebook, Amazon and Microsoft are now challenging mobile network operators (MNOs) to become more agile and flexible. Cloud-based, fully virtualised, automated models must be adopted for the next generation of converged, software-defined networks.

As criminal organisations take advantage of the latest technology to perpetrate their crimes and acts of violence, first responders need solutions that allow them to catch up and even stay one step ahead of increasingly sophisticated adversaries.

Rohill recognizes that a new model - the SM²VNE model - is needed that puts national security and public safety agencies firmly back in control of their communications solutions. A SM²VNE is the missing link that public safety agencies have been waiting for:

Its sole purpose is the delivery of the most advanced, best-in-class, fully integrated multi-vendor mission-critical communications platform.

Comprehensive SLAs (service level agreements) are signed with all parties setting out performance goals within a public-private partnership for fully managed services.

Requirements analysis, tender evaluations, acceptance testing, negotiations with MNOs and other similar activities are all taken care of.

Standardised interfaces, commercial-off-the-shelf (COTS) hardware, open interfaces and multi-vendor support are all developed and maintained for the lifetime of the agreement.

A positive relationship is built and maintained with all stakeholders on the customer's behalf.

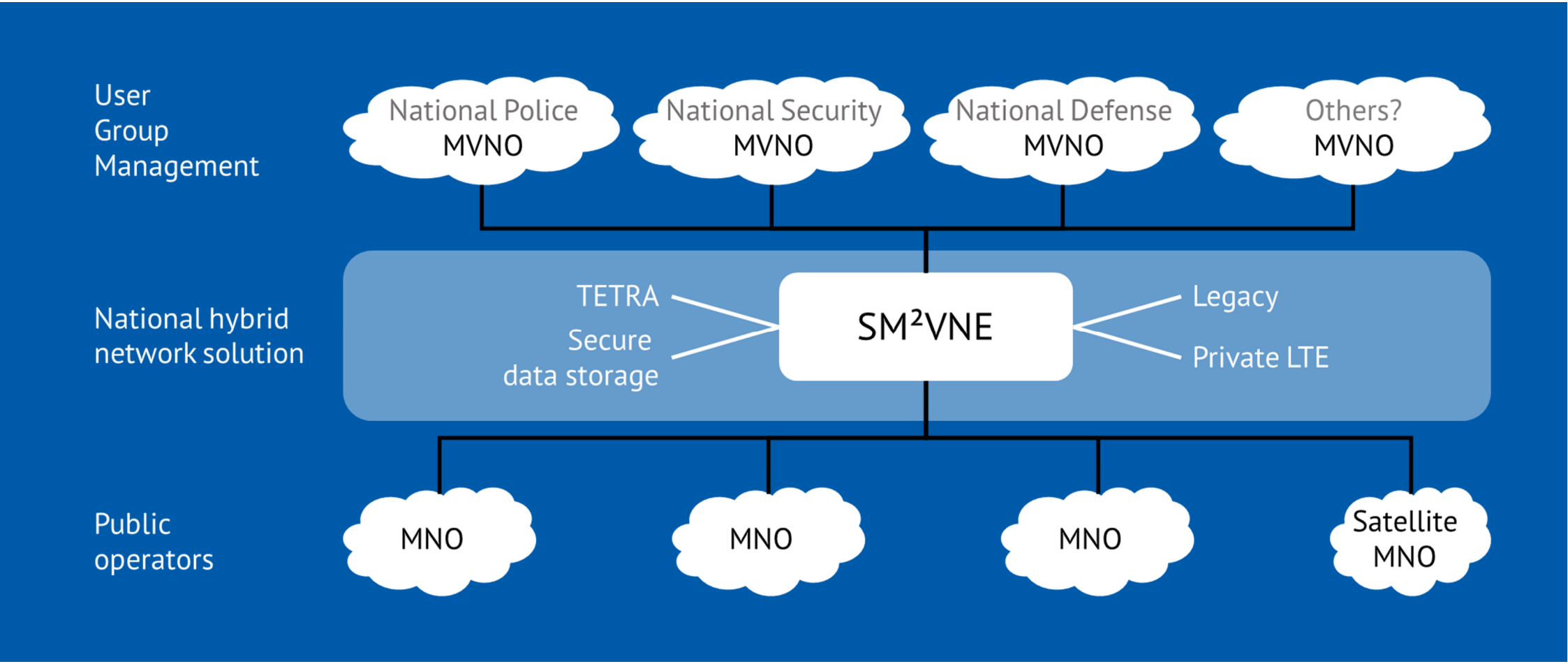
Local and national provision and control of resources makes end-to-end solutions inherently more secure.

State-of-the-art, network-agnostic blockchain solutions can be developed for integrity purposes.

Backdoor protection is guaranteed by allowing source code inspection and full software build sign-off.

Cross-border interoperability is also guaranteed by developing and using common, open interfaces.

[1] Secure Multiple Mobile Virtual Network Enabler


User
Group
Management
National Police
MVNO
National Security
MVNO
National Defense
MVNO
Others?
MVNO
National hybrid
network solution
TETRA
Secure
data storage
SM²VNE
Legacy
Private LTE
Public
operators
MNO
MNO
MNO
Satellite
MNO

7 BRINGING SIMPLICITY TO COMPLEX, CRITICAL SYSTEMS

More complex systems tend to be harder to manage, more prone to failure, more expensive to maintain, harder to upgrade and migrate. Therefore, agencies are increasingly searching for greater operational simplicity, without giving up on increased functionality and more powerful solutions.

What are the key steps required for public safety agencies to move to future public safety mobile broadband networks that are more open and simple to operate and upgrade?

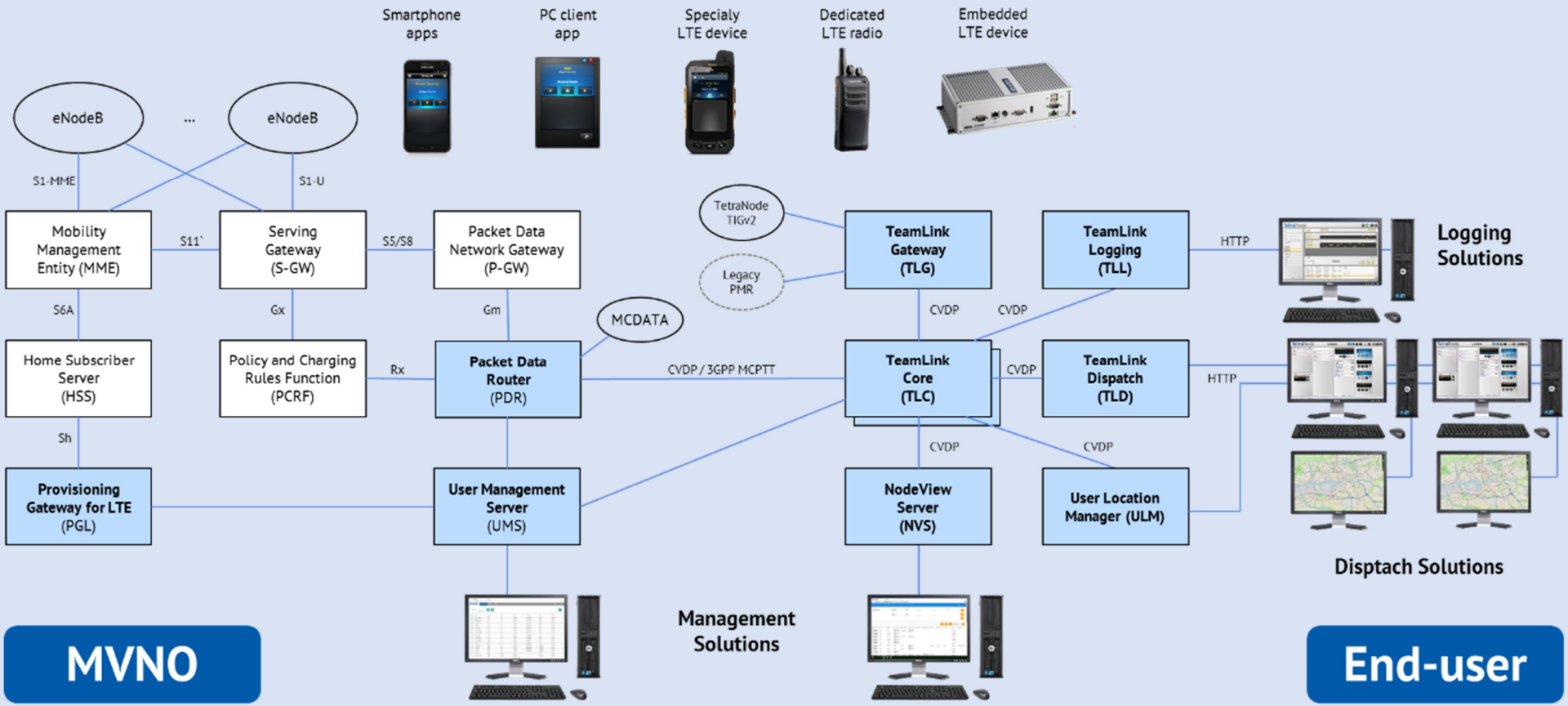
Many public safety agencies must start by switching over their first-generation TETRA networks to a more up-to-date, state-of-the-art, future-proof TETRA solution. A good example of the latter is Rohill's TetraNode system architecture, based on open standard interfaces and COTS hardware and software, including carrier-grade Linux for core, application server and radio access platforms. Rohill also has a proven record of replacing existing TETRA networks with minimal hassle for end-users, as well as connecting, integrating and/or migrating non-TETRA PMR solutions such as analogue or DMR in low-density rural locations.

Once such upgrades have taken place, agencies are ready to choose a hybrid TETRA + LTE solution. Solutions such as Rohill's LTEtraNode - or similar - support full, seamless integration, where TETRA is complemented and perhaps one day replaced by both public and private LTE/5G networks.

Rohill's TeamLink suite of applications for real-time voice, status, text, location, image and video delivery allows end-users to communicate quickly and efficiently across multiple networks without restrictions. For example, TeamLink uses the Critical Voice and Data Protocol (CVDP) which adheres to the 3GPP MCPTT standard, offering advanced PMR voice and data services over LTE with fast call set-up times, using well-defined, standard QoS mechanisms. All MCPTT enhancements provided by CVDP are available to third parties via an open specification, providing additional features to end-users over an open platform.

The diagram on the next page gives a complete overview of TeamLink showing clearly where and how CVDP/MCPTT is implemented.

As Governments tackle the difficult, once-in-a-generation task of migrating from one mission-critical communications platform to another, it is imperative to choose a technology partner that understands the steps required to make the most successful transition. Rohill is such a partner. The new SM^{2}VNE Model also provides reassurance to agencies that they will never again be tied into a single vendor relationship for any subset of the overall solution.


Smartphone apps
PC client app
Specialy LTE device
Dedicated LTE radio
Embedded LTE device
eNodeB
...
eNodeB
S1-MME
S1-U
Mobility Management Entity (MME)
S11`
Serving Gateway (S-GW)
S5/S8
Packet Data Network Gateway (P-GW)
S6A
Gx
Gm
Home Subscriber Server (HSS)
Policy and Charging Rules Function (PCRF)
Rx
Packet Data Router (PDR)
MCDATA
Sh
Provisioning Gateway for LTE (PGL)
User Management Server (UMS)
TetraNode TIGv2
Legacy PMR
TeamLink Gateway (TLG)
TeamLink Logging (TLL)
HTTP
Logging Solutions
CVDP
CVDP
TeamLink Core (TLC)
CVDP / 3GPP MCPTT
CVDP
TeamLink Dispatch (TLD)
HTTP
CVDP
CVDP
NodeView Server (NVS)
User Location Manager (ULM)
Disptach Solutions
Management Solutions
MVNO
End-user

8 OPENING UP THE FUTURE OF CRITICAL COMMUNICATIONS

The public safety and critical communications community stands at a crossroads. It can either continue on its current path, allowing an acceptance of the status quo to stifle innovation or it can take a leap into the unknown by embracing commercial MNO models. We believe it is possible to combine the best of both worlds, but only if all the important conditions referred to in this document are met. Agencies can afford to be bold while reducing risk.

Rohill's revolutionary SM^{2}VNE Model and its experience in the critical communications field makes SUMMUM the ultimate goal for the future. Agencies gain access to best-in-class TETRA and LTE, with the added promise of 5G in the future, in a totally secure, controllable and future-proof solution.

The SUMMUM future guarantees:

Fully open standards and best-in-class technology with multiple vendor sourcing.

Full integration and seamless migration, following a clear roadmap from narrowband to broadband.

The continuous capability to integrate and tailor applications for specific tasks using the most suitable devices.

Open software, facilitating inspection and cyber control as well as enabling customised solutions.

Fully measurable performance of all network parameters for both private networks and public operator networks, allowing flexible airtime service packages across all networks.

The time when Government, critical national infrastructure and other critical users were locked into a single network solution is coming to an end. Future societies will be controlled by open mission-critical applications that are private and secure by design. Smarter, safer cities and nations will require intelligent, responsive and predictive systems that allow smarter services to be implemented on demand across new, seamless, integrated platforms.

Ubiquitous, eco-friendly mission-critical communications networks will be the driving force behind future societies and economies, improving the overall well-being of citizens. SUMMUM is the mission-critical goal, ready for 5G and should contribute to the United Nations Sustainable Development Goals (SDGs) nationally and globally, making sure that by 2030, we will be living in a better, smarter, safer world.

Agencies around the world deserve the very best communications solutions. Do not accept anything less than the SUMMUM!