Why Secure MVNO is your next smart move

Adopt LTE while maintaining control

Contents

1 Executive summary

Public safety agencies have been accustomed to using highly capable, secure communications systems based on TETRA and Tetrapol.

However, new opportunities are arising to adopt the latest technologies, advanced high rate data applications and other solutions that give more information, better situational awareness and improved support for decision making. These solutions require more capabilities than narrowband systems can offer.

TETRA and Tetrapol are secure solutions, but they cannot deliver broadband-like services. Something else is required, yet, public service agencies have invested much capital and effort in building up operations and processes based on TETRA and Tetrapol and it would not be realistic or cost-effective to simply abandon them.

To enable the new solutions, a Professional Mobile Radio (PMR) operator could choose to use infrastructure from a commercial mobile network operator (MNO). However, this option has two significant drawbacks.

The first is control. Even in such a simple event as the loss of a terminal, for example, the PMR operator would need to wait for someone else to take action. Essentially, they would have lost control.

The other issue is security. Using a commercial MNO would mean that the PMR operator would have no say over where and how the user data is stored or processed.

A better solution, one that satisfies the control and security requirements, is for a PMR operator to become a Secure Mobile Virtual Network Operator, or SMVNO, a role that would give them ownership of the security and control of the network, subscribers and devices.

A Mobile Virtual Network Operator (MVNO) is a mobile service provider that does not own spectrum, but does own some infrastructure while leasing the rest. The MVNO contracts with traditional mobile operators to buy network time, which it then sells to its own customers.

The SMVNO operates the mobile virtual network in an exceptionally secure way. It is regarded as the smart step towards broadband and the solution with the lowest risk for public safety and security

PMR operators can adopt this approach by using the Tactilon Secure Mobile Virtual Network Operator (Tactilon SMVNO) solution from Airbus. Tactilon SMVNO allows operators to evolve their network to LTE. It gives them control over the critical LTE security, as well as offering additional layers of security to meet the needs of demanding professionals.

Tactilon SMVNO is available today and several critical communication network operators have run pilots or trials and brought it into use.

2 The challenge of broadband for public safety

Public safety and security officers face danger every day. The risks come not only from natural and man-made disasters and assorted accidents, but also from criminals and terrorists who pose an active threat.

Many criminals use advanced technology to defeat the forces of law and order and so public safety agencies must also use technology and tools to defeat them.

One of the prime tools of public safety agencies is an advanced and capable communications system. The latest tools are applications and other solutions that give them more information, better situational awareness and support for decision making.

These new solutions, however, do not work naturally or easily with the current mission-critical networks that public safety and security organizations rely on. TETRA and Tetrapol are secure solutions, but they are limited to narrowband.

The question is, how can public safety and security organizations adopt new solutions today, stay ahead of the threats and use these new solutions with their existing networks?

This is not simply a question of buying new products. A PMR operator needs a trusted vendor who understands the specific needs of public safety.

In addition, the operator, as well as the user organizations, will have spent time, effort and money to build operations and processes on top of the current technologies of TETRA and Tetrapol. It is understandable that they do not want to simply throw these networks out and start again. A much better way forward is to deploy the new solutions so that they work with the operator's established organization, processes and working methods.

Broadband for public safety is not simply a question of buying new products

3 Meeting the challenge

PMR operators are essentially providers of services that run on infrastructure and technologies that need to be purchased. Today's enabler for mission critical communications is typically a TETRA or Tetrapol network, which forms the core around which user organizations have built and continue to build their own operations and services.

To adopt the new broadband solutions, the PMR operator could choose to use normal commercial subscriptions. However, this option has two significant drawbacks.

Who has control?

Today, the PMR operator is in control. For example, should a police officer lose a TETRA/Tetrapol radio, the PMR operator can take instant action using its own internal processes. The radio would be disabled, either temporarily or permanently. Although a radio may have been lost, the data related to the radio would stay within the PMR operator's boundaries.

By contrast, if the PMR operator opts to be only a middle man between an MNO and the public safety organizations, control will shift to the MNO, as this is where the subscriber data resides.

In this case, if a police officer loses a mobile device, the police organizations would still be dealing with the PMR operator, who would need to take action. The PMR operator would in turn contact the MNO providing the broadband service.

The PMR operator would need to wait for someone else to take action. Essentially, it would have lost direct control.

Of course, the PMR operator could purchase a better class of service from the MNO and be guaranteed faster service, but this would also require paying a premium. Control would still lie with the MNO and the cost would be higher.

The risk of exposure of sensitive data grows whenever a new party has access to it

In addition to the loss of control, there is also the significant issue of the loss of transparency.

Who can access the data?

In the commercial world, things are different than in public safety. A service provider may outsource a variety of its services to other parties, who might in turn subcontract some services to yet other providers, who might be from a foreign country.

Subscriber data related to public safety and security personnel is extremely sensitive. The risk of exposure of this data grows whenever a new party has access to it. The PMR operator would never be able to control which company in which country would end up handling its customer data.

A better solution

A better solution, one that satisfies the control and security requirements, is for a PMR operator to become a Secure Mobile Virtual Network Operator, or SMVNO.

A mobile virtual network operator (MVNO) does not own spectrum or have its own network infrastructure. Instead, it contracts with traditional MNOs to buy network time, which it then sells to its own customers.

MVNOs work independently of MNOs and can therefore set their own pricing structure. They own some of mobile network-related infrastructure and some MVNOs will run their own billing and customer care solutions.

The Secure MVNO is an MVNO that operates the mobile virtual network in an exceptionally secure way.

This arrangement makes it easier for public safety organizations, as the PMR operator understands the specific needs of the organizations that it has served for many years. By contrast, a commercial operator running business operations in its accustomed way may find it especially challenging to satisfy the specific needs of public safety organizations.

The PMR operator will also be more skilled in dealing with commercial mobile operators compared to single public safety organizations.

Acting as an SMVNO also means that they do not compromise the control and security they enjoy with their TETRA and Tetrapol networks.

Becoming an SMVNO

TETRA and Tetrapol technologies have evolved substantially to meet the mission-critical public safety requirements of high availability, security and network control. They also provide advanced features and functions such as encryption, faster call setup, group calls, priority calls and direct calls without the need for connection via a base station. Nevertheless, these technologies, which offer only narrowband data, cannot serve the latest advanced data hungry applications.

With advances in broadband communications and the availability of new powerful devices, innovative high data rate applications have emerged, providing sophisticated value-added services to private citizens and businesses. Thus, for data it seems that the logical next step for public safety and security operators is to embrace LTE without compromising the security and control they currently experience with TETRA or Tetrapol technology.

Efforts continue to address public safety requirements on 3GPP. However, to have fully compliant 3GPP public safety and security solutions available on a large scale will take many years. The current commercial LTE technology and its deployments, as such, do not comply with the operational and security requirements of public safety operations.

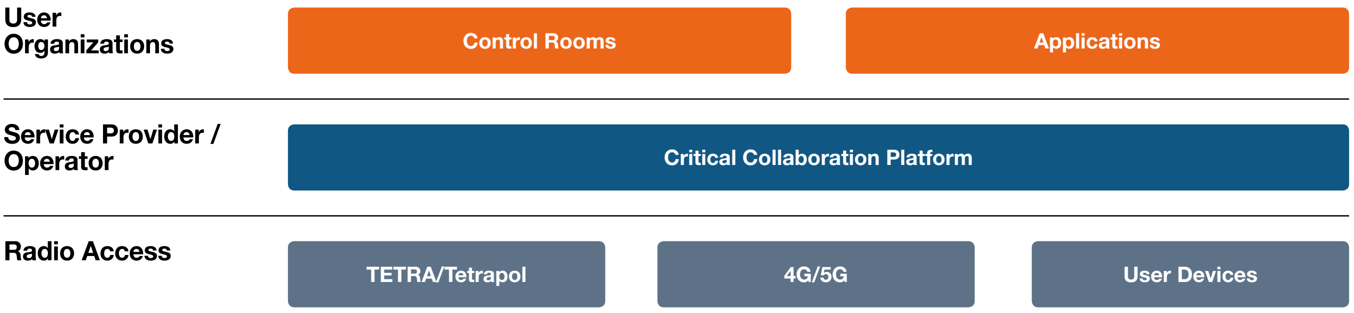
Today's critical communication and PMR operators need a reliable and cost-effective solution that allows them to confidently extend their current data security applications to broadband networks, as well as to adopt new broadband apps.

Embrace LTE today – but do not compromise security and control

There is a reliable and cost-effective solution available in the form of Tactilon Suite from Airbus. Tactilon Suite is a portfolio of solutions designed to be the first step towards mobile broadband for public safety and security operators. Tactilon Secure Mobile Virtual Network Operator (Tactilon SMVNO) allows PMR operators to complement TETRA/Tetrapol services with broadband. It gives the operators control over the critical LTE security, as well as offering additional layers of security to meet the needs of demanding professionals.

Airbus customers benefit from further synergies from Tactilon Suite because it includes an organizational and user management solution that can be used for TETRA, Tetrapol and SMVNO infrastructure.

Key areas of Mission Critical communications evolution



User Organizations

Control Rooms

Applications

Service Provider / Operator

Critical Collaboration Platform

Radio Access

TETRA/Tetrapol

4G/5G

User Devices

4 Tactilon Secure MVNO

The only way to assign broadband subscribers to organizational structures

Tactilon SMVNO makes it possible for critical communication operators to introduce broadband services to their customers. These services can run either on the operator's own dedicated broadband network or on commercial mobile operator networks. Using Tactilon SMVNO, the critical communication operator can remain in control of the security of the user data and of the communications.

Several commercial mobile networks can be used. This improves broadband coverage in two ways. Firstly, because more than one broadband network is available, a wider coverage can be achieved. In addition, if one mobile network is very congested or completely down, another may still provide connectivity, improving high availability of broadband services.

Tactilon SMVNO includes a tool for provisioning and managing subscribers, and most importantly, provisioning and managing them in the same way as in PMR networks – assigning them into organizational structures. This is a key capability because hierarchical organizational structures are the basis of operational models and processes for public safety authorities.

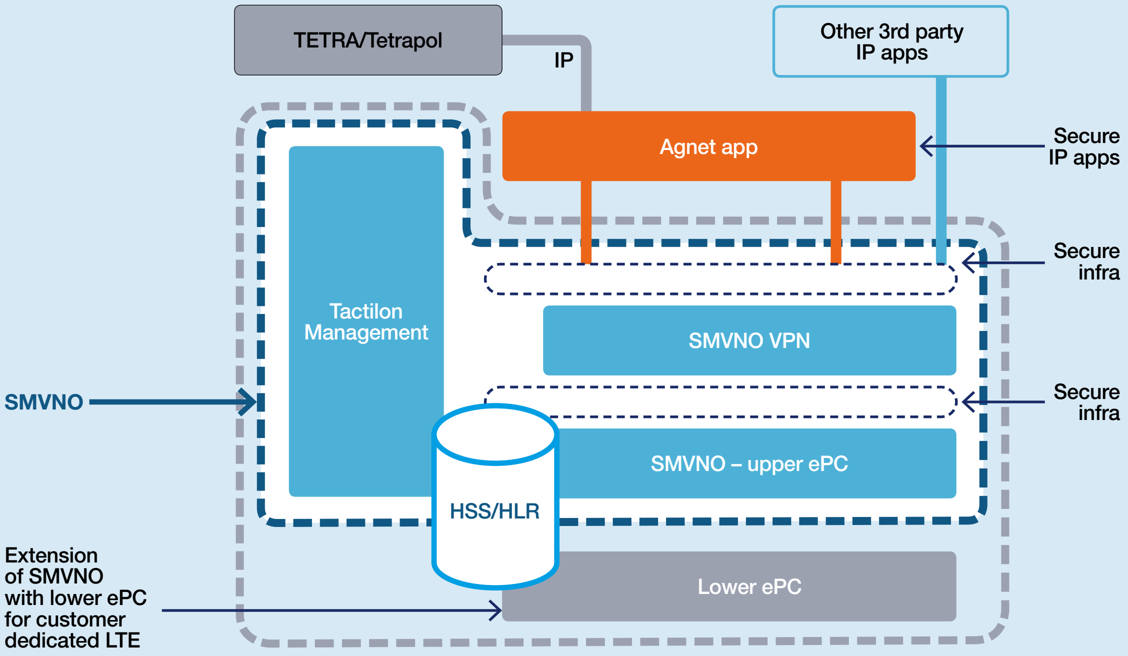
The Tactilon Management solution is the only way to assign broadband subscribers into organizational structures. It also manages the TETRA or Tetrapol subscribers, so all subscribers, devices and services can be managed from a single point.

Tactilon SMVNO enables broadband services to run on one or more commercial mobile networks, using the standard roaming interface between the SMVNO's network and the commercial mobile network. This solution is fully compliant with 3GPP standards and is designed to be flexible and scalable while remaining easy to evolve to 5G technologies and beyond.

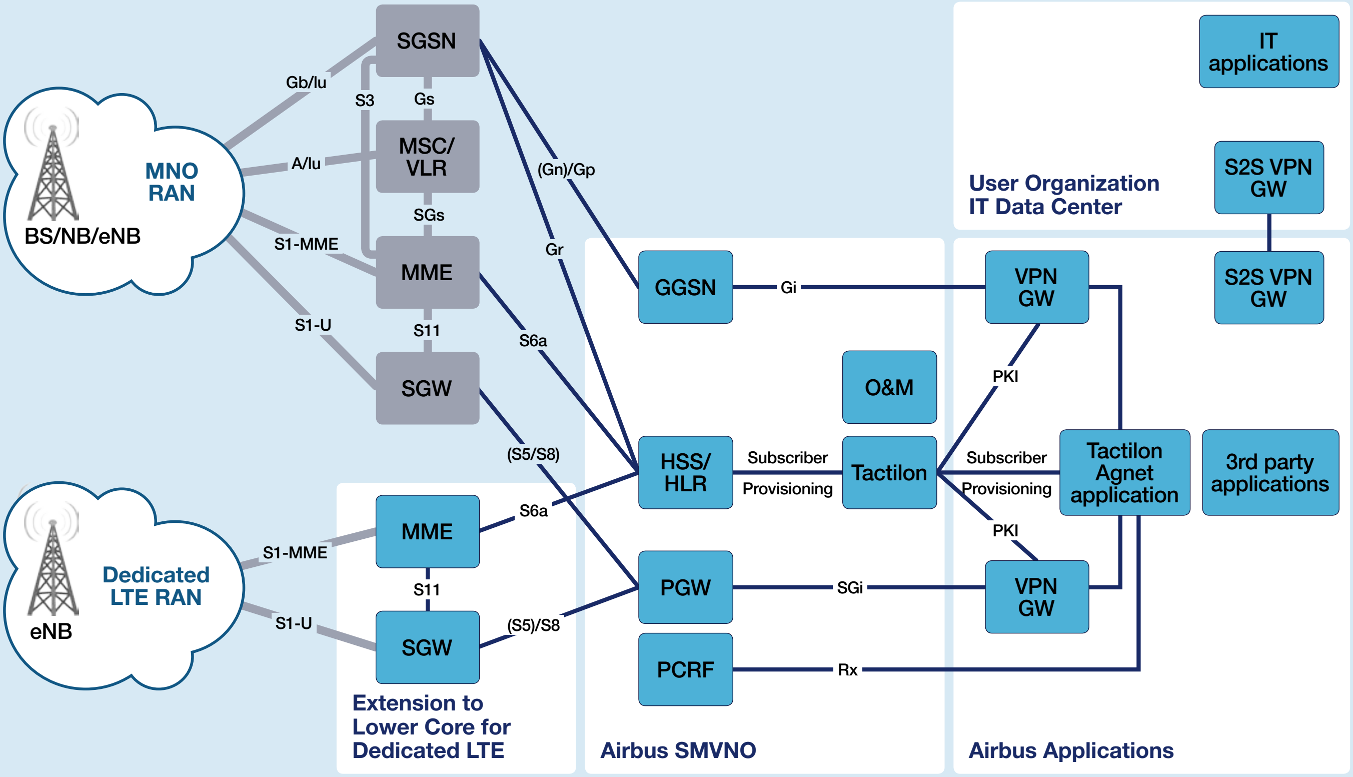
Tactilon SMVNO comes with a 3GPP evolved Packet Core (ePC) upper-core for 2G / 3G / 4G, built so that the critical communications operator can easily adopt a hybrid TETRA/Tetrapol and broadband network. The operator needs to extend the solution with EPC lower-core elements to run a dedicated LTE broadband radio access network with its own LTE base stations. The radio access network can be managed with the same EPC upper-core elements as the MVNO.

Tactilon Management

The Tactilon Management tool brings the concept of hierarchical organizations into the world of broadband. The tool manages and displays the hierarchical organizational



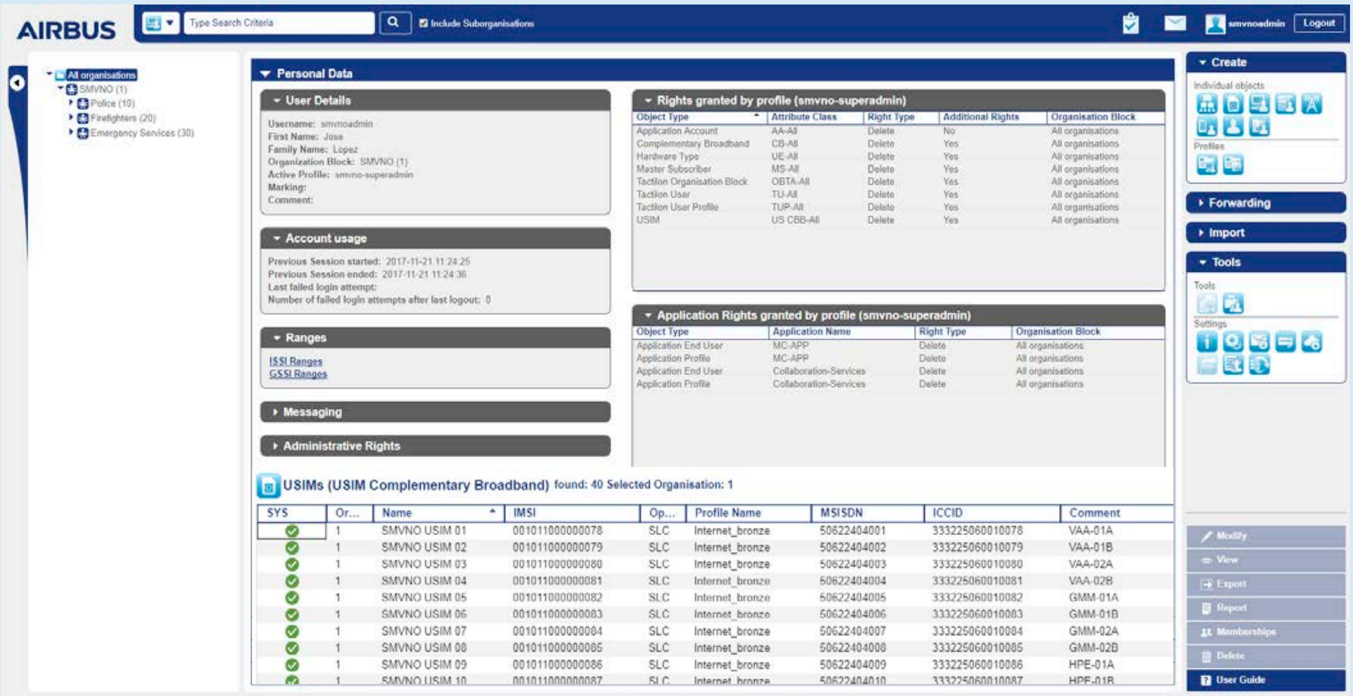
Tactilon Secure MVNO enables the use of both existing and new public safety and security smartphone applications



Tactilon Secure MVNO can include a lower ePC core to support a dedicated LTE network

structure in use, supporting the organization's internal processes.

Tactilon Management is the subscriber management and provisioning system for TETRA, Tetrapol and broadband subscribers, as well as the certificate authority. It also keeps track of all changes, making it an essential tool for auditing, administration and for maintaining the non-repudiation part of data security.



User Details

Username: smvnoadmin
First Name: Jose
Family Name: Lopez
Organization Block: SMVNO (1)
Active Profile: smvno-superadmin
Marking:
Comment:

Account usage

Previous Session started: 2017-11-21 11:24:25
Previous Session ended: 2017-11-21 11:24:36
Last failed login attempt:
Number of failed login attempts after last logout: 0

Ranges

ISSI Ranges
GSSI Ranges

Rights granted by profile (smvno-superadmin)

Object Type	Attribute Class	Right Type	Additional Rights	Organisation Block
Application Account	AA-All	Delete	No	All organisations
Complementary Broadband	CB-All	Delete	Yes	All organisations
Hardware Type	UE-All	Delete	Yes	All organisations
Master Subscriber	MS-All	Delete	Yes	All organisations
Tactilon Organisation Block	OBTA-All	Delete	Yes	All organisations
Tactilon User	TU-All	Delete	Yes	All organisations
Tactilon User Profile	TUP-All	Delete	Yes	All organisations
USIM	US CBB-All	Delete	Yes	All organisations

Application Rights granted by profile (smvno-superadmin)

Object Type	Application Name	Right Type	Organisation Block
Application End User	MC-APP	Delete	All organisations
Application Profile	MC-APP	Delete	All organisations
Application End User	Collaboration-Services	Delete	All organisations
Application Profile	Collaboration-Services	Delete	All organisations

USIMs (USIM Complementary Broadband) found: 40 Selected Organisation: 1

SYS	Or...	Name	IMSI	Op...	Profile Name	MSISDN	ICCID	Comment
✓	1	SMVNO USIM 01	001011000000078	SLC	Internet_bronze	50622404001	333225060010078	VAA-01A
✓	1	SMVNO USIM 02	001011000000079	SLC	Internet_bronze	50622404002	333225060010079	VAA-01B
✓	1	SMVNO USIM 03	001011000000080	SLC	Internet_bronze	50622404003	333225060010080	VAA-02A
✓	1	SMVNO USIM 04	001011000000081	SLC	Internet_bronze	50622404004	333225060010081	VAA-02B
✓	1	SMVNO USIM 05	001011000000082	SLC	Internet_bronze	50622404005	333225060010082	GMM-01A
✓	1	SMVNO USIM 06	001011000000083	SLC	Internet_bronze	50622404006	333225060010083	GMM-01B
✓	1	SMVNO USIM 07	001011000000084	SLC	Internet_bronze	50622404007	333225060010084	GMM-02A
✓	1	SMVNO USIM 08	001011000000085	SLC	Internet_bronze	50622404008	333225060010085	GMM-02B
✓	1	SMVNO USIM 09	001011000000086	SLC	Internet_bronze	50622404009	333225060010086	HPE-01A
✓	1	SMVNO USIM 10	001011000000087	SLC	Internet_bronze	50622404010	333225060010087	HPE-01B

Features of Tactilon SMVNO

Tactilon SMVNO provides the following capabilities to the critical communications operator.

Control

- The critical communications operator is in control of the network and its security
- Subscriber data stays in the secure network
- Only SMVNO USIMs are allowed inside the trusted network (this is intrinsic 3GPP functionality)
- USIMs, encryption keys and devices are all under the control of the trusted operator

Security and encryption

- The critical communications operator will add a security layer on top of the commercial mobile network layer
- The confidentiality, integrity and availability of data is protected
- Using more than one mobile network creates a multi-layer security system (backdoor counter-measure)

Improved availability of broadband services

- The ability to use more than one commercial mobile network for broadband data means improved geographical coverage and better availability
- The ability to use multiple network technologies (2G/3G/4G/5G) means additional availability

Priorities

- It is possible to set different priorities to applications for each user

Scalability

- Subscribers can be provisioned or edited en masse, from a single management point

Cost savings

- Client certificates can be delivered automatically via SCEP (Simple Certificate Enrolment Protocol), which is designed to make the issuing of digital certificates as scalable as possible. This greatly reduces operational expenses

Integration opportunities

- It is possible to provision third party applications into the system using the Tactilon API, achieving better service integration

Data analysis

- The operator can collect, analyze and visualize SMVNO data. This can give valuable insights into system use and security, providing a solid basis for planning improvements or for taking action
- A bulk of information can be transformed into actionable data so the operator and user organizations can plan improvements or create new opportunities
- Output logs can be collected into external tools, where further data modelling is possible

Virtualization

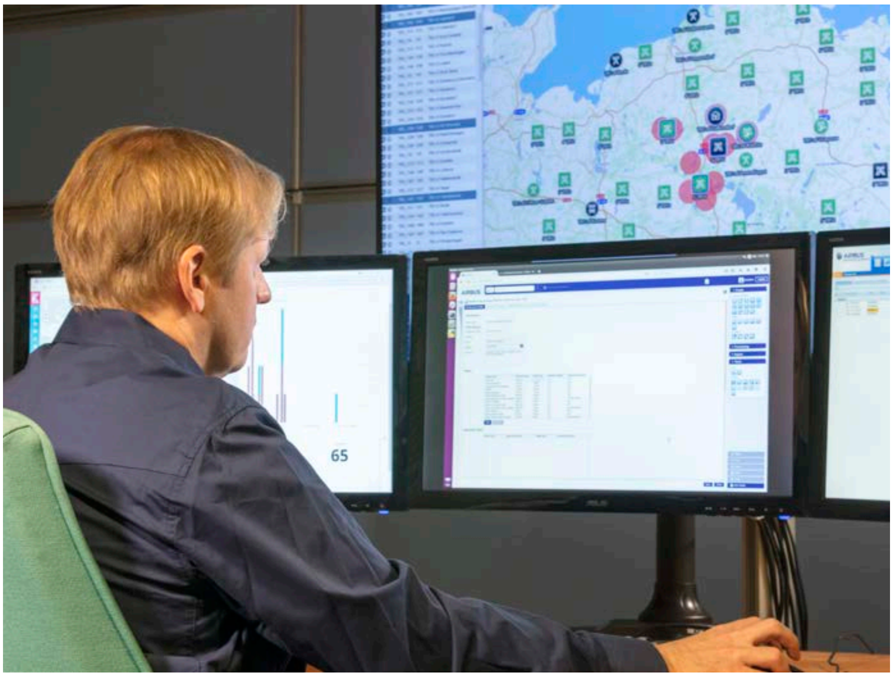
- The core elements of Tactilon SMVNO are virtualized, making the solution easy to integrate into the operator's current data centers, for example. The need for new hardware would be minimal
- There is also the option to purchase a complete Tactilon SMVNO solution including all necessary hardware, racks and software

Controlling the use of bandwidth

- The LTE data rate policing feature allows the operator to define a profile and user policy for each USIM and for each APN. This allows the operator to limit the use of bandwidth. The defined profiles can then be assigned to certain subscribers or en masse to a group of subscribers

LTE Public Safety 3GPP QoS Management:

- Manage and configure QCI for public safety subscriptions in PCRF
- Support of Rx interface



Secure MVNO Security

The Tactilon SMVNO solution gives the PMR operators control over the critical LTE security and it also offers additional layers of security. This way, the level of security that is required in the public safety and security sector can be reached.

Layered security architecture

- Cellular access
  - 3GPP AKA authentication using tamper-proof security module UICC with USIM application for mutual authentication between device and infrastructure
  - UICC card and credentials (identities, keys) and authentication algorithm are owned by SMVNO operator.
  - Radio interface encryption and message authentication using 3GPP standardized algorithms based on selected by the RAN owner.
- Transport
  - Site-to-site VPN between MNO, SMVNO and user organization IT data center sites integrated into PKI
  - Site ingress points firewalled and inspected with IPS/IDS
- Access VPN
  - Traversing untrusted MNO and transport network using access VPN integrated into PKI
  - RADIUS network access controlled policies separating user organizations' flows into their own routing domain (VRF)
- Trust areas
  - with different security levels
  - traversing trust areas through firewalls
  - traffic entering trust area is inspected with IPS/IDS
  - sensitive area analyzed for APT

Tiered vendor architecture

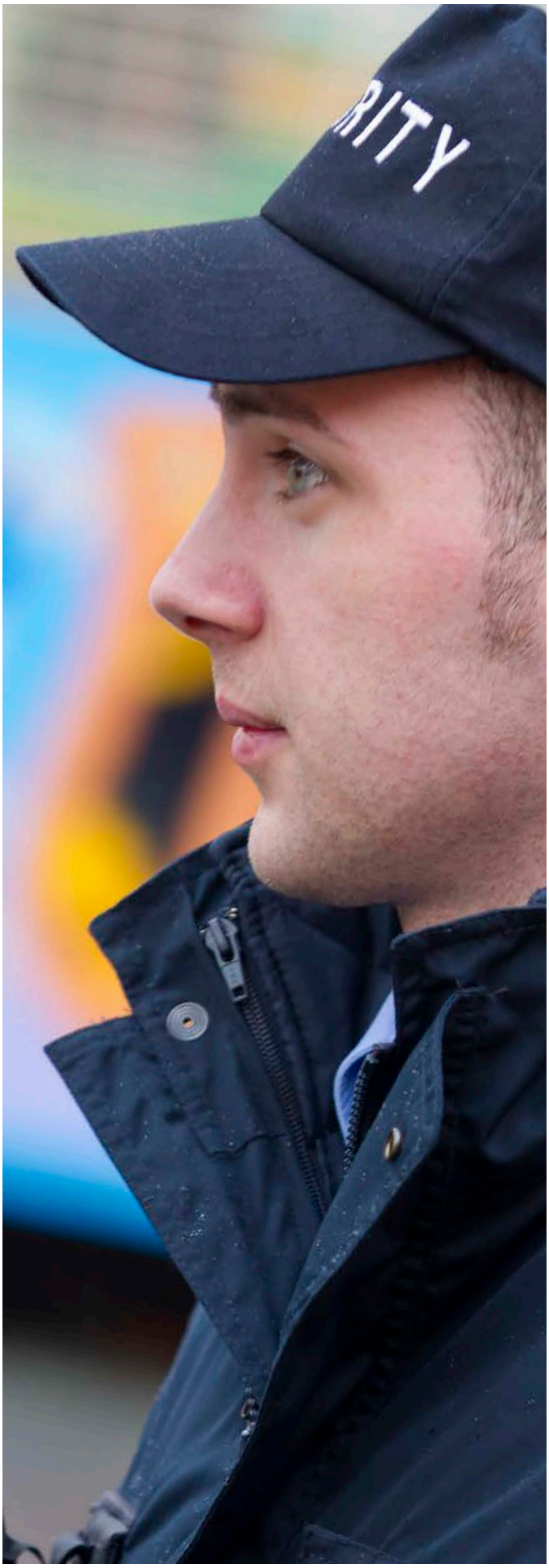
- security tiers built with different vendors' technology
- countermeasure against backdoors

Dedicated system security features

- system architecture includes PKI, IDS/IPS, SIEM, SOC unless they are already part of the IT security infrastructure in the SMVNO network

Security customized based on local regulatory requirements

- Airbus will collaborate with the customer to integrate their preferred security solution and vendor into the SMVNO design.



5 Tactilon SMVNO – available and ready

The Secure Mobile Virtual Network Operator (SMVNO) approach is the trend among European public safety agencies. It is regarded as the smart step towards broadband and the solution with the lowest risk.

This centralized way of providing Secure MVNO services is more beneficial than each public safety organization making its own arrangements for using commercial mobile data services. The advantages include professionally managed security, lower cost and new opportunities in data applications and their hosting.

Operators - start today

Public safety and security operators looking to become SMVNOs can start today by building broadband competences, adjusting their existing organizations and processes and developing new ones. They can begin this evolution even while 3GPP standardization addresses the requirements of public safety and security, a process that will take years to produce compliant standards and systems for operation.

Starting today with the SMVNO approach, PMR operators can quickly grow to fully understand the broadband market and position themselves as the trusted broadband provider for public safety and other professional organizations.

At the forefront

SMVNO allows the PMR operator to be at the forefront with technology, which enables field agents to be equipped with the latest tools, technologies and applications. By combining Tactilon SMVNO capability and the Tactilon Agnet application from Airbus, group communication is fully transparent for end users between TETRA/Tetrapol and broadband networks.

Tactilon SMVNO is available today and several critical communications network operators have started pilots or trials and brought the solution into use.

Take your first step towards Tactilon SMVNO today:
Contact: marketing@securelandcommunications.com

The secure MVNO approach is the solution with the lowest risk

AIRBUS

The content of this document is provided "as is", without warranties of any kind with regards its accuracy or reliability, and specifically excluding all implied warranties, for example of merchantability, fitness for purpose, title and non-infringement. In no event shall Airbus be liable for any special, indirect or consequential damages, or any damages whatsoever resulting from loss of use, data or profits, arising out of or in connection with the use of the document. Airbus reserves the right to revise the document or withdraw it at any time without prior notice.

For more information please contact
Airbus Defence and Space
Hiomotie 32
00380 Helsinki, Finland
T: +358 10 4080 000
e-mail: marketing@securelandcommunications.com

MetaPole
1, boulevard Jean Moulin
CS 40001
78996 Elancourt Cedex, France
T: +33 (0)1 61 38 50 00

Airbus Defence and Space
Wörthstraße 85
89077 Ulm, Germany
T: +49 (0) 731.392-0