ETSI TR 102 970 V1.1.1 (2013-01)

Technical Report

Reconfigurable Radio Systems (RRS); Use Cases for spectrum and network usage among Public Safety, Commercial and Military domains

Reference

DTR/RRS-04009

Keywords

radio, safety, system

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

Copyright Notification

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://ipr.etsi.org).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Report (TR) has been produced by ETSI Technical Committee Reconfigurable Radio Systems (RRS).

Introduction

The present document provides a study of the use cases for network and spectrum sharing among Public Safety (PS), Commercial and Military domains.

The capability of exchanging information (e.g. voice or data) is essential to improve the coordination of public safety officers during an emergency crisis. Wireless communications are particularly important in field operations to support the mobility of first responders. While in their routine service, the operators may have learned to work around the shortcomings of their communication systems, the situation changes dramatically when an emergency causes additional stress for the system and the operators. Emergency scenarios usually lead to exceptionally high traffic loads, which the existing wireless communication systems may not be able to support. This situation can be worsened in scenarios with limited radio coverage (e.g. a truck accident in a tunnel) or when parts of the communications infrastructures are damaged in the incident area. Sharing of network and spectrum can increase the traffic capacity, provide higher coverage and improve the connectivity availability.

The present document investigates the potential use cases for network and spectrum sharing among the public safety, commercial and military networks. The potential benefits, feasibility and related technical challenges are identified for each use case.

In the present document, the identification of the use cases for network and spectrum sharing is only aimed to non-mission critical applications.

1 Scope

The scope of the present document is to investigate the various use cases for spectrum and network sharing, which can enhance the capabilities of public safety organizations in non-mission critical operations.

"Mission critical operations" for public safety organisations address situations where human life and goods (rescue operations, law enforcement) and other values for society are at risk, especially when time is a vital factor. This means we define 'mission critical information' as the vital information for public safety to succeed with the operation. Mission critical communication solutions' therefore means that the public safety organisations need secure, reliable and available communication and as a consequence cannot afford the risk of having failures in their individual and group communication (e.g. voice and data or video transmissions).

Beyond mission critical operations, public safety officers may be involved in non-mission critical operations and applications for crisis management, where demand for broadband connectivity and traffic capacity can be very important.

As the requirements of mission critical operations can be quite restrictive, the present document will address only the application of spectrum and network sharing for non-mission critical operations.

In this regard the following aspects are covered:

- The public safety operational scenarios, where spectrum and network sharing can be applied.
- Potential operational and technical requirements for spectrum and network sharing.
- Taxonomy of the use cases for spectrum and network sharing.

The scope of the present document is not to suggest changes to the spectrum regulatory framework.

2 References

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

NOTE: While any hyperlinks included in this clause were valid at the time of publication ETSI cannot guarantee their long term validity.

2.1 Normative references

The following referenced documents are necessary for the application of the present document.

Not applicable.

2.2 Informative references

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] ETSI TR 102 745: "Reconfigurable Radio Systems (RRS); User Requirements for Public Safety".

[i.2] ECC-ETSI, European process of standardisation and regulation for new radio communications devices or systems - cooperation between CEPT and ETSI.

NOTE: Available online at http://www.etsi.org/WebSite/document/Technologies/cooperation%20process%20between%20ECC%20and%20ETSI.pdf.

[i.3] ITU Terms and Definitions database.

NOTE: Available online at http://www.itu.int/ITU-R/index.asp?category=information&link=terminology-database&lang=en.

[i.4] CEPT ECC Report 169, "Description of practises relative to trading of spectrum rights of use", May 2011.

[i.5] William Lehr and Nancy Jesuale, "Spectrum Pooling for Next Generation Public Safety Radio Systems", 3rd IEEE Symposium on New Frontiers in Dynamic Spectrum Access Networks (DYSPAN), October 2008.

[i.6] Radio Spectrum Policy Group: RSPG10-348 Final, RSPG Opinion on Cognitive Technologies. February 2011.

NOTE: Available at http://rspg.ec.europa.eu/_documents/documents/meeting/rspg24/rspg_10_348_ct_opinion_final.pdf.

[i.7] ETSI TR 102 628: "Electromagnetic compatibility and Radio spectrum Matters (ERM); System reference document; Land Mobile Service; Additional spectrum requirements for future Public Safety and Security (PSS) wireless communication systems in the UHF frequency range".

[i.8] ETSI TR 121 905: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; Vocabulary for 3GPP Specifications ((3GPP TR 21.905 version 10.3.0 Release 10)".

[i.9] CEPT ECC FM49 on "Radio Spectrum for Public Protection and Disaster Relief (PPDR)".

NOTE: Working documents available at public website: http://www.cept.org/ecc/groups/ecc/wg-fm/fm-49/page/terms-of-reference.

[i.10] PPDR Spectrum Harmonisation in Germany, Europe and Globally by WikConsult on behalf of the German Ministry of Economics and Technology.

NOTE: Available at http://www.bmwi.de. Last accessed 18/07/2012.

[i.11] Radio Spectrum Policy Group: Report on Collective Use of Spectrum (CUS) and other spectrum sharing approaches, November 2011. RSPG11-392 Final.

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

Cognitive Radio (CR): radio, which has the following capabilities:

- to obtain the knowledge of radio operational environment and established policies and to monitor usage patterns and users' needs;
- to dynamically and autonomously adjust its operational parameters and protocols according to this knowledge in order to achieve predefined objectives, e.g. more efficient utilization of spectrum; and
- to learn from the results of its actions in order to further improve its performance.

Incident Area Network (IAN): network providing connectivity to the public safety personnel for the local area where the incident happened

NOTE: An IAN, for instance, can be a local wireless network with a limited range (e.g. 1 Km) around a building on fire.

incumbent radio service: radio service authorized for operation on a given frequency band with a regulatory priority

public safety organization: organization, which is responsible for the prevention and protection from events that could endanger the safety of the general public

NOTE: Such events could be natural or man-made. Example of Public Safety organizations are police, fire-fighters and others.

Professional Mobile Radio (PMR): radio system designed for a closed user group

NOTE: PMR networks consist of one or more base stations and a number of mobile terminals to support communication over relatively short distances with a central base station/dispatcher. PMR technology is usually adopted by public safety organizations and it is designed on the basis of public safety technical and operational requirements. PMR systems generally provide facilities for closed user groups, group call and push-to-talk, and have call set-up times which are generally short compared with cellular systems. Many PMR systems allow Direct Mode Operation in which terminals can communicate with one another directly when they are out of the coverage area of a network.

Public Mobile Network (PMN) Operator: operator maintaining and running the telecom infrastructure, which provides wireless connectivity and services to the commercial users (i.e. the generic citizen)

NOTE: A mobile network operator has usually acquired from the government one or more radio spectrum licenses.

Public Safety Network (PSN) Operator: operator maintaining and running the telecom infrastructure, which provides wireless connectivity and services to the public safety organizations

NOTE: A professional mobile network operator is usually granted by the government one or more radio spectrum licenses.

radio technology: technology for wireless transmission and/or reception of electromagnetic radiation for information transfer

reconfigurable radio systems: generic term for radio systems encompassing Software Defined and/or Cognitive Radio Systems

Use case: description of a system's behaviour as it responds to a request that originates from outside of that system

NOTE: In other words, a use case describes "who" can do "what" with the system in question. The use case technique is used to capture a system's behavioural requirements by detailing scenario-driven threads through the functional requirements.

User Equipment (UE): device allowing a user access to network services

White Space (WS): part of the spectrum, which is available for a radio communication application (service, system) at a given time in a given geographical area on a non-interfering/non-protected basis with regard to primary services and other services with a higher priority on a national basis

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

3GPP	3rd Generation Partnership Project
ASA	Authorized Shared Access
BBDR	BroadBand Disaster Relief
BSC	Base Station Control site
CBRNE	Chemical Biological Radiological Nuclear Explosive
CEPT	European Conference of Postal and Telecommunications Administration

CN	Cellular Networks?
CORASMA	COgnitive RAdio for dynamic Spectrum MAnagement
CR	Cognitive Radio
CUS	Collective Use of Spectrum
ECC	Electronic Communication Committee
EDA	European Defence Agency
EIAN	Extended Incident Area Network
GSM	Global System for Mobile communications
HF	High Frequency
IAN	Incident Area Network
ICT	Information and Communication Technology
IMSK	Integrated Mobile Security Kit
IP	Internet Protocol
ISM	Industrial Scientific and Medical (frequency band)
LSA	License Shared Access
LTE	Long Term Evolution
MAC	Medium Access Control layer
MVNO	Mobile Virtual Network Operator
NGO	Non Governmental Organization
NRA	National Regulatory Agency
PMN	Public Mobile Network
PMR	Professional Mobile Radio
PPDR	Public Protection and Disaster Relief
PS	Public Safety
PSCE	Public Safety Communication Europe
PSN	Public Safety Network
PSTN	Public Services Telephone Network
QoS	Quality of Service
RAN	Radio Access Network
RNC	Radio Network Control
RRS	Reconfigurable Radio Systems
SDR	Software Defined Radio
SLA	Service Level Agreement
TETRA	TErrestrial Trunked Radio
TVWS	TV White Spaces
TX	signal Transmitter
UE	User Equipment
UMTS	Universal Mobile Telecommunications System
VMNO	Virtual Mobile Network Operator

4 Relevant input from other organizations

This clause provides the list of input documents and information sources, which are relevant to the present document. The list includes deliverables and other documentation produced by organizations or projects.

4.1 Organizations

4.1.1 ETSI Technical Committee (TC) TErrestrial Trunked RAdio TETRA

TErrestrial Trunked RAdio (TETRA) is a digital trunked mobile radio standard developed to meet the needs of traditional Professional Mobile Radio (PMR) user organizations for Public Safety, Transportation, Utilities, Government, Military, Mining Oil and Gas exploration.

ETSI TC TETRA has identified the spectrum requirements for wideband and broadband communications for public safety in reference [i.7]. Reference [i.7] also investigates the possibility of spectrum sharing among military, public safety and commercial stakeholders through a pre-emptive mechanism. Details on the pre-emptive mechanism are provided in [i.7].

4.1.2 Public Safety Communication Europe (PSCE)

Public Safety Communication Europe (PSCE) has been created to facilitate the development of new communication technologies for Public Safety organizations. PSCE has an extensive membership drawn from civil protection groups, government, industry, academia and NGOs. The PSCE aims to build a consensus through dialogue between stakeholders, and it has created a European Public Safety Stakeholder Forum, intended as a permanent forum to deal with public safety communication issues. Reports on the investigation are available at the PSCE web site http://www.psc-europe.eu/.

PSCE has investigated wireless communication technologies like TETRA, Long Term Evolution (LTE), Satellite Communications and ad-hoc networks for field communications.

4.2 Projects

4.2.1 EULER project

The FP7 EULER project (www.euler-project.eu) gathers major players in Europe in the field of wireless systems communication integration and software defined radio (SDR), is supported by a strong group of end-users, and aims to define and actually demonstrate how the benefits of SDR can be leveraged in order to enhance interoperability in case of crisis needed to be jointly resolved. The proposed activities span the following topics: proposal for a new high-data-rate waveform for homeland security, strengthening and maturing ongoing efforts in Europe in the field of SDR standardisation, implementation of Software defined radio platforms, associated assessment of the proposal for high-data-rate waveform for security, and realisation of an integrated demonstrator targeted towards end-users. Significant interaction with E.U stakeholders in the field of security forces management will contribute in shaping a European vision for interoperability in joint operations for restoring safety after crisis.

4.2.2 COGEU project

The FP7 COGEU project has the objective to investigate the use of TV White Spaces (TVWS) and the introduction and promotion of real-time secondary spectrum trading and the creation of new spectrum commons regime. COGEU will also define new methodologies for TVWS equipment certification and compliance addressing coexistence with the Digital Video Broadcasting - Terrestrial/Handheld (DVBT/H) European standard.

COGEU has also investigated the possibility to use TV White Space for Public Safety organizations.

4.2.3 IMSK project

The FP7 Integrated Mobile Security Kit (IMSK) project had the objective to design a mobile system, which uses innovative applications and technologies to address emergency crisis and unpredictable terrorist activity. The Integrated Mobile Security Kit (IMSK) project will combine technologies for area surveillance; checkpoint control, CBRNE detection into a mobile system for rapid deployment at venues and sites (hotels, sport/festival arenas, etc.) which temporarily need enhanced security.

The project will employ legacy and novel sensor technologies, that will integrate sensor information to provide a common operational picture where information is fused into intelligence, perform a field demonstration to validate the concept, adapt the system to local security forces and finally disseminate the results after accreditation by end-users.

The Consortium consists of 27 parties spread all over Europe ranging from large, internationally recognised defence companies to small-medium enterprises, universities and operational counter-terror professionals.

The IMSK project has investigated the application of wireless communication systems to support wideband data connectivity to fields personnel and the command and control centres.

4.2.4 EDA CORASMA

The European Defence Agency (EDA) has financed a project called CORASMA (COgnitive RAdio for dynamic Spectrum MAnagement).

The main objective of CORASMA is to use CR technology to enable a more flexible usage of the spectrum resources to allow the systems to adapt according to their context while maintaining its performance, robustness, availability and QoS. The objective of the CORASMA project is to study the application of the CR to military needs and to assess the benefits of such technique.

The CORASMA project will report to the EDA every 6 months through seven Milestones. The outputs of the CORASMA project will be technical and management reports and a hardware/software simulation platform demonstrator.

The objectives and the results of the CORASMA project may be quite relevant to the present document but they are not specifically focused to the spectrum sharing with the commercial and public safety domains. Furthermore, CORASMA deliverables have restricted access.

4.2.5 HELP project

The FP7 HELP project (http://www.fp7-sec-help.eu/) will establish a comprehensive solution framework aspiring to significantly enhance the secured communications resilience and responsiveness in emergency situations. The proposed solution framework is built on the following two pillars:

1) The capacity and efficiency of public safety communications networks can be increased by implementing "network sharing" concepts between different PMR networks (e.g. a PMR network belonging to a given public safety organisation is made available to other first responder agencies that participate in the crisis management) as well as between PMR and commercial cellular networks. "Network sharing" refers to the capability of sharing network resources like traffic capacity, communication services and broadband connectivity between networks, which may have been designed for different tasks. This approach is particularly beneficial since it is very unlikely that a new private globally harmonised public safety multimedia communication solution will be introduced in the foreseeable future.

2) Network capacity and efficiency can be increased by implementing "spectrum sharing" techniques between public safety and commercial networks in case of emergencies or natural or man-made disasters. "Spectrum sharing" refers to the possibility of managing spectrum in a flexible way.

5 Network and Spectrum sharing concepts

5.1 Network sharing

A formal definition for "network sharing" has not been addressed within telecommunications regulatory and standardisation bodies. Instead, "network sharing" term has been used in a broad manner encompassing different perspectives. Hence, in order to establish a solid common understanding, the following definition is adopted:

- "Network sharing" refers to the shared use of a network, or a part of it, by multiple users. Different types of services for different user organizations may be provided through the shared network by one or several network operators that may have a different degree of control over the resources of the shared network.

Different views on "network sharing" approaches considered in different contexts are discussed here to assess the suitability of the proposed definition.

In the context of mobile cellular networks, "network sharing" has been mainly used to refer to the sharing of network infrastructure in the core and radio access networks among multiple operators. Reference [i.8] provides the following definition:

"RAN sharing: Two or more CN operators share the same RAN, i.e. a RAN node (RNC or BSC) is connected to multiple CN nodes (SGSNs and MSC/VLRs) belonging to different CN operators."

5.2 Spectrum sharing

The concept of "spectrum sharing" is defined in [i.2] as follows:

- "spectrum sharing" is a term usually used to describe co-existence with an incumbent radiocommunications application (-s) within the same frequency band as proposed for new application(s)".

In the regulatory domain, ITU Radiocommunication Sector (ITU-R) does not provide a formal definition for spectrum sharing in [i.3]. The ICT Regulation Toolkit co-produced by ITU, comprises a module for "Radio Spectrum Management" where the following ideas about spectrum sharing are stated:

"*Spectrum sharing typically involves more than one user sharing the same piece of spectrum for different applications or using different technologies*".

"*Spectrum sharing encompasses several techniques - some administrative, technical and market-based. Sharing can be accomplished through licensing and/or commercial arrangements involving spectrum leases and spectrum trading. Spectrum can also be shared in several dimensions; time, space and geography*".

6 Operational scenarios

The purpose of the following clauses is to define operational scenarios where the sharing of spectrum resource among commercial, public safety and/or military domains could be applied.

The list of scenarios includes the scenarios already defined in [i.1].

6.1 Routine Operations

This operational scenario includes all the routing activities performed by Public Safety organizations including patrolling, routing law enforcement, protection of the citizens from theft and others.

An example of this operational scenario is the prevention of theft in an urban environment.

This operational scenario is characterized by:

1) Well defined traffic patterns in the jurisdiction area. There are not peak demands of traffic or capacity.

2) Limited demand for broadband data.

3) Limited geographical or time extension.

4) Limited number of public safety officers involved in the scenario.

On account of these characteristics, dedicated public safety networks are usually suitably sized for routine operations and additional network or spectrum resources are usually not needed.

6.2 Emergency Crisis

An emergency crisis includes various types of events due to intentional or unintentional causes, which create disruption to the normal business flow, may endanger life of civilians and destroy public or private facilities.

An example of this operational scenario is fire in a building in an urban environment.

This operational scenario is characterized by:

1) Emergency crises are usually unexpected events with peaks of traffic demand in the first hours after the crisis.

2) Emergency crises are usually concentrated in one jurisdiction, but they can occasionally spans more than one jurisdiction.

3) Various public safety organizations can be involved in this operational scenario. The presence of various communication systems can create interoperability barriers.

4) On account of the risk of loss of lives and assets, timely access to communication resources is essential.

As a result of these characteristics, dedicated public safety networks normally have a reasonable amount of extra capacity to handle these kind of events. But if it is a big event, the capacity may not be suitably sized for such operational scenario's, and additional network or spectrum resources are then needed. The challenge is to provide these resources within the time constraints imposed by the operational scenario.

6.3 Major Event

A major event is a planned event, which may include a large number of people and organizations in a specific geographic area for a limited duration of time.

An example of this operational scenario is a large sport event.

This operational scenario is characterized by:

1) Possibility to plan the allocation of communication resource in advance.

2) Large number of citizens.

3) A major event is usually concentrated in a specific geographical area or jurisdiction.

4) Various public safety organizations can be involved in this operational scenario but interoperability barriers can be mitigated through careful planning. Communication interoperability issues among different communication technologies outside the context of sharing network or spectrum resources are out of scope of the present document and they will not be addressed here.

As a result of these characteristics, dedicated public safety networks normally have a reasonable amount of extra capacity to handle these kind of events. But if it is a big event, the capacity may not be suitably sized for such operational scenario's. Additional network or spectrum resources are then needed and their deployment can be planned in advance.

6.4 Natural disaster

A natural disaster is caused by natural phenomena, which can impact a large geographical area and a huge number of people and assets. The causes of a natural disaster may be still present for hours or days as in the case of a flooding or earthquake.

An example of this operational scenario is a tsunami or an earthquake.

This operational scenario is characterized by:

1) A large number of citizens and assets may be involved.

2) Existing communication infrastructures can be destroyed or degraded.

3) Various public safety organizations can be involved in this operational scenario. The presence of various communication systems can create interoperability barriers.

4) A natural disaster could impact a large geographical area and various jurisdictions.

5) Military forces could be involved in the response to a natural disaster.

In this operational scenario, there may be a large need of traffic demand and connectivity for various applications. Such unexpected requests of traffic may be worsened by the degraded conditions of public safety and commercial networks. Local or tactical communication networks could be used in absence of a fixed infrastructure.

6.5 Search and Rescue

This operational scenario is focused on the search & rescue of one or more persons or a significant asset (i.e. lost ship or airplane). It is usually executed in a very isolated or difficult environment both due to difficult terrain or bad weather conditions.

An example of this operational scenario is the search & rescue of a lost airplane.

This operational scenario is characterized by:

1) A large geographical area to be searched.

2) Most likely there will not be adequate communication coverage in the area.

3) One or few public safety organizations may be involved.

In this operational scenario, the demand for traffic and connectivity is quite limited. Coverage of the communication systems may be an issue, but it can be addressed through specific long range communications systems (e.g. HF, Satellite).

7 Taxonomy of network and spectrum sharing use cases

7.1 Introduction

The purpose of this clause is to provide an overview of all the possible network sharing or spectrum sharing use cases. The clause is divided in the identification of the network sharing use cases and the identification of spectrum sharing use cases. Each use case is also evaluated against the requirements defined in clause 8.

7.2 Definition of the stakeholders

This clause describes the potential stakeholders, which can be involved in the network and spectrum sharing scenarios.

The following stakeholders are identified:

- **Military:** Military is the organization responsible for the national defence policy. Because military is responsible for the nation protection and security, it may also support public safety organizations in case of a large national disaster. Military forces use tactical communication networks or long range communications (e.g. HF, satellite) rather than cellular communication networks. Military forces also have strict security requirements for the sharing of information or resources with non-military parties. This constraint may strongly limit all the network and spectrum sharing scenarios because the coordination on the use of network resources may not be possible.

- **Public Safety Organization:** an organization, which is responsible for the prevention and protection from events that could endanger the safety of the general public.

- **Commercial user:** the user of the private mobile network operator (i.e. a generic citizen).

- **Mobile Network Operator:** the operator, which maintains and runs the telecom infrastructure.

- **Public Mobile Network (PMN) Operator:** the operator, which maintains and runs the telecom infrastructure, which provide wireless connectivity and services to the commercial users (i.e. the generic citizen). A mobile network operator has usually acquired from the government one or more radio spectrum licenses. See definitions in 3.1.

- **Public Safety Mobile Network (PSN) Operator:** the operator, which maintains and runs the telecom infrastructure, which provide wireless connectivity and services to the public safety organizations. See definitions in 3.1.

- **Spectrum Regulator:** it is the national or international body charged with any of the regulatory tasks assigned by European Directives on radio frequency spectrum**.**

- **Mobile Virtual Network Operator (MVNO):** it is a mobile network operator that provides services to users but it does not own the network assets and the radio spectrum licenses, which are instead owned by a PMN or a PSN.

7.3 Network Sharing Use Cases

Several use cases of "network sharing" can be identified on the basis of the relationships, which may exist among the stakeholders.

7.3.1 User organizations sharing the same network: only one network operator is in charge of the network management and communication services provisioning

This use case is illustrated in Figure 1. Network 1 is managed exclusively by network Operator 1 providing communication services to several user organizations User i, (i=1..n). These organizations can be both public safety organizations and commercial users. All users might have access to a set of common services from the network (e.g. PSTN voice calls, Internet access) together with a set of private/customised services per user (e.g. talk group services, directory services, information databases, etc.). This use case is also identified as **Network Sharing Use Case A** in the rest of the present document.

An example is a Mobile Network Operator, which provides services both to commercial users and public safety organizations.

Another example is a PSN Operator, which provides services to Public Safety Organizations as it was designed to do, but it can also use spare capacity for specific users (e.g. energy utilities) on a best effort basis.

Two main technical challenges can be identified in this scenario:

1) How the capacity of the shared network is effectively shared among the different user organizations. This could be required in the case of a crisis scenario where there is network congestion and the different responding organizations need to have access to different communication resources. There is a clear need of a prioritization scheme for this purpose.

2) How communications services can be dynamically provisioned to allow communications between different user organizations. This could be required in the case of a crisis scenario, where inter-organization communications need to be supported.

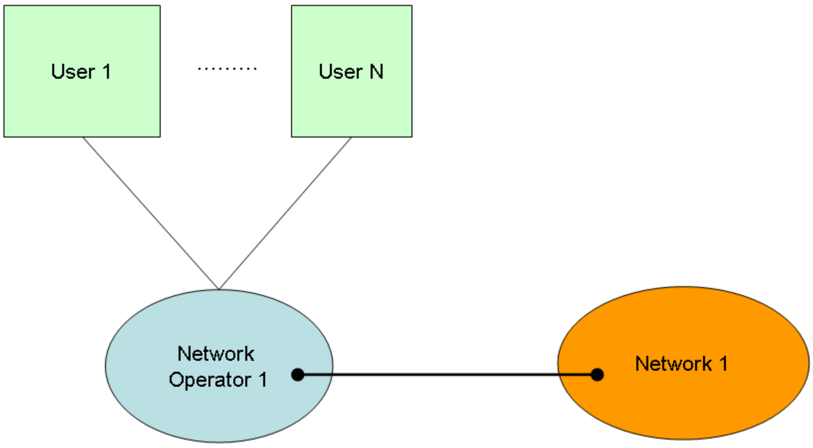

Figure 1: Illustration of "network sharing" referred to as "Case A"

7.3.2 User organizations sharing the same network: several network operators are in charge of network management and communication services provisioning in the shared network

This use case is illustrated in Figure 2. Mobile Network operators 1 (NO1) and 2 (NO2) offer communication services to their respective users (1-A NO1 and 1-B NO2) over the same shared network or part of its components. Users can be both public safety organisations and commercial users. This use case is also identified as **Network Sharing Use Case B** in the rest of the present document.

An example is a mobile network, used by various Virtual Mobile Network Operators (VMNOs). For instance, one VMNO provides services only to public safety organizations and another one provides services only to commercial users.

The technical challenges to be addressed in this scenario are the following:

1) How the capacity of the shared network is effectively shared among Mobile Network Operators and user organizations. This could be required in the case of a crisis scenario where there is network congestion and the different responding organizations need to have access to different communication resources. There is a clear need of a prioritization scheme for this purpose.

2) How communications services can be dynamically provisioned to allow communications between different user organizations belonging to the same Mobile Network Operator or between different Mobile Network Operators. This could be required in the case of a crisis scenario, where inter-organization communications need to be supported.

The advantage of this use case in comparison to the one described in clause 7.3.1 is that Mobile Network Operators can define specific network configuration and service level agreements with different classes of users: public safety organizations, energy utilities, generic citizens and so on. In this way, specific requirements can be accommodated on a case by case basis.

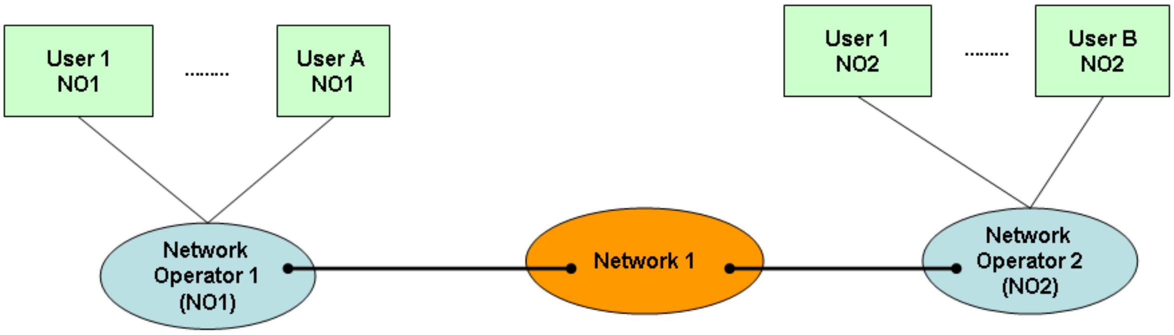

Figure 2: Illustration of "network sharing" where Mobile Network Operators share the management of the same network

7.3.3 Several user organizations sharing the same network. The home network of some of the users is not the shared network

This use case is illustrated in Figure 3. Mobile Network Operator NO2 is the home operator for users Ui-NO2, with i=1..A. Mobile Network Operator O2 could have its own Network 2 (N2). This network would be the home network for users Ui-NO2. However, users Ui-NO2 might also be served over network N1 managed by operator NO1. In this case, users Ui-NO2 are referred to as visiting users and the network N1 as visited network. This situation is enabled under appropriate roaming agreements between Mobile Network Operators. Also in this case users can be both public safety organizations and commercial users. This use case is also identified as Network Sharing Use Case C in the rest of the present document.

Compared to the other use cases, the main novel technical challenge arising in this scenario is that networks N1 and N2 will interwork to allow visiting users (Ui-NO2) to get access to communication services (either provided by the visited network N1 itself or provided by the home network (N2) over the visited network (N1). In this context, this use case allows roaming among networks.

An example of this use case are two networks, which are located in different nations and public safety users need to roam from one nation to another in case of a cross-border emergency crisis like a large flooding or earthquake.

The technical challenges to be addressed in this scenario are:

1) How the capacity of the shared network is effectively shared among Operators and user organizations. This could be required in the case of a crisis scenario where there is network congestion and the different responding organizations need to have access to different communication resources. There is a clear need of a prioritization scheme for this purpose.

2) How communications services can be dynamically provisioned to allow communications between different user organizations belonging to the same Operator or between different Operators. This could be required in the case of a crisis scenario, where inter-organization communications need to be supported.

3) Which interfaces and architecture elements need to be designed and deployed to provide roaming for users among networks.

4) How security requirements can be satisfied for users belonging to different public safety organizations or nations.

5) The provision of group calls and broadcasts among users belonging to different public safety organizations or nations.

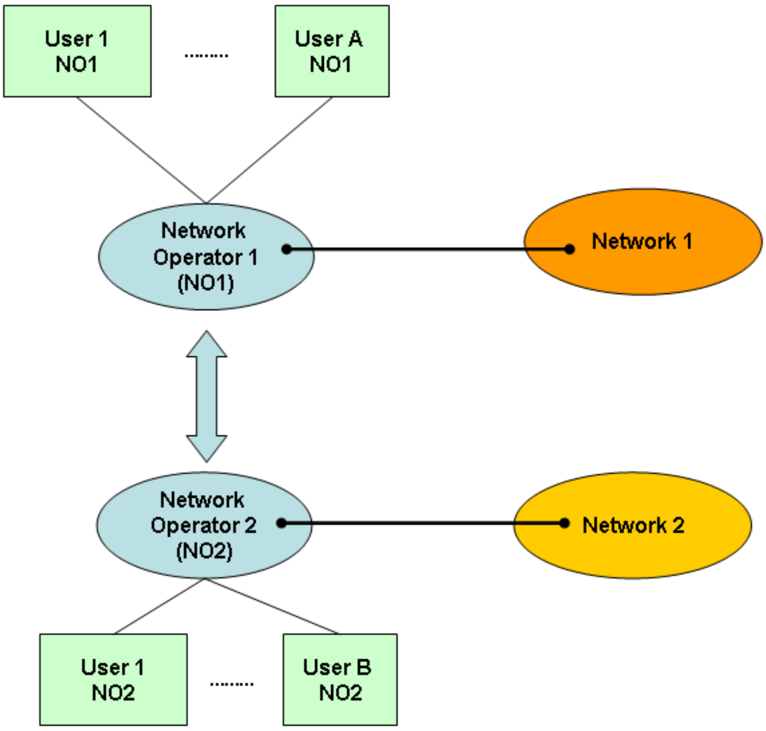

Figure 3: Illustration of "network sharing" where the home network of some of the users is not the shared network

7.3.4 Conclusions on network sharing scenarios

The three use cases are captured in Figure 4.

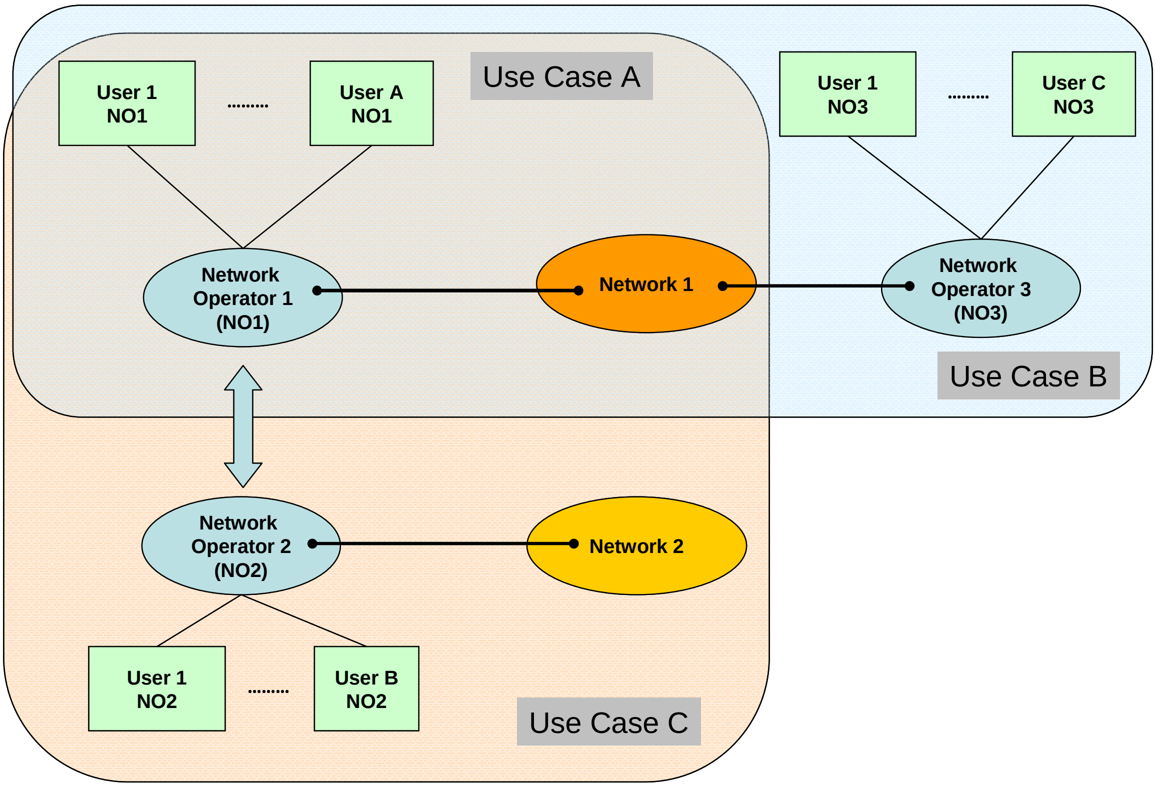

Figure 4: Illustration of different "network sharing" scenarios

Table 1 summarises the operational and technical challenges for the different network sharing cases.

Table 1: Operational and technical challenges underlying network sharing cases

Operational and Technical challenges	Case A	Case B	Case C
Network capacity sharing - How the capacity of the shared network is effectively shared among the different user organisations.	All users served by the same Mobile Network Operator.	Multiple operators share the network or part of it.	Roaming capability for users among multiple networks.
Service provisioning - How communications services can be flexibly and dynamically provisioned to allow communications between and among different user organisations.	All users served by the same Mobile Network Operator.	Multiple operators share the network or part of it.	Roaming capability for users among multiple networks.
Resource management and roaming interworking - How networks will interwork to allow user roaming, service interworking and coordinated resource management	N/A	N/A	Different types of networks may be involved and service level agreements should be put in place.
Definition of new contracts and service level agreements (SLA) among user organizations - The sharing of network resources will require new processes and organization changes.	Specific SLA and contracts need to be defined for PS organizations, which use commercial networks for guaranteed access to resources.	Specific SLA and contracts need to be defined for PS organizations, which use commercial networks for guaranteed access to resources. SLAs need to be defined between telecom operators for sharing the network resources.	Specific SLA and contracts need to be defined for PS organizations, which use commercial networks for guaranteed access to resources. SLAs need to be defined between telecom operators for sharing the network resources. Roaming agreements should be defined among Mobile Network Operators.

Table 2 summarises the feasibility of the network sharing user cases for the operational scenarios identified in clause 6.

Table 2: Feasibility of the network sharing cases for the operational scenarios

Operational scenario	Case A	Case B	Case C
Routine Operations	Routine Operations have predictable traffic patterns. A dedicated public safety network would provide the needed capacity. The capability of network sharing may not be needed for this operational scenario.	Routine Operations have predictable traffic and capacity needs. A dedicated public safety network would provide the needed capacity. Network sharing may not be needed for this operational scenario.	Routine Operations have predictable traffic and capacity needs. A dedicated public safety network would provide the needed capacity. Network sharing may not be needed for this operational scenario.
Emergency Crisis	Emergency crisis create unexpected needs for traffic and broadband connectivity. Network sharing with broadband commercial networks could provide the additional capacity, which is needed by first time responders within a specific time frame. Network sharing is feasible in urban environments where broadband commercial networks have adequate coverage while it may not be feasible in remote areas. Because emergency crisis are usually unpredictable, contingency plans for the reallocation of the resources should be set in place. Because Emergency crisis have a wide range of potential sub-cases, this may be difficult to achieve.	Emergency crisis create unexpected needs for traffic and broadband connectivity. Network sharing with broadband commercial networks could provide the additional capacity, which is needed by first time responders within a specific time frame. Network sharing is feasible in urban environments where broadband commercial networks have adequate coverage while it may not be feasible in remote areas. This use case provides the possibility to have, for instance, mobile virtual operators specific for public safety organizations.	Emergency crisis create unexpected needs for traffic and broadband connectivity. Network sharing with broadband commercial networks could provide the additional capacity, which is needed by first time responders within a specific time frame. Network sharing is feasible in urban environments where broadband commercial networks have adequate coverage while it may not be feasible in remote areas. This use case provides the possibility to have, for instance, mobile virtual operators specific for public safety organizations and the capability of roaming among different networks.
Major Event	The capability of network sharing can provide the additional capacity to public safety organizations during the time of a major event. The allocation of communication resources can be planned in advance as part of the overall arrangements for major events. Major events are usually hosted in urban environments where broadband commercial networks have adequate coverage.	The capability of network sharing can provide the additional capacity to public safety organizations during the time of a major event. The allocation of communication resources can be planned in advance as part of the overall arrangements for major events. Major events are usually hosted in urban environments where broadband commercial networks have adequate coverage. This use case provides the possibility to have, for instance, mobile virtual operators specific for public safety organizations.	The capability of network sharing can provide the additional capacity to public safety organizations during the time of a major event. The allocation of communication resources can be planned in advance as part of the overall arrangements for major events. Major events are usually hosted in urban environments where broadband commercial networks have adequate coverage. This use case provides the possibility to have, for instance, mobile virtual operators specific for public safety organizations and the capability of roaming among different networks.

Operational scenario	Case A	Case B	Case C
Natural disaster	A large natural disaster creates unexpected needs for traffic and broadband connectivity, which are also due to degraded or destroyed fixed networks. Network sharing with any existing and operative broadband commercial networks in the area could provide the additional capacity. Because a large natural disaster may affect a very large area, broadband commercial networks may not have the adequate coverage. Because emergency crisis are usually unpredictable, contingency plans for the reallocation of the resources should be set in place. Because natural disasters have a wide range of potential sub-cases, this may be difficult to achieve.	A large natural disaster creates unexpected needs for traffic and broadband connectivity, which are also due to degraded or destroyed fixed networks. Network sharing with any existing and operative broadband commercial networks in the area could provide the additional capacity. Because a large natural disaster may affect a very large area, broadband commercial networks may not have the adequate coverage. Because emergency crisis are usually unpredictable, contingency plans for the reallocation of the resources should be set in place. Because natural disasters have a wide range of potential sub-cases, this may be difficult to achieve. This use case provides the possibility to have, for instance, mobile virtual operators specific for public safety organizations.	A large natural disaster creates unexpected needs for traffic and broadband connectivity, which are also due to degraded or destroyed fixed networks. Network sharing with any existing and operative broadband commercial networks in the area could provide the additional capacity. Because a large natural disaster may affect a very large area, broadband commercial networks may not have the adequate coverage. Because emergency crisis are usually unpredictable, contingency plans for the reallocation of the resources should be set in place. Because natural disasters have a wide range of potential sub-cases, this may be difficult to achieve. This use case provides the possibility to have, for instance, mobile virtual operators specific for public safety organizations and the capability of roaming among different networks, which is extremely important in the large geographical areas impacted by a natural disaster.
Search & Rescue	The need for additional traffic capacity is extremely limited in search & rescue operations. In addition, broadband commercial networks may not have the needed coverage in remote areas where the search & rescue operations should be executed. For these reasons, this network sharing use case may not be applicable to this operational scenario.	The need for additional traffic capacity is extremely limited in search & rescue operations. In addition, broadband commercial networks may not have the needed coverage in remote areas where the search & rescue operations should be executed. For these reasons, this network sharing use case may not be applicable to this operational scenario.	The need for additional traffic capacity is extremely limited in search & rescue operations. In addition, broadband commercial networks may not have the needed coverage in remote areas where the search & rescue operations should be executed. For these reasons, this network sharing use case may not be applicable to this operational scenario.

7.4 Spectrum Sharing Use Cases

7.4.1 Introduction

The allocation of dedicated, exclusive-use spectrum has been so far the traditional approach to support Public Safety communications. An exclusive allocation of spectrum for public safety is the preferred option of the public safety community because it provides them full control over the resource. In Europe, public safety agencies and industry have for the fast growing need for mission critical mobile data communication, identified a need of at least 2 MHz × 10 MHz for broadband public safety mobile data networks [i.7] while other studies [i.10] are indicating more (e.g. uplink at least 15 MHz). If voice will be integrated in those new mission critical data networks, the needed harmonised frequency band has to be more, to cover also the voice capacity.

The Spectrum regulatory authorities have recently started the process of finding a proper spectrum allocation [i.9].

As a matter of fact, the allocation of new dedicated spectrum to satisfy increasingly data-intensive public safety operational needs is nowadays becoming a challenging issue for spectrum regulatory authorities. One important handicap is that suitable spectrum bands needed to build cost-effective public safety networks are the same highly valued bands demanded by the commercial market to provide key services such as TV broadcasting and 3G/4G mobile communications. Another important requirement for the identification of public safety spectrum bands in Europe is harmonization. New public safety bands should be harmonized across European member states to facilitate cross-border interoperability and an economy of scale for public safety communications equipment.

These two factors are the main reason why it is extremely difficult to allocate new spectrum bands for public safety in Europe. This can become a serious limitation for PPDR users in the future, because it will stop the development of various applications for public safety, which are supposed to be based on the availability of broadband connectivity.

Alternative options to allocate spectrum to public safety organizations are investigated in this clause.

New approaches for spectrum management are based on the concept of "pool" the spectrum resources [i.5].

In the most general case, spectrum pooling is the situation wherein multiple users share spectrum access rights to a common "pool" of spectrum. This spectrum pool can be created from the contribution of several holders of exclusive spectrum individual rights of use (i.e. licence rights are transferred to the pool from individuals), from the allocation of a new spectrum band for explicit spectrum sharing or a combination of both

In fact, spectrum sharing schemes are already in place by National Regulatory Agencies (NRA) in various countries in Europe as described in CEPT report 159 [i.4]. Current spectrum transfer procedures can take some days, which is suitable for long-planned events (e.g. G20 summit or Olympic games). Operation at lower timescales needs further regulatory and technical developments.

An option for spectrum sharing is dynamic transfer of exclusive rights of use, where the rights of spectrum use can be exchanged among different users for a limited time or a limited space. This option is also related to the concept of License Shared Access (LSA) where the sharing and exchange of the spectrum rights of use is subject to a central coordination and authorization. The basic principle of the LSA method can be found already in the Authorized Shared Access (ASA) proposed by Qualcomm [i.6]. The core idea behind ASA resides in the possibility of issuing additional individual authorisations (i.e. licensing) on a shared and non-interference basis to users other than existing incumbent(s) in a given band.

Another option for spectrum sharing is based on opportunistic spectrum access or secondary spectrum access, where a primary user is the licensee and secondary users can access the spectrum in an opportunistic way without causing harmful interference to the primary user.

Finally, Collective Use of Spectrum (CUS) is used as an umbrella term to designate all spectrum management approaches allowing more than one user to occupy the same range of frequencies at the same time, without the need for individual (exclusive) licensing (see [i.11]). Collective use of spectrum can be application-specific, technology-specific, or neither of these. Each approach has its own merits depending on the applications that are expected to use the spectrum in particular, the required quality of service and the likely interference environment. Although the CUS model is very much associated with spectrum used on a licence-exempt basis, it should be seen in a broader context than merely licence-exempted usage.

The following categories of CUS are defined:

1) Licence-Exempt (commons) - non-specific applications: No individual authorisation or co-ordination is required. Access is regulated solely by adherence to pre-defined regulatory conditions. Any application is permitted so long as the regulatory conditions are adhered to, which are typically low power, short range devices and applications. Examples of bands operated under this model are the well-established 2,4 GHz and 5 GHz ISM bands.

2) Licence-Exempt (commons) - specific applications: only one or more applications/technologies are allowed, Pre-defined regulatory conditions (for instance max TX power) apply. An example is the PMR446 band designated for digital short range voice communications.

3) Light licensing - few restrictions: Registration or notification is required. No limits on the number of users but use may be application-specific. Typically, light licensing permits greater power than licence-exempt bands. For example, some European countries allow the use of the 5,8 GHz band for fixed wireless access services on a light licensing basis without the need to apply for an exclusive licence or right of use.

4) Light licensing - with restrictions: Registration or notification is required, and there are limits on the number of users and/or requirements for coordination permits greater power than licence-exempt bands. Recent examples include:

    i) a registration scheme proposed in the U.S for use of the 3 650 MHz - 3 700 MHz band on a collective basis for fixed wireless access where the risk of interference is mitigated by technical means, and where licensees are mutually obliged "to cooperate and avoid harmful interference to one another";

    ii) the UK regulator Ofcom recently awarded through auction, twelve low power concurrent rights of use through auction for the frequencies 1 781,7 MHz - 1 785 MHz paired with 1876,7 MHz - 1 880 MHz. Licensees are expected to co-ordinate their use of the spectrum to avoid harmful interference.

All these spectrum sharing models (i.e. dynamic transfer of exclusive spectrum rights, secondary access and CUS) will be investigated in the following clauses.

7.4.2 Taxonomy of stakeholders and spectrum allocations.

The purpose of this clause is to identify all the potential use cases for spectrum sharing among various stakeholders. To facilitate the identification of use cases, we define the following spectrum sharing options and related spectrum allocations:

1) Spectrum allocation S0. This represents a portion of spectrum where no individual and exclusive spectrum usage rights are in place. Instead, this spectrum is considered to be managed under a "collective use of spectrum (CUS)" model and be available for public safety communications in the incident zone.

2) Spectrum allocation S1. Individual rights of use owned by O1 ensure that spectrum S1 is always available in the incident area. In any case, individual spectrum usage right does not preclude the possibility that, whenever and wherever S1 is not required by O1, this spectrum can be shared with other users.

3) Spectrum allocation S2. This spectrum allocation is similar to S1. However, the consideration of the spectrum pool formed by S1 and S2 as the overall spectrum available for operators O1 and O2 enables the introduction of spectrum sharing solutions for S1 and S2 between operators O1 and O2.

4) Spectrum allocation S3. Individual usage rights of this spectrum belong to O3 that in this case does not have any network infrastructure covering the incident area. Hence, spectrum sharing solutions are needed to facilitate S3 spectrum to be used as required in the incident area. Considering that some of the users served by O3 are expected to participate in the incident response, part of S3 spectrum might be needed for the operation of fast deployable communication equipment these users could bring into the affected place.

5) Spectrum allocation S4. This spectrum is owned by operator O4 and totally or partially used in network N4 deployed in the incident area. This network is not considered to directly support communications services for the responding organizations.

6) Spectrum allocation S5. This spectrum is owned by operator O5 that does not have neither any network infrastructure covering the incident area or any user participating in the incident response.

Figure 5 provides a pictorial description of the relationships between the different types of stakeholders and spectrum allocations, which defines the potential use cases.

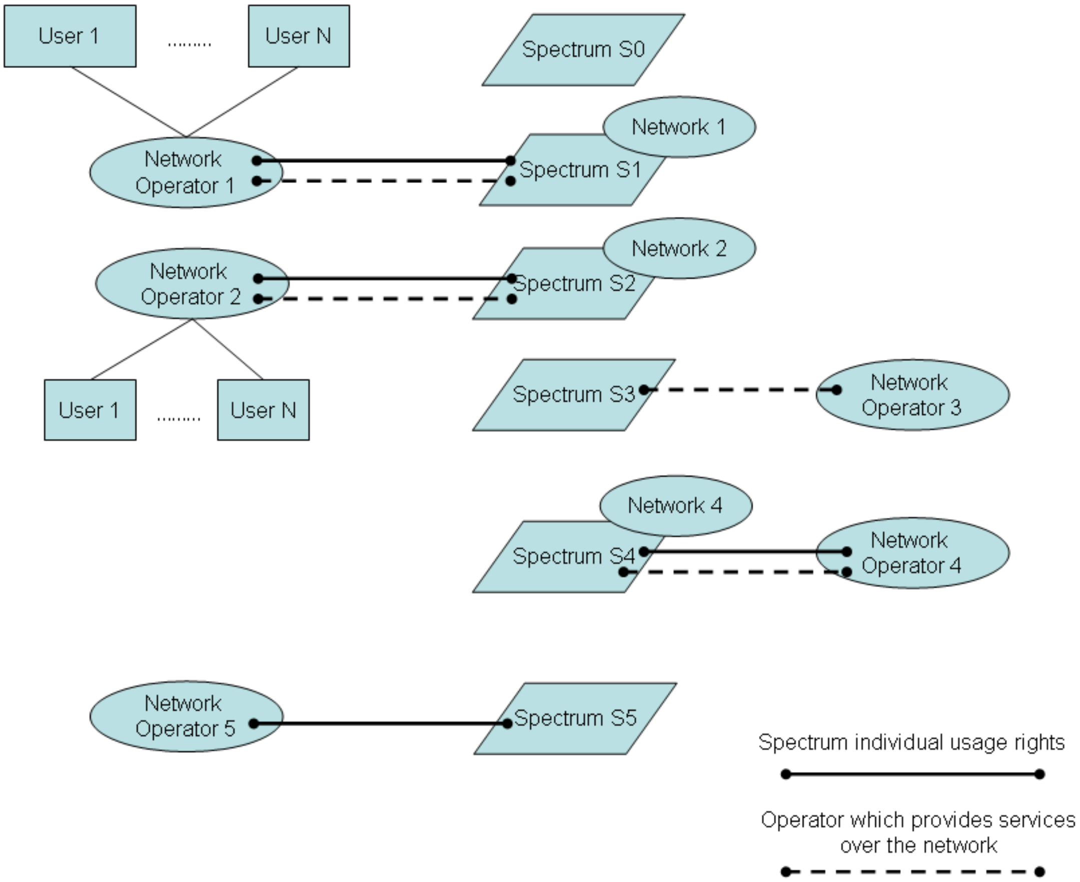

Figure 5: Illustration of different "spectrum sharing" use cases

The following use cases are defined:

1) Operator 1, whose network N1 is deployed in the incident area, has spectrum usage rights over S1. O1's users will be using communication services in the incident area.

2) Operator 2, whose network N2 is deployed in the incident area, has spectrum usage rights over S2. O2's users will be using communication services in the incident area. As such, this spectrum when considered alone is analog to S1. However, the consideration of the spectrum pool formed by S1 and S2 as the overall spectrum available for operators O1 and O2 enables the introduction of spectrum sharing solutions for S1 and S2 between operators O1 and O2.

3) Operator 3 does not have a network deployed in the incident area. However, O3's users will need to get access to communication services in the incident area, thanks to network sharing principles with N1. Operator 3 has spectrum usage rights over S3 spectrum in the incident area.

4) Operator 4, whose network N4 is deployed in the incident area, has spectrum usage rights over S4. In this case, there are not sharing principles in place between N1 and N4.

5) Operator 5 does not have a network deployed in the incident area. Operator 5 has spectrum usage rights over S5 in the incident area.

6) S0 is accessible under non-individual usage rights.

The spectrum allocations and use cases are discussed in detail in the following clauses for the different spectrum sharing management approaches and stakeholders.

7.4.3 Dynamic transfer of exclusive rights of use

In this use case, spectrum rights of use are temporarily transferred from the licensee to other users by means of leasing mechanisms. Prioritization and pre-emption principles can be put in place in the leasing model.

We can consider the following sub-cases:

- Dynamic transfer of exclusive rights of use between commercial and public safety domains.
- Dynamic transfer of exclusive rights of use between military and public safety domains
- Dynamic transfer of exclusive rights of use between commercial and military domain

The advantage of the dynamic transfer of exclusive rights of use is that one single actor (a public safety Mobile Network Operator in the first case or a telecom operator in the third case) will have full control of the portion of the spectrum temporary "transferred". Needless to say that guaranteed QoS is an essential requirement in public safety operational scenarios regardless of the "actors" involved in the transfer.

7.4.3.1 Dynamic transfer of exclusive rights of use between commercial and public safety domains

In this use case, commercial and public safety entities can dynamically transfer exclusive rights of use in occurrence of a specific event like an emergency crisis of a natural disaster or simply when the spectrum is not used.

We can identify the following sub-cases:

1) A Public Safety organization is the licensee of the spectrum and leasing is restricted to other public safety organizations. For example, PS Operator#3 is the licensee of the spectrum S3 but it cannot use it because it does not have the network equipment in the crisis area. Then PS Operator#3 could temporary transfer S3 usage rights to either PS Operator#1 or PS Operator#2.

2) A Public Safety organization is the licensee of the spectrum and leasing can be provided to non-PS organizations. For example, PS Operator#1 is the licensee of the spectrum S1 when there is no emergency situation and part of S1 is not used for public safety routine tasks. Then spectrum usage rights could be leased to e.g. Operator#4 for commercial services delivery through Network#4 (e.g. rural Internet wireless access). This leasing can also be interruptible under strict guarantees when required by PS Operator#1.

3) A non-Public Safety user is the licensee and leasing for public safety organizations is permitted. For example, Commercial Operator#5 is the licensee of S5 usage rights. Public safety organizations may need additional traffic capacity in correspondence to a major planned event (e.g. Olympics games) and they could request Commercial Operator#5 to lease part of this spectrum for Public Safety use.

In the first case we can talk about "intra-domain transfer", while in the other two cases we talk about "inter-domain transfer"

7.4.3.2 Dynamic transfer of exclusive rights of use between military and non-military domains

In this use case, military and public safety entities can dynamically transfer exclusive rights of use in the occurrence of a specific event like an emergency crisis of a natural disaster.

We can identify the following examples:

1) Military-Public Safety transfer: a military organization is the licensee of the spectrum and leasing is restricted only to public safety organizations for disaster management. For example, Military Operator#3 is the licensee of the spectrum S3 but it cannot use it because it does not have the network equipment in the crisis area. Then Military Operator#3 could temporary transfer S3 usage rights to a PS Operator. In another example, Military Operator#1 is the licensee of the spectrum S1, but this can be shared with other public safety organizations when the military and public safety organizations are working together in a natural disaster.

2) Military-Commercial transfer: a military organization is the licensee of the spectrum and leasing can be provided to a telecom operator. For example, Military Operator#3 is the licensee of the spectrum S3 but it does not use it all the time. Then PS Operator#3 could temporary transfer S3 usage rights to a commercial Operator. This is an unlikely use case, because commercial operators may not have the technology to use spectrum for a short-term time, which is usually allocated for military use. The reason is that it will not be economically viable to manufacture and deploy network equipment and terminals, which cannot use the spectrum for most of the time. The feasibility of this use case is anyway strictly connected with the frequency band in question.

7.4.4 Secondary access

Other users (denoted as secondary users) than the licensee can get access to the spectrum provided that the licensee (denoted as the primary user) is not impacted by harmful interference.

We can identify two sub use cases of secondary access:

- Secondary access based on coordination mechanisms. In this use case, the primary user can have some control on the secondary access (e.g. dynamically decide whether secondary access is allowed or not).

- Secondary access based on coexistence mechanisms. In this case, there is no primary-secondary coordination mechanism and primary users have no control over secondary access (i.e. primary and secondary users coexist without explicit interactions).

7.4.4.1 Secondary access based on coordination mechanisms

In this use case, the primary user can have some control on the secondary access (e.g. dynamically decide whether secondary access is allowed or not).

We can identify the following use cases:

1) Secondary access is allowed to public safety users in non-PS spectral bands. The commercial operator is the primary user in the bands and the PS operator is the secondary user. For example, Operator#4 in charge of e.g. a cellular network can unleash part of spectrum S4 in the incident area and advertise it through e.g. a beacon signal sent via Network#4. Unleashed S4 spectrum could then be exploited by PS users. This use case is recommended only for very specific non mission critical applications and not during an emergency crisis. For example, secondary access can be allowed for environmental purposes to send environmental data on water to a remote monitoring station.

2) Secondary access is allowed in PS bands or Military bands. For example, PS Operator#2 may advertise that part of S2 is not used under routine operation and make this spectrum available for secondary access. Secondary users can be restricted to PS applications or be open to non-PS services (e.g. commercial Operator#4 may benefit). Whenever PS#2 requires the entire S2 band again (e.g. crisis response), PSN#2 infrastructure stops advertising the availability of this spectrum for secondary access. This use case is recommended only when the PS spectral bands are not used for mission critical applications all the time or the PS bands are used only in very specific geographical locations. For example, some military bands are only used for training in specific areas, which are remotely located in relation to civilian populations. In this case, commercial users could use these frequency bands if protection mechanisms are put in place, which will stop the transmissions behind a boundary zone. In case of emergency and the bands need to be used over a wider area, the Military operator can deny the communication to the secondary devices.

7.4.4.2 Secondary access based on coexistence mechanisms

In this case, there is no primary-secondary coordination mechanisms and primary users have no control over secondary access (i.e. primary and secondary users coexist without explicit interactions).

We can identify the following use cases:

1) Secondary access is allowed in PS bands, but it is restricted to PS applications. For example, communication devices such as local equipment brought in the incident area by PS agencies served by PS Operator#1 and PS Operator#2 could detect (by e.g. sensing or geolocation database) the unused S3 spectrum and exploit it.

2) Secondary access is allowed to PS users in non-PPDR bands. For example, monitoring stations for the environment could detect that part of S4 (e.g. used to run a commercial PMN network) and/or S5 (e.g. exploited by military users) is not being utilized and use it for enhancing ad-hoc connectivity of the monitoring system.

7.4.5 Collective use of spectrum

A number of users are authorised to use the band as a result of either a general authorisation regime (e.g. license-exempt band with no limitations in the number of users) or a light-licensing regime (i.e. users are to be registered within the spectrum regulatory authority which might place limits on the number of authorisations).

We can identify two sub use cases of secondary access:

- Collective use of spectrum based on coordination mechanisms. In this case, coordination among authorised users/devices is required through a common management protocol in order to cope with mutual interference

- Collective use of spectrum based on coexistence mechanisms. In this case, no common management protocol is defined among authorised devices. Instead, coping with mutual interference is mainly pursued through the compliance of devices to the specific regulator-imposed rules (i.e. spectrum etiquettes).

7.4.5.1 Collective use of spectrum based on coordination mechanisms

In this case, coordination among authorized users/devices is required through a common management protocol in order to cope with mutual interference.

We can identify the following use case:

- S0 could be a band managed under a light-licensing regime and restricted to PS organizations. All registered and explicitly authorized PS users might use S0 to setup fast deployable equipment (e.g. wireless access points, point-to-point links). Coordination for e.g. channel assignment is carried out through a common protocol supported by all authorized devices. The development of such a common protocol is facilitated by the restriction of this band to PS applications.

7.4.5.2 Collective use of spectrum based on coexistence mechanisms

In this case, there is no primary-secondary coordination mechanisms and primary users have no control over secondary access (i.e. primary and secondary users coexist without explicit interactions).

We can identify the following use case:

- S0 can be a general purpose license-exempt band such as the 2,4 GHz or 5 GHz ISM bands. The use of this band can bring additional capacity in the incident area for local area communications, yet no preferential access or coordination mechanisms will be available for PS users to control the interference from any other legitimate user of the band (e.g. personal devices or private/public wireless access networks).

7.4.6 Conclusions on spectrum sharing scenarios.

The purpose of this clause is to evaluate the applicability of the use cases defined in this clause to the operational scenarios defined in clause 6 and to identify operational and technical challenges.

Table 3 summarises the operational and technical challenges for the different spectrum sharing cases.

Table 3: Operational and technical challenges underlying spectrum sharing cases

Operational and Technical challenges	Dynamic transfer of exclusive rights of use	Secondary access	Collective use of spectrum
Definition of pre-emptive schemes among PS, Military and commercial organizations - The schemes and rules to reallocate the spectrum based on pre-emptive schemes should be defined before the crisis occurs.	The transfer of spectrum among different domains is already possible and regulated in many European countries [i.4] but it may take a considerable time (days) to implement the transfer of spectrum. Operation at lower timescales needs further regulatory and technical developments.	N/A	N/A
Definition of geo-location databases for secondary access - Geo-location database and cognitive channel should be defined to ensure protection of primary users from secondary devices.	N/A	Solutions for PS spectrum sharing may benefit from proposals and achievements within the TV White Space domain, based on the definition of geolocation databases.	N/A
New procedures for PS organizations - New procedures should be put in place to coordinate the sharing of spectrum resources during an emergency crisis.	New procedures should be integrated in the existing arrangement and procedures for disaster management.	New procedures should be integrated in the existing arrangement and procedures for disaster management.	Application-specific bands for PPDR communications are already available in US (4,9 GHz band) and in some European countries (BroadBand Disaster Relief, BBDR, band in the 5 GHz frequency range), especially to implement on-scene broadband wireless networks. Authorised users are responsible for interference prevention, mitigation, and resolution coordination among them. The use of the 4,9 GHz band is already supported by some PS equipment vendors.

Table 4 summarises the feasibility of the spectrum sharing use cases for the operational scenarios identified in clause 6.

Table 4: Feasibility of the spectrum sharing cases for the operational scenarios

Operational scenario	Dynamic transfer of exclusive rights of use	Secondary access	Collective use of spectrum
Routine Operations	Routine Operations have predictable traffic patterns. A dedicated public safety network would provide the needed capacity. The capability of spectrum sharing may not be needed for this operational scenario. The time requested to transfer the exclusive rights of use may not be compliant with the time requirements or routine operations in urban environment.	Routine Operations have predictable traffic patterns. A dedicated public safety network would provide the needed capacity. The capability of spectrum sharing may not be needed for this operational scenario. Furthermore, uncoordinated secondary access may not provide the needed QoS for mission critical operations.	Routine Operations have predictable traffic patterns. A dedicated public safety network would provide the needed capacity. Furthermore, uncoordinated collective use of spectrum may not provide the needed QoS for mission critical operations.
Emergency Crisis	Emergency crisis creates unexpected needs for traffic and broadband connectivity. Dynamic transfer of exclusive rights of use may provide the needed traffic capacity, while ensuring the appropriate QoS. Its implementation requires cognitive or (at least) tuneable radios which can be configured to operate in different spectral bands. Initial deployment could be restricted to spectrum transfers among public safety users, including the possibility to create spectrum pools Extension to military and/or commercial marketplace users could be addressed in a subsequent stage. Another significant challenge is to ensure that the transfer of rights is executed in the time constraints defined by the operational requirements.	Emergency crisis creates unexpected needs for traffic and broadband connectivity. Various sub scenarios for the application of secondary access can be envisaged. Secondary access can be implemented both in time and space. The most significant challenge is to ensure guaranteed QoS to primary users. For this reason, a coordinated approach is preferable.	Emergency crisis creates unexpected needs for traffic and broadband connectivity. Collective use of spectrum could be used in IAN to implement wireless local area networks. The challenge is to implement common protocols, which can be used by different public safety organizations in the field. To ensure guaranteed QoS, a coordinated approach is preferable.
Major Event	Major events create higher demand of traffic in comparison to routine operations, but this demand of traffic can be planned in advance. As a consequence, the dynamic transfer of exclusive rights of use can be executed in an easier way than other scenarios.	Because of the large density of people and public safety officers in the major event, spectrum utilization can be quite high and secondary access may not be feasible for this scenario.	Because a major event is usually local to a specific time and space, collective use of spectrum could be a feasible approach for this operational scenario. A potential challenge is scalability because of the large number of actors present in the scenario and the need to implement common protocols, which can be used by different public safety organizations in the field. To ensure guaranteed QoS, a coordinated approach is preferable.

Operational scenario	Dynamic transfer of exclusive rights of use	Secondary access	Collective use of spectrum
Natural disaster	A large natural disaster creates unexpected needs for traffic and broadband connectivity, which are also due to degraded or destroyed fixed networks. Dynamic transfer of exclusive rights can be suitable in sub-scenarios where a specific network infrastructure is not able to use its licensed spectrum and the spectrum is idle. In this context, the unused spectrum can be transferred to another party, which does not need a fixed infrastructure like a wireless local area network.	Because a large natural disaster can impact a very large area, secondary access could be used for environment monitoring, where QoS are not so restrictive like in other public safety applications.	Collective use of spectrum could be used to deploy wireless local area networks in specific areas impact by the natural disaster. Because the response phase of a large natural disaster can involve many different stakeholders, a potential challenge is related to scalability.
Search & Rescue	The need for additional traffic capacity is extremely limited in search & rescue operations; as a consequence the suitability of this spectrum model for this operational scenario is limited.	Secondary access could be used to provide connectivity for operations where wide coverage is needed and primary user networks are not present (e.g. sea, remote or rural areas). A significant challenge is to guarantee QoS.	Because this operational scenario may be related to large geographical areas and traffic capacity requirements are limited, Collective Use of Spectrum may not be a suitable approach.

8 Potential operational and technical requirements

8.1 Introduction

The potential operational and requirements are classified in two main categories:

- **Functional requirements**, which describe what the system should provide to support specific functions. The following sub-categories can be identified:
    - prioritisation requirements;
    - interoperability and interworking requirements;
    - resource management requirements.
- **Non-Functional requirements**, which are transversal to the functions. The following sub-categories can be identified:
    - availability requirements;
    - security requirements;
    - usability requirements.

The following clauses describe the potential operational and technical requirements associated to the above mentioned categories/sub-categories.

8.2 Potential Functional Requirements

8.2.1 Prioritisation requirements

- PMN should offer priority services to give precedence to public safety communications over other types in accordance with some pre-established criteria. Pre-emption capabilities should be supported. Different levels of prioritisation should be considered.

- Prioritisation services should be either permanently activated in the PMN or activated on-demand in less than a pre-established time.

- A given fraction of PMN capacity should be available for public safety users' communications in accordance with some pre-established criteria when priority services are activated.

- Prioritisation services should be permanently activated in the PMN.

- Direct mode communications between UEs should support prioritisation. Pre-emption capabilities should be supported. Different levels of prioritisation should be considered.

- Prioritisation services should consider public safety users' access rights and role within the incident command structure.

- Prioritisation services should consider the type of application (e.g. messaging, video streaming) and also allow for content prioritisation (e.g. messaging data with information related to the safety of the public versus messaging data with non-critical information).

- Prioritisation should consider the context (e.g. rural, urban).

- Prioritisation services should consider location of communication endpoints (e.g. different precedence for those at and in close proximity to the scene than external sources such as tactical-level command units)

- Public safety users' intervention for the configuration and setting up of prioritised communications should be minimised.

- Priority rights should be associated to end users and not to terminals.

- Prioritisation services should be dynamically configurable.

- The system should support mechanisms to facilitate the management of prioritisation services of coexisting PSNs, PMNs, IANs and UEs (e.g. coordinated configuration of equivalent priority levels and eligibility conditions across communications elements).

8.2.2 Interoperability and interworking requirements

- IAN, PSN and PMN should provide roaming capability.

- Roamer end users should perceive as little difference as possible in the service offerings and capabilities.

- Service interworking should be possible between end users attached to different serving networks (i.e. IAN, PSN or PMN), whenever each individual serving network has the ability to support the same or similar service (e.g. voice services, short data message services, IP connectivity services for client-server transactions).

- Inter-agency public safety communications should be possible (e.g. between public safety users attached to the same or different serving networks irrespectively of those networks being home or visited networks).

- The system should support mechanisms for dynamic public safety service provisioning (e.g. dynamic group network assignment configured over-the-air).

- Service continuity should be supported for a public safety user handing over networks.

- Interfaces between communication elements (i.e. PMNs, PSNs, IANs, UEs) should be open.

- Interfaces between infrastructure communication elements (i.e. PMNs, PSNs) should support IP-based transport.
- UE terminals should be able to operate the most common public safety and commercial radio access technologies (e.g. TETRA/TETRAPOL and 3GPP UMTS/LTE).

NOTE: There may be differences related to the type of Public Safety UE: handheld, vehicular and fixed.

8.2.3 Resource management requirements

- The system should support mechanisms to enable an efficient and effective use of available radio communication resources of coexisting PSNs, PMNs, IANs and UEs (e.g. coordinated operation of resource management functions).
- The mechanisms for resource management should be scalable (e.g. able to cope with scenarios with a high number of networks and terminals, and potentially involving several Mobile Network Operators).
- The mechanisms for resource management should facilitate the provision of broadband radio connectivity for public safety.
- The system should implement mechanisms to facilitate information gathering about operational communication needs of public safety users in a specific geographical area at a given point of time.
- The system should implement mechanisms to facilitate the collection and distribution of information about available and operative communication infrastructure and resources in a specific geographical area at a given point of time.
- Radio parameters (e.g. transmit power level, operating frequency, etc.) of PSNs, PMNs, IANs and UEs should be dynamically configurable.
- The mechanisms for resource management should be able to adapt radio parameters under changes in the internal network structure of PMNs and PSNs (e.g. addition of a portable base station, base station failure).
- The management entity should also be able to reconfigure dynamically or demand the resources for UEs, IANs, EIANs, and PSNs. The reconfiguration could involve the adjustments of MAC, routing protocols and/or radio parameters.
- The system should have the capability to reconfigure radio and protocol parameters, within specified time constraints, on the basis of changing resource needs and environmental conditions.
- The mechanisms for resource management should be able to control the capacity distribution among public safety users.
- The system should be aware of and should be conformant to the spectrum regulations valid in the coverage area.
- The system should support dynamic spectrum management mechanism to obtain or lease exclusive rights of spectrum usage for a specific area and for a specific period of time.
- The system should be aware of unused spectrum (through e.g. spectrum sensing, geo-location database) that can be utilised on as secondary basis.

8.3 Non-functional requirements

8.3.1 Availability

- The system should be able to provide coverage and communication services to public safety users regardless of the operational scenarios and within the capabilities of the available communications elements.
- The system should be able to recover from failures in some of the involved communications networks (PMN, PSN, IAN) or parts therein.

- The hardware and software components of the system should be fault tolerant.
- The system should be able to provide coverage and communications services to public safety users within pre-defined timing constraints.

8.3.2 Security

- The system should authenticate and authorise users to grant access to communications services and resources.
- End-to-end secure communications should be supported among any pair of endpoints irrespective of the networks (IAN, PSN, and PMN) involved in the communication path.
- The system should prevent misuse of the spectrum and network resources in the area of responsibility from intentional (e.g. malicious attacker, mobile malware) or unintentional threats (e.g. failure of a communication node).
- The system should validate and be conformant to the security requirements already defined for communication technologies and networks with which it interfaces and interworks (e.g. cryptographic services used by the existing communication networks should be supported).
- The system should provide accountability on the utilisation of the spectrum and networks resources.
- The use of PMNs should not compromise communications' security.

8.3.3 Usability

- The system's usability should fit with existing procedural and operational frameworks defined in public safety organisations.
- The system should hide its complexity to the end user and should minimise end user intervention.
- The usability of UE used in emergency situations should be the same as that used in day-to-day operations.
- The implementation of the new system functionalities should not degrade the usability of existing communication elements.
- The system should ensure that communication services are transparently provisioned to end users regardless of the serving network.
- The introduction of new functionalities in affected communication elements should not negatively impact on their backward-compatibility.

9 Conclusions

The present document has provided a comprehensive view of the potential spectrum and network sharing use cases which can enhance the operational capabilities of public safety officers and provide enhanced communication capacity for crisis management. The objective of the proposed models is:

a) to provide enough radio frequency spectrum to satisfy stringent spectrum demanding operational needs in major incidents; and

b) improve efficiency of spectrum utilization by avoiding situations where spectrum is unused when not required for routine public safety tasks.

In the current operational and technological context, due to the severe requirements of mission critical operations, the proposed use cases are suitable only for non-mission critical applications, which are still very relevant for public safety officers.

The network and spectrum sharing use cases presented in the present document could be used for a future communication framework for public safety, which could be based on two main components:

1) a dedicated network infrastructure with dedicated spectrum bands for mission-critical operations (e.g. the current TETRA infrastructure)

2) network and spectrum sharing solutions with commercial and military domains for non-mission critical operations

Progressing towards the realisation of these sharing models can overcome or mitigate the current spectrum deadlock faced by many spectrum regulatory authorities that have significant challenges to identify additional harmonized spectrum at European level for public safety exclusive use.

History

Document history		
V1.1.1	January 2013	Publication