



## **Pre-Commercial Procurement (PCP)**

### **BroadWay**

**Innovation activity to enable a pan-European interoperable broadband mobile system for PPDR**

## **TENDER DOCUMENT 2:**

### **PCP Challenge**

Version dated 15 February 2019

## ***SUBMISSION TO EC AS D2.2***

This description of the PCP Challenge, designated as Tender Document 2 (TD2), should be read in conjunction with other documents related to this Pre-Commercial Procurement (PCP), listed hereunder:

- Tender Document 1: Request for Tenders (TD 1)
- Tender Document 3: Framework Agreement (TD 3)
- Tender Document 4: Specific Contract for Phase 1 (TD 4)

All documents can be downloaded from and uploaded to the Broadway website [www.broadway-info.eu](http://www.broadway-info.eu)

## TABLE OF CONTENTS

<b>1</b>	<b>DESCRIPTION OF SERVICES TO BE PROCURED</b>	<b>12</b>
1.1	INTRODUCTION	12
1.2	PREPARATION FOR THE PCP	12
1.2.1	<i>BroadMap</i>	12
1.2.2	<i>SpiceNet</i>	13
1.2.3	<i>Open Market Consultation</i>	17
<b>2</b>	<b>THE BROADWAY COMMON CHALLENGE</b>	<b>17</b>
2.1	OPENING STATEMENT	18
2.2	PCP CHALLENGE - OBJECTIVES LIST	20
2.2.1	<i>Objective 1: Pan-European Architecture</i>	22
2.2.1.1	PEAr Pan-European Architecture Sub-objectives	23
	PEAr1 Involvement of Radio access provision and consumer/commercial operation:	23
	PEAr2 Organisational schemes:	23
	PEAr4 Standardised commercial solutions:	23
	PEAr5 Standardised mission critical broadband solutions	23
	PEAr6 PPDR networks	24
	PEAr7 PPDR users	24
2.2.2	<i>Objective 2: Pan-European Availability</i>	25
2.2.2.1	PEAv Pan-European Availability Sub-objectives	25
	PEAv1 Harmonised Availability	25
	PEAv2 Harmonised Quality of Service	25
	PEAv3 Capacity	25
	PEAv4 Seamless Operation	25
	PEAv5 Assuring Quality of Experience	25
	PEAv6 Air Ground Air	25
2.2.2.2	PEAv-Pan-European Availability Sub-objectives (Nice to Have)	25
	PEAv7 National Coverage	25
	PEAv8 Disconnected network	25
2.2.3	<i>Objective 3: Pan-European Security</i>	26
2.2.3.1	PESAr-Pan-European Security Architecture Sub-objectives	26
2.2.3.1.1	PESAr1 Fundamental Security	26
	PESAr2 Vulnerability	26
	PESAr3 Standardised and Certification encryption	26
	PESAr4 End 2 End Encryption	26
	PESAr5 User and Control Plane	26
	PESAr6 Device/User Authentication	26
	PESAr7 Mutual Authentication	26
	PESAr8 Rights Management	27
	PESAr9 Over the Air Re-keying	27
	PESAr10 Enterprise Mobility Management	27
	PESAr11 Integrity	27
	PESAr12 Security Policies	27
	PESAr13 Software Quality Assurance	27
	PESAr14 Service Assurance	27
	PESAr15 Harmonised Security Assurance	27
2.2.3.2	PESAr-Pan-European Security Architecture Sub-objectives (Nice to Have)	27
	PESAr16 EMM innovations	27
2.2.4	<i>Objective 4: Pan-European SpiceNet Governance</i>	28
2.2.4.1	PESg-Pan-European SpiceNet Governance Sub-objectives	28
	PESg1 Legal framework for SpiceNet governance	28
	PESg2 System management	28
	PESg3 Authorised Administration	28
	PESg4 Management technology	28
	PESg5 Monitoring	29
	PESg6 Provisioning	29
	PESg7 Billing	29
2.2.5	<i>Objective 5: Pan-European Operational Mobility</i>	30
2.2.5.1	PEOm-Pan-European Operational mobility Sub-objectives	30
	PEOm1 Seamless communication groups spanning networks and authorities	30
	PEOm2 Seamless Access to information sources	30

## TD2 BroadWay PCP Challenge

PEOm3 Seamless Access to applications and databases	30
PEOm4 Harmonised Operational mobility - Same as home	30
2.2.5.2 PEOm-Pan-European Operational mobility Sub-objectives (Nice to Have)	30
PEOm5 Forced network selection	30
<b>2.2.6 Objective 6: Standardised Solutions</b>	<b>31</b>
2.2.6.1 Ss-Standardised solutions Sub-objectives	31
Ss1 Use of Open Common Standards	31
Ss2 3GPP Mission Critical Services	31
Ss3 Release compatibility and upgradability	31
Ss4 Radio Equipment Directive	31
Ss5 3 <sup>rd</sup> party Applications, Equipment and Users	31
Ss6 Statement of Compliance	31
Ss7 Standardisation roadmap	31
Ss8 Locating Users	31
Ss9 Security architecture framework	31
Ss10 Standardised technical policies supporting information exchange	31
Ss11 Standardisation contribution obligation	31
Ss12 Informational interoperability	31
<b>2.2.7 Objective 7: Application Eco-system</b>	<b>32</b>
2.2.7.1 AEs - Application Eco-system Sub-objectives	32
AEs1 Open APIs	32
AEs2 MCX service APIs and extension	32
AEs3 Platform compatibility	32
AEs4 Standardised codecs	32
AEs5 Audio and Video quality	32
AEs6 Open Application Development Platform	32
AEs7 Application acceptance by Practitioners	32
AEs8 Application Scalability	32
AEs9 Application reliability	33
AEs10 Notification of Degraded application operation	33
AEs11 Availability of authorised MCX services	33
AEs12 Application support for Operational Mobility	33
2.2.7.2 AEs Application Eco-system Sub-objectives (Nice to have)	33
AEs13 Internet of Public Safety Things (IoPST)	33
<b>2.2.8 Objective 8: Device Eco-system</b>	<b>34</b>
2.2.8.1 DEs - Device eco-system Sub-objectives	34
DEs1 Deployment of Applications	34
DEs2 Ergonomic and User Friendly	34
DEs3 Programmable buttons	34
DEs4 Simple group selection	34
DEs5 Mobile Device Management	34
DEs6 Robust and Ruggedised	34
DEs7 Battery Life	34
DEs8 Peripheral Equipment Interfaces	34
DEs9 Open APIs/SDKs for MC application development	34
DEs10 Device Management and Monitoring	34
DEs11 Display quality	34
2.2.8.2 DEs - Device eco-system Sub-objective (Nice to have)	35
DEs12 Induction charging	35
DEs13 Bring your own Device	35
DEs14 Terminal to Terminal	35
<b>2.2.9 Objective 9: Innovation Eco-system</b>	<b>36</b>
2.2.9.1 IEs - Innovation Eco-system Sub-objectives	36
IEs1 New innovation	36
IEs2 Common test facilities for new innovation	36
2.2.9.2 IEs - Innovation Eco-system (Nice to Have)	36
IEs3 Integration of existing components	36
IEs4 Supporting future Innovation	36
<b>2.2.10 Objective 10: Technical validation</b>	<b>37</b>
2.2.10.1 Tv - Technical Validation	37
Tv1 Technical Validation process	37
Tv2 Sustainable Technical validation capabilities	37
Tv3 Plugtest™ style events	37
Tv4 PEAv Technical Validation - Pan-European Availability	37
Tv5-PESAr Technical Validation - Pan-European Security	37

## TD2 BroadWay PCP Challenge

Tv6-PESg Technical Validation - Pan-European SpiceNet Governance	38
Tv7-PEOm Technical Validation - Pan-European Operational Mobility	38
Tv8-AEs Technical Validation - Application Eco-system	38
2.2.11 <i>Objective 11: Practitioner evaluation</i>	39
2.2.11.1 PREv- Practitioner evaluation and acceptance Sub-objectives	39
The Practitioner Evaluation Team (PEVT) will be supported by Suppliers to assist with the logistics to carry out evaluation of the Pilot. Please refer to section 1.5 of the RFT.	39
PREv1 Practitioner Evaluation methodology and process	39
PREv2 Practitioner Evaluation of MC services	39
PREv3 Practitioner Evaluation of MC Applications, making use of MC services	39
PREv4 Practitioner Evaluation of Information services enhanced by Operationally mobile MC Applications and Services	39
2.2.11.2 PEaA1- Practitioner evaluation and acceptance (Nice to have)	39
PREv5 Existing or enhanced applications to support the pilot	39
2.2.12 <i>Disclaimer</i>	40
2.3 PHASE 1 – SOLUTION DESIGN	41
2.4 PHASE 2 – SOLUTION PROTOTYPE	41
2.5 PHASE 3 – PILOT	41
2.5.1 <i>Use case scenarios (Trials)</i>	41
UCS1 Rescue operation - Barge of Irregular Migrants	41
UCS2 Rescue operation - A Cruising ship on fire at Adriatic Sea	42
UCS3 VIP protection and escort on high level summit in Brussels	42
UCS4 Following a “go fast” drug convoy from south of Spain to Germany	42
UCS5 Heavy Truck and Tourist Bus collision at Finnish-Norwegian border	42
UCS6 Database queries from other EU country’s PPDR organisation	42
UCS7 Natural Disaster – Forest Fire	42

**GLOSSARY**

Term	Explanation
<b>3GPP</b>	3 <sup>rd</sup> Generation Partnership Programme
<b>ACB</b>	Access Class Barring
<b>AGA</b>	Air ground Air connections
<b>API</b>	Application Programming Interface
<b>Application</b>	We consider applications with a human interface to be primarily 'Mission Critical' for use by Public Safety Responder Practitioners.
<b>AVPL</b>	Automatic Vehicle & Personal Location
<b>Broadband systems</b>	A broadband mobile system
<b>BroadMap</b>	Project BroadMap <a href="http://www.broadmap.eu">www.broadmap.eu</a> . Please note publicly available deliverables. <a href="http://www.broadmap.eu/download-final-deliverable">http://www.broadmap.eu/download-final-deliverable</a>
<b>BroadNet services</b>	Services provided from BroadNet
<b>BroadNet system</b>	BroadNet is the finally procured solution as defined during BroadWay.
<b>BroadWay Common Challenge</b>	The BroadWay Common Challenge is defined by this package of procurement documentation, primarily TD2.
<b>BroadWay Group of Procurers</b>	The up to date membership list of the BroadWay Group of Procurers can be found on the website <a href="https://www.broadway-info.eu/broadway-team/">https://www.broadway-info.eu/broadway-team/</a>
<b>BSS</b>	Business Support System
<b>Business logic</b>	Process and procedures that fulfil the SpiceNet governance policy
<b>BYOD</b>	Bring Your Own Device
<b>COTS</b>	Referring to technological components that are available as Commercial Off The Shelf

TD2 BroadWay PCP Challenge

<b>Device</b>	A UE (3GPP TS 22.280), a communication device without a MMI, or peripheral
<b>EAL</b>	Common Criteria Evaluation Assurance Level
<b>EE2E / E2E</b>	End to End Encryption
<b>eMLPP</b>	enhanced Multi-Level Precedence and Pre-emption as defined by 3GPP
<b>EMM</b>	Enterprise Mobility Management
<b>ETSI CTI</b>	European Telecommunication Standards Institute Centre for Testing and Interoperability
<b>Foundation agreement</b>	Agreements between BroadWay group of procurers and other organisations, integrating with, providing, and consuming BroadNet services
<b>Group</b>	A group of public safety practitioners that will use Mission Critical services
<b>HW</b>	Hardware
<b>IEEE</b>	The Institute of Electrical and Electronic Engineers
<b>IETF</b>	Internet Engineering Task Force
<b>Information</b>	Data in the context of a situation
<b>information service</b>	A service that will process information
<b>Interoperability</b>	Primarily non-technical: Political, strategy, Operations and Procedures benefiting from knowledge and awareness, derived from technical communication exchange in terms of semantic/syntactic interpretations of a data object transferred over a communication system, that may use any particular standardised protocol defined in terms of a logical and physically (RF/Electronic) interpretable form.
<b>IoPST</b>	Internet of Public Safety Things. IoT designed to support Public Safety Responder Practitioners with their operations
<b>IoT</b>	Internet of Things
<b>IPR</b>	Intellectual Property Rights
<b>KPI</b>	Key Performance Indicator
<b>MAM</b>	Mobile Application Management
<b>MC Application</b>	An application making use of MCX services
<b>MC-data</b>	Mission Critical Data Services (e.g. Short Data Service, File Distribution, Database Queries) TS23.282

TD2 BroadWay PCP Challenge

<b>MC device</b>	Mission Critical Device (All Devices used by PPDR Users on MC BB Services) "MCX UE: A UE that can be used to participate in MCX Services 3GPP TR 22.280"
<b>MCM</b>	Mobile Content Management
<b>MC-PTT</b>	Mission Critical Push to Talk
<b>MC-video</b>	Mission Critical Video
<b>MCX</b>	Mission Critical Services
<b>MDM</b>	Mobile Device Management
<b>MIM</b>	Mobile Identity Management
<b>Mission Critical</b>	A mission critical communication service shall provide the ability for an operating organisation (or delegated organisation) to be accountable for communication services in the face of public safety response and lifesaving situations. Quality or characteristic of a communication activity, application, service or device, that requires short responsive communication setup time, low transfer latency, high availability and reliability.
<b>Mission Critical Application</b>	A Mission critical application that can support our definition of Mission Critical
<b>Mission Critical Service</b>	Mission Critical Service: Communication service providing enabling capabilities for Mission Critical Applications that are provided to end users from Public safety Mobile Operators or other Mission Critical businesses and organisations (e.g., utilities, railways). 3GPP TS 22.280
<b>MMI</b>	Man Machine Interface
<b>MNO</b>	Mobile Network Operator
<b>Mobility</b>	Equivalent to Practitioner Operational Mobility (see below)
<b>MOS</b>	Mean Opinion Score - a measure used in the domain of Quality of Experience and telecommunications engineering ITU-T P800
<b>MVNO</b>	Mobile Virtual Network Operator
<b>Narrowband Systems</b>	Typically referring to narrowband communication technology used by public safety responder practitioners (TETRA, TETRAPOL, etc...)
<b>National broadband PPDR mobile network</b>	A broadband mobile communication capability provided for national use by responder practitioners

TD2 BroadWay PCP Challenge

<b>National public safety broadband network</b>	National Broadband PPDR mobile network (above)
<b>NCP</b>	National Contact Point
<b>OMA</b>	Open Mobile Alliance
<b>Operating Model</b>	A model used by a Public Safety Mobile Operator to deliver its services (Dedicated Network, Dedicated Commercial Network, Commercial Operator, MVNO or Hybrid). See BroadMap Deliverable D4.1 Section 10. <a href="http://www.broadmap.eu/download-final-deliverable">http://www.broadmap.eu/download-final-deliverable</a>
<b>Organisational schemes</b>	Organisational schemes as defined by BroadMap D4.1 Section 10. <a href="http://www.broadmap.eu/download-final-deliverable">http://www.broadmap.eu/download-final-deliverable</a>
<b>OS</b>	Operating System
<b>OSS</b>	Operations Support System
<b>Pan – European</b>	Spanning the geopolitical nature of Europe (EU Member states, Associated States, and other non-EU countries). 'of or relating to all European countries or the advocacy of political or economic unity among European countries' - Collins English dictionary
<b>pan-European PPDR broadband network</b>	The ultimate challenge to be solved by BroadWay to provide communication services to operation mobility for public safety responder practitioners - BroadNet
<b>Peripheral</b>	An ancillary device used to inject information into and obtain information out from a UE
<b>PESQ</b>	Perceptual Evaluation of Speech Quality ITU-T P862
<b>PEVQ</b>	Perceptual Evaluation of Video Quality e.g. ITU-T P910
<b>Pilot</b>	The outcome of BroadWay Phase 3 will be a pan-European pilot system at Technology Readiness Level 8 (TRL8)
<b>Plugtest</b>	Refers to ETSI Plugtest™ <a href="https://www.etsi.org/about/what-we-do/plugtests">https://www.etsi.org/about/what-we-do/plugtests</a>
<b>PPDR</b>	Public Protection and Disaster Relief (All Safety and Security Agencies)
<b>Practitioner Evaluation</b>	A non-functional evaluation of a system. For BroadWay, the final pilot system will be evaluated by public safety responder practitioners; those who will use the system in their daily work.

TD2 BroadWay PCP Challenge

<b>Operational Mobility</b>	Public Safety Operations will be enhanced by the availability of pan-European mobile broadband. Operational Mobility refers to the fact that a public safety responder practitioner will be able to carry out their operations wherever they physically are, and with anyone in their communication group wherever they are. All communications shall not be restricted by geopolitical boundaries.
<b>Pre-emption</b>	Pre-emption as define by 3GPP eMLPP
<b>Priority</b>	Priority as defined related to Quality Class Indicators (QCI) in 3GPP specifications
<b>Public safety</b>	Keeping our public safe
<b>Public Safety Responder Practitioner</b>	Practitioners who's daily work devotes his or her time to the practice of providing, administering or promoting justice, civil protection and public protection and disaster relief (PPDR) response services according to the laws, policies and practices of the government entity that they serve. They are mindful of national standards and codes of conduct and often are members of state or national organisations that seek to improve the efficiency, effectiveness and quality of their profession. Volunteers, local/regional/national authorities, military and utility organisations will also act as practitioners.
<b>PEVT</b>	Practitioner Evaluation Team – A team of practitioners from all disciplines who have already expressed their support to take part in evaluation of BroadWay solutions. PEVT is chaired by Bayerisches Rotes Kreuz (Bavarian Red Cross) <a href="https://www.broadway-info.eu/broadway-team/">https://www.broadway-info.eu/broadway-team/</a>
<b>QCI</b>	Quality Class Indicators – 3GPP TS 23.203
<b>QoE</b>	Quality of Experience
<b>QoS</b>	Quality of Service
<b>Robust and ruggedized</b>	When a device is sufficiently dust proof, water proof and shock proof as required by the intended use of the device.
<b>SDK</b>	Software Development Kit
<b>Satellite Network Operator</b>	Providers of Satellite communication services
<b>seamless</b>	Seamless communication in the face of mobile conditions. See service continuity roaming.
<b>Security Architecture Framework</b>	A business-driven, risk and opportunity focused Security Architecture at pan-European solution level that traceably supports the Objectives of the BroadWay common challenge. This should include information assurance architecture and risk management to align and seamlessly integrate security and risk management into BroadWay solutions.

<b>Security Architecture</b>	Security Architecture Framework
<b>Security component</b>	A software component or collection on components that implement security functionality, working to protect the system from security threats.
<b>Security Threat</b>	Any circumstance or event with the potential to adversely impact operations (including mission, functions, image, or reputation), assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.
<b>Service</b>	Mission Critical Service
<b>Service continuity roaming</b>	Automatic roaming shall ensure service continuity. The on-going service (voice, video, data) or on the application in use, the systems and devices will choose the right moment to switch between the networks without loss of information (without interruption) and no action needed from users.
<b>SIS</b>	Schengen Information System
<b>SoC</b>	Statement of Compliance
<b>Solution</b>	A solution to the BroadWay common Challenge
<b>Software component</b>	Software components are parts of a system or an application. Components are a means of breaking the complexity of software into manageable parts. Each component implements a specific function and exposes access to that function through interfaces.
<b>SpiceNet</b>	Standardised PPDR Interoperable Communication Service for Europe as defined in BroadMap D5.2 Section 6 <a href="http://www.broadmap.eu/download-final-deliverable">http://www.broadmap.eu/download-final-deliverable</a>
<b>SpiceNet governance policy</b>	A business level policy that governs the operation of the pan-European broadband for public safety capability. Operational aspects of this policy may be adaptable in real time to accommodate the changing needs of responder practitioners
<b>SpiceNet model</b>	SpiceNet
<b>SpiceNet service</b>	A communication and/or information exchange service offered for use by responder practitioners to assist their operations.
<b>Supplier(s)</b>	When used pre-award of Contracts, Supplier(s) shall have the same meaning as Tenderer(s) as defined in TD1. When used post-award of Contracts, it shall have the same meaning as Contractor(s) as defined in TD1, TD3 and TD4.

<b>Supply Team(s)</b>	When used pre-award of Contracts, Supply Team(s) shall have the same meaning as Tenderer(s) as defined in TD1. When used post-award of Contracts, it shall have the same meaning as Contractor(s) as defined in TD1, TD3 and TD4.
<b>SW</b>	Software
<b>Technical policy</b>	A technical policy that governs the operation of a technical system.
<b>Technical Validation</b>	The functional assessment of a technical component or system that meets a set of requirements. The granularity of requirement (user, system, technical) will be applicable to the purpose of the verification and validation required. For BroadWay, the solutions offered at prototype and Pilot Phase will be subject of technical verification and validation carried out within and between Supply Teams, and reported to the TVC.
<b>Terminal</b>	A UE
<b>TRL</b>	Technology Readiness Level - <a href="https://ec.europa.eu/research/participants/data/ref/h2020/wp/2014_2015/annexes/h2020-wp1415-annex-g-trl_en.pdf">https://ec.europa.eu/research/participants/data/ref/h2020/wp/2014_2015/annexes/h2020-wp1415-annex-g-trl_en.pdf</a>
<b>Trial</b>	The process of trialling and evaluating a new technology from the perspective of a Public Safety Responder Practitioner
<b>TVC – Technical Validation Committee</b>	The parties within the Group of Procurers that will collectively make technical decisions to support the different Phases of the PCP, including the formation of award criteria for the selection of Tenderers in the three (3) Phases of the PCP: (1) Solution Design (2) Solution Prototype (3) Pilot. See TD1 section <b>Error! Reference source not found.</b>
<b>UE</b>	User Equipment 3GPP TR 21.905
<b>Use case</b>	A description of a situation and associated actors who may carry out actions related to the specified situation. This is often specified in terms of high-level scenarios that describe a situation and actors, supported by a more detailed description of activities and interactions with a technological solution that aims to assist in the actors role. Primary actors in BroadWay include, but are not limited to, Responder Practitioners. Actors may procure, govern, configure and use the systems of BroadWay.

## 1 Description of Services to be Procured

### 1.1 Introduction

This document provides Tenderers with a detailed look at the BroadWay PCP. It gives Tenderers an in depth understanding of the PCP Challenge, the different Project Phases, the requirements, the deliverables. Tenderers are informed of the different milestones, the deliverables that will have to be provided during the different Phases and the way they will be scored.

To avoid confusion, this PCP is **not intending to primarily solve national public safety broadband issues**. However, national broadband programmes do share common Objectives to those found here. Each of these national public safety broadband networks and services shall be integrated in the proposed designs and solutions utilising interfaces based on open standards and solutions based on 3GPP standards. They will form pan-European PPDR broadband mobile network.

Many aspects may be transferable and may be of interest to members of our Group of Procurers.

### 1.2 Preparation for the PCP

The BroadWay Project implements a Pre-Commercial Procurement (PCP) with the purpose of realising innovative solutions for the implementation of the 'SpiceNet Reference' architecture to all European countries. This will include, and not be limited to, those important mission critical broadband services, and provision for an application and service eco-system that will make use of these services. Important outcomes are expected here regarding the availability of technology solutions. Technology solutions...

- ...used in each country will be interoperable
- ...will become more technically mature, catalysed by PCP activity
- ...will become lowest cost, due a richer and competitive supplier eco-system
- ...will not be locked into individual suppliers
- ...will provide efficiency gains to and not provide hindrance to PPDR operations

The common challenge of BroadWay is the design, development and testing of the innovation activity to develop technologies to enable a pan-European interoperable broadband mobile system for PPDR, based on national networks and service providers, validated by sustainable testing facilities and practitioner evaluation.

The following 3 subsections describe important precursory activities that have led to the detailed description of the BroadWay Common Challenge which is described in this document.

#### 1.2.1 BroadMap

In preparation of the BroadWay PCP Project, "Phase 0 – Curiosity Driven research" was project BroadMap, from May 2016 to April 2017. In the BroadMap project, there were 15 project partners in 15 countries involved. National and international workshops were organised for gathering requirements from PPDRs. Over 270 organisations (police, ambulance, fire brigades, ministry of defence, coast guard, customs, prisons, utilities– critical Infrastructure) from 18 countries attended workshops. In total there was more than 600+ participants involved.

BroadMap delivered these goals:

- To collect, assess and validate the PPDR's wireless broadband communication existing requirements
- To establish a core set of specifications to fulfil the requirements
- To define transition roadmaps for research and standardisation for future evolution of European interoperable radio communication solutions, within legal procurement constraints

## TD2 BroadWay PCP Challenge

- To prepare the ground for a new eco-system to catalyse new applications, services and processes making use of broadband capabilities for public safety and security
- To utilise the strength of the PPDR community through our partners, their expertise, knowledge, networks and relations with the aim to achieving interoperability across Europe. This importantly includes nuances of societal differences, including different cultures, geography, processes and legal frameworks

### 1.2.2 SpiceNet

Public safety services shall address a series of new challenges such as disasters, crime and terrorism which are not confined to geopolitical borders. Sharing information between national and international agencies is critical. Also, technology capable of sending and receiving large amounts of data can help emergency and security services to do their work more effectively and safely.

The forerunner of the BroadWay Project is project BroadMap. BroadMap was funded under topic DRS-18-2015 from May 2016 to April 2017.

A major aspect carried forward from BroadMap to BroadWay is the **SpiceNet Reference Architecture**. The Standardised PPDR Interoperable Communication Service for Europe (SpiceNet). The SpiceNet model proposes a reference architecture for harmonised pan-European PPDR mission critical broadband services which contains three layers:

#### 1) Harmonisation

- a. Organisational schemes,
- b. Tuning ranges
- c. Standardised commercial solutions

#### 2) Interoperability and governance

- a. Standardised Mission Critical Solutions for public safety,
- b. SpiceNet governance
- c. Standardised PPDR Interoperable Communication for Europe (SpiceNet)

#### 3) Networks and users

- a. PPDR Networks,
- b. PPDR Users

#### Organisational schemes:

All member states are in different phases of the transition towards MC PPDR broadband services. Some member states have developed strategies, some have already started transition (e.g. UK) and some member states are still rolling out narrow band TETRA networks. Thus there is no common organisational scheme which can be used as a general solution. Organisational schemes can vary from dedicated networks and services to full MVNO services and to all combinations between hybrid and OSP (Outsourced Service Provider).

#### Harmonised tuning ranges:

All networks are based on standardised frequency bands. Depending on national regulations and service models, PPDR can use any combination of (450 MHz, 700 MHz, 800 MHz, 900 MHz, 1800 MHz, 2100 MHz and 2600 MHz) tuning ranges. Frequencies from standardised bands are also used for direct mode operation (proximity services) when networks are not available. During the transition period from legacy systems, narrow band digital PPDR radio networks can also be used.

Harmonised tuning ranges allow commercial devices to operate globally with all tuning ranges used by commercial operators. Chipsets and devices are manufactured based on 3GPP standards. This means that PPDR users can use SpiceNet services in any commercial network adopted for SpiceNet services.

**Standardised commercial solutions:**

All commercial mobile broadband networks, devices and some of the applications are based on 3GPP standards. This allows PPDR organisations to use or develop systems based on commercial off the shelf (COTS) solutions. COTS products are commercially available. By using networks based on 3GPP standards there will be a wide range of possibilities for PPDR users to benefit from all commercial innovations. However, PPDR specific needs of reliability, coverage and security must be guaranteed. Through standardisation, for example international roaming has already been enabled for more than 20 years.

The interoperability layer has three components as follows:

**Standardised MC PPDR solutions:**

MC broadband services are now part of the commercial 3GPP standards, although it is important to note that international roaming does not equate to PPDR cross-border interoperability. Current ongoing work of 3GPP enables a set of mission critical features and services. These PPDR-specific services form the foundation to enable versatile and interoperable solutions for PPDR organisations across the EU.

**SpiceNet governance:**

A pan-European governance function is needed to allow countries and agencies to use SpiceNet services. This function needs to be defined and appointed to some legal entity or organisation at the EU level. In addition, each SpiceNet user organisation must have a SpiceNet function, which consists of administration, finance, technology and security and maintenance functions.

A global agreement is needed for pan-European organisations to confirm governance above national legislations and in conformity with the current common regulations at the EU level.

**Standardised PPDR Interoperable Communication for Europe (SpiceNet):**

Due to cross-border interoperability and pan-European PPDR interoperability needs, a set of standardised, basic PPDR services must be defined. To establish these activities, and to maintain cross-border interoperability and preparedness, bi- tri- or multilateral cross-border agreements are also necessary.

Pan-European cooperation and interoperability is based on harmonised 3GPP tuning ranges and standardised infrastructure. Regardless of their location, PPDR users must be able to communicate based on agreements with other users and organisations in different countries. SpiceNet can provide MC services like for example MC PTT, MC Data, MC Video, status messaging, AVL, alerting, SDS messaging.

No matter the type of national organisation scheme employed, communication with any country and PPDR authority must be possible when the SpiceNet services are developed and established.

Validation and testing for SpiceNet services is mandatory in order to maintain interoperability in multi-vendor environment.

SpiceNet services are based on a distributed model where each country has their own service HUB (SpiceNet HUB), which includes business logic for all interoperability agreements related to each country. In addition to SpiceNet governance also bi-, tri- and multi-lateral interoperability functions shall be provided.

In addition, each European agency (e.g. Frontex, Europol, civil protection mechanism) has their own operational solutions.

**PPDR networks:**

The integration of SpiceNet services will be established by national network operators and service providers. Depending on organisational schemes, there are variations for implementing the services. More or less they are based on virtualized networks. Virtualization can have variations depending on the level of integration.

**PPDR users:**

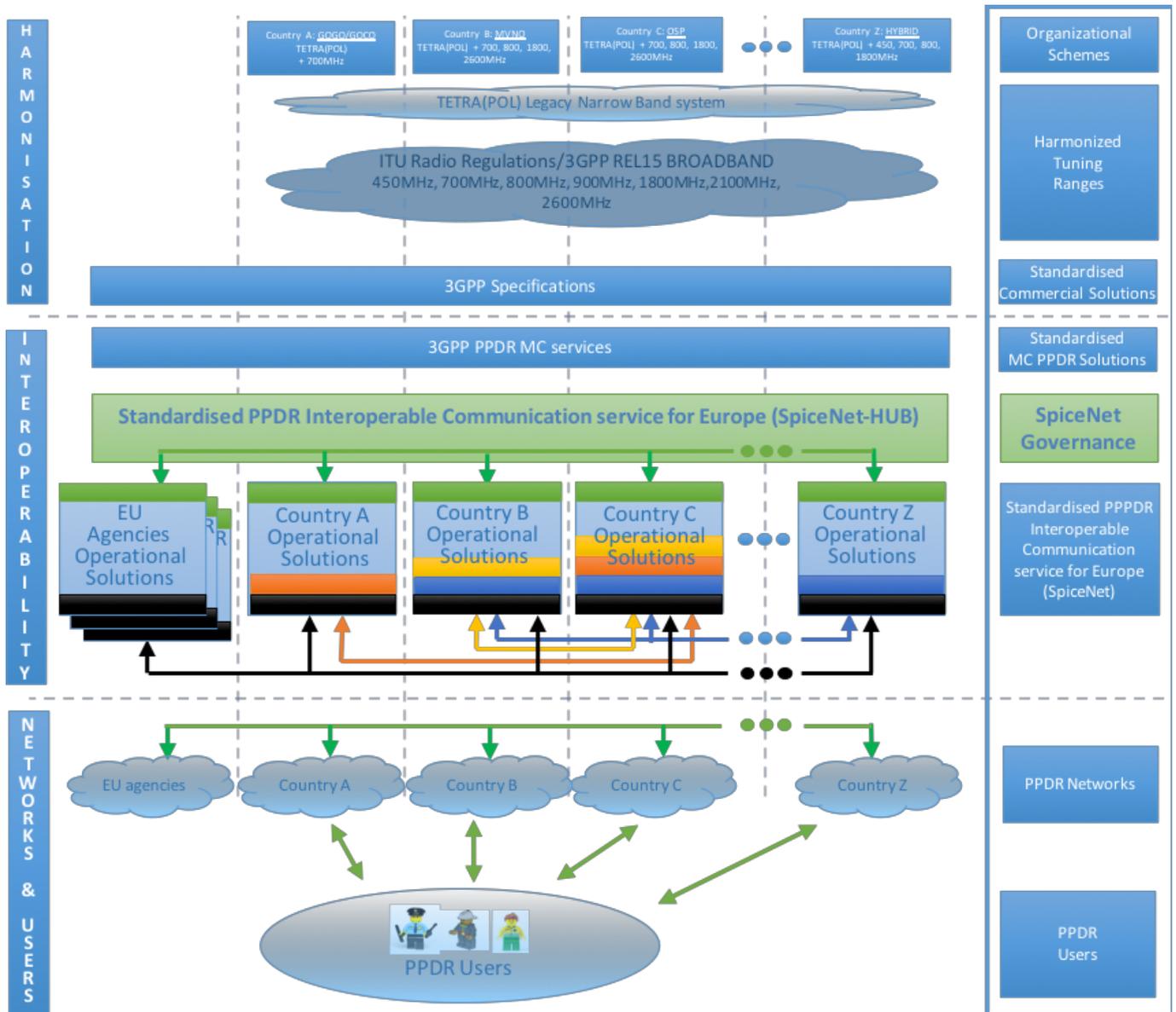
## TD2 BroadWay PCP Challenge

Depending on agreed user specified SpiceNet services, PPDR end users will be able to communicate, using their devices, with PPDR users within their own country and across borders, assuming local PPDR MC broadband service availability.

Next generation PPDR MC broadband services allow new possibilities for all authorities to develop new ways of European cooperation on all levels. This means benefiting from new technology innovations for all areas of PPDR operations to improve efficiency and situational awareness, e.g. augmented reality, sensors, video, robotics, smart clothing, etc. The new technology will offer opportunities to use real time translation of spoken language (SpiceNet translator).

Non-technical governance and operational issues (see SpiceNet governance above) will be solved together with neighbouring countries and other organisations to enable cooperation.

# TD2 BroadWay PCP Challenge



## Key principles of SpiceNet

The SpiceNet model has been developed based on the following key principles:

1. The SpiceNet service allows PPDR users to use pan-European interoperability, cross country interoperability and domestic inter-agency interoperability, based on the availability of mission critical broadband networks.
2. Each country uses their own national roadmap to implement the next generation mission critical broadband services.
3. Each country uses their individual schedule to ramp down legacy PPDR radio communication systems.

## TD2 BroadWay PCP Challenge

4. There is a broad mixture of organisational schemes across countries.
5. Harmonised tuning ranges based on 3GPP frequency bands exist for dedicated and commercial spectrum. According to a WRC15 decision, band 68 can also be used if adopted by the national regulator.
6. All networks, devices and most of the features are based on 3GPP standards.
7. Supported services may vary across countries and for certain network operators based on the system supplier and their supported features and releases.
8. International roaming for almost all commercial services has been available more than 20 years. It is important to note that cross-border interoperability for PPDR services is not synonym with international roaming.
9. A set of common MC services interoperability (SpiceNet services) is necessary to ensure pan-European PPDR cooperation based on 3GPP mission critical specifications.
10. Cross-border and pan-European interoperability can be implemented by mutual bi-lateral and multilateral agreements between countries, PPDR organisations and pan-European organisations (e.g. Frontex, Europol and EGTC23). The SpiceNet model can be used as reference architecture to provide the interoperability.

### 1.2.3 Open Market Consultation

The objective of the Open Market Consultation (OMC) was to collect the information regarding the state of art, keeping in mind that BroadWay has to procure innovations to develop and demonstrate TRL8 technologies that will enable a pan-European interoperable broadband mobile system for PPDRs.

The OMC encompassed a questionnaire, 2 briefing webinars (20<sup>th</sup> July and 9<sup>th</sup> August) and a Briefing, Consultation and Networking event held in Brussels on 13th September 2018. Combined, over 80 people participated in the various events and 27 filled questionnaires were received from potential Suppliers.

This newly formed community provides a good basis for the promotion of the PCP and has given potential Suppliers a strong understanding of the intentions and needs of the Group of Procurers.

The full OMC report is available on the BroadWay website: [www.broadway-info.eu](http://www.broadway-info.eu).

The results of the OMC and BroadMap project formed the basis of this PCP and related Tender Documents.

## 2 The BroadWay Common Challenge

Solutions procured have to be within the SpiceNet reference architecture, collectively usable by all procuring partners for the purpose to enable European interoperable operation, neutral and not biased to individual geo-political, technological or supplier preferences, free from dependencies associated with on background IPR and original (does not already exist).

Test and Validation shall be based upon criteria defined at an appropriate level to assure European Interoperable operation. This shall be carried out independently and with impartiality and should not replace existing test and validation activities. It should be sustainable beyond the lifetime of the BroadWay Project to maintain European interoperable mobile broadband communications systems for public safety.

**The requirements are defined in Objectives on a high level to maximize the creativity and to allow for innovation over the course of the process.**

The common Challenge is stated as: **design, development and testing of the innovation activity to develop technologies to enable a pan-European interoperable broadband mobile system for PPDR, validated by sustainable testing facilities and practitioner evaluation.**

## 2.1 Opening statement

The BroadWay Project intends to procure innovative designs and common standard solutions to implement innovative interoperable public safety broadband services, system of systems (interconnection between future national public safety broadband mobile networks). This will be tested and evaluated during the prototyping and pilot activities. The pilot will consist of several different operational scenarios across Europe, between bordering, but also non-bordering countries. A single pan-European pilot will be implemented by the preferred Tenderer(s) as a service and will operate as a common, transparent, wide area broadband mobile network with mutual interconnection between all operational scenarios areas in order to:

- facilitate mobile communication between users in different operational areas of a PPDR Organisation
- facilitate mobile communication between different users of different PPDR Organisations
- facilitate mobile communication between different users of different PPDR Organisations independent of their geographical location.

The service shall accommodate user communication groups and be flexible to adapt to required operational and organisational changes within each operational scenario area. The broadband service shall be delivered, at a minimum, using two different deployment options i.e. organisation schemes<sup>1</sup>.

A maximum of 5 Supply Teams will be invited to agree Framework Agreements, together with an initial Specific Contract to produce designs that will be required to provide an architectural, system of systems view. These designs will aim to achieve or exceed our Objectives. Designs will provide a realistic viewpoint of the scope of achievable functional capabilities, and their expected performance criteria. Development will continue with 2 subsequent Phases, developing, testing and evaluating prototypes and pilots.

A maximum of 3 Supply Teams producing the best designs will be invited to produce solution prototypes and to test them both:

- 1) To technically assess performance of the solution, using innovative, independent and impartial testing,
- 2) by 'plugging' together with each other to assure interoperability on a technical level

To reach a TRL8 level pilot, the TVC will select a maximum of two (of 3) Supply Teams producing the best prototypes to separately develop their instantiations of the pilot and then working together to provide a single final Pilot.

The Pilot evaluation will be completed on two levels:

- 1) Technical validation – further assess improved performance,
- 2) Practitioner evaluation – to allow the system to be trailed and evaluated by responder practitioners

The technical validation will provide independent and impartial testing to validate different functions/features that support our Objectives: availability, security, governance tools, operational mobility and applications, etc. Technical verification and validation will be carried out by independent and impartial Subcontractors of Suppliers and results will be reported to the TVC.

Responder Practitioners will evaluate operational effectiveness employing a number of case scenarios trialling the technology in simulated response to cross border incidents and events.

Satisfaction of the BroadWay TVC will be based on technical test results and the opinions gathered during the practitioner evaluation. One or both Suppliers in the Pilot Phase will be awarded the SpiceNet certification. This will be a mark of satisfaction that the pilot solutions will be suitable for procurement into live production use following an additional procurement programme which is expected to follow after this PCP has concluded.

---

<sup>1</sup> See BroadMap D4.1 section 10; <http://www.broadmap.eu/download-final-deliverable>

## TD2 BroadWay PCP Challenge

For a better understanding of the following BroadWay Objectives, the terminology is explained in the Glossary at the start of this document.

## 2.2 PCP Challenge - Objectives list

This section describes each Objective, which comprises a number of Sub-objectives. The word ‘shall’ is written throughout, in the context of the finally procured live and operational BroadNet system.

In the context of the BroadWay PCP Phases, the Design Phase ‘shall’ address each of the Sub-objectives considering the finally procured BroadNet system. Prototype and Pilot Phases shall strive to achieve those Objectives leaving only minor developmental enhancements required between the Pilot Phase and final procurement of the BroadNet system. The competitive nature of the PCP will reward Supply Teams that achieve closest to the final live system objectives, and expected targets and KPI's, at the end of the Prototype Phase.

All Tenders shall include sufficient information to describe how each Objective and Sub-objective will be achieved. The Scoring Model for the Award Criteria in Appendix 5 will be applied. Some Sub-objectives are identified as – ‘nice to have’. These will not be formally assessed individually as Sub-objectives of the related Objective, but shall have an impact in selecting a successful Tenderer from an unsuccessful Tenderer in a situation where two Tenderers receive the same scores for their Tenders. ‘Nice to have’ Sub-objectives are specified in the context of the BroadWay PCP activity. All Sub-objectives shall be required for the BroadNet system.

KPI's shall be specified in the Tender and at the end of each Phase to describe each of the KPI's for each Objective:

- In the Tender – KPIs that the design should specify to achieve the final live system
- End of Design Phase – KPIs to be achieved for the final live system
- End of Solution Prototype Phase – KPIs that the solution prototype has achieved
- End of Pilot Phase – KPIs that the pilot has achieved

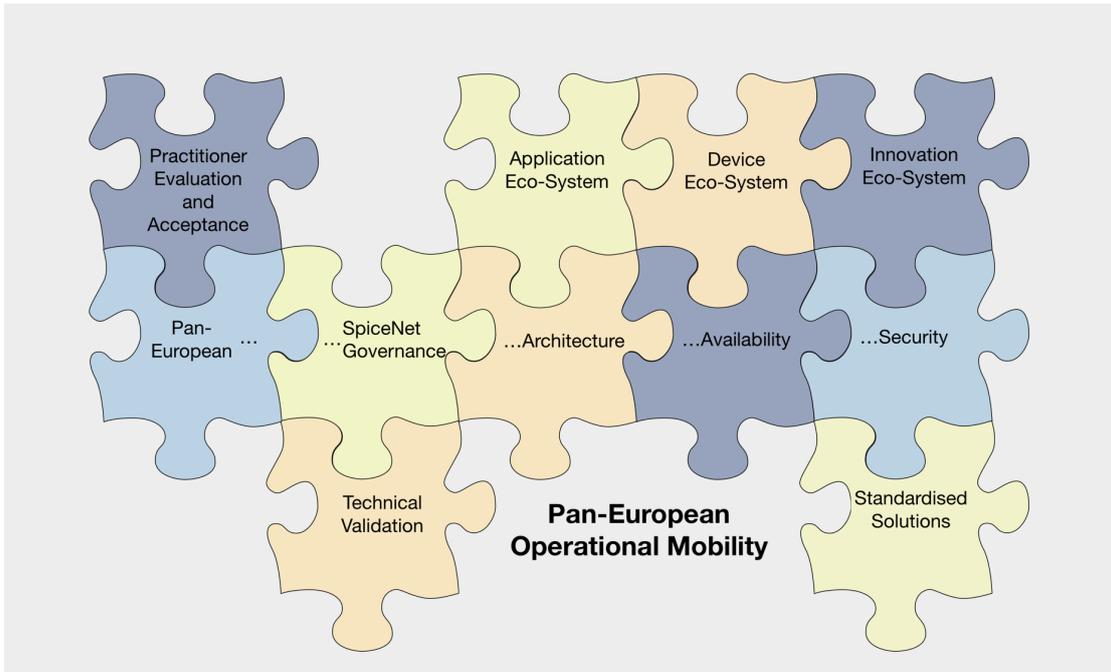
Where it is not appropriate to provide an objective KPI, then a statement should be made that the Objective will be fulfilled and, if appropriate, how.

The BroadWay TVC shall decide the final KPIs for BroadNet, to determine SpiceNet conformance criteria. This determination will be dialogue between BroadWay TVC and Suppliers based on provided designs and solutions.

BroadWay has the following 11 Objectives that are described in detail in the remainder of this section:

Pan-European...	Standardised solutions
... Architecture	Application Eco-system
... Availability	Device Eco-system
... Security	Innovation Eco-system
... SpiceNet Governance	Technical validation
... Operational mobility	Practitioner evaluation

TD2 BroadWay PCP Challenge



## 2.2.1 Objective 1: Pan-European Architecture

The target architecture for solution designs, prototypes and pilots aims to be based on a pan-European architecture that provides seamless interoperable mission critical broadband services to PPDR users across Europe and facilitates pan-European operational mobility, cross country operational mobility and domestic inter-agency operational mobility. The architecture shall be based on the SpiceNet (standardised PPDR Interoperable Communication for Europe) model and provide a set of common mission critical services, based on 3GPP mission critical specifications, to enable pan-European PPDR cooperation.

The SpiceNet model proposes a reference architecture for harmonised pan-European PPDR mission critical broadband services which contains three layers.

These three layers are:

- 1) Harmonisation layer,
- 2) Interoperability and governance layer and
- 3) Networks and users layer

The Tenderer confirms to have understood the SpiceNet model which is illustrated in this document, summarised here and in more detail in section 1.2.2.

The proposed designs and solutions shall take into account all principles and layers described in the SpiceNet model. All of these elements shall be represented and identified in the proposed solution designs, prototypes and pilots.

### 1) Harmonisation layer

The harmonisation layer has three components:

- a. Organisational schemes,

The proposed designs and solutions shall facilitate various organisational schemes covering various ownership, operation, development and deployment models of a whole solution or its components (ownership/operation/development - government or company, deployment - dedicated network/MVNO model/OSP/Hybrid/...) on both pan-European and national level.

Each country can have a different implementation of their mission critical broadband networks. Each of these networks and services shall be integrated in the proposed designs and solutions utilising interfaces based on open standards and solutions based on 3GPP standards.

- b. Harmonised tuning ranges

The proposed designs and solutions shall operate in harmonised tuning ranges based on 3GPP frequency bands to allow devices to operate globally with all tuning ranges used by national broadband PPDR mobile networks. This means that PPDR users can use SpiceNet services in any national broadband PPDR mobile network adopted for SpiceNet services, without restrictions.

- c. Standardised commercial solutions

The proposed designs and solutions shall use 3GPP standards for mobile broadband networks, devices and some of the applications. These shall allow PPDR organisations to use or develop mission critical broadband solutions based on commercial off the shelf (COTS) products and benefit from all commercial innovations and economies of scale.

### 2) Interoperability and governance layer

The interoperability and governance layer has three components: Standardised mission critical broadband solutions

- a. The proposed designs and solutions shall use 3GPP standards for mobile broadband networks, devices and some of the applications.
- b. SpiceNet governance

## TD2 BroadWay PCP Challenge

Solutions finally procured in a live system by the BroadNet programme shall be governed by the organisational arrangement formed initially by the BroadWay TVC.

### c. SpiceNet agreements

Pan-European cooperation and operational mobility is based on harmonised 3GPP tuning ranges and standardised network infrastructure. Bi/multi-lateral agreements shall be necessary between e.g. national broadband PPDR mobile network operators in different European countries to allow PPDR users, regardless of their location, to be able to communicate based on such agreements with other users in different European countries utilising SpiceNet services.

## 3) Networks and users layer

SpiceNet services shall be integrated by the national broadband PPDR mobile operators.

PPDR users shall be able to communicate, using their devices, with other PPDR users within their own country and in other countries, assuming the availability of the national broadband PPDR mobile network adopted for the SpiceNet services.

### 2.2.1.1 PEAR Pan-European Architecture Sub-objectives

**(All Tenders shall include sufficient information to describe how they will achieve each Sub-objective)**

#### **PEAR1 Involvement of Radio access provision and consumer/commercial operation:**

Every Tenderer shall include at least 1 mobile and/or satellite network operator in order to include appropriate consideration of different organisational schemes and operating models. (stand-alone bid, lead/partner in a Consortium or Subcontractor to a consortium).

#### **PEAR2 Organisational schemes:**

The proposed designs and solutions shall facilitate various organisational schemes covering various ownership, operation, development and deployment models of a whole solution or its components (ownership/operation/development - government or company, deployment - dedicated network/MVNO model/OSP/Hybrid/...) on both pan-European and national level.

The broadband service shall be delivered, at a minimum, using two different deployment options i.e. organisation schemes. Please refer BroadMap D4.1 Section 10, for details.

Each country can have a different implementation of their national public safety broadband networks. Each of these networks and services shall be integrated in the proposed designs and solutions utilising interfaces based on open standards and solutions based on 3GPP standards.

#### **PEAR3 Harmonised tuning ranges:**

The proposed designs and solutions shall operate in harmonised tuning ranges based on 3GPP frequency bands to allow devices to operate globally with all tuning ranges used by national broadband PPDR mobile networks. This means that PPDR users can use SpiceNet services in any national broadband PPDR mobile network adopted for SpiceNet services without restrictions.

#### **PEAR4 Standardised commercial solutions:**

The proposed designs and solutions shall use 3GPP standards for mobile broadband networks, devices and some of the applications. These shall allow PPDR organisations to use or develop mission critical broadband solutions based on commercial off the shelf (COTS) products and benefit from all commercial innovations and economies of scale.

#### **PEAR5 Standardised mission critical broadband solutions**

Mission critical broadband services are part of the commercial 3GPP standards which enable a set of mission critical features and services for operational mobility.

## TD2 BroadWay PCP Challenge

### **PEAr6 PPDR networks**

National public safety broadband mobile networks shall form pan-European PPDR broadband network integrating SpiceNet services.

### **PEAr7 PPDR users**

PPDR users shall be able to communicate, using their devices, with other PPDR users within their own country and across borders, assuming the availability of the national broadband PPDR mobile network adopted for the SpiceNet services.

## **2.2.2 Objective 2: Pan-European Availability**

### **2.2.2.1 PEAv Pan-European Availability Sub-objectives**

**(All Tenders shall include sufficient information to describe how they will achieve each Sub-objective)**

The main goal of availability is to ensure that mission critical services are made available to authorised parties across different authorities and different users from different broadband PPDR networks in order to access and share the information as necessary. The critical nature of these services requires that the underpinning networking infrastructure shall be designed, delivered and maintained in a high availability and resilient manner.

#### **PEAv1 Harmonised Availability**

The pan-European SpiceNet services shall be designed for continuous operation (99,999% availability) enabling information services with the same level of availability. The Pan-European solution shall be implemented using RAS (reliability, (high) availability, serviceability) principles and as a fault-tolerant system.

#### **PEAv2 Harmonised Quality of Service**

The PPDR QoS and standardised access class mechanisms shall be available in each country with the same service level as the one available for national users. The provided solution shall be as transparent as possible but agreements between MNOs shall be required for the priority, pre-emption and access class barring mechanism.

#### **PEAv3 Capacity**

The capacity of the pan-European broadband PPDR network and SpiceNet services shall be sufficient for all the mission critical applications as used by the PPDR users. The capacity of the system shall be defined and sufficient to deal with daily use, several simultaneous major crises or scale/grow rapidly as usage requires.

#### **PEAv4 Seamless Operation**

Seamless SpiceNet service continuity across Europe shall be provided by the pan-European broadband PPDR network.

#### **PEAv5 Assuring Quality of Experience**

SpiceNet services availability, quality and performance shall be continuously measured and regularly evaluated and reported. Concept for Quality of user experience (QoE) shall be integral part of the pan-European interoperability solution. Proof and assurance monitoring of the BroadNet system, network and service availability and quality shall be decided by the BroadWay TVC (SpiceNet conformance criteria).

#### **PEAv6 Air Ground Air**

The design and solution shall be able to provide an AGA service. Devices installed in airborne units shall be able to communicate with an agency on the ground guaranteeing seamless continuity at various altitudes with no loss of service and security on the air interface.

### **2.2.2.2 PEAv-Pan-European Availability Sub-objectives (Nice to Have)**

#### **PEAv7 National Coverage**

In area where there is no coverage (radio service) solutions shall enable additional means to provide localised or wider geographical coverage.

#### **PEAv8 Disconnected network**

In circumstances where base stations are isolated from the rest of the network, users connected to those base stations are still able to communicate with each other.

### **2.2.3 Objective 3: Pan-European Security**

When it comes to information that can be created, exchanged and stored on the pan-European PPDR broadband network, security is one of the most important aspects to address due to physical and cyber threats for the PPDR communications. Users must have trust that the information they transmit or receive has been exchanged in a confidential manner and that the integrity of that information has not been compromised. The services required will, amongst other things, be used for sensitive operations in the emergency and security areas. Consequently, security is paramount.

Each country will have its own solutions to accommodate national security requirements. It is not within the scope of BroadWay to be depend upon national requirements at this stage. However, Suppliers should anticipate that national requirements that develop during the BroadWay programme may have an impact on the final procurement of the BroadNet system.

End-to-end (E2E) security shall be provided across the complete pan-European interoperability solution – national public safety broadband mobile networks adapted for SpiceNet services, interconnection of the networks, underlying transport networks, OSS and BSS applications, devices, OS, SW, HW, etc.

This E2E security shall be based on public, non-secret algorithms.

#### **2.2.3.1 PESAr-Pan-European Security Architecture Sub-objectives**

**(All Tenders shall include sufficient information to describe how they will achieve each Sub-objective)**

##### **2.2.3.1.1 PESAr1 Fundamental Security**

For all information on pan-European broadband PPDR network providing SpiceNet services, following shall ensure:

- Information confidentiality- protecting the information from disclosure to unauthorised parties
- Information integrity- protecting information from being modified by unauthorised parties
- Information availability- ensuring that authorised parties are able to access the information when needed

##### **PESAr2 Vulnerability**

From an operational and technical point of view, the pan-European broadband PPDR network shall not be vulnerable to known and future threats.

##### **PESAr3 Standardised and Certification encryption**

Pan-European broadband PPDR network shall use standardised and certified encryption algorithms.

##### **PESAr4 End 2 End Encryption**

Common end-to-end encryption is mandatory to secure all intra and inter agency communications within own country and cross border irrespective of geographical situation. For the E2E security only public, open, non-secret algorithms and implementations shall be used. Key management responsibility is split between the pan-European interoperability solution and the respective national authority responsible for security.

##### **PESAr5 User and Control Plane**

Security of the user plane information (voice, data, and video) and control plane information (mobile network signalling) shall contain multiple layers reflecting 3GPP standards and business best practices.

##### **PESAr6 Device/User Authentication**

Device/user authentication and authorisation is mandatory in order to register a Device/user with the home/visited network in a secure manner and provide SpiceNet services.

##### **PESAr7 Mutual Authentication**

Mutual authentication shall be done using strong authentication algorithms with single sign-on capability providing easy and efficient use of device and applications by the PPDR users.

TD2 BroadWay PCP Challenge

### **PESAr8 Rights Management**

Global rights management system (for example: user management, group management...) shall cover all the functionalities implemented by the SpiceNet architecture.

### **PESAr9 Over the Air Re-keying**

Over-the-Air re-keying shall be supported.

### **PESAr10 Enterprise Mobility Management**

The solution shall support Enterprise Mobility Management (EMM). EMM is a comprehensive method of remotely managing devices, to secure company PPDR owned applications and data on PPDR devices. The EMM solution shall be primarily focused on: Mobile device management (MDM), Mobile application management (MAM), Mobile content management (MCM), Mobile identity management (MIM).

### **PESAr11 Integrity**

Integrity of information and applications shall be certified and verified according to the SpiceNet governance.

### **PESAr12 Security Policies**

Application and services shall conform to the security policies and requirements imposed by the SpiceNet governance.

### **PESAr13 Software Quality Assurance**

High software quality assurance shall be achieved to EAL4+ for all security components of the final procured live BroadNet system, reviewed by at least two national Certificate Authorising Members of Common Criteria, from EU member states. Provide a list of all software components indicating EAL target level. Where level below EAL4+ will be the target for non-security components, it must be clearly justified. Reference to Common Criteria <https://www.commoncriteriaportal.org>

### **PESAr14 Service Assurance**

High level assurance of all BroadWay services shall be conveyed to all PPDR network operators and practitioners.

### **PESAr15 Harmonised Security Assurance**

SpiceNet security assurance shall be maintained in visited networks when devices register to any national public safety broadband mobile network according to SpiceNet Governance. A process shall be available to assure, document and provide security and associated software assurance mechanisms for each of the different aspects and the entire BroadWay solution (with reference to PESAr13)

## **2.2.3.2 PESAr-Pan-European Security Architecture Sub-objectives (Nice to Have)**

### **PESAr16 EMM innovations**

The EMM solution shall be able to interwork/integrate with existing implemented solutions in the PPDR organisations.

The EMM solution shall be using the most advanced encryption and identity tools that complies with PPDR security policies.

The EMM solution shall support on-premise solutions.

## **2.2.4 Objective 4: Pan-European SpiceNet Governance**

### **2.2.4.1 PESg-Pan-European SpiceNet Governance Sub-objectives**

**(All Tenders shall include sufficient information to describe how they will achieve each sub-objective)**

The governance of the pan-European operational mobility solution (result of the BroadWay and BroadNet procuring) shall include a full set of operational, technical and tactical capabilities. It shall also include sustainable testing capabilities.

SpiceNet services are based on a distributed model where each country has their own service which includes business logic and technical policies that fulfil the SpiceNet governance policy for all operational mobility agreements related to each country.

A necessary precondition for this is: bi-lateral and multilateral agreements between countries, PPDR organisations, pan-European practitioner organisations (e.g. Frontex, Europol), and national public safety broadband mobile network operator.

The governance shall develop international communication groups for each agency.

Legal framework for SpiceNet governance shall include:

- Foundation agreement (Initial Agreements between BroadWay group of procurers and other national public safety broadband mobile networks, with the intent to integrate with, provide, and consume BroadNet services)
- Existing mobile roaming agreements need to be extended in future to support the challenge of pan-European PPDR broadband network.
- Agreements between foundation and pan-European practitioner organisations - will be done by the BroadWay team

International agreements shall be legally sufficient and shall be elaborated to enable operational mobility abroad and/or between countries. In collaboration between SpiceNet governance, BroadWay team, Suppliers and all other national public safety operators involved in BroadNet, operational mobility of PPDR organisations of cross border countries will be achieved.

#### **PESg1 Legal framework for SpiceNet governance**

Existing roaming mobile agreements shall be extended to support the challenge of pan-European PPDR broadband network. These agreements shall take in to account national regulations issues that may hinder some agreement possibilities between MNOs in some countries. Suppliers shall describe indications how to achieve this, defining any constraints, barriers and risks.

#### **PESg2 System management**

System management shall facilitate correct and efficient operation of the pan-European broadband solution providing operational mobility.

#### **PESg3 Authorised Administration**

Authorised administrators shall be able to create, control, and configure different users and user groups on pan-European level. Creation of different levels of users shall be possible. (e.g. Only limited access, or full administration rights) shall be possible to create.

#### **PESg4 Management technology**

The BroadWay solution shall provide a technical and tactical management mechanism able to dynamically, and in real-time, change user and application priorities to address the changing needs of the PPDR users when operating on pan-European circumstances. All connected national public safety broadband mobile networks shall adhere to this management mechanism.

## TD2 BroadWay PCP Challenge

### **PESg5 Monitoring**

The monitoring of the BroadWay solution shall log all activities of the involved users and be accessible only by authorised users.

### **PESg6 Provisioning**

Provisioning shall be governed by a limited number of authorised users according to a SpiceNet governance policy.

### **PESg7 Billing**

Suppliers shall describe solutions for billing towards the different authorities as a function of services, traffic used in the BroadNet network, etc.

## **2.2.5 Objective 5: Pan-European Operational Mobility**

### **2.2.5.1 PEOm-Pan-European Operational mobility Sub-objectives**

**(All Tenders shall include sufficient information to describe how they will achieve each Sub-objective)**

The pan-European broadband PPDR network and SpiceNet services shall create a common area of operational mobility in order to allow PPDR organisations of different types, from different jurisdictions and from different countries across Europe to work jointly and efficiently. A network infrastructure through which all PPDR organisations, down to individual practitioner level, shall be able to use their own devices to communicate securely among them, to share applications and information, resulting in greater efficiency, both in day-to-day operations and during major events and emergencies.

Pan-European Operational mobility is a key point for all our objectives. Everything has to be interoperable and based on Standardised solutions: Pan-European Architecture, Pan-European Availability, Pan-European Security Architecture, Pan-European SpiceNet governance, Application Eco-system, Device Eco-system and Innovation eco-system.

#### **PEOm1 Seamless communication groups spanning networks and authorities**

The designs and solutions shall ensure availability and capability to operate using common communication groups across different authorities and different users from different networks, in order to facilitate seamless operation to accommodate both cross border operations and country specific operations.

#### **PEOm2 Seamless Access to information sources**

The designs and solutions shall ensure availability and capability to access different information sources across different authorities and different information resources, in order to facilitate seamless operation to accommodate both cross border operations and country specific operations.

#### **PEOm3 Seamless Access to applications and databases**

The designs and solutions shall ensure availability and capability to allow access to any application or database in a full compliance with the rights granted to each user by national law and international agreements.

#### **PEOm4 Harmonised Operational mobility - Same as home**

PPDR users shall be able to register within all national public safety broadband mobile networks that are forming the pan-European broadband PPDR network and use the SpiceNet services seamlessly. The pan-European operational mobility solution shall provide capabilities, functionalities and parameters like in the home network in a harmonised manner.

### **2.2.5.2 PEOm-Pan-European Operational mobility Sub-objectives (Nice to Have)**

#### **PEOm5 Forced network selection**

Implementation of a process to force a device to select the best network at the given location depending of the availability of the network for the SpiceNet services without the intervention from the user.

## **2.2.6 Objective 6: Standardised Solutions**

### **2.2.6.1 Ss-Standardised solutions Sub-objectives**

**(All Tenders shall include sufficient information to describe how they will achieve each Sub-objective)**

Solutions shall follow global or European standards on all levels of SpiceNet architecture. Proprietary or non-standard solutions can not be part of the standardised solutions.

#### **Ss1 Use of Open Common Standards**

Pan-European broadband PPDR network, devices and services shall be based on open common standards (e.g. 3GPP, ETSI, IETF, IEEE, OMA). Open standards shall be made in a transparent and open process by organisations who's membership is open to all and who's standards are available to all.

#### **Ss2 3GPP Mission Critical Services**

3GPP standardised MCX services shall be offered. MCX 3GPP release 15 is considered as a recommendation. All other 3GPP components and services shall be interoperable to support MCX services.

#### **Ss3 Release compatibility and upgradability**

All solutions shall be both backwards compatible and upgradable to future releases of standards.

#### **Ss4 Radio Equipment Directive**

Solutions shall be compliant to RED 2014/53/EU.

#### **Ss5 3<sup>rd</sup> party Applications, Equipment and Users**

Communication protocols and interfaces based on open standards and 3GPP based solutions shall be used and shall allow interoperation with 3rd party applications (e.g. Control room application), equipment and users.

#### **Ss6 Statement of Compliance**

All solutions shall be provided with the statement of compliance (SoC) to relevant standard(s).

#### **Ss7 Standardisation roadmap**

All solutions shall provide a roadmap for at least three years and shall be revised on yearly basis.

#### **Ss8 Locating Users**

All solutions shall use standardised protocol for determination of location of PPDR users (indoor/outdoor).

#### **Ss9 Security architecture framework**

Standardised Security architecture framework shall be offered (e.g. data and system protection, visibility of technologies attached to the enterprise network) as well as defined principles used to develop cyber secure system designs and solutions.

#### **Ss10 Standardised technical policies supporting information exchange**

Implementation of policies and standards enhanced and developed to facilitate cross border exchanges of information in a secure, efficient and harmonised manner.

#### **Ss11 Standardisation contribution obligation**

Where solution is not possible within the existing standards, standardisation activity shall be initiated to allow for future procurement of the final solution within the expected timeframe for BroadNet procurement.

#### **Ss12 Informational interoperability**

Applications shall use object formats available from standards to develop common information exchange model.

## **2.2.7 Objective 7: Application Eco-system**

### **2.2.7.1 AEs - Application Eco-system Sub-objectives**

**(All Tenders shall include sufficient information to describe how they will achieve each Sub-objective)**

Innovative Services and Applications shall be developed to take advantage of pan-European broadband PPDR network for different types of PPDR organisations.

Improved information exchange on the field will help PPDR practitioners to improve situational awareness through use of rich and immersive media for more efficient response operations. Applications can take advantage of new techniques for information interaction including Advanced Augmented Reality, Internet of Public Safety Things, Geospatial applications, access to necessary databases, voice, data and video contact with user group members.

#### **AEs1 Open APIs**

The technology used in service provisioning shall provide open Application Programming Interfaces (APIs) and/or equivalent forms of intercommunication, and data formats for the technology used in the service provision. These APIs, etc. and data formats shall be available without delay, without licensing or confidentiality constraints, and royalty-free, to nominated Suppliers.

#### **AEs2 MCX service APIs and extension**

The designs and solutions of the pan-European broadband PPDR network shall provide e.g. MCX services standardised in 3GPP while at the same time they shall provide new and innovative services, increasing operational efficiency, that are associated mostly with the broadband capabilities of the 3GPP standardised technologies

#### **AEs3 Platform compatibility**

Applications shall be cross platform compatible.

#### **AEs4 Standardised codecs**

MCPTT and MC video applications shall use using standardised CODECs, allowing interface with standardised applications and existing national system.

#### **AEs5 Audio and Video quality**

The quality level for audio and video shall be assessed by e.g. PESQ and PEVQ family of standards and results shall be principally modelled using mean opinion scores (MOS) and shall reach at least 4.

#### **AEs6 Open Application Development Platform**

An Open Application Development Platform shall be established to support development of SpiceNet Application Ecosystem, which shall allow applications to be built following common standards and open interfaces (APIs) for use of SpiceNet PPDR Mobile Broadband applications and solutions.

#### **AEs7 Application acceptance by Practitioners**

SpiceNet applications shall be tested by Suppliers and evaluated by practitioners. It will be certified by TVC for operational use.

#### **AEs8 Application Scalability**

Applications shall be able to scale to the number of active users without degrading the application functionality to the users.

## TD2 BroadWay PCP Challenge

### **AEs9 Application reliability**

Applications shall work reliable; no matter if they need network access or not. They shall be able to handle session interruption events without terminating functionality and resuming operation from point of interruption.

### **AEs10 Notification of Degraded application operation**

Users shall receive explicit notification of degraded application operational conditions.

### **AEs11 Availability of authorised MCX services**

PPDRs users and their affiliated organisations shall be able to use applications (communicate) within and across agencies, jurisdictions and cross borders via MCPTT (voice), MC data, or MC video on-demand, in real time, when needed, and when authorised.

### **AEs12 Application support for Operational Mobility**

All features in applications shall be usable by PPDR users and their affiliated organisations when moving to another PPDR network

## **2.2.7.2 AEs Application Eco-system Sub-objectives (Nice to have)**

### **AEs13 Internet of Public Safety Things (IoPST)**

Internet of Public Safety Things applications shall be supported in the final system and offers within the BroadWay PCP are welcomed.

## **2.2.8 Objective 8: Device Eco-system**

### **2.2.8.1 DEs - Device eco-system Sub-objectives**

**(All Tenders shall include sufficient information to describe how they will achieve each Sub-objective)**

MC Devices are essential communication tool for PPDR users. The physical attributes, accessories and capabilities/functions of the devices will be specified below. Using available tools and equipment shall provide improved operational mobility and effective response by responder practitioners. Fulfilling PPDR organisations' requirements for MC Devices shall ensure the highest benefit for the PPDR users and whole European community in general.

#### **DEs1 Deployment of Applications**

MC device shall provide operating system enabling deployment of applications.

#### **DEs2 Ergonomic and User Friendly**

Devices shall have an ergonomic design and shall be "user friendly", with controls that require little or no visual contact.

#### **DEs3 Programmable buttons**

The MC Devices shall be equipped with programmable buttons and indicators to facilitate user applications.

#### **DEs4 Simple group selection**

The process of selecting and calling a pre-arranged talk group shall be simple and require no more than three actions of the user.

#### **DEs5 Mobile Device Management**

Mobile device management shall be provided as described in Security architecture.

#### **DEs6 Robust and Ruggedised**

MC device shall be appropriately robust and ruggedised, adopting suitable industry standards for ingress protection, vibration and shock tolerance.

#### **DEs7 Battery Life**

MC device shall optimise energy consumption. Battery life shall support extended tour of duty ( 16 hours +).

#### **DEs8 Peripheral Equipment Interfaces**

Standard interfaces shall be used (physical as well as wireless) for connection to any peripheral equipment/external devices.

#### **DEs9 Open APIs/SDKs for MC application development**

Open APIs shall be used with availability of SDKs to support MC application development

#### **DEs10 Device Management and Monitoring**

Management and monitoring capabilities shall be provided for all MC Devices in PPDR MCX ecosystem.

#### **DEs11 Display quality**

Display shall be readable on direct bright sunlight.

**2.2.8.2 DEs - Device eco-system Sub-objective (Nice to have)**

**DEs12 Induction charging**

Charging the MC device wireless, using induction pads.

**DEs13 Bring your own Device**

BYOD shall be supported and supporting framework shall be defined.

**DEs14 Terminal to Terminal**

Ability for all broadband devices and their information services to have the possibility to work in terminal to terminal mode without utilisation of the network infrastructure.

## **2.2.9 Objective 9: Innovation Eco-system**

### **2.2.9.1 IEs - Innovation Eco-system Sub-objectives**

**(All Tenders shall include sufficient information to describe how they will achieve each Sub-objective)**

The BroadWay innovation eco-system allows Suppliers to think outside the scope of the Project and offer wide range of innovations to achieve BroadWay Objectives. Offered solutions shall not already exist.

#### **IEs1 New innovation**

Each solution shall include innovations to support new 3GPP releases.

#### **IEs2 Common test facilities for new innovation**

Common test facility shall become the point for innovation and cooperation with public sector and between European states and their PPDR organisations.

### **2.2.9.2 IEs - Innovation Eco-system (Nice to Have)**

#### **IEs3 Integration of existing components**

Integration of existing components shall form a primary contribution to innovation towards pan-European operational mobility.

#### **IEs4 Supporting future Innovation**

Innovation should be targeted to innovative domains, for example but limited to, User interfaces, MMI, Robotics, IoPST, Artificial intelligence, Augmented Reality, Devices.

## 2.2.10 Objective 10: Technical validation

### 2.2.10.1 Tv - Technical Validation

(All Tenders shall include sufficient information to describe how they will achieve each Objective)

#### Tv1 Technical Validation process

Technical validation shall test all functional Sub-objectives. KPIs will be defined initially by Suppliers during the Design Phase as explained in section 2.1. Technical validation will be carried out using independent and impartial subcontracting as described in section 2.1. Results and detailed documentation will be provided to the TVC to assess their satisfaction towards the possibility to award SpiceNet certification to BroadWay solutions at the conclusion of the Pilot Phase.

#### Tv2 Sustainable Technical validation capabilities

It is expected that innovative technologies and processes will be developed to be able to carry out technical validation of the solutions developed within BroadWay. The full portfolio of test capabilities shall be sustainable beyond BroadWay, and available for testing of continual provision of innovative solutions as they are integrated within the BroadNet system.

#### Tv3 Plugtest™ style events

During the prototype and Pilot Phase, prototypes and pilots of each Supplier will be integrated together in a way similar to how this is achieved by ETSI CTI<sup>2</sup>. The main difference in the scope of testing, to that of the ETSI MCX Plugtests™, relates to the higher level TRL7 (prototype) and TRL8 (pilot).

The BroadWay team are currently discussing with ETSI CTI for provisioning their support to this Plugtest™ activity which will also include the possibility to involve solution providers who are not funded by BroadWay. Confirmation and further detail will be given in the Call-Off documents at the end of the Design Phase.

#### Tv4 PEAv Technical Validation - Pan-European Availability

PEAv2	Harmonised Quality of Service
PEAv4	Seamless Operation
PEAv5	Assuring Quality of Experience

#### Tv5-PESAr Technical Validation - Pan-European Security

PESAr4	End 2 End Encryption
PESAr5	User and Control Plane
PESAr6	Device/User Authentication
PESAr7	Mutual Authentication
PESAr8	Rights Management
PESAr9	Over the Air Re-keying
PESAr10	Enterprise Mobility Management
PESAr15	Harmonised Security Assurance

---

<sup>2</sup> <https://www.etsi.org/news-events/news/1330-etsi-mission-critical-plugtests-event-reports-a-92-success-rate>

**Tv6-PESg Technical Validation - Pan-European SpiceNet Governance**

- PESg3      Authorised Administration
- PESg4      Management technology
- PESg5      Monitoring

**Tv7-PEOm Technical Validation - Pan-European Operational Mobility**

- PEOm1      Seamless communication groups spanning networks and authorities
- PEOm2      Seamless Access to information sources
- PEOm3      Seamless Access to applications and databases
- PEOm4      Harmonised Operational mobility - Same as home

**Tv8-AEs Technical Validation - Application Eco-system**

- AEs1      Open APIs
- AEs5      Audio and Video quality
- AEs6      Open Application Development Platform
- AEs8      Application Scalability
- AEs9      Application reliability
- AEs10      Notification of Degraded application operation
- AEs11      Availability of authorised MCX services
- AEs12      Application support for Operational Mobility

## **2.2.11 Objective 11: Practitioner evaluation**

### **2.2.11.1 PREv- Practitioner evaluation and acceptance Sub-objectives**

**(All Tenders shall include sufficient information to describe how they will achieve each Sub-objective)**

This Objective will aid the TVC to assess the suitability of the solutions integrated in the live pilot and will be an important contribution to the decision to award SpiceNet certification at the end of Phase 3.

Practitioner evaluation and acceptance shall use a sustainable methodology which shall guide on how the Practitioner Evaluation Team (PEVT) can self-organise themselves to define their own use cases, scenarios and evaluation criteria in order to carry out an independent activity during the Pilot Phase to evaluate the utility and usefulness of the BroadWay pilot.

They will use this evaluation to

- 1) Inform the BroadWay TVC of the process and results of their assessment
- 2) Assess themselves, how this new capability could be used in live practice; to understand whether the newly offered capabilities that intend to facilitate 'Operational Mobility' are likely to be fit for purpose.

Applications shall be provided which will support multiple use case scenarios in the pilot. This will allow practitioners to evaluate the benefit of the pan-European BroadWay solutions.

Practitioners are from different PPDRs domains, so evaluation shall incorporate: Police, Ambulance, Fire brigades, Coast guard, Customs, Ministry of Defence, Prison, Utilities, etc.

An initial set of scenarios is explained in section 2.5.1. These will be elaborated by the PEVT during the early stages of the BroadWay PCP and details will be provided during the Call-off's for Prototype and Pilot, in order to inform Suppliers of the evaluation intention of the PEVT.

The Practitioner Evaluation Team (PEVT) will be supported by Suppliers to assist with the logistics to carry out evaluation of the Pilot. Please refer to section 1.5 of the RFT.

#### **PREv1 Practitioner Evaluation methodology and process**

The PEVT will evaluate the Pilot and report directly to the TVC to contribute to their assessment of the Pilot, and its constituent components. This shall also include the provision of a guidance methodology to help support the PEVT to define activities, referred to as trials where use of the pilot system is made using realistic use cases and scenarios.

#### **PREv2 Practitioner Evaluation of MC services**

MCPTT, MC video, MC data - for group, emergency and broadcast communication.

#### **PREv3 Practitioner Evaluation of MC Applications, making use of MC services**

Geospatial applications: Automatic Vehicle & Personal Location (AVPL) for outdoor geospatial positioning for all PPDR assets.

#### **PREv4 Practitioner Evaluation of Information services enhanced by Operationally mobile MC Applications and Services**

MC data services for database query across different countries shall be supported for BroadWay scenarios.

### **2.2.11.2 PEaA1- Practitioner evaluation and acceptance (Nice to have)**

#### **PREv5 Existing or enhanced applications to support the pilot**

Based on the use case scenarios, Tenderers can offer existing, enhanced and/or additional applications.

### **2.2.12 Disclaimer**

Additional Sub-criteria may be added for the Call-offs for Phases 2 and 3, as a way of making the Award Criteria more precise, provided that they do not substantially change the existing criteria.

## **2.3 Phase 1 – Solution Design**

In the Design Phase awarded Suppliers will commence to develop solutions for the BroadWay Objectives.

Independent and impartial Technical validation and Practitioner Evaluation will be carefully monitored as they are crucial for evaluation of the Solutions.

The mandatory milestones and deliverables are listed in TD1, chapter 3.5 Expected Outcomes.

## **2.4 Phase 2 – Solution Prototype**

In the Prototype Phase, it has to be demonstrated that the prototype realises the BroadWay Objectives. In order to do so, the system prototype demonstration will be in an operational environment, according to the TRL7. And then later, if the Supplier advances to Phase 3, this system prototype will be piloted and tested against live use cases and evaluated by practitioners on TRL8 - system complete and qualified.

Prototype testing will be assessed according to predefined criteria. One or more (maximum 2) Plugtest™ style events will take place. They may, or may not be on the site of the prototype and will take place combining the solution prototypes and technical validation.

In the Prototype Phase Suppliers will provide tests for availability, security, management, operational mobility and applications. The goal of testing is whether the prototype meets the initial default requirements.

The mandatory milestones and deliverables are listed in TD1, chapter 3.5 Expected Outcomes.

## **2.5 Phase 3 – Pilot**

In the Pilot Phase has to be demonstrated that Solution Pilot in liveuse realises BroadWay Objectives. In order to do so, Final Solution Acceptance Testing consists of two parts: Technical and Objective Testing and Operational Evaluation by Practitioners.

During the Pilot Phase for technical validation, it is expected that Suppliers provide live testing for availability, security, management, operational mobility and applications.

Technical and Objective testing are planned to be carried out by our BroadWay Suppliers with a contractual obligation to assure that this is carried out independently and impartially. Testing will be overseen by the BroadWay Technical Validation Committee (TVC) which is comprised of the BroadWay Group of Procurers.

The technical performance of the supplied solutions will be tested and will be carried out across the pilot system by the chosen test Suppliers, using the test systems supplied.

Operational Evaluation by Practitioners will be done on several operational test scenarios (trials). Practitioners will evaluate offered features. A series of operational evaluation criteria will be used to guide practitioners on their assessment of the utility of the pilot system.

Once the technical testing and operational evaluation have been individually scored, a meeting of the TVC will be held to draw a consensus, and to select the favoured solutions to receive a formal BroadWay (SpiceNet) certification.

The mandatory milestones and deliverables are listed in TD1, chapter 3.5 Expected Outcomes.

### **2.5.1 Use case scenarios (Trials)**

Use case scenarios will be elaborated by BroadWay Practitioner Evaluation Team (PEVT) with the aim to align with Practitioner Evaluation activities during the Pilot Phase.

#### **UCS1 Rescue operation - Barge of Irregular Migrants**

A barge of irregular migrants needs urgent rescue action based on safety of life at sea. The vessel is drifting without steering with about 300 migrants on-board 100 Nm from the shore, in the Gulf of Cadiz. It will be a joint rescue operation by Portugal and Spain.

### **UCS2 Rescue operation - A Cruising ship on fire at Adriatic Sea**

A cruise ship bound from Brindisi (Italy) to Patras (Greece) with 1500 passengers on board has a fire on-board. The position is 40 miles east from Corfu. The mission principles are the same as the previous case – only the number of proceeding merchant vessels will be added to the case.

### **UCS3 VIP protection and escort on high level summit in Brussels**

Every year, several European Summits are organised in Brussels where heads of state or government of EU member states meet each other. These heads of state arrive at Brussels using different types of transportation, where some are surrounded by bodyguards and security people using satellite or radio communications systems, or even sometimes a combination of these with cellular or landline configurations. In this use case, there can be several partners from different European Countries. The idea is that bodyguards and security people use all the time their own radio without any disruption when crossing the borders and without any additional intervention to change settings on their radio.

### **UCS4 Following a “go fast” drug convoy from south of Spain to Germany**

Spanish anti-drug investigation services gained intelligence about a go-fast convoy starting from Malaga. The presumed destination is Hamburg (Germany). The vehicle is driving via southern France to Germany via Belgium and Holland. The original group from Spain moves to be active in countries where the convoy is, at that moment.

### **UCS5 Heavy Truck and Tourist Bus collision at Finnish-Norwegian border**

During the last years, tourism in northern Finland has increased rapidly. Despite arctic conditions, tourist groups are moving also during the winter season across the Norwegian border towards Nordkapp. During the Arctic winter, the driving conditions vary and can be extremely difficult. After collision of a heavy truck and a tourist bus, a joint rescue operation by Finland and Norway has begun. Land rescue forces and paramedic helicopter are used.

### **UCS6 Database queries from other EU country’s PPDR organisation**

It is quite common that a Police Organisation needs to rapidly identify a second nationality person or vehicle. In many cases this is usually done by making a phone call or an email to the specific point e.g. SIRENE offices, which are acting as NCP for the Schengen information system. Quite often, other contact points are used for practical reasons (language, personal contacts etc.).

The queries can be made quickly by integration to national databases and Schengen Information System (SIS). One option to access with a mobile client could be the integration straight to the SIS central database via SpiceNet Services.

### **UCS7 Natural Disaster – Forest Fire**

A huge forest fire has been raging for several days in a Southern Europe country A. Countries B and C agree to send each two water bombers to provide backup to the firefighters of country A. Planes and technical teams are based on a field one hundred kilometres away from the fire. Joint operation of countries A, B and C will use voice but also will exchange geographical information of fire propagation and local status including local environmental analysis data.



This Project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No **786912**.

**End of Document**

All rights reserved by the BroadWay consortium partners. No part of this document may be reproduced without the written approval of the author.

