

**Innovation activity to develop technologies to enable a pan-European interoperable broadband mobile system for PPDR, validated by sustainable testing facilities**

**BroadWay Open Market Consultation**

BroadWay will procure Innovation activity to enable a pan-European broadband mobile system for PPDR, validated by sustainable test and evaluation capabilities.

We cordially invite you to help the BroadWay Group of Procurers to understand the market status of broadband mobile for public safety.

To find out more, please join one of our briefing events. To attend our events and/or have your details added to our partnering tool, please also register here:

[www.broadway-info.eu/supplier-registration](http://www.broadway-info.eu/supplier-registration)

**This Document provides an editable template for preparation of your answers to our open market consultation questionnaire**

**We will only consider answers entered into our online system which can be found here:**

<https://work.psc-europecollab.eu/survey/index.php/541192>

**Questionnaire Explanation**

Our BroadWay Group of Procurers have already collated their views during the BroadMap project ([www.broadmap.eu](http://www.broadmap.eu)) and now it’s time to ask suppliers to tell us their view on what is possible, considering:

* the current state-of-the-art,
* what innovation activity is now required,
* which direction BroadWay should focus our Pre-Commercial Procurement (PCP).

This questionnaire will ask you for a lot of details. This is an opportunity for you to influence our BroadWay Group of Procurers while we prepare our Technical Specifications for our Pre-Commercial procurement.

Please answer as many questions as you can with concise explanations. Some questions will ask you if you already have some technical solutions. In most cases we expect the answer to be ‘no’. In which case, we would appreciate your opinion on ‘how’ to achieve a solution so to help us to achieve the BroadWay challenge. If the answer is ‘yes’, that’s great. Please provide details.

If you want to add an attachment, please share this using your own file sharing system (e.g. dropbox), and provide a link to it in the text box of our form.

The BroadWay Common Challenge, Ambition, and all other details are explained on our website <https://www.broadway-info.eu>. You may also choose to understand our background by reading the deliverables of BroadMap <https://www.broadmap.eu>.

Please remember - many of our BroadWay Group of Procurers will also be considering their national programme to implement Broadband for public safety.

**Sell your capability well !**

There are more than 400 questions in this system. Don’t worry, you don’t have to answer all of them.

Questions are grouped in 2 ways:

* by Supplier type - you will be asked which type of supplier you are
* by Objective - according to our 11 BroadWay objectives - Click here to see our objectives

All questions are mandatory, but you don’t have to answer everything. Many questions will be Yes/No/No Answer.

If you have a text box but have nothing to say. That’s OK, just type ‘NA’ (not applicable), click next, and the system will take you to the next question.

Occasionally, you may be presented with a blank page. If this occurs, please click 'previous' and then 'next' to refresh to page.

You can choose which supplier type you are. This will determine which questions you will be asked. You can choose more than one supplier type. There are roughly 30-40 questions, depending which supplier type you chose. If you fall into more than one supplier type, then please select appropriately and fill out the questions as they are presented. You may be asked the same question more than once, in this case. Please answer again in the context of the different supply type.

The full set of questions are available by downloading this word document. This is provided to allow you to:

1. see all questions for all supplier types
2. prepare your detailed answers, before entering your answers into our online tool.

Feel free to copy/paste into this questionnaire.

If you run into problems, you can cancel by clicking ‘Exit and Clear Survey’ at the top.

If you need a break, to complete later, click the ‘Resume Later’. You will be asked for your name, a password and email address to save your survey. This can be used to return later.

At the end, you will be offered the opportunity to print your answers. The link for this is on the bottom of the 'Thank You' page, at the end.

Any company may participate in this Questionnaire. Participating in this Questionnaire is free of any engagement and will never lead to any obligation between the group of procurers and your company. (Non) participation by a company will neither exclude this company from future tenders nor will it have any influence on its opportunities. Companies will not be bound by the answers provided in the Questionnaire in any subsequent Tender which may be submitted after a Call for Competition has been launched.

All data provided by a company will be handled confidentially unless statutory obligations demand the publication of this data and/or the company agrees with the publication of the provided data.

All ideas submitted by industry will be treated as Commercial in Confidence. No part of these will be made public. However, relevant insights shared in the Questionnaire are subject to publication and may be used by procuring entities to shape future strategies.

**How to find the different questions**

Questions are separated by supplier type. You can choose to answer for more than one supplier type. Pages for each separate questions are found in this document referring to the following page numbers:

* 1-4 : this introduction
* 5-7 : General Questions (all suppliers)
* 8-13 : Mobile Operators
* 14-17 : Security Architect
* 18-22 : Mobile Infrastructure Equipment Supplier
* 23-27 : Terminal Supplier
* 28-32 : Mission Critical Service Developer
* 31- 36 : Mission Critical Application Developer
* 37-40 : Test Equipment Supplier
* 41-44 : Communication Software Test Stack Developer
* 45-48 : Testing Services
* 49-50 : Security Assurance
* 51 : Practitioner Evaluation Support

**GENERAL QUESTIONS**

**General information: all about your organisation**

|  |  |
| --- | --- |
| 1. | Please provide the following information on your organisation: |
| Organisation name \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| City \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| Country \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| Contact person: Name \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| Contact person: Job title \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| Contact person: E-mail \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| Contact person: Mobile phone \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| 2. | We expect consortia of suppliers to submit to our tender process, so we offer an opportunity for you to give us permission to share some of your details to a public list to allow those building teams to learn about your capabilities. We won't release your contact details publicly, but we will share them privately with anyone who requests your details according to your consent expressed in this form.  Does the BroadWay consortium have your permission to share the data of your organization and your contact details (name, last name and e-mail) with other organizations who are intending to prepare a tender for BroadWay, and are looking for partners to form a consortium? Y/N |
| If you answered "Y", Can we make your company name, website, organisation type, core competence and specific expertise available on the BroadWay website to allow other potential suppliers to find you and request your contact details if they wish to invite you to join a consortium? Y/N  Details will be added to [www.broadway-info.eu/partnering-tool/](http://www.broadway-info.eu/partnering-tool/) |
| 3. | Please tick the box(es) best describes your organisation (you can choose more than one): |
| Small company (staff <50) |
| Medium-sized company (staff 50-250) |
| Large company (staff >250) |
| Multinational |
| Research institute |
| Not-for-profit organisation |
| Start-up |
| Spin-off |
| Other |
|  |
| 4. | Please briefly outline the main focus of your company, core competence, specific expertise and experience in public safety domain. |

**Advancing innovation: The BroadWay PCP call**

|  |  |
| --- | --- |
| 1. | In your view, is the scope of the BroadWay Pre-Commercial Procurement (PCP) challenge clear, do you consider it realistic? Y/N  Please read about our common challenge here: [www.broadway-info.eu/challenge/](http://www.broadway-info.eu/challenge/)  If you answered "Y", please elaborate.  If you answered "N", please specify what is not clear and suggest how the BroadWay consortium could further clarify the scope. |
| 2. | Taking into consideration what the PCP wants to achieve, please describe in your view what award criteria do you consider most important to evaluate bidders’ proposals. |
| 3. | Please describe in your opinion what will be the main challenges in fulfilling the PCP ambitions.  Please read our objectives here: <https://www.broadway-info.eu/?da_image=750> |
| 4. | At this stage is your organisation/company/consortium interested in submitting a PCP tender respose to BroadWay, Y/N  If you answered "Y", please outline the factors encouraging you to bid, and if "N", please outline the factors discouraging you from bidding. |
| 5. | Please describe the biggest cost drivers for you in determining price. |

|  |
| --- |
|  |

|  |  |
| --- | --- |
| 1. | In order for us to ask you the right questions and save you the pain to answer all 400 of our questions, please tell us which type of supplier you are?  You can choose one or more of the following.  If you are not represented in this list, please check all and feel free to only answer the questions that you are able to answer.  Before you start, we would like to sincerely thank you in advance for providing your expert opinions which will help shape the future of pan-European public safety broadband mobile communications.  Check all that apply |
| Mobile operator |
| Security architect |
| Mobile Infrastructure Equipment Supplier |
| Terminal Supplier |
| Mission Critical Service Developer |
| Mission Critical Application Developer |
| Test Equipment Supplier |
| Communication Software Test Stack Developer |
| Testing Services |
| Security assurance |
| Practitioner Evaluation Support |

**Mobile operator**

**Pan – European architecture**

|  |  |
| --- | --- |
| 1. | Please provide us with your comments and development ideas regarding the proposed SpiceNet Architecture.  The SpiceNet Architecture is available here: [www.broadway-info.eu/spicenet/](http://www.broadway-info.eu/spicenet/) |
| 2. | Do you already have an available solution for any or all BroadWay objectives? Y/N  Please read our objectives here: <https://www.broadway-info.eu/?da_image=750>  If you answered "Y", then: (a) please provide details (b) are there any specific additional requirements needed to make your solution work?  Please elaborate. |
| 3. | Do you have a roadmap for future Mission Critical broadband solutions? Y/N  If you answered "Y", please elaborate. |
| 4. | Do you foresee any significant risks in meeting BroadWay objectives? Y/N  Please read our objectives here: <https://www.broadway-info.eu/?da_image=750>  If you answered "Y", please elaborate. |
| 5. | What do you see as the most important KPIs for the delivery of SpiceNet? (max 5) |
| 6. | Does your product portfolio include Mission Critical broadband services/products? Y/N If you answered "Y", please provide details. |
| How would you describe the position of your organisation in the Mission Critical broadband ecosystem? |
| 7. | Please evaluate/summarize the value (number of users, revenues, societal benefits) of the public safety broadband market in which you participate. |
| 8. | How does this opportunity to implement BroadWay solutions fit with your organisational strategy? Please briefly elaborate. |
| 9. | What do you see are the requirements for mobile operators for the delivery of Mission Critical services? (preemption, priority, delay, jitter, frequency bands, unicast/multicast, releases, etc.). |
| 10. | Do you already offer Mission Critical services? Y/N If you answered "Y", (a) please provide details |
| (b) What are the capacity limitations? |

**Pan-European Security**

|  |  |
| --- | --- |
| 1. | Please describe your company's/consortium's security policies. Which national security legislation do you comply with? Is it in line with EU legislation - NIS directive, GDPR, etc?  Reference: BroadMap - MC policy gap, available at <https://www.psc-europe.eu/library/psce-policy-papers/mission-critical-policy-gap/download.html> |
| 2. | Please describe your ideas to ensure high quality security on end to end Mission Critical broadband services and solutions. |
| 3. | Please describe your principles on security measures that are in place for development of your solutions. |
| 4. | Please describe your ideas and innovations to improve PPDR user experience and usability in a high security Mission Critical broadband ecosystem (e.g. balancing better usability with higher security). |
| 5. | Please descibe your principles/ideas regarding an (a) existing or (b) planned authentication or encryption solution in the context of it being open standard or proprietary. |
| 6. | Please describe your view on which Common Criteria EAL level a solution should be compliant with in order to be adopted for software and system quality, for use by public safety practitioners. |
| 7. | Please describe which kind of end-to-end (E2E) security solution you offer. |
| 8. | Please describe your ideas regarding adoption of Strong Authentication and Single Sign on in future Mission Criticle broadband service environment. |
| 9. | Please give your opinion on the type of cyber attacks which could occur on the integrated SpiceNet system. |

**Standardised Solutions**

|  |  |
| --- | --- |
| 1. | Please describe your ideas regarding your roadmap implementing 3GPP Mission Critical services on your solutions (networks, devices, applications...). Please also refer to <http://www.3gpp.org/news-events/3gpp-news/1875-mc_services> |
| 2. | Are you participating in 3GPP or other standardisation work relating to Mission Critical Communication, Networks, Devices, Applications and/or Aligned Public Safety Operations? Y/N If you answered "Y", please provide details of working groups, recent attendance and recent contributions. |
| 3. | Do you see any further public safety standardization needs for 3GPP or other standards? Y/N If you answered "Y", please elaborate. |
| 4. | Do you offer mission critical mobile broadband solution? If you answered "Y", is it fully compliant with 3GPP standards (and which release) or does it implement proprietary protocols? |
| 5. | Please describe the structure of the supply chain for your area of public safety broadband services. |
| 6. | Please describe which standards are relevant for assessing (a) audio and (b) video quality. |

**Pan-European Availability**

|  |  |
| --- | --- |
| 1. | Please describe your ideas on how to guarantee high service availability on networks in all conditions and in different network models (Hybrid, MVNO, MOCN, Dedicated, etc.) |
| 2. | Have you implemented any kind of radio access sharing with other real/virtual operators (MOCN or MVNO or other)? Y/N If you answered "Y", please provide details. If you answered "N", please provide details regarding risks, restrictions, etc. |
| 3. | Have you solved Mission Critical service availability, when local RAN access becomes unavailable?Y/N  If you answered "Y", please explain how.  If you answered "N", do you have any ideas? |
| 4. | Have you solved Mission Critical broadband service for Air ground air? Y/N  If you answered "Y", please explain how.  If you answered "N", do you have any ideas? |
| 5. | Have you implemented monitoring of network and service availability to an acceptable quality? Y/N  If you answered "Y", please explain how.  If you answered "N", do you have any ideas? |
| 6. | Please describe your ideas for seamless data service continuity supporting mobility across Europe. |

**Pan-European SpiceNet Governance**

|  |  |
| --- | --- |
| 1. | Please describe your ideas on which management solutions should be provided to support subscriber and service operation management. |
| 2. | Do you know of any existing agreements or policies that promote and enable public safety broadband mobility between countries? Y/N  If you answered "Y", please describe further. If you answered "N", please provide details regarding risks, restrictions, preconditions, issues etc. |
| 3. | Do you have any ideas about future policy needs in this area, at national or pan-European level? Y/N If you answered "Y", please describe further. |
| 4. | Are you aware of any available technical solution to implement secure public safety broadband mobility across countries? Y/N |
| If you answered "Y", please provide details of the solution including any limiting factors |
| 5. | Please describe your ideas regarding the management of group communication in the Public Safety environment. |
| 6. | Please describe your ideas regarding the possibility of broadcasting voice services and data for public safety. |
| 7. | Do you have existing methods for billing to support public safety operations (eg. bulk services charging)? Y/N  If you answered "Y", please explain how.  If you answered "N", do you have any suggestions? |
| 8. | Please describe where your capability and solution fits into our 11 objectives.  Please read our objectives here: <https://www.broadway-info.eu/?da_image=750> |

**Pan-European Operational Mobility**

|  |  |
| --- | --- |
| 1. | Have you already solved interoperability between 3GPP and LMR systems? Y/N  If you answered "Y", please explain how. If you answered "N", do you have any suggestions? |

**Application Eco-System**

|  |  |
| --- | --- |
| 1. | Have you implemented Mission Critical services over existing broadband network? Y/N  If you answered "Y", please describe how. If you answered "N", do you have any plans to implement? |

**Innovation Eco-System**

|  |  |
| --- | --- |
| 1. | Please describe your (a) current and (b) future plans for innovation to support public safety broadband. |
| 2. | Are any of your innovations in broadband technology in operational use in the public safety or in private industry? Y/N  If you answered "Y", please describe further. |
| 3. | Do you know of any intellectual property issues (e.g. patents) which may block the use of open standards for Mission Critical broadband?  If you answered "Y", please explain. |

**Security architect**

**Pan-European Architecture**

|  |  |
| --- | --- |
| 1. | Please provide us with your comments and development ideas regarding the proposed SpiceNet Architecture.  Please read about the SpiceNet Architecture here: <https://www.broadway-info.eu/spicenet/> |
| 2. | Do you already have an available solution for any or all BroadWay objectives? Y/N  Please read our objectives here: <https://www.broadway-info.eu/?da_image=750>  If you answered "Y", then: (a) please provide details (b) are there any specific additional requirements needed to make your solution work? |
| 3. | Do you have a roadmap for future Mission Critical broadband solutions? Y/N  If you answered "Y", please provide details. |
| 4. | Do you foresee any significant risks in meeting BroadWay objectives? Y/N  Please read our objectives here: <https://www.broadway-info.eu/?da_image=750>  If you answered "Y", please provide details. |
| 5. | What do you see as the most important KPIs for the delivery of SpiceNet? (max 5) |
| 6. | Does your product portfolio include Mission Critical broadband services/products? Y/N If you answered "Y", please provide details. |
| How would you describe the position of your organisation in the Mission Critical broadband ecosystem? |
| 7. | Please evaluate/summarize the value (number of users, revenues, societal benefits) of the public safety broadband market in which you participate. |
| 8. | How does this opportunity to implement these solutions fit with your organisational strategy? Please briefly elaborate. |
| 9. | What do you see are the requirements for mobile operators for the delivery of Mission Critical services? (preemption, priority, delay, jitter, frequency bands, unicast/multicast, releases, etc.). |
| 10. | Do you already offer Mission Critical services? Y/N If you answered "Y", (a) please provide details |
| (b) What are the capacity limitations? |

**Pan-European Security**

|  |  |
| --- | --- |
| 1. | Please describe your company's/consortium's security policies. Which national security legislation do you comply with? Is it in line with EU legislation - NIS directive, GDPR, etc?  Reference: BroadMap - MC policy gap, available at <https://www.psc-europe.eu/library/psce-policy-papers/mission-critical-policy-gap/download.html> |
| 2. | Please describe your ideas to ensure high quality security on end to end Mission Critical broadband services and solutions. |
| 3. | Please describe your principles on security measures that are in place for development of your solutions. |
| 4. | Please describe your ideas and innovations to improve PPDR user experience and usability in a high security Mission Critical broadband ecosystem (e.g. balancing better usability with higher security). |
| 5. | Please descibe your principles/ideas regarding an (a) existing or (b) planned authentication or encryption solution in the context of it being open standard or proprietary. |
| 6. | Please state your view about up to which Common Criteria EAL level a solution should be compliant with in order to be adopted for software and system quality. |
| 7. | Please describe your ideas regarding adoption of Strong Authentication and Single Sign on in future Mission Criticle broadband service environment. |
| 8. | Please give your opinion on the type of cyber attacks which could occur on the integrated SpiceNet system. |

**Standardised Solutions**

|  |  |
| --- | --- |
| 1. | Please describe your ideas regarding your roadmap implementing 3GPP Mission Critical services on your solutions (networks, devices, applications...). Please also refer to <http://www.3gpp.org/news-events/3gpp-news/1875-mc_services> |
| 2. | Are you participating in 3GPP or other standardisation work relating to Mission Critical Communication, Networks, Devices, Applications and/or Aligned Public Safety Operations? Y/N If you answered "Y", please provide details of working groups, recent attendance and recent contributions. |
| 3. | Do you see any further public safety standardization needs for 3GPP or other standards? Y/N If you answered "Y", please explain. |
| 4. | Please describe the structure of the supply chain for your area of public safety broadband services. |

**Pan-European Availability**

|  |  |
| --- | --- |
| 1. | Please describe your ideas on how to guarantee high PPDR service availability on networks in all conditions and in different network models (Hybrid, MVNO, MOCN, Dedicated, etc.). |
| 2. | Have you ever been involved in (a) the implementation or (b) security development of any kind of radio access sharing with other real/virtual operators? (MOCN or MVNO) Y/N  For (a) and (b), if you answered "Y" please describe your involvement. For (a) and (b), if you answered "N" please provide details regarding risks, restrictions, and other limiting factors. |
| 3. | Have you solved Mission Critical service availability, when local RAN access becomes unavailable?Y/N  If you answered "Y", please explain how.  If you answered "N", do you have any ideas? |
| 4. | Have you implemented monitoring of network and service availability to an acceptable quality?Y/N  If you answered "Y", please explain how.  If you answered "N", do you have any ideas? |
| 5. | Please describe your ideas for seamless data service continuity supporting mobility across Europe. |

**Pan-European SpiceNet Governance**

|  |  |
| --- | --- |
| 1. | Please describe your ideas on which management solutions should be provided to support subscriber and service operation management. |
| 2. | Do you know of any existing agreements or policies that promote and enable public safety broadband mobility between countries? Y/N  If you answered "Y", please describe further. If you answered "N", please provide details regarding risks, restrictions, preconditions, issues etc. |
| 3. | Do you have any ideas about future policy needs in this area, at national or pan-European level?Y/N If you answered "Y", please describe further. |
| 4. | Are you aware of any available technical solution to implement secure public safety broadband mobility across countries? Y/N If you answered "Y", please provide details of the solution including limiting factors. |

**Application Eco-system**

|  |  |
| --- | --- |
| 1. | Please describe the principles on how to secure access from Mission Critical mobile device to Mission Critical Backbone services, Intranet and internet PPDR agencies, social media, news etc. |
| 2. | Please provide your opinion on how to secure object level data protocols (e.g. CAP Common Alerting Protocol) which should be supported by Mission Critical services. |
| 3. | Please provide your opinion regarding the security processes that will be necessary for the formation of a pan- European public safety App-store. |

**Device Eco-system**

|  |  |
| --- | --- |
| 1. | In your opinion, what security API's should be provided for application and device level security? |
| 2. | What is your opinion of future evolving threats that could target the pan-European mobile broadband system? |

**Innovation Eco-system**

|  |  |
| --- | --- |
| 1. | Please describe your (a) current and (b) future plans for innovation to support secure public safety broadband. |

**Mobile Infrastructure Equipment Supplier**

**Pan-European Architecture**

|  |  |
| --- | --- |
| 1. | Please provide us with your comments and development ideas regarding the proposed SpiceNet Architecture.  The SpiceNet Architecture is available here: [www.broadway-info.eu/spicenet/](http://www.broadway-info.eu/spicenet/) |
| 2. | Do you already have an available solution for any or all BroadWay objectives? Y/N  Please read our objectives here: <https://www.broadway-info.eu/?da_image=750>  If you answered "Y", then: (a) please provide details (b) are there any specific additional requirements needed to make your solution work? |
| 3. | Do you have a roadmap for future Mission Critical broadband solutions? Y/N  If you answered "Y", please provide details. |
| 4. | Do you foresee any significant risks in meeting BroadWay objectives? Y/N  Please read our objectives here: <https://www.broadway-info.eu/?da_image=750>  If you answered "Y", please provide details. |
| 5. | What do you see as the most important KPIs for the delivery of SpiceNet? (max 5) |
| 6. | Does your product portfolio include Mission Critical broadband services/products? Y/N If you answered "Y", please provide details. How would you describe the position of your organisation in the Mission Critical broadband ecosystem? |
| 7. | Please evaluate/summarize the value (number of users, revenues, societal benefits) of the public safety broadband market in which you participate. |
| 8. | How does this opportunity to implement these solutions fit with your organisational strategy? Please briefly elaborate. |
| 9. | What do you see are the requirements for mobile operators for the delivery of Mission Critical services? (preemption, priority, delay, jitter, frequency bands, unicast/multicast, releases, etc.). |
| 10. | Do you already offer Mission Critical services? Y/N If you answered "Y", (a) please provide details, including whether there are any capacity limitations. |

**Pan-European Security**

|  |  |
| --- | --- |
| 1. | Please describe your company's/consortium's security policies. Which national security legislation do you comply with? Is it in line with EU legislation - NIS directive, GDPR, etc?  Reference: BroadMap - MC policy gap, available at <https://www.psc-europe.eu/library/psce-policy-papers/mission-critical-policy-gap/download.html> |
| 2. | Please describe your ideas to ensure high quality security on end to end Mission Critical broadband services and solutions. |
| 3. | Please describe your principles on security measures that are in place for development of your solutions. |
| 4. | Please describe your ideas and innovations to improve PPDR user experience and usability in a high security Mission Critical broadband ecosystem (e.g. balancing better usability with higher security). |
| 5. | Please descibe your ideas on how best to deal with a) security, b) performance, and c) data management in multitenant virtual data. |
| 6. | Please descibe your ideas on how best to deal with (a security, (b performance, and (c data management in multitenant slices. |
| 7. | Please descibe your principles/ideas regarding (a) an existing or (b) planned authentication or encryption solution in the context of it being open standard or proprietary. |
| 8. | Please state your view about up to which Common Criteria EAL level a solution should be compliant with in order to be adopted for software and system quality. |
| 9. | Please describe which kind of end-to-end (E2E) security solution you offer. |
| 10. | Please describe your ideas regarding adoption of Strong Authentication and Single Sign on in future Mission Critical broadband service environment. |
| 11. | Please give your opinion on the type of cyber attacks which could occur on the integrated SpiceNet system. |

**Standardised Solutions**

|  |  |
| --- | --- |
| 1. | Please describe your ideas regarding your roadmap implementing 3GPP Mission Critical services on your solutions (networks, devices, applications...). Please also refer to <http://www.3gpp.org/news-events/3gpp-news/1875-mc_services> |
| 2. | Are you participating in 3GPP or other standardisation work relating to Mission Critical Communication, Networks, Devices, Applications and/or Aligned Public Safety Operations? Y/N If you answered "Y", please provide details of working groups, recent attendance and recent contributions. |
| 3. | Do you see any further public safety standardization needs for 3GPP or other standards? Y/N If you answered "Y", please explain. |
| 4. | Do you offer mission critical mobile broadband solution? Y/N If you answered "Y", is it fully compliant with 3GPP standards (and which release) or does it implement proprietary protocols? |
| 5. | Please describe the structure of the supply chain for your area of public safety broadband services. |
| 6. | Please describe which standards are relevant for assessing quality of (a) audio and (b) video. |

**Pan-European Availability**

|  |  |
| --- | --- |
| 1. | Please describe your ideas on how to guarantee high service availability for public safety mobile broadband communication networks in all conditions and in different network models (Hybrid, MVNO, MOCN, Dedicated, etc.) |
| 2. | Have you implemented any kind of radio access sharing with other real/virtual operators (MOCN or MVNO)? Y/N  If you answered "Y", please provide details. If you answered "N", please provide details regarding risks, restrictions, etc. |
| 3. | Have you solved Mission Critical service availability, when local RAN access becomes unvailable? Y/N  If you answered "Y", please explain how. If you answered "N", do you have any ideas? |
| 4. | Have you solved Mission Critical broadband service for Air ground air? Y/N  If you answered "Y", please explain how.  If you answered "N", do you have any ideas? |
| 5. | Please describe your ideas for seamless data service continuity supporting mobility across Europe. |

**Pan-European SpiceNet Governance**

|  |  |
| --- | --- |
| 1. | Are you aware of any available technical solution to implement secure public safety broadband mobility across countries? Y/N |
| If you answered "Y", please provide details of the solution including any limiting factors |
| 2. | Please describe your ideas regarding the possibility of broadcasting voice services and data for public safety. |
| 3. | Please describe where your capability or solution fits within our 11 objectives.  Please read our objectives here: <https://www.broadway-info.eu/?da_image=750> |

**Pan-European Operational Mobility**

|  |  |
| --- | --- |
| 1. | Have you already solved interoperability between 3GPP and LMR systems? Y/N  If you answered "Y", please explain how. If you answered "N", do you have any suggestions? |

**Application Eco-system**

|  |  |
| --- | --- |
| 1. | Have you implemented Mission Critical services over existing broadband network? Y/N  If you answered "Y", please describe how. If you answered "N", do you have any plans to implement? |
| 2. | Do you already provide API's and Value Added Services(VAS's) (Business Models, Mission Critical)?Y/N  If you answered "Y", please provide details.  If you answered "N", do you plan to provide these services in the future? Y/N If you answered "Y", please provide details. |

**Device Eco-system**

|  |  |
| --- | --- |
| 1. | Please describe how you provide (a) management and (b) monitoring capabilities for devices in the Mission Critical broadband system. |

**Innovation Eco-system**

|  |  |
| --- | --- |
| 1. | Please describe your current and future plans for innovation to support public safety broadband. |
| 2. | Are any of your innovations in broadband technology in operational use in the public safety or in private industry? Y/N  If you answered "Y", please describe further. |
| 3. | Do you know of any intellectual property issues (e.g. patents) which may block the use of open standards for Mission Critical broadband?  If you answered "Y", please explain. |
| 4. | Please describe the scope of development tools that will be necessary to catalyze development of innovative applications. |

**Terminal Supplier**

**Pan-European Architecture**

|  |  |
| --- | --- |
| 1. | Do you already have an available solution for any or all BroadWay objectives? Y/N  Please read our objectives here: <https://www.broadway-info.eu/?da_image=750>  If you answered "Y", then: (a) please provide details (b) are there any specific additional requirements needed to make your solution work? |
| 2. | Do you have a roadmap for future Mission Critical broadband solutions? Y/N  If you answered "Y", please provide details. |
| 3. | Do you foresee any significant risks in meeting BroadWay objectives? Y/N  Please read our objectives here: <https://www.broadway-info.eu/?da_image=750>  If you answered "Y", please provide details. |
| 4. | What do you see as the most important KPIs for the delivery of SpiceNet? (max 5) |
| 5. | Does your product portfolio include Mission Critical broadband services/products? Y/N If you answered "Y", please provide details. |
| How would you describe the position of your organisation in the MC BB ecosystem? |
| 6. | Please evaluate/summarize the value (number of users, revenues, societal benefits) of the public safety broadband market in which you participate. |
| 7. | How does this opportunity to implement these solutions fit with your organisational strategy?  Please briefly elaborate. |
| 8. | What do you see are the requirements for mobile operators for the delivery of Mission Critical services? (preemption, priority, delay, jitter, frequency bands, unicast/multicast, releases, etc.). |

**Pan-European Security**

|  |  |
| --- | --- |
| 1. | Please describe your company's/consortium's security policies. Which national security legislation do you comply with? Is it in line with EU legislation - NIS directive, GDPR, etc? Reference: BroadMap - Mission Critical policy gap, available at [www.psc-europe.eu/library/psce-policy-papers/mission-critical-policy-gap/download.html](http://www.psc-europe.eu/library/psce-policy-papers/mission-critical-policy-gap/download.html) |
| 2. | Please describe your ideas to ensure high quality security on end to end Mission Critical broadband services and solutions. |
| 3. | Please describe your principles on security measures that are in place for development of your solutions. |
| 4. | Please describe your ideas and innovations to improve PPDR user experience and usability in a high security Mission Critical broadband ecosystem (e.g. balancing better usability with higher security). |
| 5. | Please descibe your principles/ideas regarding an (a) existing or (b) planned authentication or encryption solution in the context of it being open standard or proprietary. |
| 6. | Please state your view about up to which Common Criteria EAL level a solution should be compliant with in order to be adopted for software and system quality. |
| 7. | Please describe which kind of end-to-end (E2E) security solution you offer. |
| 8. | Please describe your ideas regarding adoption of Strong Authentication and Single Sign on in future Mission Critical broadband service environment. |
| 9. | Is any connectivity needed to/for internet provided services to make your solution work? Y/N If you answered "Y", (a) is any information sent to other parties?  If you answered "Y", (b) is all traffic, management, data and voice, managed by private cache? |
| 10. | Are there any special restrictions on the terminals? Y/N  If you answered "Y", please describe further. |
| 11. | Do you provide or support Mobile Device Management in your solution? Y/N  If you answered "Y", please provide details. |
| 12. | Please give your opinion on the type of cyber attacks which could occur on the integrated SpiceNet system. |

**Standardised Solutions**

|  |  |
| --- | --- |
| 1. | Please describe your ideas regarding your roadmap implementing 3GPP Mission Critical services on your solutions (networks, devices, applications...). Please also refer to <http://www.3gpp.org/news-events/3gpp-news/1875-mc_services> |
| 2. | Are you participating in 3GPP or other standardisation work relating to Mission Critical Communication, Networks, Devices, Applications and/or Aligned Public Safety Operations? Y/N If you answered "Y", (a) please provide details of working groups, recent attendance and recent contributions. |
| 3. | Do you see any further public safety standardization needs for 3GPP or other standards? Y/N If you answered "Y", please explain. |
| 4. | Do you offer mission critical mobile broadband solution?  If you answered "Y", is it fully compliant with 3GPP standards (and which release) or does it implement proprietary protocols? |
| 5. | Please describe the structure of the supply chain for your area of public safety broadband services. |
| 6. | Please describe which standards are relevant for assessing quality of (a) audio and (b) video. |

**Pan-European Availability**

|  |  |
| --- | --- |
| 1. | What do you think are the challenges for terminals to support priority and pre-emption? |
| 2. | Have you solved Mission Critical broadband service for Air ground air? Y/N  If you answered "Y", please describe your solution. |

**Pan-European SpiceNet Governance**

|  |  |
| --- | --- |
| 1. | Are you aware of any available technical solution to implement secure public safety broadband mobility across countries? Y/N |
| If you answered "Y", please provide details of the solution including any limiting factors |
| 2. | Please describe your ideas regarding the possibility of broadcasting voice services and data for public safety. |
| 3. | Please describe where your capability or solution fits within our 11 objectives .  Please read our objectives here: <https://www.broadway-info.eu/?da_image=750> |

**Pan-European Operational Mobility**

|  |  |
| --- | --- |
| 1. | Have you already found a solution for interoperability between 3GPP and LMR systems? Y/N  If you answered "Y", please describe your solution.  If you answered "N", do you have any ideas? |

**Application Eco-system**

|  |  |
| --- | --- |
| 1. | Please describe principles on how to create access from MC mobile device to MC Backbone services, Intranet and internet PPDR agencies, socialmedia, news etc. |
| 2. | Please provide information on which platforms your terminals work (e.g. Android, iOS, Windows). |
| 3. | Please provide information if you require testing and certifications to allow applications to operate on your devices. |
| 4. | Please describe your view on publishing and securing solution interfaces (e.g. northbound APIs). |
| 5. | Have you tested Mission Critical services over existing broadband network? Y/N  If you answered "Y", please describe. |
| 6. | Do you provide development tools ? Y/N  If you answered "Y", please elaborate. |

**Device Eco-system**

|  |  |
| --- | --- |
| 1. | Please describe your view regarding which 3GPP Mission Critical Services you (a) currently support or (b) plan to support. |
| 2. | Please describe API's and Value Added Services(VAS's) which you (a) currently provide and/or (b) plan to provide (Business Models, Mission Critical). |
| 3. | Please describe how you provide (a) management and (b) monitoring capabilities for devices in the Mission Critical broadband system. |
| 4. | Please describe what provision for peripheral attachments you provide. |
| 5. | Please describe what peripherals are available. |
| 6. | Please provide details of your experience regarding ruggedized terminals and terminals which can withstand heat, cold, rain, humidity, dust and vibration. |
| 7. | What would you suggest as a solution for direct mode (infrastructureless terminal to terminal)? |
| 8. | What is your opinion regarding the maximum operating hours of terminals? |
| (a) How should this be benchmarked? |
| 9. | What is your opinion on LMR, 3GPP integration? |
| 10. | Are the broadband devices developed by your business in operational use in public safety or private industry? Y/N  If you answered "Y", please describe the use of the devices. |
| 11. | What is your forecast on the volume and/or number of mission critical broadband terminals that will be in use in 2025 for private and public safety? |

**Innovation Eco-system**

|  |  |
| --- | --- |
| 1. | Please describe your (a) current and (b) future plans for innovation to support public safety broadband. |
| 2. | Are any of your innovations in broadband technology in operational use in the public safety or in private industry? Y/N  If you answered "Y" please describe further. |
| 3. | Do you know of any intellectual property issues (e.g. patents) which may block the use of open standards for Mission Critical broadband? Y/N If you answered "Y", please explain. |
| 4. | Please describe the scope of development tools that will be necessary to catalyze development of innovative applications. |

**Mission Critical Service Developer**

**Pan-European Architecture**

|  |  |
| --- | --- |
| 1. | Please provide us with your comments and development ideas regarding the proposed SpiceNet Architecture.  The SpiceNet Architecture is available here: [www.broadway-info.eu/spicenet/](http://www.broadway-info.eu/spicenet/) |
| 2. | Do you already have an available solution for any or all BroadWay objectives? Y/N  Please read our objectives here: <https://www.broadway-info.eu/?da_image=750>  If you answered "Y", then: (a) please provide details (b) are there any specific additional requirements needed to make your solution work? |
| 3. | Do you have a roadmap for future Mission Critical broadband solutions? Y/N  If you answered "Y", please provide details. |
| 4. | Do you foresee any significant risks in meeting BroadWay objectives? Y/N  Please read our objectives here: <https://www.broadway-info.eu/?da_image=750>  If you answered "Y", please provide details. |
| 5. | What do you see as the most important KPIs for the delivery of SpiceNet? (max 5) |
| 6. | Does your product portfolio include Mission Critical broadband services/products? Y/N If you answered "Y", please provide details. |
| How would you describe the position of your organisation in the Mission Critical broadband ecosystem? |
| 7. | Please evaluate/summarize the value (number of users, revenues, societal benefits) of the public safety broadband market in which you participate. |
| 8. | How does this opportunity to implement these solutions fit with your organisational strategy?  Please briefly elaborate. |
| 9. | What do you see are the requirements for mobile operators for the delivery of Mission Critical services? (preemption, priority, delay, jitter, frequency bands, unicast/multicast, releases, etc.). |

**Pan-European Security**

|  |  |
| --- | --- |
| 1. | Please describe your company's/consortium's security policies. Which national security legislation do you comply with? Is it in line with EU legislation - NIS directive, GDPR, etc?  Reference: BroadMap - MC policy gap, available at <https://www.psc-europe.eu/library/psce-policy-papers/mission-critical-policy-gap/download.html> |
| 2. | Please describe your ideas to ensure high quality security on end to end Mission Critical broadband services and solutions. |
| 3. | Please describe your ideas to ensure high quality security on end to end Mission Critical broadband services and solutions. |
| 4. | Please describe your ideas and innovations to improve PPDR user experience and usability in a high security Mission Critical broadband ecosystem (e.g. balancing better usability with higher security). |
| 5. | Please describe your ideas on how services may make use of multitenant virtual data. |
| 6. | Please describe your ideas on how services may make use of multitenant slices. |
| 7. | Please state your view about up to which Common Criteria EAL level a solution should be compliant with in order to be adopted for software and system quality. |
| 8. | Please describe which kind of end-to-end (E2E) security solution you offer. |
| 9. | Please describe your ideas regarding adoption of Strong Authentication and Single Sign on in future Mission Critical broadband service environment. |
| 10. | Is any connectivity needed to/for internet provided services to make your solution work? Y/N If you answered "Y", is any information sent to other parties? Y/N |
| 11. | Do you provide or support Mobile Device Management in your solution? Y/N  If you answered "Y", please provide details. |
| 12. | Please give your opinion on the type of cyber attacks which could occur on the integrated SpiceNet system. |

**Standardised Solutions**

|  |  |
| --- | --- |
| 1. | Please describe your ideas regarding your roadmap implementing 3GPP Mission Critical services on your solutions (networks, devices, applications...). Please also refer to <http://www.3gpp.org/news-events/3gpp-news/1875-mc_services> |
| 2. | Are you participating in 3GPP or other standardisation work relating to Mission Critical Communication, Networks, Devices, Applications and/or Aligned Public Safety Operations? Y/N If you answered "Y", please provide details of working groups, recent attendance and recent contributions. |
| 3. | Do you see any further public safety standardization needs for 3GPP or other standards? Y/N If you answered "Y", please explain. |
| 4. | Do you offer mission critical mobile broadband solution?  If you answered "Y", is it fully compliant with 3GPP standards (and which release) or does it implement proprietary protocols? |
| 5. | Please describe the structure of the supply chain for your area of public safety broadband services. |
| 6. | Please describe which standards are relevant for assessing quality of (a) audio and (b) video. |

**Pan-European Availability**

|  |  |
| --- | --- |
| 1. | Please describe your ideas on how to guarantee high service availability for public safety mobile broadband communication networks in all conditions and in different network models (Hybrid, MVNO, MOCN, Dedicated, etc.) |
| 2. | Have you solved Mission Critical broadband service for Air ground air? Y/N  If you answered "Y", please explain how.  If you answered "N", do you have any ideas? |
| 3. | Please describe your ideas for seamless data service continuity supporting mobility across Europe. |

**Pan-European SpiceNet Governance**

|  |  |
| --- | --- |
| 1. | Please describe your ideas on which management solutions should be provided to support subscriber and service operation management. |
| 2. | Are you aware of any available technical solution to implement secure public safety broadband mobility across countries? Y/N |
| If you answered "Y", please provide details of the solution including any limiting factors. |
| 3. | Please describe your ideas regarding the management of group communication in the Public Safety environment. |
| 4. | Please describe your ideas regarding the possibility of broadcasting voice services and data for public safety. |
| 5. | Please describe where your capability and solution fits into our 11 objectives.  Please read our objectives here: <https://www.broadway-info.eu/?da_image=750> |

**Application Eco-system**

|  |  |
| --- | --- |
| 1. | Briefly set out how you would design/architect mobile Mission Critical services to allow users from multiple agencies (e.g, Fire Departments ) access to, for example, an incident report. |
| 2. | Please describe the principles on how to secure access from Mission Critical mobile device to Mission Critical Backbone services, Intranet and internet, PPDR agencies, social media, news etc. |
| 3. | Have you developed Mission Critical services on any existing commercial 3G, 4G, or LTE network? Y/N If you answered "Y", please provide details including the location where the service is deployed. |
| 4. | On which types of devices are your services supported (smartphone, tablet, notebook)? |
| 5. | Please provide information on which platforms your services work (e.g. Android, iOS, Windows). |
| 6. | Would you expect to certify applications that are going to use your services? Y/N  If you answered "Y", please provide details. |
| 7. | Please provide your view on which object level data protocols should be supported by Mission Critical services. |
| 8. | Please provide your view on which Application Programming Interface(s) Mission Critical services should offer. (b) Are 3GPP standards suficient? |
| 9. | Have you implemented Mission Critical services over existing broadband mobile networks? Y/N  If you answered "Y", please describe how.  If you answered "N", do you have the intention of implementing Mission Critical services in the future? |

**Innovation Eco-system**

|  |  |
| --- | --- |
| 1. | Please describe your (a) current and (b) future plans for innovation to support public safety broadband. |
| 2. | Are any of your innovations in broadband technology in operational use in the public safety or in private industry? Y/N  If you answered "Y", please describe further. |
| 3. | Do you know of any intellectual property issues (e.g. patents) which may block the use of open standards for Mission Critical broadband? Please explain. If you answered "Y", please explain. |

**Mission Critical Application Developer**

**Pan-European Architecture**

|  |  |
| --- | --- |
| 1. | Do you already have an available solution for any or all BroadWay objectives? Please read our objectives here: <https://www.broadway-info.eu/?da_image=750>  If you answered "Y", then: (a) please provide details (b) are there any specific additional requirements needed to make your solution work? |
| 2. | Do you have a roadmap for future Mission Critical broadband solutions? Y/N  If you answered "Y", please provide details. |
| 3. | Do you foresee any significant risks in meeting BroadWay objectives? Y/N  Please read our objectives here: <https://www.broadway-info.eu/?da_image=750>  If you answered "Y", please provide details. |
| 4. | What do you see as the most important KPIs for the delivery of SpiceNet? (max 5) |
| 5. | Does your product portfolio include Mission Critical broadband services/products? Y/N If you answered "Y", please provide details. |
| How would you describe the position of your organisation in the Mission Critical broadband ecosystem? |
| 6. | Please evaluate/summarize the value (number of users, revenues, societal benefits) of the public safety broadband market in which you participate. |
| 7. | How does this opportunity to implement these solutions fit with your organisational strategy? Please briefly elaborate. |
| 8. | What do you see are the requirements for mobile operators for the delivery of Mission Critical services? (preemption, priority, delay, jitter, frequency bands, unicast/multicast, releases, etc.). |

**Pan-European Security**

|  |  |
| --- | --- |
| 1. | Please describe your company's/consortium's security policies. Which national security legislation do you comply with? Is it in line with EU legislation - NIS directive, GDPR, etc? Reference: BroadMap - Mission Critical policy gap, available at [www.psc-europe.eu/library/psce-policy-papers/mission-critical-policy-gap/download.html](http://www.psc-europe.eu/library/psce-policy-papers/mission-critical-policy-gap/download.html) |
| 2. | Please describe your ideas to ensure high quality security on end to end Mission Critical broadband services and solutions. |
| 3. | Please describe your principles on security measures that are in place for development of your solutions. |
| 4. | Please describe your ideas and innovations to improve PPDR user experience and usability in a high security Mission Critical broadband ecosystem (e.g. balancing better usability with higher security). |
| 5. | Please state your view about up to which Common Criteria EAL level a solution should be compliant with in order to be adopted for software and system quality. |
| 6. | Please describe which kind of end-to-end (E2E) security solution you offer. |
| 7. | Please describe your ideas regarding adoption of Strong Authentication and Single Sign on in future Mission Critical broadband service environment. |
| 8. | Is any connectivity needed to/for internet provided services to make your solution work? Y/N If you answered "Y", is any information sent to other parties? Y/N |
| 9. | Do you provide or support Mobile Device Management in your solution? Y/N  If you answered "Y", please provide details. |
| 10. | Please give your opinion on the type of cyber attacks which could occur on the integrated SpiceNet system. |

**Standardised Solutions**

|  |  |
| --- | --- |
| 1. | Please describe your ideas regarding your roadmap implementing 3GPP Mission Critical services on your solutions (networks, devices, applications...). Please also refer to <http://www.3gpp.org/news-events/3gpp-news/1875-mc_services> |
| 2. | Are you participating in 3GPP or other standardisation work relating to Mission Critical Communication, Networks, Devices, Applications and/or Aligned Public Safety Operations? Y/N If you answered "Y", please provide details of working groups, recent attendance and recent contributions. |
| 3. | Do you see any further public safety standardization needs for 3GPP or other standards? Y/N If you answered "Y", please explain. |
| 4. | Do you offer mission critical mobile broadband solution?  If you answered "Y", is it fully compliant with 3GPP standards (and which release) or does it implement proprietary protocols? |
| 5. | Please describe the structure of the supply chain for your area of public safety broadband services. |
| 6. | Please describe which standards are relevant for assessing quality of (a) audio and (b) video. |

**Pan-European Availability**

|  |  |
| --- | --- |
| 1. | Have you solved Mission Critical broadband service for Air ground air? Y/N  If you answered "Y", please explain how.  If you answered "N", do you have any ideas? |
| 2. | Please describe your ideas for seamless data service continuity supporting mobility across Europe. |

**Pan-European SpiceNet Governance**

|  |  |
| --- | --- |
| 1. | Are you aware of any available technical solution to implement secure public safety broadband mobility across countries? Y/N |
| If you answered "Y", please provide details of the solution including any limiting factors. |
| 2. | Please describe your ideas regarding the management of group communication in the Public Safety environment. |
| 3. | Please describe your ideas regarding the possibility of broadcasting voice services and data for public safety. |
| 4. | Please describe where your capability and solution fits into our 11 objectives.  Please read our objectives here: <https://www.broadway-info.eu/?da_image=750> |

**Application Eco-system**

|  |  |
| --- | --- |
| 1. | Briefly set out how you would design/architect mobile Mission Critical services to allow users from multiple agencies (e.g, Fire Departments ) access to, for example, an incident report. |
| 2. | Please describe the principles on how to secure access from Mission Critical mobile device to Mission Critical Backbone services, Intranet and internet, PPDR agencies, social media, news etc. |
| 3. | Have you developed Mission Critical services on any existing commercial 3G, 4G, or LTE network?Y/N If you answered "Y", please provide details including the location where the service is deployed. |
| 4. | On which types of devices are your services supported (smartphone, tablet, notebook)? |
| 5. | Please provide an information on which platforms your applications work (e.g. Android, iOS, Windows). |
| 6. | Please provide your view on which object level data protocols should be supported by Mission Critical services. |
| 7. | What is your view on the formation of pan-European public safety App-store? |
| 8. | Have you implemented Mission Critical services over existing broadband mobile networks? Y/N  If you answered "Y", please describe how. If you answered "N", do you have any plans to implement? |

**Innovation Eco-system**

|  |  |
| --- | --- |
| 1. | Please describe your (a) current and (b) future plans for innovation to support public safety broadband. |
| 2. | Are any of your innovations in broadband technology in operational use in the public safety or in private industry? Y/N  If you answered "Y", please describe further. |
| 3. | Do you know of any intellectual property issues (e.g. patents) which may block the use of open standards for Mission Critical broadband? If you answered "Y", please explain. |

**Test Equipment Supplier**

**Coverage of test and validation process**

|  |  |
| --- | --- |
| 1. | Please tick the box beside the technologies which you test and validate:  For 3GPP explanations, please find specifications and definitions here:  3GPP Mission Critical Specs  ETSI Terms and Definitions Database Interactive (TEDDI) |
| Mission Critical Device (MC Device) |
| Mission Critical Push to Talk (MC PTT) |
| Proximity Services (ProSe) |
| Mission Critical Video (MC Video) |
| Mission Critical Data (MC Data) |
| Isolated Operation for Public Safety (IOPS) |
| evolved Multimedia Broadcast Multicast Service (eMBMS) |
| Mission Critical broadband service roaming with prioritisation and pre-emption (INT-OP) |
| End 2 End Encryption (EE2E) |
| Internet of Things (IoT), or Internet of :Public Safety Things (IoPST) |
| Mission Critical Mobile broadband networks (MC-NW) |
| Air - Ground - Air (AGA) |
| 2. | In your view, are there additional technologies or part of technologies which should be also validated? Y/N  If you answered "Y", please provide details. |
| 3. | Do you follow a standardised validation system? Y/N  If you answered "Y", which standards are followed. |
| 4. | In your opinion, is there something which does not require technical validation? Y/N  If you answered "Y", please provide details. |

|  |  |
| --- | --- |
| 5. | Please provide information on which 3GPP releases for which you do testing and validation on, by clicking in the matrix below:  For 3GPP explanations, please find specifications and definitions here:  3GPP Mission Critical Specs  ETSI Terms and Definitions Database Interactive (TEDDI)  Our terms: |
|  |
| 6. | Do you test any RAN technologies? Y/N  If you answered "Y", which RANs do you test? |

|  |  |
| --- | --- |
| 7. | If you validate the following, please tick the box. |
| Security |
| Reliability |
| Availability in different load situations |
| Immunity for interferences |
| Data transfer rate |
| Delay |
| Coverage |
| Compatibility and Interoperability |
| Usability |
| Energy consumption |
| System management |
| Priority and Pre-emption |
| Devices and Applications |
| Interworking with legacy systems |
| Please provide any further details. |
| 8. | Please describe your opinion on any test and validation areas that have not been covered in previous questions in this questionnaire. |
| 9. | Do you know of any test references which should be taken into account in order for BroadWay to achieve its objectives? Y/N  Please read our objectives here: <https://www.broadway-info.eu/?da_image=750>  If you answered "Y", please provide details. |
| 10. | Please give references to relevant test specifications or processes (a) already defined or (b) in the process of being defined. |

**Security assurance**

|  |  |
| --- | --- |
| 1. | Please give your opinion on the type of cyber attacks which could occur on the integrated SpiceNet system. |
| 2. | Please describe your view on which Common Criteria EAL level a solution should be compliant with in order to be adopted for software and system quality, for use by public safety practitioners. |
| 3. | Please describe your view on how to test end to end solutions for security purposes. |

**Test and validation environment**

|  |  |
| --- | --- |
| 1. | Please describe your view on how extensive validation tests should be (lab, room, building, residential area / interior and exterior, vehicles). |
| 2. | Please give references to standards used on harsh environment testing (testing in extreme conditions- temperature, humidity, harsh conditions, humidity...). |
| 3. | Please provide references to standard test methodologies that we should consider for use (test design, test execution, test quality assurance processes). |
| 4. | Please give your opinion on scenario-specific testing (eg. indoor, high speed, air ground air). |
| 5. | Please provide your opinion on the use of simulated and emulated functionality during prototype testing and pilot evaluation. |
| 6. | Please give your opinion on the effectiveness of compatibility tests with different manufacturers. |
| 7. | Please provide your view on networked test and validation where testing can be carried out on different facilities. |
| 8. | Please provide your opinion regarding the kind of security accreditation levels that should be required for a test and validation centre. |

**Reliability and impartiality of validation**

|  |  |
| --- | --- |
| 1. | Please give your opinion how would you handle independant and impartial validation both in terms of (a) functional testing and (b) security assurance. |
| 2. | Please provide your views on the logistical limitations of test and validation on live commercial mobile networks at TRL8. |

**Communication Software Test Stack Developer**

**Coverage of test and validation process**

|  |  |
| --- | --- |
| 1. | Please tick the box beside the technologies which you test and validate:  For 3GPP explanations, please find specifications and definitions here:  3GPP Mission Critical Specs  ETSI Terms and Definitions Database Interactive (TEDDI) |
| Mission Critical Device (MC Device) |
| Mission Critical Push to Talk (MC PTT) |
| Proximity Services (ProSe) |
| Mission Critical Video (MC Video) |
| Mission Critical Data (MC Data) |
| Isolated Operation for Public Safety (IOPS) |
| evolved Multimedia Broadcast Multicast Service (eMBMS) |
| Mission Critical broadband service roaming with prioritisation and pre-emption (INT-OP) |
| End 2 End Encryption (EE2E) |
| Internet of Things (IoT), or Internet of :Public Safety Things (IoPST) |
| Mission Critical Mobile broadband networks (MC-NW) |
| Air - Ground - Air (AGA) |
| 2. | In your view, are there additional technologies or part of technologies which should be also validated? Y/N  If you answered "Y", please provide details. |
| 3. | Do you follow a standardised validation system? Y/N  If you answered "Y", which standards are followed. |
| 4. | In your opinion, is there something which does not require technical validation? Y/N  If you answered "Y", please provide details. |

|  |  |
| --- | --- |
| 5. | Please provide information on which 3GPP releases for which you do testing and validation on, by clicking in the matrix below:  For 3GPP explanations, please find specifications and definitions here:  3GPP Mission Critical Specs  ETSI Terms and Definitions Database Interactive (TEDDI)  Our terms: |
|  |
| 6. | Do you test any RAN technologies? Y/N  If you answered "Y", which RANs do you test? |

|  |  |
| --- | --- |
| 7. | If you validate the following, please tick the box. |
| Security |
| Reliability |
| Availability in different load situations |
| Immunity for interferences |
| Data transfer rate |
| Delay |
| Coverage |
| Compatibility and Interoperability |
| Usability |
| Energy consumption |
| System management |
| Priority and Pre-emption |
| Devices and Applications |
| Interworking with legacy systems |
| Please provide any further details. |
| 8. | Please describe your opinion on any test and validation areas that have not been covered in previous questions in this questionnaire. |
| 9. | Do you know of any test references which should be taken into account in order for BroadWay to achieve its objectives? Y/N  Please read our objectives here: <https://www.broadway-info.eu/?da_image=750>  If you answered "Y", please provide details. |
| 10. | Please give references to relevant test specifications or processes (a) already defined or (b) in the process of being defined. |

**Security assurance**

|  |  |
| --- | --- |
| 1. | Please give your opinion on the type of cyber attacks which could occur on the integrated SpiceNet system. |
| 2. | Please describe your view on which Common Criteria EAL level a solution should be compliant with in order to be adopted for software and system quality, for use by public safety practitioners. |
| 3. | Please describe your view on how to test end to end solutions for security purposes. |

**Test and validation environment**

|  |  |
| --- | --- |
| 1. | Please describe your view on how extensive validation tests should be (lab, room, building, residential area / interior and exterior, vehicles). |
| 2. | Please give references to standards used on harsh environment testing (testing in extreme conditions- temperature, humidity, harsh conditions, humidity...). |
| 3. | Please provide references to standard test methodologies that we should consider for use (test design, test execution, test quality assurance processes). |
| 4. | Please give your opinion on scenario-specific testing (eg. indoor, high speed, air ground air). |
| 5. | Please provide your opinion on the use of simulated and emulated functionality during prototype testing and pilot evaluation. |
| 6. | Please give your opinion on the effectiveness of compatibility tests with different manufacturers. |
| 7. | Please provide your view on networked test and validation where testing can be carried out on different facilities. |
| 8. | Please provide your opinion regarding the kind of security accreditation levels that should be required for a test and validation centre. |

**Reliability and impartiality of validation**

|  |  |
| --- | --- |
| 1. | Please give your opinion how would you handle independant and impartial validation both in terms of (a) functional testing and (b) security assurance. |
| 2. | Please provide your views on the logistical limitations of test and validation on live commercial mobile networks at TRL8. |

**Testing Services**

**Coverage of test and validation process**

|  |  |
| --- | --- |
| 1. | Please tick the box beside the technologies which you test and validate:  For 3GPP explanations, please find specifications and definitions here:  3GPP Mission Critical Specs  ETSI Terms and Definitions Database Interactive (TEDDI) |
| Mission Critical Device (MC Device) |
| Mission Critical Push to Talk (MC PTT) |
| Proximity Services (ProSe) |
| Mission Critical Video (MC Video) |
| Mission Critical Data (MC Data) |
| Isolated Operation for Public Safety (IOPS) |
| evolved Multimedia Broadcast Multicast Service (eMBMS) |
| Mission Critical broadband service roaming with prioritisation and pre-emption (INT-OP) |
| End 2 End Encryption (EE2E) |
| Internet of Things (IoT), or Internet of :Public Safety Things (IoPST) |
| Mission Critical Mobile broadband networks (MC-NW) |
| Air - Ground - Air (AGA) |
| 2. | In your view, are there additional technologies or part of technologies which should be also validated? Y/N  If you answered "Y", please provide details. |
| 3. | Do you follow a standardised validation system? Y/N  If you answered "Y", which standards are followed. |
| 4. | In your opinion, is there something which does not require technical validation? Y/N  If you answered "Y", please provide details. |

|  |  |
| --- | --- |
| 5. | Please provide information on which 3GPP releases for which you do testing and validation on, by clicking in the matrix below:  For 3GPP explanations, please find specifications and definitions here:  3GPP Mission Critical Specs  ETSI Terms and Definitions Database Interactive (TEDDI)  Our terms: |
|  |
| 6. | Do you test any RAN technologies? Y/N  If you answered "Y", which RANs do you test? |
| 7. | If you validate the following, please tick the box. |
| Security |
| Reliability |
| Availability in different load situations |
| Immunity for interferences |
| Data transfer rate |
| Delay |
| Coverage |
| Compatibility and Interoperability |
| Usability |
| Energy consumption |
| System management |
| Priority and Pre-emption |
| Devices and Applications |
| Interworking with legacy systems |
| Please provide any further details. |
| 8. | Please describe your opinion on any test and validation areas that have not been covered in previous questions in this questionnaire. |
| 9. | Do you know of any test references which should be taken into account in order for BroadWay to achieve its objectives? Y/N  Please read our objectives here: <https://www.broadway-info.eu/?da_image=750>  If you answered "Y", please provide details. |
| 10. | Please give references to relevant test specifications or processes (a) already defined or (b) in the process of being defined. |

**Security assurance**

|  |  |
| --- | --- |
| 1. | Please give your opinion on the type of cyber attacks which could occur on the integrated SpiceNet system. |
| 2. | Please describe your view on which Common Criteria EAL level a solution should be compliant with in order to be adopted for software and system quality, for use by public safety practitioners. |
| 3. | Please describe your view on how to test end to end solutions for security purposes. |

**Test and validation environment**

|  |  |
| --- | --- |
| 1. | Please describe your view on how extensive validation tests should be (lab, room, building, residential area / interior and exterior, vehicles). |
| 2. | Please give references to standards used on harsh environment testing (testing in extreme conditions- temperature, humidity, harsh conditions, humidity...). |
| 3. | Please provide references to standard test methodologies that we should consider for use (test design, test execution, test quality assurance processes). |
| 4. | Please give your opinion on scenario-specific testing (eg. indoor, high speed, air ground air). |
| 5. | Please provide your opinion on the use of simulated and emulated functionality during prototype testing and pilot evaluation. |
| 6. | Please give your opinion on the effectiveness of compatibility tests with different manufacturers. |
| 7. | Please provide your view on networked test and validation where testing can be carried out on different facilities. |
| 8. | Please provide your opinion regarding the kind of security accreditation levels that should be required for a test and validation centre. |

**Reliability and impartiality of validation**

|  |  |
| --- | --- |
| 1. | Please give your opinion how would you handle independant and impartial validation both in terms of (a) functional testing and (b) security assurance. |
| 2. | Please provide your views on the logistical limitations of test and validation on live commercial mobile networks at TRL8. |

**Security assurance**

**Coverage of test and validation process**

|  |  |
| --- | --- |
| 1. | Do you follow a standardised security assurance process ? Y/N If you answered "Y", which standards are followed. Amongst this/these standard(s), is there anything, in your opinion, that does not require security assurance? |
| 2. | Have you carried out security assurance?  If you answered "Y", on which 3GPP releases. |
| 3. | Please describe your opinion on the most important security assurance issues related to our challenge. Please read about our common challenge here: <https://www.broadway-info.eu/challenge/> |
| 4. | Please give references to relevant security assurance specifications or processes already defined or in the process of being defined. |

**Security assurance**

|  |  |
| --- | --- |
| 1. | Please give your opinion on the type of cyber attacks which could occur on the integrated SpiceNet system. |
| 2. | Please describe your view on which Common Criteria EAL level a solution should be compliant with in order to be adopted for software and system quality, for use by public safety practitioners. |
| 3. | Please describe your view on how to test end to end solutions for security purposes. |

**Test and validation environment**

|  |  |
| --- | --- |
| 1. | Please describe yout view on how extensive security assurance tests should be (lab, room, building, residential area / interior and exterior, vehicles). |
| 2. | Please provide references to standard security assurance methodologies that we should consider for use (test design, test execution, test quality assurance processes). |
| 3. | Please provide your view on networked test and validation where testing can be carried out on different facilities. |
| 4. | Please provide your opinion regarding the kind of security accreditation levels that should be required for a test and validation centre. |

**Reliability and impartiality of validation**

|  |  |
| --- | --- |
| 1. | Please give your opinion how would you handle independant and impartial validation both in terms of (a) functional testing and (b) security assurance. |
| 2. | Please provide your views on the logistical limitations of test and validation on live commercial mobile networks at TRL8. |

**Practitioner Evaluation Support**

|  |  |
| --- | --- |
| 1. | Please briefly describe the principles/models/algorithms that you follow for non-functional evaluation to support public safety practitioner acceptance. |

**Your work is complete !!**

**Many thanks for your contribution !!**

We currently aim to release a contract notice and invitation to tender towards the end of 2018. We encourage you to build your teams and prepare early. If you have any questions, please post those through the BroadWay website by clicking here.

**Ongoing Dialogue for Innovation**

PSCE encourages the ongoing discussion regarding innovation for future Public Saftey Communication. Please join us at our next conference which will be held in:

Bled, Slovenia on 4-6th December 2018.

www.psc-europe.eu

Please consider becoming a member or sponsor of PSCE. It's not expensive...

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.