Critical communications
for all professional users

Follow us on @TCCAcritcomms

October 2021

TCCA White Paper

Mission-Critical Broadband Device Procurement

First issued by TCCA's Critical Communications Broadband Group, October 2021

The Grainger Suite, Dobson House, Regent Centre,
Gosforth, Newcastle NE3 3PF, UK
T +44 (0) 191 231 4328 E admin@tcca.info

TCCA Limited is a company incorporated under the Companies Act in England and Wales, company number 04155039.
Registered office: The Grainger Suite, Dobson House, Regent Centre, Gosforth, Newcastle NE3 3PF, UK

Table of Contents

Executive summary

Today’s PPDR (Public Protection and Disaster Relief) devices are still mostly built on narrowband technologies, providing mission-critical voice and short messaging services. These services are often available within nationwide PPDR network coverage, utilising dedicated frequency bands.

The narrowband PPDR device ecosystem is well established, including infrastructure and terminal suppliers, system integrators, service providers and resellers. From a device procurement perspective, there are existing frame agreements in place. The solution costs are well known, device lifecycles are long, and there are no major changes in the product specifications. Finally, TCCA’s TETRA interoperability (IOP) process allows for multi-vendor procurement.

Now, as the PPDR industry is transitioning to a new era with the adoption of 4G and 5G broadband communications, there are several issues that need to be considered. In addition, from the procurement perspective, the transition to mission-critical broadband will require a series of well-planned steps.

Bringing devices to market that support these new device technologies, and meet various PPDR requirements, will require investments by the vendors, as well as commitment from customers in terms of development support, minimum order quantities, user testing and acceptance, etc.

Many current procurement models also allow device purchases from other sources. User organisations can run their own procurements, broadband devices can be leased from IT service companies, or even purchased by individual employees (BYOD - Bring Your Own Device).

Device and OS/software lifecycles of modern broadband devices are short compared to LMR/PMR radios, even though vendors are doing their best to extend them. The current procurement, testing, certification and approval processes required for PPDR usage therefore need to be adapted accordingly.

At the same time, the vendors must be able to provide information on their existing capabilities and present a roadmap that shows how they plan to meet the evolving customer needs and requirements throughout the contract period.

As in any change there is room for improving the status quo. We should look back on what has been working well and what has been a problem, and then try to find a better way forward.

The aim of this TCCA white paper is to provide a holistic overview of PPDR broadband device related requirements, to list the main topics and issues to be considered, as well as provide recommendations for a successful procurement. Hence this paper is mainly written to address public safety organisations who are planning new device procurements.

Introduction

This white paper is focusing on PPDR broadband device procurement. This topic is very large and complex, for example technical device requirements alone could easily fill hundreds of pages.

Therefore, we have made some omissions to keep the document focused and easier to digest. The main question in all discussed topics has been: “How does it affect the PPDR device procurement?”

The categories of PPDR broadband devices considered in this white paper are:

- Handsets and tablets.
- Vehicle devices.

The procurement of mission-critical applications and accessories is not included in this white paper. However, their impact on the device procurement and technical requirements is considered.

Similarly, even though the PPDR narrowband and broadband systems will continue to co-exist for many years, and in many countries there will be a gradual transition, we have focused on broadband devices and their functionalities. Therefore we have excluded some of the details of hybrid devices and LMR/PMR interworking solutions from the document scope. They are a topic for further research, and another white paper.

Finally, the reader should note that the relevance and priority of the different requirements described in this white paper will vary, depending on the specific needs of individual PPDR organisations or user groups. Requirements that are mandatory for some organisations may be optional or not even relevant to other organisations.

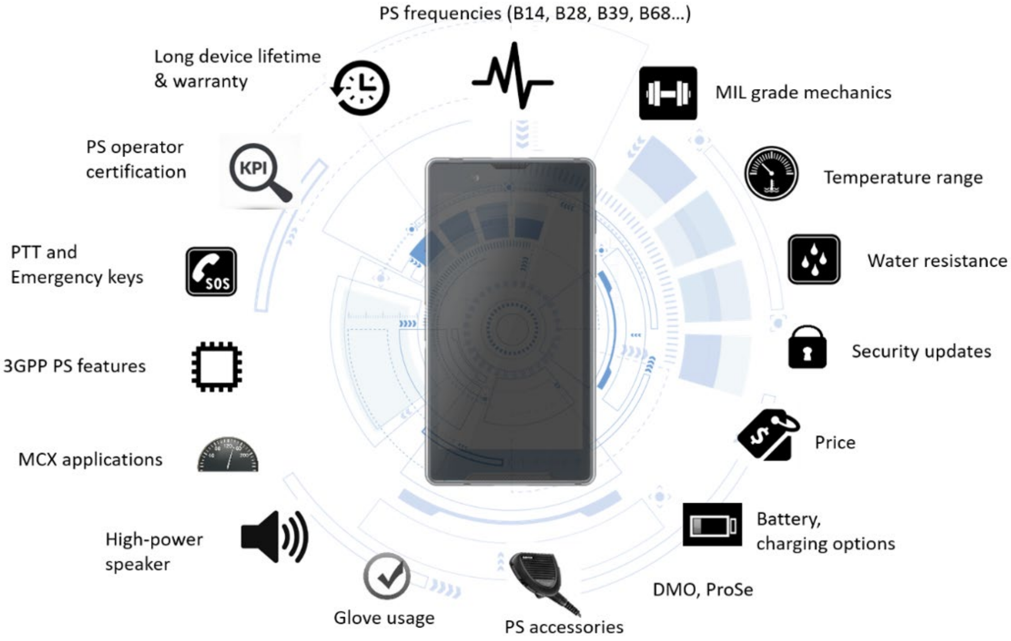


Figure 1: Typical MC broadband device requirements

It is expected that PPDR organisations will use the list of requirements in the graphic as a basis to create their own device procurement specifications, selecting what is relevant, ignoring what is not applicable and adding their own specific needs where appropriate.

Wherever possible this white paper will reference external sources and initiatives to maximise the longevity of the document.

1 Operational needs, technical requirements

This chapter describes the technical and operational requirements that PPDR organisations - user groups and network operators - should consider when procuring mission-critical broadband devices.

1.1 User Requirements

An essential part of creating a mission-critical device procurement specification is to fully understand the user needs. The user community will consist of multiple groups, each with its specific requirements and operational processes.

Once the distinct user groups have been identified, close engagement will be necessary to fully understand their use cases and device requirements. This may be achieved via interviews, questionnaires, workshops, etc. It is likely that the diverse needs can be grouped to simplify analysis.

When describing their use cases and requirements it is important that the user groups look ahead to how the new broadband technology will transform and enhance their operations. Functionality delivered by existing LMR/PMR systems is the reference, but users should not just focus on replicating the voice and messaging functionality and reliability of their existing narrowband system. The evolution from a voice-centric to a data-dominated working environment requires considerable investment in business process redesign.

It is also very important that the user groups fully describe their use cases, covering:

- Type, frequency, and duration of event.
- Other organisations involved.
- The location and operating environment – understanding the coverage scenarios.
- What level of availability/QoS will be expected?

- How will the device be used, worn, carried or installed within a vehicle?
- Do users wear gloves? What type of gloves?
- What are the associated voice and data communications?
- What apps will be used?
- Will video applications be required? These have significant impact on screen, battery and camera for example.
- What is the likely data bandwidth requirement?
- What accessories are required – e.g. RSMs (Remote Speaker Microphone) and helmet microphones.
- When installed within a vehicle, what vehicle communication systems will the device need to interface to?
- Are devices individually allocated or shared in a pool?
- What level of interoperability with legacy devices/systems is required?
- Will direct mode (device-to-device) communication be required? How often? What communication range is required?
- Will roaming (national and international) be necessary?

Analysis of use cases could include also other segments beyond PPDR such as transport, utilities, and manufacturing. As the underlying technology becomes more affordable more user groups will start using it. For example, one may need to consider the mobility requirements in high-speed train and aircraft (AGA, air-ground-air) communications, which are likely to impact network and device specifications.

Typical PPDR broadband services include:

- Mission-critical PTT.
- Messaging, operational status, broadcast.
- Emergency call/alert.
- Video push and pull.
- Geolocation.
- Database queries.
- Multiple file exchange.
- Workflow applications.
- Off-network, direct mode use.
- Supervisory Override.
- Ambient listening.

Purchasing organisations should detail their specific local operational requirements. For example, the requirement to combine a PTT and phone call so that during a phone call it is possible to listen to the PTT conversation simultaneously. The device should support flexibility to decide the priority of phone calls/PTT calls. In practice this priority will be determined by PPDR policy: in the UK the ESN policy is to prioritise PTT calls over phone calls.

Analysis of the operational use cases will identify and define the user requirements to be included in the device procurement specification. The following sections summarise some key requirements.

1.1.1 Device Categories

The operational use cases will help to define the different device categories and form factors required by the user groups. These device categories may include:

- Non-rugged smartphone (e.g. covert police users).
- Rugged smartphone (e.g. firefighters).
- Feature phone (physical buttons, small non-touch display).
- ATEX (ATmosphères EXplosibles) / intrinsically safe variants.

- Dual-mode (i.e. TETRA/LTE/5G) variants.
- Vehicle devices (cars, vans, trains, aircraft, motorcycles, boats).
- Fixed devices (not a focus of this white paper).

1.1.2 Physical Requirements

The range of device physical requirements will depend on the user groups and use cases – some examples of typical considerations include:

- Environmental specifications - e.g. water and dust Ingress Protection (IP). The specific use cases will determine the most appropriate IP rating (as defined by IEC standard 60529 or CENELEC EN 60529). For example, the water/rain protection requirement will be different for a first responder on foot compared to on a motorcycle.
- Ruggedness – e.g. drop and impact testing – compliance with appropriate Military Standards (MIL STDs).
- Operating and storage temperature ranges.
- Minimum screen size.
- Internal storage and memory card capacity.
- Audio specification / speaker output (dBm).
- Portability, carrying options.
- Glove usage and wet-screen operation.
- Dedicated PTT & emergency buttons.
- External / configurable buttons.
- Dual-SIM, eSIM, iSIM.
- Camera - used instead of, or in conjunction with, body-worn cameras. Evidence-quality or nice-to-have?
- High-power user equipment (HPUE)
- Batteries:
  - Battery life – how long will a battery last before it needs to be re-charged/swapped.
  - Battery swapping / charging / reconditioning mechanism.
  - Battery lifecycle – when will a new battery need to be purchased.
  - Accessory battery life must also be considered.
  - ATEX (which specific zones are required?). Other Intrinsically Safe standards?
- RF performance in defined use cases - e.g. how does the device perform when is it is worn/carried on the body.
- Accessory connectors and specialist accessories. Will the device become the hub at the centre of a Private Area Network (PAN)?
- Specialist requirements – e.g. IR camera, scanner.
- Sensors – e.g. accelerometers for man-down alerting, barometric sensor for enabling in-building vertical positioning.
- Vehicle-based devices have specific considerations:
  - Vehicle-specific standards (e.g safety).
  - Vehicle powering, mounting and cabling.
  - External antenna connection, HPUE option.
  - Physical controls, peripheral interfaces (screens, keyboards, loudspeakers).
  - Specialist accessories – e.g. microphones, buttons and displays.
  - Connectivity to vehicle communication bus (CANbus).

It is recommended that PPDR organisations should focus on WHAT is required, rather than specifying HOW the requirement should be met by device vendors – there may be multiple innovative ways to meet a requirement and all should be considered. Procurers may also capture future requirements (and likely timing) for supplier device roadmap consideration.

1.1.3 Voice Quality

Speech will continue to be the most effective and efficient method of communication for first responders at the scene of incident – it is essential that their devices deliver high-quality audio performance. The reference for audio quality has been set by LMR/PMR devices which have evolved to provide very high levels of speech intelligibility, even in extreme environments. As a minimum, mission-critical broadband devices must provide the same high levels of audio quality. To fully evaluate audio quality, the following factors must be considered, and tested together with the MCX (collectively for MCPTT, MCVideo and MCData) application:

- **Speech intelligibility:** Mean Opinion Score (MOS) algorithms are traditionally used to assess the quality of audio transmissions. However, MOS scores (e.g. 3.5 is a typical score achieved by VoLTE) are not considered sufficient for assessing speech intelligibility in PPDR use cases where background noise is encountered.
- **Audio loudness:** the loudness of the device audio output is another important consideration – PPDR users typically demand mission-critical devices that can deliver a minimum audio loudness of 100dB with low distortion.
- **Howling suppression:** when multiple devices are operating in close proximity, positive feedback can cause screeching or howling that can disrupt communications when lives are on the line. It is important that mission-critical devices and/or applications support howling suppression to ensure clear, uninterrupted voice communications.
- **Background noise cancellation:** first responders typically operate in noisy environments – e.g. sirens, crowds, engines and wind. Mission-critical devices must therefore incorporate background noise cancellation (typically utilising multiple microphones and digital signal processing) to eliminate unwanted background noises and allow listeners to clearly understand voice communications.
- **High audio quality in carry case/holster:** in many PPDR use cases, the device will be used within a case or holster for most of the time – the carry solution must not comprise the audio quality. The device and carry solution must be designed to optimise audio quality.
- **High audio quality when using accessories:** audio quality must not be compromised when using accessories such as headsets and remote speaker microphones.

1.1.4 RF Performance

Good RF performance is an important requirement for mission-critical devices to maximise coverage and availability. For hand-held devices operating on frequencies below 1GHz it is advised that the device has an external antenna to improve RF performance. Also, to enable the use of an accessory incorporating its own antenna – e.g. a speaker microphone or vehicle mounting kit - an antenna port may be provided on the device.

An external antenna interface should also be provided on vehicle-mounted devices.

1.1.5 Location services

In an emergency situation every second counts – it is crucial to get information about the specific location of the incident, proximity of other first responders as well as tracking of mission-critical assets (e.g. fleet management of drones and vehicles).

There are various technologies and methods that are already in use, from GNSS positioning to network assisted methods and indoor location services. Some of them are implemented in the device hardware, while some are utilising software algorithms, dedicated beacons or network services. What is common is that their use and importance are expected to grow in the future.

The upcoming 5G networks may allow positioning accuracy down to centimetre range, which is important for many use cases such as autonomous vehicles and smart factories. For handheld devices the positioning is based on collecting and combining information from GNSS, WiFi and 4G/5G networks.

When it comes to mission-critical broadband device procurement, especially if the user requirements are not clear, the vendors should be asked details of which location services they have tested, and which they are/will be able to support.

3GPP compliance is discussed in Chapter 2 of this document. However, it should be noted here that the mission-critical devices shall support 3GPP features for LCS (Location Services), including compliance with mandatory emergency call requirements.

At the time of publication of this white paper (October 2021), work is still ongoing within 3GPP related to many mission-critical-specific requirements. The upcoming 3GPP Release 17 will introduce new LCS features and improved performance. The first product implementations are expected in 2024/2025 timeframe.

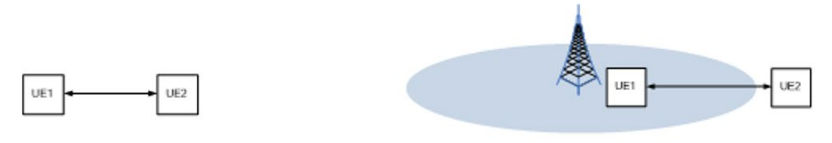
3GPP compliance is ensured by conformance and regulatory testing, described in Chapter 2.

1.1.6 Off-network Communications

The ability to maintain mission-critical communications, even when broadband network coverage is not available, is an essential requirement for PPDR users. In existing LMR/PMR systems, off-network communication is supported by Direct Mode Operation (DMO), where the devices can communicate directly on dedicated channels, without the need for network infrastructure.

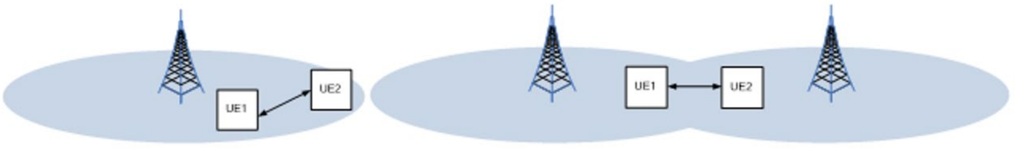
DMO is used extensively by fire-fighters and specialist police users who routinely operate in locations and environments where network coverage cannot be assured. DMO provides essential fallback communications for all users when the network is not operational. Devices may also operate in gateway mode, where an on-network device provides connectivity to nearby off-network devices. The requirements for off-network communications will not change with the migration to broadband technologies.

The 3GPP specifications define four scenarios for device to device (D2D) proximity-based services (ProSe) as shown in the diagram below.



(a) Scenario 1A

(b) Scenario 1B



(c) Scenario 1C

(d) Scenario 1D

Figure 8.3.1-1 D2D Scenarios

Scenarios	UE1	UE2
1A: Out-of-Coverage	Out-of-Coverage	Out-of-Coverage
1B: Partial-Coverage	In-Coverage	Out-of-Coverage
1C: In-Coverage-Single-Cell	In-Coverage	In-Coverage
1D: In-Coverage-Multi-Cell	In-Coverage	In-Coverage

Figure 2; From 3GPP TR 36.843 V12.0.1 (2014-03) "3rd Generation Partnership Project; Technical Specification Group Radio Access Network; Study on LTE Device to Device Proximity Services; Radio Aspects (Release 12)"

At the time of publication, device-to-device (D2D) proximity-based Services (ProSe), as defined in the 3GPP specifications, is not seen as a valid option for PPDR off-network operation due primarily to:

- Limited communication range. Broadband devices operate with lower transmit power and (typically) in higher frequency bands than LMR/PMR devices – this means significantly reduced communication range.
- Limited availability of chipsets and devices supporting ProSe on the market.

TCCA is providing inputs and driving mission-critical specific enhancements to the 3GPP device-to-device specifications but these will not be available in the mid-term. Hence alternative methods of providing mission-critical off-network communications must be considered. Communication in the absence of network coverage must not compromise the high levels of availability, security and quality of service demanded by PPDR users – the following bullet points highlight the key considerations:

- **Communication range*:** From practical experience, the maximum RF coverage performance required for DMO is approximately 250 metres for most localised communication applications and 1 km for major incidents (with repeaters).
- **Quality of Service:** to ensure availability of mission-critical off-network communication channels it is strongly recommended that privately-owned spectrum is utilised. Availability and lack of interference cannot be assured with solutions based on shared unlicensed spectrum.
- **Security:** the off-network communications must remain encrypted.

**From TCCA website: https://tcca.info/tetra/direct-mode-operation-dmo/*

There are several different technical options to achieve DMO functionality in conjunction with broadband devices. Taking into considering the points above, it is recommended that LMR/PMR technologies provide the optimal method for providing off-network communications for voice and SDS. i.e.:

- TETRA, P25, Digital Mobile Radio (DMR) and Tetrapol.

Alternative wireless communications technologies such as WiFi and Bluetooth have been discounted primarily due to range limitations. It should be noted that other (proprietary) solutions exist but are not recommended as they would not facilitate a multi-vendor ecosystem.

There are different options available for utilising LMR/PMR technologies with broadband devices:

- First responders carry two independent devices – broadband and LMR/PMR – as they typically do today.
- Utilise converged hybrid broadband/LMR/PMR devices
- Deploy collaborative devices – i.e. an LMR/PMR device that communicates intelligently with the broadband devices. The LMR/PMR device could be configured as an accessory to the broadband device – e.g. a Remote Speaker Mic (RSM) with integrated LMR/PMR technology.

To select the optimal broadband/LMR/PMR option, the specific use cases of individual user communities must be well understood - for example would the LMR/PMR technology start DMO mode automatically when the broadband connection is lost, and will it revert back to LTE/5G when the connection is re-established? The total cost of ownership of the different options must also be carefully assessed.

1.2 PPDR Network Requirements

Many of the device technical requirements are driven by the implementation and configuration of the specific PPDR broadband network.

1.2.1 Spectrum

There have been considerable efforts to harmonise the allocation and use of PPDR broadband frequencies, but at the time of publication spectrum requirements still vary from country to country. Depending on the deployment model adopted by the PPDR operator, the spectrum to be utilised will be one of the following:

- Private frequency bands allocated exclusively for PPDR use.
- Shared commercial frequency bands allocated for PPDR use.
- A combination of private and commercial frequency bands.

Where dedicated PPDR spectrum has been allocated, mission-critical devices will be required to operate in these specific frequency bands.

Revised Resolution 646 adopted by ITU WRC-2015 recognised 694-894MHz (700-800) as the globally harmonised frequency range for broadband PPDR. This includes:

- 700MHz LTE bands – 3GPP bands 14, 28 & 68.
- 800MHz LTE bands – 3GPP bands 20 & 26.

See: http://www.itu.int/pub/R-ACT-WRC.12-2015/en

However, is should be noted that in Europe there is no harmonised spectrum exclusively for PPDR use. The 700MHz band has been harmonised for "terrestrial systems capable of providing wireless broadband electronic communications services and for flexible national use" – including PPDR. See the EU Commission Implementing Decsison (EU) 2016/687 https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A32016D0687

Other examples of 4G/5G frequency bands that have been allocated or considered for PPDR use currently include:

- B8, B31, B38, B43, B72, B87, B88, N78, N258.

Some of the bands mentioned above have yet to establish an ecosystem of chipsets, infrastructure and devices. This obviously creates a challenge for device procurement. Where feasible, the requirement for a specific band not currently supported by device/chipset suppliers should be defined as a future roadmap item, rather than an immediate mandatory requirement.

The requirement for country-specific bands may also mean higher device costs and limited choice of vendors. Individual PPDR operators and user groups do not constitute the necessary volumes for device and chipset suppliers to invest in providing support for customer-specific frequency bands. Hence a combined effort is required, coordinated for example by governments, national regulators and regional regulators (e.g. the European Commission) and industry bodies (e.g. TCCA) to consolidate demand.

A good example is the LTE frequency Band 14 in the US. In 2008 a dedicated 20MHz band of spectrum was licensed to the First Responder Network Authority (FirstNet) to create a nationwide public safety wireless broadband network. Initially there were concerns due to lack of compatible devices and LTE chipsets. However, the ecosystem began to build as the business case became apparent. The first compatible device prototype was announced in 2012, and today there are plethora of devices with Band 14 support, thanks to the growing number of FirstNet users, and support by commercial chipset vendors.

The use of unlicensed frequency bands is not considered a good option for mission-critical use due to the risk of interference and restricted transmit power. However, in future, in combination with an anchor in licensed bands, unlicensed bands may be a consideration to increase capacity.

1.2.2 PPDR network settings and features

Individual network settings may impact the choice of suitable devices – these settings include:

- Public Land Mobile Networks (PLMNs).
- Mobility & re-selection.
- Discontinuous reception (DRX).
- Evolved Multimedia Broadcast and Multicast Services (eMBMS).
- Voice over LTE (VoLTE) settings*.
- Voice over WiFi (VoWiFi) settings*.

** Note: VoLTE and VoWiFi settings are defined in GSMA TS.32 "Technical Adaptation of Devices through Late Customisation" available at: https://www.gsma.com/newsroom/resources/technical-adaptation-of-devices-through-late-customisation/*

PPDR network-specific settings are not configured in devices as standard; they require customisation and additional testing by the device vendors. PPDR operators should consider working with GSMA (potentially via TCCA) to ensure their network settings are included in the device library.

1.3 Compliance with Device Standards

Proven compliance with industry standards is key to an interoperable, multi-vendor device ecosystem. Mandatory compliance with the relevant device standards and specifications should be defined in the procurement specification. Examples of these are shown in the picture on the next page.

In addition to common device certifications and standards listed above, there may be regional, country-specific or customer-specific requirements depending on the device type and/or target environment. These include for example vehicle, aircraft, maritime and rail device approvals.

1.4 Mission-Critical Service Requirements

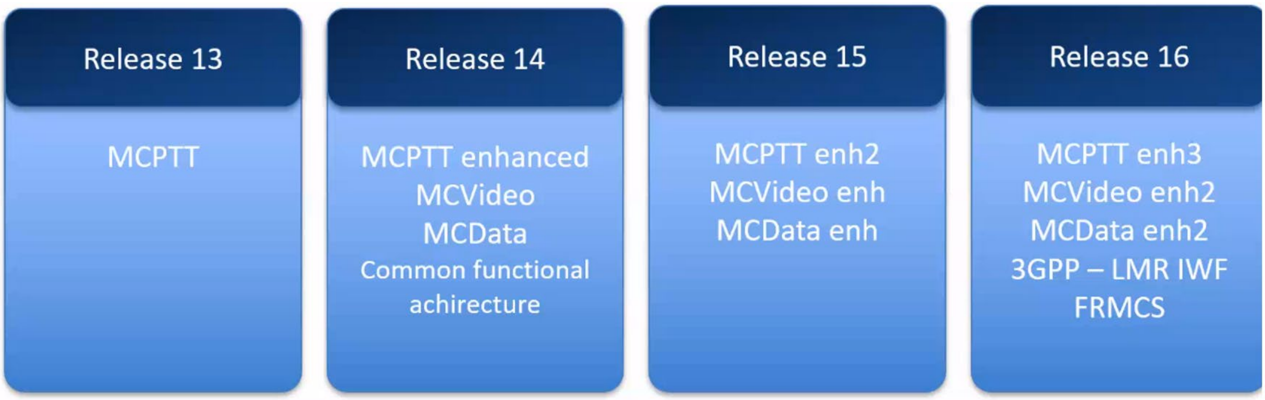
This section advises on the minimal 3GPP Release that should be supported by the mission-critical devices and highlights mission-critical specific 3GPP-defined requirements that must be supported.

1.4.1 3GPP Releases

3GPP unites several telecommunications standard development organisations (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC), and provides Reports and Specifications that define 3GPP technologies.

The 3GPP technologies are constantly evolving through a series of Releases. New features are ’functionality frozen’ and ready for implementation when a Release is completed. Once a new 3GPP Release has been published there will typically be a period of 12-36 months before compliant chipsets and devices become commercially available on the market. It is important to note that the roadmap to commercial availability is driven by demand – mission-critical features that are not mainstream – e.g. ProSe – may take even longer to become available.

It should also be noted that the hardware platform may support later Release software and applications – for example, mission-critical applications compatible with Release 13 or 14, are able to run on devices with Release 12 chipsets.



Release 13	Release 14	Release 15	Release 16
MCPTT	MCPTT enhanced MCVideo MCData Common functional achirecture	MCPTT enh2 MCVideo enh MCData enh	MCPTT enh3 MCVideo enh2 MCData enh2 3GPP – LMR IWF FRMCS

Mission-Critical Functionality Supported in 3GPP Releases

Further details on the 3GPP Releases are available at:

https://www.3gpp.org/specifications/67-releases

https://www.3gpp.org/news-events/1875-mc_services

1.4.2 Mission-Critical Quality of Service (QoS) Class Identifiers (QCIs)

Mission-critical services demand the highest levels of QoS and priority. 3GPP LTE networks utilise Quality of Service (QoS) Class Identifiers (QCIs) to ensure bearer traffic is allocated the appropriate QoS. Examples of the QoS parameters defined by the QCI include Guaranteed Bit Rate (GBR) or non-Guaranteed Bit Rate (non-GBR), Priority Handling, Packet Delay Budget and Packet Error Loss rate. Specific QCIs have been defined within 3GPP for MCX services - see the table within the appendices. It is essential that all elements of the broadband system, including the devices, are able to support these QCIs.

1.4.3 Mission-Critical PTT Key Performance Indicators (KPIs)

To ensure mission-critical PTT services achieve the same high levels of performance as existing LMR/PMR system, 3GPP defines specific Key Performance Indicators (KPIs) to ensure call access time and latency requirements are met. Therefore it is essential that all components of the broadband system can achieve these KPIs.

1.4.4 Evolved Multimedia Broadcast Multicast Services (eMBMS)

eMBMS (aka “LTE broadcast”) is a spectrally efficient means of supporting group calls and real-time video for mission-critical scenarios, especially when there are many first responders operating in the same area. Where eMBMS is implemented in the broadband network it is essential that the devices are also able to support this functionality.

1.5 Security

The importance of Cybersecurity has been well recognised in public safety, and its importance continues to grow as mission-critical devices are used to access government databases and handle sensitive information.

TCCA recommends that all public safety agencies have a cybersecurity policy in place. PSTA Cybersecurity Technical Subcommittee further reported that “users could take advantage of multi-layered mobile security solutions that can protect devices against online threats, malicious applications, and even data loss.” They also identified several key areas of focus for cybersecurity threat and mitigation, including updating OS, apps, and most recent security patches on mobile devices, and managing access through secure VPNs.

The following sections provide an example of device security topics that should be included in PPDR device procurement. As mentioned, details of these are subject to the cybersecurity policies and data classification requirements of the intended users.

Although accessories and device peripherals are beyond the scope of this document, the security around wireless connectivity technologies (e.g. Bluetooth) should be also be carefully considered where used. Wireless connections to microphones and headsets, for example, must not compromise the security of the overall device solution.

Hardware based security

Today, many professional LTE devices and commercial LTE chipsets readily support hardware “root of trust” in one way or another, which may be referred to as a Trusted Execution Environment (TEE), Secure Element (SE), security co-processor, secure enclave or sometimes TPM (Trusted Platform Module). These secure elements provide fundamental cryptographic services like true random number generation (TRNG) and secure key storage.

Secure elements also enable features like verified boot, operating system rollback prevention, runtime integrity checks, among others. They also enable secure memory storage for data-at-rest protection, and, in some cases, even physical tamper detection.

Hardware based security is not currently required by all PPDR user organisations, but at the same time it is becoming common even in COTS devices - either as part of processor (chipset) architecture and/or device vendor implementation. The vendors should be asked to provide information about their security solution.

Cryptographic compliance

Cryptographic libraries on the device provide functions that ensure the soundness of the device’s security implementation. The cryptographic libraries shall support required security algorithms (like AES, Advanced Encryption Standard) with sufficient key lengths (like AES-256). The key storage mechanisms, especially for asymmetric keys (like RSA, Rivest-Shamir-Adleman or elliptic curve ECDSA) should support key lengths that provide security for the targeted lifetime of the system and should increasingly consider quantum safety/resistance.

For users with high security level needs (e.g. Restricted, Confidential), the cryptographic libraries should also provide assurance that the implementation is of high quality. This assurance is typically provided in the form of third party evaluation of the cryptographic library implementation (e.g. FIPS 140-3, Federal Information Processing Standard).

In the device procurement the vendors should be asked to provide information on the cryptographic compliance, and whether / how it has been validated. It is also important to ensure that the MCX applications running on the device can fully utilise the cryptographic services that the device and the operating system provide.

Regulatory security compliance

In addition to the cryptographic libraries, the overall security of the device can be audited according to national or international approval criteria. Such approvals are typically carried out by national communication security authorities (NCSA) and they qualify the products to be used to handle national classified information according to certain classification level (such as Restricted or Confidential). Such approvals can also be accepted by international entities like the EU or NATO. Several countries also recognise Common Criteria (CC) evaluations as a basis for mobile device security. There is an ongoing planning to broaden the recognition of Common Criteria schemes in the EU, under the EUCC certification scheme (Common Criteria based European candidate cybersecurity certification scheme).

Security updates and monitoring

These include aspects like frequent security patching, operating system updates, firmware over the air (FOTA) updates and proper audit logging.

Enterprise Mobility Management (EMM)/(Mobile Device Management (MDM) support is discussed in Chapter 4. As recommended by organisations such as the UK National Cyber Security Centre data-in-transit protection for example in the form of VPNs should be considered as well.

Also other security tools and/or applications may be required to fully utilise fleet and mobile device management, data-in-transit protection and identity and access management (IAM). It is worthwhile ensuring that the device itself provides relevant enablers for these features and services.

Authentication

The users must provide credentials to access sensitive information on the device or applications. Typically they are requested to provide a PIN/password/pattern on the device user interface.

For mission-critical devices and applications the use of biometric sensors (face recognition, fingerprint recognition) and/or two-factor authentication (e.g. PIN code and NFC dongle) should be considered.

Also, the support for multi persona, e.g. through the use of Android for Work profiles or similar isolation techniques should be considered as a requirement. This is particularly important for use cases where classified and personal data are handled in the same device.

User authentication on devices that have no keypad or display requires special consideration – NFC tag, fingerprint or voice recognition may be viable options, depending upon the use case. Also, where devices are shared between users, individual authentication (login) may be deployed, although the user experience should not be negatively impacted.

1.6 Interoperability

Interoperability is a must for creating a healthy, competitive multivendor ecosystem. It is a wide topic, including standard compliance and testing, and hence it will be discussed in Chapter 2.

1.7 Operating System

All communications devices are controlled by an operating system, and each operating system has its own developer community and applications ecosystem. At the time of publication, many if not most PPDR broadband devices are using Android OS, which supports 3GPP compliant mission-critical applications.

Linux OS is used in some vehicle devices, as well as in wearables. With exception of FirstNet, Apple mobile operating system (iOS) is currently not used, due to lack of many mission-critical features and compatible MCX applications.

From a security perspective it is important to keep the device OS up to date. On the other hand, version control is required to ensure interoperability and consistent operation of PPDR devices and MCX applications. OS updating process and version control is therefore an essential part of device in-life management, discussed in Chapter 4.

OS testing is also a significant part of the overall PPDR device testing and certifications. For example, Google has CTS (compatibility test suite) and GMS (Google Mobile Services) test processes that ensure that Android devices are fully compatible with Android applications.

Even though Android is now the de-facto standard in most PPDR devices, there are some considerations that should be taken into account in device procurement / requirements:

- Google develops many new features into GMS and Android Enterprise that are not (at least initially) available in Android Open Source Project (AOSP).
- Many commercial apps and Google services rely on Google Play for updates, or they use other GMS services like Google Push. If they are not available the apps may need to be modified to use other service mechanisms, e.g. from an MDM system.
- Procurers should define if they require GMS or AOSP versions. The choice is mainly dependent on the level of security, control and privacy the end users need.

1.8 Accessories

Although accessory procurement is not within the scope of this white paper, accessory-related requirements must be understood and included in the device procurement specification where they directly impact the device – e.g. accessory connectors, Bluetooth version, etc.

Typical PPDR accessory requirements include:

- A range of securely attached wired and wireless accessories
- A standard set of accessories will normally include:
    - RSM with wired earphones.
    - Covert PTT button (e.g. kept in pocket or up sleeve, out of sight).
    - Earphones wired and/or wireless inc. microphone.
    - RSMs with 3 to 5 programmable buttons (e.g. PTT, Emergency, volume up/down, channel/talkgroup change and request-to-speak).
- Protective cases and carrying accessories.
- Belt clips, uniform mounts etc. to ensure secure attachment of devices to prevent loss and theft.
- Break protection for audio accessories to ensure that if a connection is lost between the accessory and device, communication will switch automatically to the device.
- Power banks, multi-unit chargers.
- Gooseneck microphones.

A certification process should be established for accessories such as Remote Speaker Microphones (RSMs) - each agency should establish accessory testing and certification processes and systems to ensure the appropriate accessories are used by front line personnel.

The requirements of wireline connections between a device and accessory need to be understood as these need to be ruggedised to provide fit for purpose performance in use in PPDR scenarios. Standard commercial connectors such as USB or 3.5mm jacks are usually not rugged and may cause damage to the device in heavy usage. Bluetooth wireless connectivity may be considered as a more convenient method of connecting accessories to devices but pairing and security challenges must be addressed.

Key Takeaways from Chapter 1

- The available spectrum will significantly impact device availability, choice and pricing. It is recommended that those PPDR organisations requiring devices which support unusual bands (e.g. B31) consolidate their requirements to drive supplier investment.
- Proven compliance with industry standards is key to an interoperable, multi-vendor device ecosystem. It is recommended that PPDR procurers demand compliance with 3GPP Release 12 as a minimum. Also, to ensure the devices can enable true mission-critical services they must support the mission-critical QCIs and KPIs.
- Devices must meet the demanding requirements of PPDR users - COTS devices will not provide mission-critical capability. For example, devices must be rugged, have dedicated PTT buttons, deliver exceptional voice quality and support long battery life.

- Currently the 3GPP standards do not define off-network solutions suitable for PPDR use cases – it is recommended that standards-based LMR/PMR technologies are used to provide mission-critical off-network communications for the mid-term until the 3GPP D2D ProSe specification matures.
- Cybersecurity is an essential requirement for the PPDR market. The potential vendors must be asked to provide information about their device security implementation, cryptographic compliance and possible certifications.

2 Testing and certification requirements

The starting point for PPDR device procurement should be that the devices meet "normal" international device standards and regulations, as described in section 1.3

A common testing/certification approach should follow regional or international standards.

There is of course still a possibility that local legislation is more stringent than regional/international regulations. In that case, local legislation should be followed (e.g. local SAR (Specific Absorption Rate) regulations).

There is a need for a transparent testing process that results in an interoperable, secure, and standard-compliant device ecosystem for the PPDR community.

The aim is to describe all the factors that will apply before a device can be considered as "approved" for mission-critical operations and services. The other objective is to provide guidance and attention points for the device procurement process.

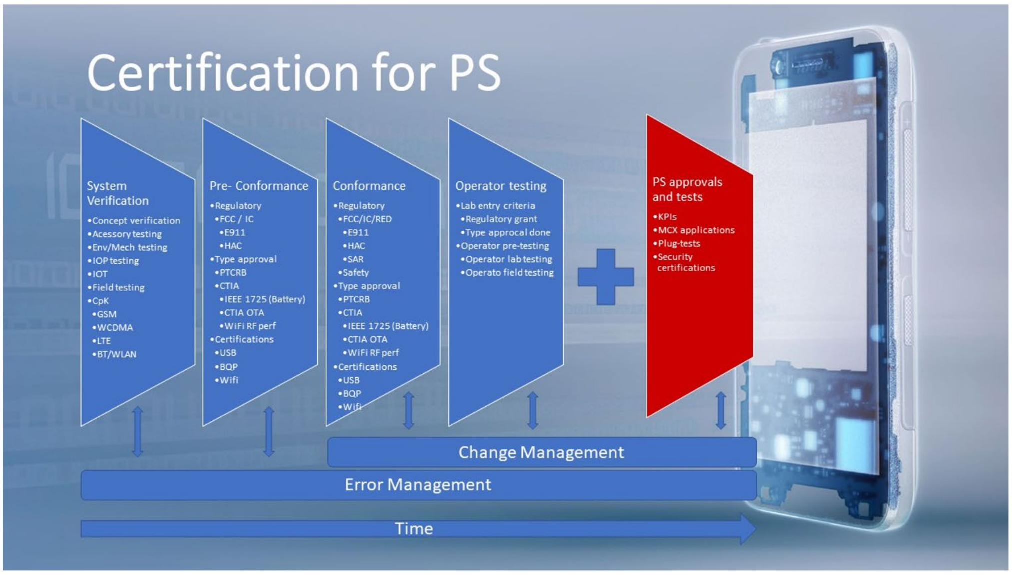
2.1 Testing Process

For LMR/PMR devices there are national and international certification processes in place that ensure standard compliance and interoperability all the way from device firmware to network software level.

For broadband devices the setup is more complex (split of hardware/applications) and the market is different (more vendors, commercial MNOs, established processes for commercial device procurement, etc.)

Mission-critical users also have more demanding testing and certification criteria than commercial users or consumers.

Rapid product cycles of hardware, operating system, applications, backend software and network hardware/ software are a big challenge for mission-critical organisations in terms of testing each update and each combination.



Certification for PS

System Verification
- Concept verification
- Acessory testing
- Env/Mech testing
- IOP testing
- IOT
- Field testing
- CpK
  - GSM
  - WCDMA
  - LTE
  - BT/WLAN

Pre- Conformance
- Regulatory
  - FCC / IC
    - E911
    - HAC
- Type approval
  - PTCRB
  - CTIA
    - IEEE 1725 (Battery)
    - CTIA OTA
    - WiFi RF perf
- Certifications
  - USB
  - BQP
  - Wifi

Conformance
- Regulatory
  - FCC/IC/RED
    - E911
    - HAC
    - SAR
  - Safety
- Type approval
  - PTCRB
  - CTIA
    - IEEE 1725 (Battery)
    - CTIA OTA
    - WiFi RF perf
- Certifications
  - USB
  - BQP
  - Wifi

Operator testing
- Lab entry criteria
  - Regulatory grant
  - Type approcal done
- Operator pre-testing
  - Operator lab testing
  - Operato field testing

PS approvals and tests
- KPIs
- MCX applications
- Plug-tests
- Security certifications

Change Management

Error Management

Time

Public safety approval for devices should also not be a separate block that would only be addressed at the end of a certification process. The specific public safety needs shall be addressed in every step of the device design, testing and approval process.

2.2 Standardisation

“A standard is a technical document designed to be used as a rule, guideline or definition”

Complying to standards is the baseline for every manufacturer that is developing equipment for PPDR users/operators. It is needed to ensure interoperability, and that the device meets the specific requirements.

As mentioned in section 1.3, vendors shall be asked to comply with certain device standards/entry criteria. They will have to ensure correct implementation. Depending on the procurement model (Chapter 5), it may still be up to the operator/users to test the implementations and interactions between them.

2.3 Conformance Testing

“Conformance testing is testing or other activities that determine whether a process, product, or service complies with the requirements of a specification, technical standard, contract, or regulation”

GCF (Global Certification Forum) provides a standardised certification of mobile devices covering conformance, interoperability, and field trials. Most mobile network operators, before they add a new device to their portfolio for sale to end customers, will have GCF (or PTCRB - PCS Type Certification Review Board) certification as a requirement.

From the operator’s viewpoint one of the benefits is that they can take confidence from the testing done in GCF and reduce their own, operator-specific testing.

At the time of publication, GCF is working with TCCA to incorporate mission-critical features for devices that are targeted for the mission-critical market. GCF/TCCA are also working with GSMA to get a field trial component up and running whilst the conformance test suites are still being built.

Ultimately to get GCF certification for mission-critical usage the device will have had to have passed the conformance test suite and a field trial element. Other activities ongoing are the development of a mission-critical specific conformance tester (NIST - National Institute of Standards and Technology- funded projects).

2.4 Network and PPDR operator testing & certifications

Most of the PPDR operators will require some form of certification and testing. It could also be that similar devices and services will be operational in other PPDR or commercial networks, and that there will be roaming agreements between these operators. In such a case, product approval in one network could be (with minimal testing) the basis for approval in the other network. Unnecessary testing or duplication of certification processes will increase the costs of the devices.

If there is an international understanding on how these tests will be executed, then a baseline of a common approach can be set. This way, not everybody has to duplicate tests that already have been performed by another operator for the same combination.

After the generic device approval, a process of implementation approval could be applicable. Items that could be considered as implementation specific are:

- Testing against RAN (Radio Access Network) configuration of the operator (ACB (Access Class Bearing), QCI, …).
- Testing of standard features like VoLTE, SMS, supplementary services, data, which very much rely on the individual configuration for the operator.
- MCPTT Client/Server testing.
- Testing with local MDM solution and profiles.
- Security testing of the device/client/MDM solution as a whole.

2.5 Interoperability

“Interoperability is the ability of different IT systems and software applications to communicate, to exchange data accurately, effectively, and consistently, and to use the information that has been exchanged”

Interoperability between mission-critical services and devices ensures that PPDR users have a choice of devices and applications that best suit their needs. Interoperability (IOP) testing is especially important now when there is not yet a global certification scheme for mission-critical devices

The IOP process established by TCCA and used for the last 20 years is unrivalled and provides a good basis for interoperability testing. Efforts will need to be made to adopt this concept to mission-critical broadband devices.

The ETSI Plugtests™ are aimed at verifying that devices, networks and applications work according to 3GPP standards, are interoperable, and identifying potential areas of misinterpretations. Whilst doing so the Plugtests also provides a basis for comparing of device and application functionalities. However, they do not provide complete tests results or standard conformance certifications. Other mission-critical interoperability-related projects such as MCOP have not yet been adopted by all device vendors.

Therefore, in this section we mainly concentrate on specific technical requirements that support interoperability of devices with broadband networks, applications, and accessories.

Network interoperability is mainly defined by 3GPP and GSMA standards:

- 3GPP standards (e.g. TS 36.101) for UE including MCPTT features (e.g. Release 12 and later QCIs).
- GSMA standards e.g VoLTE (Voice over LTE) and RCS (Rich Communications Services).

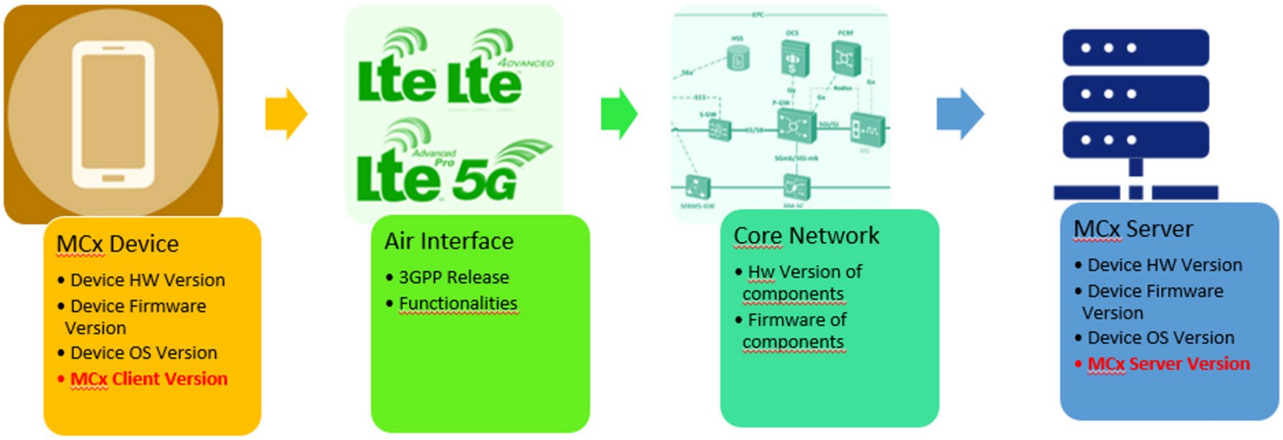
For PPDR usage 3GPP has defined specific features that were explained in Chapter 1. However, this interoperability only covers the technical interoperability of features. The implementation and the operational workflow of users with different mission-critical services/applications is not in scope.

Some elements of network interoperability may be outside of the scope of the broadband device procurement, such as interoperability with narrowband systems (TETRA/P25), which could be realised with an IWF (Interworking Function) or network gateways.

Support for multiple radio access technologies (e.g. TETRA/P25, 3G and 2G) adds complexity and therefore careful implementation is necessary to avoid degradation of the user experience – for example if the MCX service is only supported on 4G. On the other hand, LMR/PMR DMO capability will enhance the user experience when broadband coverage is not available.

Other "industry standard" expectations for interoperability include: WiFi, Bluetooth, NFC, USB, Android OS (GMS/non-GMS versions, APIs).

Finally, an important aspect of interoperability is the relationship of the mission-critical client applications on a device, and their compliance with the server(s) to which they are connecting (see next section).



2.6 Application and Accessory testing

Application procurement is outside the scope of this white paper. However, the types of applications which the device(s) will need to run may have implications on the device specification. It is recommended to list the standard APIs that shall be supported by the device.

Application testing will also be an important step in the complete process of certification of the whole solution for the end-user. This relates to the certification of the application itself and testing/certification of the device/application combination.

Accessory testing may also be part of the device requirements. However, including accessories in a general process of device testing and certification could lead to a cross matrix between devices and accessories which in the end all would be subject to complex version management. Will this approach be manageable? Depending on the procurement model (Chapter 5), it may be up to the manufacturer to certify the product.

2.7 End user testing

End user testing and user acceptance is needed in every procurement process. Is the device/client application fit for purpose? After all, end users need to have confidence in the product.

It will be difficult to specify every requirement and to document every behaviour. At what point will the end user be satisfied with the results? When will his/her needs be fulfilled and will he/she be able to take the device/application into use? If this moment is not well timed it is possible that certain shortcomings/defects will damage confidence in the product/service.

One option to streamline the implementations and the workload that comes with the testing of the available solutions is to allow user testing on an operator-controlled list of devices. This list should contain enough devices to allow the user to fulfil his/her operational needs and allow the operator the control the lifecycles of the devices.

Users should be involved in an intermediate stage of the complete testing process. This way the users would get a "hands-on" experience on existing devices and see the capabilities and potential issues.

The users however must be made aware of the technical implementation of the devices/application. Devices must for example use the designated mission-critical bearers and not be based on best-effort service through over-the-top (OTT) connections. Only then will the functionalities of the device/implementation be judged effectively.

Key Takeaways for Chapter 2:

- User expectations need to be covered from the start as they are key to the success of the implementation of the purchased solution.
- PPDR users must verify that the equipment/functionality is meeting their requirements, and that the procurement documents include compliance with relevant standards.
- Interoperability for a PPDR users relates to the specific MCX Server/Client that they intend to use. Pay close attention to the features and how they match operational requirements.
- The procuring organisation shall conduct their own additional testing process when they see that there are gaps between the current standards and implementation model.
- Accessories are a part of the operational model and must be integrated, either by verification or by manufacturers' declaration.

3 Device lifecycles and procurement timelines

PPDR users' expectations regarding device lifecycle have been set by their experience of LMR/PMR devices, which are typically in use for 7 – 10 years.

The LMR/PMR product lifecycles are therefore far superior to COTS devices, which may be on the market for just one year. Specialised broadband terminals, including those customised to public safety requirements, typically have a lifetime of 3-5 years.

The reasons behind this are the use of mass-market chipsets and other components whose life cycle can be 1-2 years, and the software lifecycles, including Android OS, which is rapidly evolving according to the needs of global consumer and enterprise markets.

The current procurements for broadband PPDR devices often require committing to several years of product deliveries, support and maintenance. Warranty term requirement is typically 3-5 years, and software and security updates shall be frequently made available.

It is also typical that the actual deployments start 1-3 years after the procurement, because the network and MCX applications must be first built and made available for the users.

It is therefore common that vendors must make a bid with a device that does not yet exist, or it would not be available throughout the whole contract lifetime.

A long procurement cycle including the integrations and testing after the procurement makes it difficult to align with technology/chipsets availability. This is another reason to use flexible purchasing methods like Dynamic Purchasing

System (DPS), which can give buyers an electronic access to a pool of pre-qualified suppliers. Buyers should also consider different procurement models described in Chapter 5.

Key Takeaways for Chapter 3:

- PPDR users' expectations regarding device lifecycle have been set by their experience of LMR/PMR devices.
- Lifecycles of broadband devices are much shorter, due to use of mass-market components and rapidly evolving software requirements.
- This "mismatch" must be understood and considered in users' Total Cost of Ownership (TCO) evaluations, as well as technical device requirements and roadmaps.

4 In-life management

In this section we concentrate on the 'in-life' part of the product lifecycle, i.e. when it is being deployed in the network, managed and serviced.

4.1 Mobile Device Management

Mobile device management (MDM) means here centralised, remote administration and control of the broadband devices. It will ensure that the devices are configured according to user organisations' policies, have a standard set of applications, software versions etc. It may also be used for diagnosing and troubleshooting equipment remotely, and for monitoring, security, and tracking purposes.

MDM is closely related to Enterprise Mobility Management (EMM), which includes also mobile information, application and content management. MDM/EMM implementations can be either on-premise or cloud-based.

From a security perspective MDM/EMM solutions can provide firmware, application and other software updates that mitigate the risk of potential vulnerabilities, viruses and malware. They may also prevent users from changing the device settings or installing unauthorised apps which may compromise the operation of their mission-critical communications.

To summarise, the MDM can reduce the overall device support and maintenance costs and lower the security risks.

For PPDR broadband devices, the use of MDM system will be inevitable. Therefore it is important to make sure that the procured devices are tested against the selected MDM system, and this requirement is included in the device procurement.

If the MDM system hasn't yet been selected, the vendors can be asked to list the supported (previously tested) MDM systems, and to list the supported device APIs.

4.2 Warranty

From a customer perspective, a device warranty means a guarantee that the procured device will be repaired or replaced if there is a defect that is determined to be the fault of the manufacturer.

The device manufacturer must therefore ensure that the device meets the requirements and is fit for the intended purpose.

The majority of manufacturers offer a standard 1-2 year warranty from the date of purchase, while mission-critical users typically expect a longer, 3-5 year warranty term. In the device procurement this could be labelled as "extended warranty" and offered separately.

In the world of modern broadband devices, one should also consider the difference between software and hardware warranties. It may even be difficult to determine immediately if the fault is within the device, in the MCX application or in the network.

Most software vendors have 90-day warranty term, and they offer yearly support and maintenance for an additional price. In the same vein, device manufacturers offer Support and Maintenance agreements to ensure the device software is kept up-to-date, including new features and improvements, security patches etc.

It is therefore important to distinguish between warranty and support/maintenance requirements, which are discussed in the next section.

4.3 Maintenance

In the past the user organisations themselves were responsible for a maintenance contract with the LMR/PMR terminal supplier. Initial programming/configuration was done by the supplier, and there was a tight coupling between the device hardware, operating system (OS) and communications application(s) on the device.

As discussed earlier, broadband devices are very different, and their support and maintenance is mainly related to software updates, device/configuration management and - in the case of severe malfunction or physical damage - replacement of faulty units.

Therefore, a transformational change in support and maintenance contracts is required, which involves moving from a device support model to a solution/service model.

There is likely going to be a new wave of service aggregators who will offer such services for end users. These aggregators may include PPDR operators, system integrators or value-added resellers (VARs).

This approach may bring economy of scale, especially if they are able to offer devices and services from multiple vendors and cover several user organisations.

4.4 Training

Training may or may not be a significant part of mission-critical broadband device procurement. This will depend on the chosen procurement model (Chapter 5), i.e. if the device vendor is responsible for providing also applications, installations, system integration, accessories etc.

For traditional device procurement it may be sufficient to require vendors to provide user and service manuals, training videos and other relevant information. The vendors could also be requested to provide contact information of local resellers and other channel partners who can provide on-site training to the users if required.

For 'Device as a Service' model (see Chapter 5) the training requirements will obviously be much more comprehensive, and could include live product demonstrations, train-the-trainer programmes, online training courses etc.

Training is also closely linked with device rollouts, technical support and warranty services, so from a procurement perspective it could be part of a separate product maintenance agreement.

4.5 End of life considerations

End-of-life (EOL) means the end of the product lifecycle which prevents users from receiving updates, support, and maintenance from the device vendor. As discussed in previous sections, the lifecycle can be prolonged by extended warranty requirements or specific support and maintenance contracts.

In this section we consider EOL to mean a situation where the device needs to be disposed also for other reasons (e.g. physical damage that is beyond repair).

End of life for TETRA terminals often requires specific measures, as they may contain encryption keys that need to be erased safely and according to national security requirements. The current process is that TETRA devices are to be returned to the manufacturer for destruction.

For mission-critical broadband devices, a suitable process will depend on the device category and security implementation.

COTS devices are often returned to electronics shops or other facilities for recycling. This approach is not recommended, as at least some data could be recovered, even after factory reset.

Appropriate methods could include return of the device to the manufacturer (as with TETRA) or using a local service provider who can erase the device data according to user and national requirements. This process may also include physical destruction of the device before recycling.

The roles and responsibilities in the EOL management will also depend on the chosen procurement model (Chapter 5).

5 Procurement models and processes

The following sections describe the three most common procurement models that are currently being used or considered by PPDR user organisations:

- Traditional device procurement.
- Device as a Service.
- Purchase elsewhere / bring your own device (BYOD).

Each of these models is described below, followed by a SWOT analysis and specific sections focusing on important considerations such as the legal aspects and affordability/pricing.

A precondition for every model is that it is mission-critical equipment that will be purchased

The outcome of the procurement process can be defined by an outright purchase, a frame contract, a call-off contract etc. This is independent of the model followed.

5.1 Description of the three models

5.1.1 Traditional device procurement

In this model a responsible organisation follows a tender procedure that results in the procurement of devices, applications and maintenance.

After the tender procedure, the organisation will own the devices and will have to take care of all the tasks that come with the deployment, user management, incident and change management, repair and replacement, update and upgrade of operating system and applications and the end of life activities.

In addition to these tasks, the responsible organisation will have to take into account all the costs that are involved with the total life cycle of the devices.

5.1.2 Device as a Service (DaaS)

In this model a responsible organisation follows a tender procedure that results in the establishment of a service agreement with a service provider. The main task for the organisation lies in preparation of the tender procedure. The organisation will have to describe what the scope of the service will be. Once the service is established the organisation is mainly responsible for the user management, whereas all other tasks as described in the first model are performed by the service provider.

The organisation will pay the service provider a fee per device per period.

5.1.3 Purchase elsewhere/ Bring your own device (BYOD)

In this model there is no responsible (central) organisation. Each individual user or user organisation is free to purchase devices and connect them to the infrastructure.

The operator therefore will have to look after a lot of tasks and to maintain the quality of the infrastructure and services (security, capacity, availability etc). These activities will also have to result in an acceptable service for the end user.

These tasks must be performed for each device manufacturer, type and version. User settings can vary, and the device fleets range from single devices to large groups of similar devices, depending on the procurement by users themselves or the user organisations.

Choose your own device (CYOD)

A CYOD model approach can be seen as a mix between the BYOD and the Traditional procurement. The individual user is limited to a set of devices that will be made available through a catalogue principle. The operator together with user representatives will define which devices can be implemented and used.

There is no separate SWOT analysis for CYOD presented in this document, because the results are quite similar to that of the traditional procurement method. The influence of the user on suitable solutions could be greater, because the users could be directly involved in the procurement processs. In general, the amount of preparations and maintenance activities will increase when more varieties are available. Also, the cost per device will be higher when fewer quantities of one device model are purchased and deployed.

5.2 Legal considerations for all three models

Public safety devices are usually procured by public bodies. For example, in the EU, this means that the procurement will need to follow an appropriate competitive process. Similar requirements exist for public procurements in non-EU countries.

Before procurement, it is recommended to conduct a request for information (RFI) with potential suppliers of devices and services, to understand the technical and commercial feasibility of the requirements, and the likely cost and timescale for delivery. The market for mission-critical devices and services is still evolving, and it is important to seek the most up-to-date view possible. While information from an RFI will normally be confidential, it may be possible to publish a summary for the benefit of other public safety operators (as the Virve 2.0 programme in Finland has done).

For public procurement in the EU, EU law defines different types of public procurement procedures:

- Open procedure - Anyone may submit a full tender.
- Restricted procedure - Anyone may ask to participate, but only those who are pre-selected may submit tenders.
- Competitive negotiated procedure - Anyone may ask to participate, but only those who are pre-selected will be invited to submit initial tenders and to negotiate. Procuring entities can only use this procedure when negotiations are necessary due to the specific or complicated nature of the purchase.
- Competitive dialogue - This procedure can be used by a contracting authority with the aim of proposing a method of addressing a need defined by the contracting authority.
- Innovation partnership - This procedure may be used when there is a need to purchase a product or service that is not yet available on the market. A number of companies may participate throughout the process.

Mission-critical devices are not yet commodity items. The requirements are more complex than for consumer devices, with trade-offs between different requirements. Not all types of devices are available as off-the-shelf hardware and development may be required. Finally, the integration of testing processes required are still operator-specific and not yet standardised. The procurement procedure should provide the opportunity to discuss and evolve requirements and solutions with bidders – other than for the most straightforward requirements, Negotiated and Dialogue procedures are likely to be the most suitable, with Innovation Partnership being considered where the device requires significant development.

5.3 Results of the SWOT analysis

5.3.1 Model A: Device as a Service

From a user perspective this model will deliver a device that is tested, configured and deployed to ensure optimal performance and operation.

The user doesn't need to worry about security, software updates and feature upgrades, operating system versions etc. because the service provider will take care of these activities.

From the viewpoint of the procurer, this model defines a contract that is simple to manage. All activities from preparation, validation, implementation, configuration, maintenance and replacement, end of life activities etc. are the responsibility of the service provider.

The annual costs are constant and clear and are established for the whole contractual period.

The service provider can organise activities around a well-defined set of quality parameters and is therefore capable of balancing costs and user benefits in and effective and efficient way.

Although the user will get a device that is fit for purpose, it could be that he/she experiences it as restrictive in terms of device choice, changing settings or adding new applications. Often this is more a perception issue than a real usage problem.

To procure and implement effectively this model requires the responsible organisation to put a lot of effort in the preparations: the scope and quality of the service being required. If this is not done properly, the users will experience negative results throughout the contractual period. Depending on the contract, this could also result in an unwanted vendor-lockin for the contractual period.

In this model it will be difficult for small vendors or vendors of special products to enter large scale tenders individually. This means that they need to rely on forming partnerships with other/bigger vendors. This could lead to fewer opportunities to present and sell their devices.

If the preparation is not done properly a long-term contract period may also create an obstacle for improvements.

If the DaaS model is implemented in the right way (flexible, user demand driven etc) there is an opportunity to develop a flourishing ecosystem that offers opportunities for both mainstream device suppliers and specialised suppliers. This can result in structured setup of a catalogue for different user groups (certified, tested).

Another opportunity is the chance to provide the DaaS as part of larger package of device services such as device integration and certification with MCX solutions, configuration and staging, and supply of accessories.

In general, this model is considered as a good opportunity to combine both flexibility, quality and pricing without having to perform many operational tasks as a governmental organisation, once preparation has taken place.

Strengths	**Weaknesses**
• Budget: constant flow, no surprises • Ease of use: fully customized • Up to date: always actual SW+ model • Legal: straight forward governance • Maintenance: part of the service contract, risk of failure carried by supplier • Security: all essential parameters centralized • Validation: central and limited • No end of life situation (logistic, discard of device)	• Budget: • Ease of use: limited liberty for end user (feeling?) • Implementation: high demand on preparation • Vendor lock in • Small vendor: dependency from partnership • No competition during contractual period
Opportunities	**Threats**
• Bigger ecosystem: high volumes (from all viewpoints) • Controlled catalogue for different user groups (certified, tested) • Opportunity to provide device as a service as part of larger package of device services such as device integration & certification with MCX solution, configuration and staging, supply of accessories • Vendor: show added value • Example FirstNet	• Expectations: miss alignment, therefore slower adoption • Special / small vendor: little chance to enter • Contract period to long: fixed service and device • Mature products: still in development phase • Budget: no view on hidden cost

SWOT Analysis - Model A - Device as a Service

5.3.2 Model B: Traditional device procurement

The traditional device procurement can be organised in different ways, the most common options are:

- Model B-1; The PPDR operator manages the whole process and is E2E responsible for the device procurement.
- Model B-2; The operator manages an open contract and end users can order via this open contract.
- Model B-3; The end user organisation manages the whole process and takes E2E responsibility for the devices.

It is obvious that there are also threats and weaknesses in some of the models, especially if there is not a clearly defined device policy from the operator and when devices do not satisfy all the mission-critical, technical and user requirements. Therefore, we must dive deeper in the models. Life-cycle management becomes more critical with the new technologies and this must be properly managed. The number of different devices (choice) must be limited in all B models to a quantity acceptable for the operator and the end users/organisations. It's impossible to recommend a minimum or maximum quantity because many factors are involved.

- Model B-1:

This model has more similarity with the procurement model A Device as a Service. It is up to the operator to manage the whole procurement process and also maybe further on the life-cycle path plus the maintenance and device management.

- ModelL B-2:

This model can guarantee competitive pricing and availability for the end user. The mission-critical operator can organise and manage the process. The end user is responsible for updating and upgrading the device(s) – however this is not so easy to manage and can lead to a mismatch of functionalities and supported software of core/MCX/RAN versus user equipment device. The open contract must be flexible and able to accommodate new devices and suppliers at any moment.

- Model B-3:

This model is the most complex of the three because we have here on top of the updating and upgrading complexity extra challenges for the operator to manage the whole process.

In this model the operator must create a pre-validated device list and this can lead to extra time being required for validation, transferring it to end users and tender process.

A mix of model B2+B3 will not make things simpler for the operator or for the device suppliers.

The best approach in this model B "traditional device procurement" seems model B-1 and if this is not possible, then model B-2.

Strengths	**Weaknesses**
• Ease of use: flexible • Maintenance: by choice • Budget: maximum control on expenses • Validation: central and limited • Customer organization has full control over devices – when to buy, which devices / OEMs, service arrangements	• Budget: no constant flow, but recurring capital investments • Ease of use: old devices, old OS, old apps • Legal: more complex governance models • Level of control: much coordination between user and vendor for operator • End of life: extra cost, logistics, ...
Opportunities	Threats
• Ease of use: introduction of new features, HW, apps • Better chances for small/special vendors • More competition for vendors	• Ease of use: difficult to maintain e-t-e services • Risk on interoperability • Budget: unexpected renewal • Unexpected handling (battery replacement, screens, etc)

SWOT Analysis - Model B - Traditional Device Procurement

5.3.3 Model C: Purchase elsewhere/ Bring your own device (BYOD)

Bring your own device (BYOD) refers to being allowed to use one's personally owned device, rather than being required to use an officially provided device.

Strengths	**Weaknesses**
• Ease of use: maximum liberty for end user • Budget (operator): fixed, or elsewhere • Legal: no governance • Vendor/ local reseller: lots of opportunities on local level	• Ease of use: no control on quality (OS, HW, security) • Validation: intensive (amount and extensively) • High pressure on device management and administration • No general device settings • A lot of unknown issues (network, device, app, ..) • No combined buying power (user, operator), effect on roadmap, app development etc. • Difficult to set up a catalogue
Opportunities	**Threats**
• More innovative solutions, chances for small vendors • Quick response on new user demands • Utilize cheap mass market devices (user pov) • Extend MCX service to volunteers, second responders or other organizations. • May need to use "over the top" implementation of MCX application with protected network path into network	• Overall security low • No interoperability • High amount of incidents • End user: no or limited service • Operator/owner of the networks is blamed (viewpoint society) • Budget: Overall cost very high • Vendor: divided market • Utilize cheap mass market devices (quality issues, vendor and operator pov) • Non-mission critical solution

SWOT Analysis - Model C - Purchase Elsewhere / BYOD

In the workplace it refers to a policy of permitting employees to bring personally owned devices (laptops, tablets, smartphones, etc.) to work, and to use those devices to access privileged company information and applications.

BYOD is making significant inroads in the business world, and the studies indicate various pros and cons in this approach. When it comes to mission-critical use, we have summarised these in the table below.

We have also included "purchase elsewhere" in this SWOT analysis. This refers to a model where the user organisations do their own device procurements, and the devices are then deployed in mission-critical broadband network.

It is obvious that the threats and weaknesses in this model outweigh the user benefits, especially if there is not a clearly defined device policy and control to ensure that the devices meet all the mission-critical, technical and user requirements. Therefore, we do not recommend this model to be used in mission-critical networks and services.

6 Economic aspects, total cost of ownership

In the PPDR world it is common to have a tender procedure where different selection criteria are used to define which offer will provide the most valuable solution.

In most tender procedures these selection criteria consist of:

- Quality (non-functionals like availability, security, redundancy, fall back)
- User requirement (functionalities)
- Technical requirements (battery lifetime, form factor, etc.)
- Legal matters (volumes, contract, life cycle management, maintenance, IPR, contract period)
- Pricing (total cost of ownership model)

It depends on the chosen procurement model and factors like product maturity, risk appetite, political exposure, competition etc. if pricing is regarded of greater or lesser influence on the decision as to which vendor will win the tender procedure.

Another aspect of pricing is related to budgeting and CAPEX vs. OPEX considerations. In the DaaS model the operational costs are well known and constant throughout the device/service lifecycle. In the traditional purchasing model the capital expenditure is initially high, and the total cost of ownership may be lower, but is also more difficult to predict.

One should also note that the market for mission-critical broadband devices is relatively small, and the user requirements call for highly specialised, rigorously tested and proven devices. To put this in context, in 2020 the global deliveries of all types of digital LMR/PMR terminals numbered 8 million units. During the same time period the sales of LTE smartphones alone exceeded 1.5 billion units.

It is therefore obvious that this economics of scale will have impact on the cost per device for the PPDR market.

Key Takeaways for Chapter 6:

- PPDR users should be educated on the differences between COTS devices and those designed specifically for PPDR use
- Buying less expensive COTS devices is false economy, as discussed in previous chapters.
- End users need to understand that the life of a LMR radio equals 2 or 3 broadband terminals. The total cost of ownership changes
- The device costs should be weighed against the user benefits like increased productivity and safety, reduced network maintenance costs etc.
- Device replacement strategy should be defined early so users have this as an input for future budgets
- Accessories are often forgotten in budget calculations
- Re-use of accessories is possible and would lower the total replacement cost

7. Conclusions and recommendations

With the development of mission-critical mobile broadband solutions for PPDR based on the 3GPP standards the international PPDR community has entered a new world of needs and possibilities for their user organisations.

This new world has a lot of potential to support the PPDR activities to make them more efficient, but also to provide more security for the users of the mission-critical services.

One of the key elements in the chain of information is the device that will be used to unlock the new possibilities. In this white paper we have seen that the mobile broadband world is a complex one. To be able to use the functional possibilities in the most effective way some key elements should be taken into account before device procurement can lead to a successful outcome:

- functional needs
- technical conditions
- end to end testing
- user and equipment management
- security

Regardless of the procurement model these key elements should be well defined.

There is no absolute right or wrong regarding the procurement models that were investigated. What is clear is the fact that the more variety and freedom lies with the users, the more risk there is that the end to end mission-critical functionalities cannot be guaranteed by the PPDR operator.

Therefore it is recommended to set up a robust system with standard set of device requirements and settings, as well as an approved device catalogue process to ensure a guaranteed level of quality for the PPDR end user.

The world of mission-critical smart devices is still developing and not yet fully mature. The ecosystem compared to standard smartphones is still small. It is therefore very important that PDDR organisations, manufacturers, standardisation and testing bodies cooperate to stimulate the growth and development of the mission-critical device market.

It is expected that the mission-critical device ecosystem will reach a mature level in the coming years. A yearly review on the progress of the different subjects as investigated in this white paper is recommended.

8. APPENDICES

3GPP Mission-Critical Requirements

Mission-Critical Quality of Service (QoS) Class Identifiers (QCIs)

As defined in 3GPP TS 23.203 v16.2.0 (2019-12)

https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=810https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=810

Mission-Critical PTT Key Performance Indicators (KPIs)

As defined in 3GPP TS 22.179 v17.0.0 (2019-12)

https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=623https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=623

ESN case study

The Emergency Services Network (ESN) will replace the TETRA network (Airwave) currently used by public safety agencies in Great Britain. ESN is built on a commercial LTE network which is being enhanced to provide the service prioritisation, coverage and resilience required by public safety users.

The ESN programme has so far conducted three centralised procurements for MCX-capable devices:

- A ruggedised Android smartphone device plus compatible accessories (such as remote speaker microphones).
- A vehicle device based on an Android smartphone platform, but with form factor, interfaces and optional accessories suitable for installation and use in a wide range of vehicles.
- An aircraft device approved for installation in fixed and rotary wing aircraft.

Further procurements will be carried out as necessary to provide the full range of devices and accessories needed by different user groups.

In the procurements so far, it has been clear that the devices being procured were not commodity off-the-shelf items, and that the market for MCX devices is still immature (though developing rapidly). This is especially true for vehicle and aircraft devices, where significant hardware development was required; however, even for handheld smartphone devices custom firmware development is required.

Requirements which have proven challenging to meet include:

- Integration of the MCX solution with the devices, and optimisation for performance. This has required firmware customisation and extensive test and debugging.
- The device test regime goes beyond standard operator testing, to maximise compliance and performance against LTE network and MCX requirements. Device suppliers must budget for the time and cost of testing and re-work.
- Capabilities for device-to-device (off network) communications.
- Device lifespan. In contrast to TETRA devices, where a lifespan of 7 years is routinely achievable, the lifespan of Android-based devices is limited by the ability of the device chipset to support new OS versions, and the availability of security patches.

9. Acknowledgements

TCCA would like to thank Jarno Majava (Chair) and work-group leaders Tim Clark (WG1), Steven Wyckaert (WG2), Catalin Gheorghiu (WG3), Anders Berghäll (WG4) and Herman van Sprakelaar (WG5).

In addition, we would like to thank all the task force members listed below in alphabetical order, for their valuable contributions and active discussions:

Anatoli Levine, Chris Telfer, Clive Rodmell, Doug Roberts, Federico Frosali, Gij Louwrier, Guy Shimon, Graham Lee, Gösta Kallner, Hannu Aronsson, Harald Ludwig, Harald Pfurtscheller, Imen Hedfi, Jake Smith, Jason Johur, Jeremy Kemp, Jos van der Mijden, Jurgen Poels, Kevin Sennitt, Lengyel Lajos, Luz Fernández del Rosal, Matthias Reinhardt, Matthieu Ettema, Michael Ruehlemann, Stary Miklos, Neal Richardson, Noel Kirkaldy, Peter Hudson, Phil Woodley, Remi Thomas, Renaud Mellies, Roland Toth, Tomas Karabinos, Tuomo Ylonen, Younes Zaki.