DSB

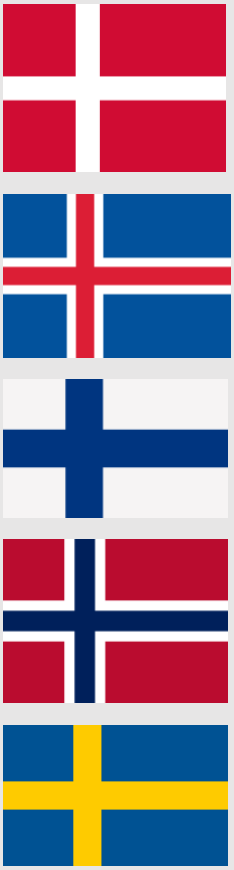
Swedish Civil Defence and Resilience Agency

DANISH EMERGENCY MANAGEMENT AGENCY

Erillisverkot

Korda

2026



NCCOM White Paper

Device categories for PPDR use v2.0

Important note: The opinions and information given in this white paper are provided in good faith. Whilst we make every attempt to ensure that the information contained in such documents is correct, NCCOM is unable to guarantee the accuracy or completeness of any information contained herein. NCCOM, forum for co-operation for the PPDR operators in the Nordic countries, their employees and agents will not be responsible for any loss, however arising, from the use of, or reliance on this information

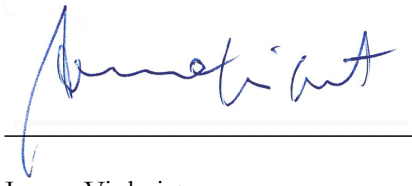
Change history

Tabell 1. Change history NCCOM White Paper v2.0

Date	Version	Comment	Author
2026-09-08	DRAFT 0.1	First draft for internal review	NCCOM
2026-09-15	DRAFT 0.2	Draft version for review	NCCOM
2026-09-22	DRAFT 0.3	Draft version for review	NCCOM
2026-10-06	DRAFT 0.4	Draft version for review	NCCOM
2026-10-12	DRAFT 0.5	Draft version for NCCOM review	NCCOM
2026-10-16	DRAFT 0.6	Draft version for NCCOM review	NCCOM
2026-10-23	DRAFT 0.7	Draft version for NCCOM review	NCCOM
2026-10-23	DRAFT 0.8	Cleaned up version for NCCOM review	NCCOM
2026-10-26	DRAFT 0.9	Updated device names	NCCOM
2026-10-27	DRAFT 0.91	Draft version for NCCOM review	NCCOM
2026-10-27	DRAFT 0.92	Draft version for NCCOM review	NCCOM
2026-10-27	DRAFT 0.93	Draft version for NCCOM review	NCCOM
2026-10-28	Final 1.0	Final version for signing NCCOM	NCCOM

Approval for publication

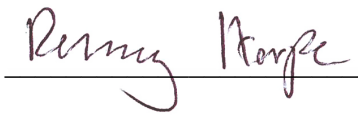
The approval for publication has been signed by authorized representatives of each country participating in NCCOM and it is ready for publication on the 17th of November 2026.



Stockholm 3.11.2026

Jarmo Vinkvist — Place and Date

Vice President – Erillisverkot Group



Stockholm 2026-11-03

Ronny Harpe — Place and Date

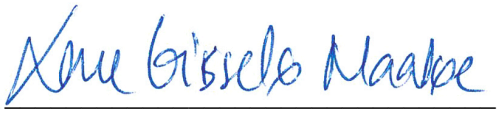
Director of Mission Critical Communications – Swedish Civil Defence and Resilience Agency



Stockholm 3/11-2026

Eline Palm Paxal — Place and Date

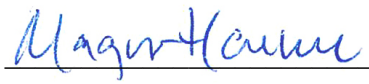
Director of Department for Critical Communications – The Norwegian Directorate for Civil Protection



Stockholm 3/11-2026

Lene Gisselø Maaløe — Place and Date

Head of Centre of Emergency Communication – Danish Emergency Management Agency



Stockholm 3.11.2026

Magnús Hauksson — Place and Date

Senior Management – Korda ehf

Introduction

PPDR network operators in the Nordic countries[1] published NCCOM White Paper PPDR Rugged Handheld Device for heavy use version 1.0 in 2023. This version 2.0 of the White Paper provides updated technical requirements and guidelines for device manufacturers to gain an understanding of our common requirements for PPDR users.

The NCCOM Whitepaper aims to provide clear and harmonized requirements and guidance for mission-critical user equipment. This will support UE vendors in developing products that meet the functional, technical and operational requirements of mission-critical environments, while providing operators with a common basis for evaluating and introducing new equipment.

In addition to regulatory and industry certifications, such as CE and GCF, user equipment intended for mission-critical services will typically be subject to additional onboarding, acceptance and lifecycle management processes defined by the mission-critical operator. The scope and implementation of these processes may vary between operators.

Although the Nordic countries follow largely harmonized European spectrum frameworks, there are notable differences in how mobile frequency bands are utilized. Despite these differences, the Nordic countries maintain close coordination on spectrum management and cross-border frequency planning, helping to ensure interoperability, reduce interference, and support a common ecosystem for mobile networks and devices.

Clear requirements and appropriate certification are expected to simplify the overall process, from product development and procurement through onboarding and acceptance to configuration, software and security updates, and ongoing lifecycle management. This approach can reduce duplication of effort, facilitate the introduction of new devices and vendors, and support the development of a broader and more sustainable ecosystem for mission-critical user equipment.

Version 2.0 broadens the scope to other UE categories

- Non-Rugged Smartphone
  Commercial off-the-shelf (COTS) phones.
- Rugged Smartphone
  Rugged Commercial off-the-shelf (COTS) phones, specifically engineered to withstand extreme conditions, physical impacts, and harsh environments that would destroy standard devices.

[1] Denmark, Finland, Iceland, Norway and Sweden.

- Broadband MC Radio
  Radio / Walkie talkie type handheld device without touch display. A rugged handheld with a physical keypad or just only physical buttons and small display. Designed for reliable operation with gloves and for users who may need to operate the device without looking at the display.
- Rugged Mission-Critical Broadband Handheld
  The baseline in the NCCOM White Paper v1.0. Full environmental and drop requirements, wide temperature range, loud audio, an external antenna connection, physical keys for push to talk, emergency and talk group selection, and long support commitment. Built for continuous outdoor duty.
- Mobile Broadband Module
  Hardware component that provides connectivity to the network

Future versions of White Paper will further broaden the scope.

PPDR users are accustomed to rugged TETRA devices with physical buttons for PTT, emergency calls, etc. Some of these requirements are carried forward to next-generation devices. A long lifecycle, with continuing support for hardware, chipset, battery, and software are also essential for these devices. The physical characteristics of the device shall support missions in all conditions, which include shifting temperatures, humidity, and wet conditions, as well as heavy-handed handling. Equally important is compliance with 3GPP standards, GCF certification including MCX services. Operating within a secure PPDR network, the devices and their vendors shall provide capabilities to maintain software and security updates without dependencies upon external networks, e.g., the internet.

This white paper is focused on devices replacing TETRA terminals and replicating existing functionality. However, the new PPDR networks will be continuously developing, and Nordic operators will ensure that new features and functionality are provided to the PPDR community in the coming years, thus placing additional requirements on the devices.

Common requirements for all Handheld Device Categories are mandatory for all Handheld devices. Other requirements for each device type may be mandatory or optional depending on the use case. Country-specific requirements will be announced through national procurement processes and could differ due to product maturity and market availability.

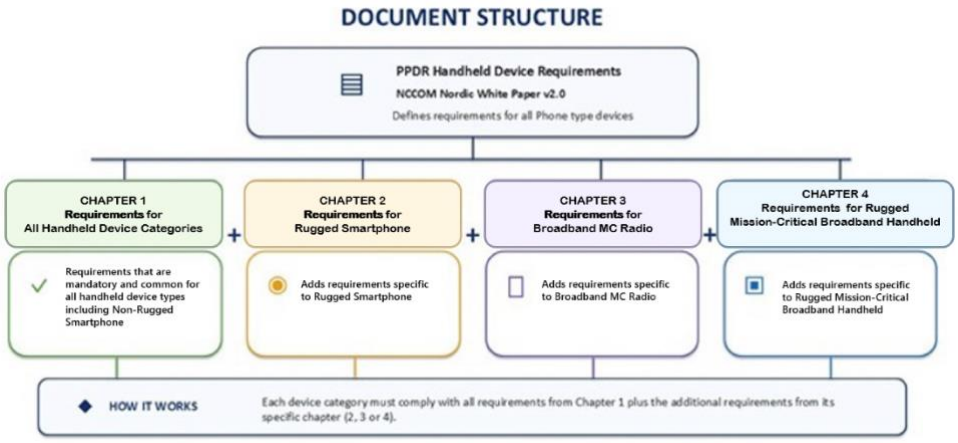


Figure 1. Document structure

Table of Contents

Change history **1**

Approval for publication **2**

Table of Contents **6**

1. Requirements for All Handheld Device Categories **9**
1.1 Environmental 9
1.2 Hardware 9
1.2.1 Band support 9
1.2.2 Carrier aggregation 9
1.2.3 5G Stand alone 10
1.2.4 Display 10
1.2.5 Battery 11
1.2.6 Camera 11
1.2.7 SIM/eSIM 11
1.3 Usability 11
1.3.1 Speaker and microphone 11
1.3.2 Peripherals connectors 11
1.4 Accessories 12
1.5 Wi-Fi Hotspot 12
1.6 Security and Firmware 12
1.6.1 Hardware-Based Security Architecture 12
1.6.2 Lifecycle support 13
1.6.3 Internet access 13
1.6.4 Third-party EMM 13
1.6.5 Controlling external IP connections 13
1.6.6 Permitted applications 14
1.6.7 Device and application access 14
1.7 Standardization and Certification 14
1.8 Location Services 14
1.9 Mission-Critical Services Support 15
1.10 Device Identification 15

2. Requirements for Rugged Smartphone **16**
2.1 Environmental 16
2.2 Hardware 16
2.2.1 Display 16
2.2.2 Battery 16
2.2.3 Camera 17
2.3 Usability 17

2.3.1 PTT Button 17
2.3.2 Emergency Button 17
2.3.3 User interface 17

3. Requirements for Broadband MC Radio 18
3.1 Environmental 18
3.2 Hardware 18
3.2.1 Display 18
3.2.2 Battery 18
3.2.3 Camera 19
3.2.4 External antenna and external antenna connector 19
3.2.5 RF OTA antenna performance 19
3.3 Usability 19
3.3.1 Speaker and microphone 19
3.3.2 PTT button 19
3.3.3 Emergency button 20
3.3.4 Talk group selection switch 20
3.3.5 Programmable buttons 20
3.3.6 User interface 20
3.3.7 MCX Client 20
3.3.8 Peripherals connectors 20
3.4 Accessories 21
3.5 Security and Firmware 21
3.5.1 Lifecycle support 21

4. Requirements for Rugged Mission-Critical Broadband Handheld ...22
4.1 Hardware 22
4.1.1 Band support 22
4.2 Accessories 22
4.3 Device-to-device communication 22
4.4 Security and Firmware 23
4.4.1 Device and application access 23
4.5 E2EE 23
4.6 NTN/LEO Direct-to-handheld device communication 23
4.7 Support for Modules 24

5. Handheld Device Compare Table 25

6. Mobile Broadband Module 27
6.1 Band support 27
6.2 Carrier aggregation 27
6.3 Form Factor 28
6.3.1 Swappable Module 28
6.3.2 Solder-on Module 28

6.4 eSIM/SIM 28
6.5 Positioning 28
6.6 MIMO Antenna Connection 28

7. Future Areas 29

Abbreviations & Terms 30

Appendix A - RF OTA for devices with internal antenna 31

Appendix B - RF OTA for devices with external antenna 33

Appendix C – UX requirements on Ruggedized devices 35

Appendix D – Gloves 40

1. Requirements for All Handheld Device Categories

Requirements that are mandatory and common for all handheld device categories including Non-Rugged Smartphone.

1.1 Environmental

The devices shall be designed to withstand repeated drops from typical operating heights onto hard surfaces without sustaining damage.

Additionally, touch screens and other displays shall be easily readable under all lighting conditions, from bright sunshine to complete darkness.

The device shall withstand at least 1,000 cleaning/disinfection cycles using the manufacturer-declared hospital disinfectant without functional failure or unacceptable deterioration of the enclosure, display, seals, buttons, labels or connectors.

Where disinfectant efficacy is claimed, the disinfectant used shall comply with applicable European medical-area disinfectant standards under EN 14885, such as EN 16615, EN 13727 and EN 13624, as applicable.

1.2 Hardware

1.2.1 Band support

The device shall support at least ITU Region 1: Band 1 (2100), Band 3 (1800), Band 7 (2600), Band 8 (900), Band 20 (800), Band 28 (700), , Band 38 (2600), B40 (2300), Band 68 (700) and NR Band n1 (2100), n3 (1800), n7 (2600), n8 (900), n20(800), n28 (700), n38 (2600), n40 (2300), , n77 (3700), n78 (3500).

Bands 31 (450), n31 (450), n48 (3500), n75 (1500) should be supported optionally, depending of the device variant.

1.2.2 Carrier aggregation

LTE carrier aggregation

The device shall support applicable 3GPP-defined LTE carrier aggregation combinations used in Nordic public mobile networks, including:

- B1+B3+B20
- B1+B3+B7

Support for the B7+B68 LTE carrier aggregation combination is preferred, subject to network availability.

5G NSA

The device shall support the following 3GPP-defined EN-DC configuration:

- B20+n28

5G SA

The device shall support the following 3GPP-defined NR carrier aggregation combinations:

- n1+n28
- n1+n78
- n28+n78

General requirements

B20+n28 is the highest-priority EN-DC configuration because of its importance for coverage in rural areas.

All frequency bands and carrier aggregation or dual-connectivity combinations declared as supported by the device shall operate correctly.

Network configurations and carrier aggregation or dual-connectivity combinations that are not supported by the device shall not cause abnormal device behavior, service interruption or loss of basic connectivity.

The antenna and RF implementation of the device should provide reliable performance across the relevant sub-1 GHz frequency ranges.

LTE B40 and NR n40 are particularly important for private mobile network deployments.

1.2.3 5G Stand alone

5G SA, or 5G Standalone, is a fully independent 5G network that operates without relying on 4G LTE infrastructure. 5G SA shall be supported by all devices

1.2.4 Display

The display and resolution shall be sized in a way that supports effective interaction with MCX applications. To conserve battery, the display shall automatically and manually adjust to changing lighting conditions.

1.2.5 Battery

The device and its battery shall be optimized according to:

- Duty cycle 80% standby / 20% for active use at +20 °C and -110 dBm RSRP signal strength, shall be at least 12h when using MCX application.
- Duty cycle 80% standby / 20% for active use at -20 °C and -110 dBm RSRP signal strength, shall be at least 6h when using MCX application.
- Maintaining at least 85% of the initial capacity after 1000 cycles (from 20% charge to 100% charge) of normal charging.

Devices shall be capable of charging from 0 to 50% in half an hour when a high-power fast charger is in use.

The battery shall be easily replaced by users without specialized tools or expertise. The IP class of the device shall not be compromised after such a replacement is performed.

1.2.6 Camera

The device shall have a camera with at least 8 Megapixel resolution. The camera system shall be able to operate both in bright daylight and under low lighting conditions.

1.2.7 SIM/eSIM

The device shall have at least eSIM + 2 physical SIM slots with support Dual SIM Dual Standby (DSDS). When one SIM is engaged in a voice call, the device shall maintain the required mission-critical packet-data connectivity on the other SIM, where supported by the device, subscription and network configuration.

1.3 Usability

1.3.1 Speaker and microphone

To ensure effective communication in all typical environments, the device should include speakers and microphones that allow for clear audio whether held to the ear or worn on the shoulder.

1.3.2 Peripherals connectors

USB-C standardized for all devices.

Bluetooth version 5.0 or higher and NFC for pairing. It shall be possible to block the use of Bluetooth via the EMM. Bluetooth shall support Secure Connections security mode 4, level 4.

1.4 Accessories

The device manufacturer shall be able to provide or support several accessories for the device:

- Single- and multi-docking stations and charger.
- Earphone with PTT button connected to device.
- Mapping physical button events to applications
- A standardized API for signaling hardware button events, including MCPTT and emergency button activations, is needed to ensure interoperability across vendors and a consistent application experience.

1.5 Wi-Fi Hotspot

The device shall have the capability to act as a Wi-Fi hotspot. It shall be possible to block the use of this Wi-Fi hotspot via the EMM.

1.6 Security and Firmware

1.6.1 Hardware-Based Security Architecture

The device shall implement a hardware-based Root of Trust, secure boot, verified boot, hardware-backed cryptographic key management and a Trusted Execution Environment (TEE) or equivalent isolated security environment.

- The device, including its hardware, firmware and software, shall meet the cybersecurity requirements applicable to mission-critical communications and comply with relevant national security regulations and requirements in the country of deployment.
- The device shall comply with Regulation (EU) 2024/2847, the Cyber Resilience Act (CRA), where applicable, including its requirements for security by design, vulnerability management and security updates throughout the declared support period.
- Additional country-specific security requirements, including those related to the protection of sensitive or classified information, shall be defined by the relevant national PPDR operator or competent authority. Compliance with these requirements shall be demonstrated as part of the national device approval or acceptance process:
- Finland Katakri — national security auditing criteria, particularly for systems handling classified information.
- Sweden Protective Security Act (2018:585) and associated regulations for security-sensitive activities.
- Norway Security Act (Sikkerhetsloven) and NSM requirements for security-sensitive information and systems.

- Denmark National Security Circular (Sikkerhedscirkulæret) concerning classified information and applicable security measures.
- Iceland Regulation No. 959/2012 on classified information and the government data security classification framework.

The product shall fulfil the requirements in the CRA regulation (2024/2847)

1.6.2 Lifecycle support

For PPDR users, it is crucial to have a long device lifecycle and the ability to provide ongoing support. This encompasses chipset maintenance, firmware updates, and security updates. All devices shall be easy to repair. Support for best EU repairability index A (A-E)

Updates to the latest operating system (OS) shall be available throughout the lifecycle, together with the latest security and firmware updates, including fault corrections. Updates containing new features and bug fixes shall be available at regular intervals. Security and emergency updates shall be made available immediately.

1.6.3 Internet access

The device shall be able to function fully without relying on internet access during enrolment to EMM (MDM) or operational use with MCX services.

1.6.4 Third-party EMM

The device shall be capable of being managed by a third-party EMM solution, which is installed on-premises and may be restricted to a closed network, i.e., completely isolated from public internet connections, for example with AOSP (Android Open Source Project).

It shall be possible to manage all software updates through the EMM.

1.6.5 Controlling external IP connections

To ensure device security, manufacturers should provide detailed information on outgoing connection endpoints during start-up, activation, and operational use, etc. This information includes IP addresses, domain names, and communication protocols. PPDR operators shall have control over these endpoints in order to monitor, block, and allow connections as needed. Device security requires collaboration between the manufacturer and PPDR operator to protect sensitive data and prevent security breaches.

1.6.6 Permitted applications

Only critical system applications and those required for the proper functionality of the device, and necessary for MCX application, should be included in the firmware and operating system. The manufacturer shall provide the PPDR operator with a list of applications and detailed information about their purpose and why they are needed on the device.

1.6.7 Device and application access

The device shall support at least one easy to use security authentication (e.g. PIN, password, fingerprints, and face unlock).

For enhanced security, the device shall support an adjustable failed password attempts feature, which initiates a factory reset when the user exceeds the specified number of incorrect password attempts. The number of failed attempts shall be configurable. The manufacturer should provide guidance on managing this feature to ensure optimal device security.

1.7 Standardization and Certification

Devices used in PPDR networks based on LTE and 5G technology shall:

- Carry a valid CE mark
- Have an EU Declaration of Conformity
- Have a unique IMEI code, i.e. one that has not and will not be used in other equipment
- Be certified by Global Certification Forum (GCF) for 3GPP compliance
- Support 3GPP Mission Critical Services including MCX client functionality that conforms with the 3GPP specifications for mission critical communications release 16 or later. Proof includes providing a GCF Mission Critical Services certificate (MCX device + a certified MCX client)
- Be accompanied with an RF OTA test report

1.8 Location Services

The device shall be compatible with Global Navigation Satellite System (GNSS) receivers, and operate, at minimum, with Galileo and GPS systems, together with locations provided by the mobile network. Open Service Navigation Message Authentication (OSNMA) shall be supported at minimum with OSNMA enabled receiver and Galileo SAS (Signal Authentication Service). Indoor location services shall be available using existing technologies, i.e. Bluetooth or Wi-Fi.

The PPDR community's access to reliable positioning and time information is essential for all mission critical services operations. PPDR users rely on accurate and high-quality positions protected from external impact.

GNSS jamming is interference with frequencies from external sources, which can lead the receiver to lose position and time information. Spoofing occurs when fake GNSS signals interfere with a receiver, thus deceiving users by displaying distinct but inaccurate locations or times.

The GNSS should have protection mechanisms to detect and avoid jamming and spoofing.

1.9 Mission-Critical Services Support

To ensure the success of all operations, it is crucial for PPDR users to have access to reliable Mission-Critical Services. Therefore, device manufacturers are required to incorporate support for 3GPP Mission-Critical Services standardized functionality and demonstrate an ongoing dedication to supporting new 3GPP releases in order to achieve this goal.

The device shall support, at least, the 3GPP Mission-Critical Services dedicated Quality-of-Service (QoS) class identifiers (QCI, 5QI) 65, 67, 69, and 70.

3GPP Mission-Critical Services require that the device supports dedicated functions that include, but are not limited to:

- Securing priority access for the MCX client to relevant device resources, such as microphone and speaker, etc.
- Dedicated bearers and associated QoS mechanisms
- Ambience listening
- Contributing to relevant KPIs, e.g. mouth-to-ear latency, can be met end-to-end.
- The device shall support 3GPP-standardised MCPTT group communications, enabling communication among multiple users.
- Where supported by the network, the device should support multicast/broadcast delivery (LTE eMBMS and/or 5G MBS) to enable efficient use of radio resources during large-scale PPDR operations

1.10 Device Identification

Hermetically sealed, especially devices without removable battery shall have an alternative way to track IMEI/serial numbers.

For example, RFID/NFC tags or standardized QR codes that produce a unified data output format.

2. Requirements for Rugged Smartphone

Rugged Commercial of-the-shelf (COTS) phones, specifically engineered to withstand extreme conditions, physical impacts, and harsh environments that would destroy standard devices.

Shall fulfill Requirements for All Handheld Device Categories and additional requirements in this chapter.

2.1 Environmental

Devices shall be able to function effectively in harsh environments and withstand physical hazards such as moisture, water, dust, heat, and cold. The devices shall be designed to withstand repeated drops from typical operating heights onto hard surfaces without sustaining damage.

Specific requirements that shall be met:

- Operational temperature range -30 to +55 Celsius
- Storage temperature range -30 to +65 Celsius
- Protection mechanism for contacts, gaskets and enclosures to avoid corrosion after contact with salt water

2.2 Hardware

2.2.1 Display

The display and resolution shall be sized in a way that supports effective interaction with MCX applications. It shall also be scratch-resistant and readable in both bright sunlight and complete darkness. To conserve battery, the display shall automatically adjust to changing lighting conditions and it shall also be possible to have the display switched off during PTT operations. Users shall be able to operate the touch screen in wet conditions while wearing gloves.

2.2.2 Battery

- Device shall support Battery Health and Charging Optimization (Limit to 80%).
- The device should support a wireless charging solution compatible with Qi 1 and Qi 2.
- The battery should be exchangeable without any disconnection in MCX communication, allowing for hot swapping functionality at minimum 30 seconds time.

2.2.3 Camera

The device shall have a front camera with at least 8 Megapixel resolution. and a back camera with at least 10 Megapixel resolution and flash. These cameras shall be capable of capturing high-quality photos and videos with the details and clarity needed for identification purposes of individuals and objects such as license plates. The camera system shall be able to operate both in bright daylight and under low lighting conditions.

2.3 Usability

2.3.1 PTT Button

To facilitate an easy and intuitive hardware platform, on the primary talk group in an MC PTT application, the device shall feature a dedicated push-to-talk button.

2.3.2 Emergency Button

To facilitate an easy and intuitive hardware platform, using the emergency function in an MC PTT application, the device shall feature a dedicated emergency button.

2.3.3 User interface

The device shall have easy to use MCX application.

See Appendix **C** – UX requirements on Ruggedized devices

3. Requirements for Broadband MC Radio

The device for voice communication only. A rugged handheld with a physical keypad or just only physical buttons and small display. Designed for reliable operation with gloves and for users who may need to operate the device without looking at the display.

Shall fulfill Requirements for All Handheld Device Categories, Rugged Smartphone and additional requirements in this chapter.

3.1 Environmental

Devices shall be able to function effectively in harsh environments and withstand physical hazards such as moisture, water, dust, heat, and cold. The devices shall be designed to withstand repeated drops from typical operating heights onto hard surfaces without sustaining damage.

Specific requirements that shall be met:

- Protection class IP68
- Dropping the device without damage from 3 meters onto hard, rough surfaces

3.2 Hardware

3.2.1 Display

The display may be small indicating talk group for example. If the functionality is built in to hardware, it might be possible that display is not needed at all. MCX connection and coarse signal strength indicator shall be visible in small display or for example single multicolor LED.

3.2.2 Battery

The device and its battery should be optimized according to:

- Duty cycle 80% standby / 20% for active use (screen is with full brightness) at +20 °C and -110 dBm RSRP signal strength, should be at least 16h when using MCX application.
- Duty cycle 80% standby / 20% for active use at -20 °C and -110 dBm RSRP signal strength, should be at least 16h when using MCX application
- Maintaining 90% of the initial capacity after 2000 cycles (from 20% charge to 100% charge) of normal charging

- The removable battery should be offered in multiple configurations, with different capacities, charging methods (e.g., cradle charging or USB charging), and temperature ratings.

3.2.3 Camera

The camera is not mandatory but if that exists 2 Megapixel resolution will be enough.

3.2.4 External antenna and external antenna connector

Device shall be equipped with external antenna for <1GHz bands.

External antenna connector to facilitate connectivity to vehicle installation kit with external antennas power supply and data connectivity (RJ-45).

When terminal is docked device transmitter should compensate feeder cable losses towards the antenna to get +23 dBm on antenna port.

3.2.5 RF OTA antenna performance

RF performance shall be the best possible, following RF OTA performance criteria measured according to the 3GPP TR 37.977 V17.0.0 (2022-03) and 3GPP TR 25.914 V17.0.0 (2022-03 Technical Specification Group Radio Access Network; Measurements of radio performances for UMTS terminals in speech mode (Release 17). Appendix A for devices with internal antenna and Appendix B for devices with external antenna.

RF OTA performance shall be optimized for < 1 GHz bands.

3.3 Usability

3.3.1 Speaker and microphone

The speaker/microphone setup shall be designed to account for factors such as wind or loud sirens and have the capability to produce intelligible and clear audio allowing for clear audio input and output for participants in a call, even in blue-light/siren situations with loudspeaker which shall generate volume with≥100 dB A when measured at 1m distance. Additionally, the device and its accessories shall protect users from sudden high-volume bursts of audio and provide warnings when selected output levels could potentially expose users to such bursts.

3.3.2 PTT button

To facilitate an easy and intuitive hardware platform, on the primary talk group in an MC PTT application, the device shall feature a dedicated push-to-talk button that

is tactile, easily identifiable, and easy to operate, including while wearing protective gloves.

3.3.3 Emergency button

To facilitate an easy and intuitive hardware platform, using the emergency function in an MC PTT application, the device shall feature a dedicated emergency button that is tactile, color-coded, e.g. red, and placed at the top of the device.

The design shall support usage of the emergency button even while wearing protective gloves.

3.3.4 Talk group selection switch

To enable easy and seamless switching between talk groups, even while wearing protective gloves and without the need for visual assistance, the device should feature a button that is easy to operate by touch alone, such as a rotatable knob switch.

3.3.5 Programmable buttons

The device should have programmable buttons that can be set by using EMM. Each button should be programmable with specific in-app functions, like a second PTT (Push-to-talk) button, sending pre-defined messages, as well as system functions like talk group selection and opening an application.

3.3.6 User interface

The device shall have user interface that is tactile, easily identifiable, and easy to operate, including while wearing protective gloves.

3.3.7 MCX Client

MCX client shall be implemented so that there is no need for display. The basic Push to Talk functionality is enough. The device manufacturer shall provide a standardized API for installing third party MCX application.

3.3.8 Peripherals connectors

All physical connectors for peripherals shall be waterproof, robust, and designed for heavy-handed use. The connectors shall provide robust, easy-to-use, secure locking mechanisms to avoid accidental disconnection. Although USB-C is standardized for all devices, additional connectors are required as a minimum:

- Side or bottom connector with support for PTT, emergency button, and audio

- Exposed charging pins that enable the device to have robust charging contacts. e.g. pogo pins to be used for charging in single- and multi-docking stations
- Bluetooth version 5.0 or higher and NFC for pairing. It shall be possible to block the use of Bluetooth via the EMM. Bluetooth shall support Secure Connections security mode 4, level 4.

3.4 Accessories

The device manufacturer shall be able to provide or support several accessories for the device:

- Earphone with PTT button connected to device via side connector using robust locking mechanism to avoid accidental disconnections
- Single- and multi-battery charging banks, for removable batteries
- RSM (Remote Speaker Mike) with adjustable volume and talk group selector, emergency button, and wired connector for earpiece (3,5 mm audio jack.) The Remote Speaker Microphone (RSM) shall provide a maximum A-weighted sound pressure level of at least 95 dB(A), measured at a distance of 30 cm under defined acoustic test conditions. A maximum output of 100 dB(A) is recommended for high-noise PPDR environments. Noise and echo cancellation included.
- Bluetooth RSM with specifications like the above wired RSM

All accessories shall be waterproof, robust and designed for heavy-handed use and able to use the device's robust, easy-to-use, secure locking mechanism to avoid accidental disconnections.

3.5 Security and Firmware

3.5.1 Lifecycle support

The device manufacturer should provide full support for operating system, security updates and bug fixes affecting usability for the device for six (6) years from its launch date.

4. Requirements for Rugged Mission-Critical Broadband Handheld

The baseline in the NCCOM White Paper v1.0. Full environmental and drop requirements, wide temperature range, loud audio, an external antenna connection, physical keys for push to talk, emergency and talk group selection, and long support commitment. Built for continuous outdoor duty.

Shall fulfill Requirements for All Handheld Device Categories, Rugged Smartphone, Broadband MC Radio and additional requirements in this chapter.

4.1 Hardware

4.1.1 Band support

Band 31, n31 (450) shall be supported optionally depending of the device variant

4.2 Accessories

The device manufacturer shall be able to provide or support several accessories for the device:

- Vehicle mount that allows for charging and facilitates connectivity with external antenna for <1GHz bands, audio accessories, MC-Data connectivity, and displays mounted in the vehicle.
- RSM as mentioned in the previous section 3.4.
- The device should support optional, attachable D2D communication modules for different communication technologies, such as 5G Sidelink, mesh/multi-hop networks, 450 MHz systems, TETRA, and other tactical radio solutions.

4.3 Device-to-device communication

End-users require access to reliable and predictable communication services even when network connectivity is lacking. TETRA DMO (direct-mode operation) operating in TETRA-band (380–430 MHz) will be used until 3GPP technologies can provide a proven solution for device-to-device (D2D) communication, and interoperability to PPDR TETRA DMO is no longer needed.

D2D Sidelink can be either built into the terminal or an addon communication module if not supported by the terminal

The device shall support 5G NR Sidelink operation in out-of-coverage and GNSS-denied conditions. Sidelink communication shall not depend on GNSS availability and shall support 3GPP-defined alternative synchronization mechanisms, including synchronization from another Sidelink UE (SyncRef UE / SLSS) and autonomous operation were supported by the applicable 3GPP specification.

4.4 Security and Firmware

4.4.1 Device and application access

The device shall support various security methods for accessing.

- PIN
- Password
- Biometric authentication
- Face unlocks
- Identity card

4.5 E2EE

PPDR organizations need to communicate and share information without risking the interception or leaking of sensitive information.

The device should have the capability to support end-to-end encryption solutions that are interoperable with currently deployed end-to-end solutions in TETRA devices.

Third-party vendors are providing this functionality based on a smart card that is to be added to the device.

4.6 NTN/LEO Direct-to-handheld device communication

PPDR users operating in rural areas without coverage from the mobile network are dependent on other ways to facilitate communication.

The device manufacturer shall follow, and preferably contribute to, the standardization initiatives within 3GPP and TCCA to find a solution for satellite-to-device communication (NTN) to be implemented in the device.

NTN and future PPDR devices

The strongest candidate for European satellite-to-handheld services is European 2 GHz MSS band n256.

4.7 Support for Modules

Devices should have support for Sidelink, Tetra, 450 MHZ by add on module to the device

5. Handheld Device Compare Table

Table 2. Handheld device compare table

Requirement	All Handheld Devices	Rugged Smartphone	Broadband MC Radio	Rugged Mission-Critical Broadband Handheld
Environmental				
1.1 Environmental	*	*	*	*
2.1 Environmental		*	*	*
3.1 Environmental			*	*
Hardware				
1.2.1 Band support	*	*	*	*
1.2.2 Carrier aggregation	*	*	*	*
1.2.3 5G Stand alone	*	*	*	*
1.2.4 Display	*	*	*	*
2.2.1 Display		*		*
3.2.1 Display			*	
1.2.5 Battery	*	*	*	*
2.2.2 Battery		*	*	*
3.2.2 Battery			*	*
1.2.6 Camera	*	*		*
2.2.3 Camera		*		*
3.2.3 Camera			*	
3.2.4 External antenna and external antenna connector			*	*
3.2.5 RF OTA antenna performance			*	*
1.2.7 SIM/eSIM	*	*	*	*
Usability				
1.3.1 Speaker and microphone	*	*	*	*
3.3.1 Speaker and microphone			*	*
2.3.1 PTT Button		*	*	*
3.3.2 PTT button			*	*
2.3.2 Emergency Button		*	*	*
3.3.3 Emergency button			*	*
3.3.4 Talk group selection Switch			*	*
3.3.5 Programmable buttons			*	*
2.3.3 User interface		*		*
3.3.6 User interface			*	
3.3.7 MCX Client			*	
1.3.2 Peripherals connectors	*	*	*	*
3.3.8 Peripherals connectors			*	*
Accessories				
1.4 Accessories	*	*	*	*
3.4 Accessories			*	*
4.2 Accessories				*

WiFi				
1.5 Wi-Fi hotspot	*	*	*	*
Device-to-device communication				
4.3 Device-to-device communication				*
Security and Firmware				
1.6.1 Hardware-Based Security Architecture	*	*	*	*
1.6.2 Lifecycle support	*	*	*	*
3.5.1 Lifecycle support			*	*
1.6.3 Internet access	*	*	*	*
1.6.4 Third-party EMM	*	*	*	*
1.6.5 Controlling external IP connections	*	*	*	*
1.6.6 Permitted applications	*	*	*	*
1.6.7 Device and application access	*	*	*	*
4.4.1 Device and application access				*
Standardisation and Certification				
1.7 Standardisation and Certification	*	*	*	*
Location services				
1.8 Location services	*	*	*	*
Mission-critical services				
1.9 Mission-critical services support	*	*	*	*
Device Identification				
1.10 Device Identification	*	*	*	*
End to End Encryption				
4.5 E2EE				*
Satellite-to-device				
4.6 NTN/LEO Direct-to-handheld device communication				*
Modules				
4.7 Support for Modules				*

6. Mobile Broadband Module

A mobile broadband module (also known as an embedded cellular module) is an internal hardware component that allows electronic devices like laptops, tablets, and routers to connect directly to cellular data networks (such as 4G LTE or 5G) without needing an external Wi-Fi connection.

Essentially, it acts as an integrated cellular modem. Unlike an external USB dongle, it is permanently attached or slotted directly into the device's motherboard and works in tandem with a built-in SIM card slot or eSIM to authenticate with a mobile network provider.

The cellular module is the common technical building block across all fixed and vehicle-mounted solutions. Any 4G/5G mission-critical user equipment therefore incorporates module functionality within a larger device or system. Irrespective of the final packaging, the module provides a fundamental connection to the mobile network.

The following section defines the scope of the cellular module and presents a set of basic requirements.

6.1 Band support

The module shall support at least ITU Region 1: Band 1 (2100), Band 3 (1800), Band 7 (2600), Band 8 (900), Band 20 (800), Band 28 (700), Band 38 (2600), B40 (2300), Band 68 (700) and NR Band n1 (2100), n3 (1800), n7 (2600), n8 (900), n20(800), n28 (700), n38 (2600), n40 (2300, n77 (3700), n78 (3500).

Bands 31 (450), n31 (450), n48 (3500), n75 (1500) should be supported optionally depending of device variant.

6.2 Carrier aggregation

LTE carrier aggregation

The device shall support applicable 3GPP-defined LTE carrier aggregation combinations used in Nordic public mobile networks, including:

- B1+B3+B20
- B1+B3+B7

Support for the B7+B68 LTE carrier aggregation combination is preferred, subject to network availability.

5G NSA

The device shall support the following 3GPP-defined EN-DC configuration:

- B20+n28

5G SA

The device shall support the following 3GPP-defined NR carrier aggregation combinations:

- n1+n28
- n1+n78
- n28+n78

6.3 Form Factor

6.3.1 Swappable Module

Connector type M.2 or Mini PCIe

6.3.2 Solder-on Module

LGA (Land Grid Array) or LCC (Leadless Chip Carrier)

6.4 eSIM/SIM

A SIM card is typically installed in a separate SIM holder, and the module shall be able to access at least eSIM + 2 physical SIM slots with support for Dual SIM Dual Standby (DSDS).

6.5 Positioning

The module shall have built-in GNSS receiver for positioning and timing. SAS-capable GNSS receiver with OSNMA

6.6 MIMO Antenna Connection

Antennas are typically designed on device level, and the module shall be able to connect to the antennas. Following antenna signals shall be supported, either one by one or in combinations.

- Tx (Transmitter)
- Rx (Receiver)
- Rx Diversity (Receiver Diversity)
- Positioning (for positioning and timing)

7. Future Areas

Upcoming versions of the NCCOM white paper should broaden their scope beyond smartphones to cover, for example, vehicle-mounted equipment, fixed or mobile IoT and telematics solutions, and 4G/5G-connected wearables.

Vehicle-mounted User Equipment. In today's TETRA market, vehicle equipment is supplied either as complete radio packages or as PEI-based connectivity units linked to vehicle systems. It needs to be assessed whether these packaging models remain suitable for 4G LTE and 5G. Key considerations include user and machine-to-machine interfaces, controls, local computing, management, environmental characteristics and the accessory ecosystem. It needs to be considered that vehicle mounted use cases may largely vary between countries and generate varying requirements.

IoT/Telematics User Equipment. Today's integrated modules often combine a TETRA modem, business logic, power and I/O within a single package forming complete RTUs. 4G/5G-based RTUs similarly often incorporate I/O, local computing, IoT protocol support, Ethernet, Wi-Fi, GNSS and multi-SIM connectivity. The required core components and accessory ecosystem need to be assessed. It needs to be considered that use cases may largely vary between countries and thus generate varying requirements.

4G/5G-connected wearables. E.g. body-worn cameras, smart glasses, biometric sensors, alerting devices and other connected wearables.

Direct-mode and alternative-coverage operation. 3GPP-based Sidelink offers potential for direct device-to-device communication without terrestrial network coverage, while non-terrestrial networks (NTN) could provide an alternative connectivity path via satellite. Both technologies show promise as complements to terrestrial On-Net MCX and are candidates for inclusion in future NCCOM white-paper versions, subject to ongoing evaluations of maturity, interoperability, device support and operational suitability.

Additional OS. Although Android is currently the predominant operating system for push-to-talk (PTT) over 3GPP networks, the mission-critical device ecosystem will increasingly include other operating systems. Examples include Linux, particularly for equipment with long and inflexible product life cycles such as telematics devices; iOS; and proprietary operating systems used in devices with physical controls and an embedded native PTT client. To accommodate this, the NCCOM requirement structure separates an operating-system-agnostic core from operating-system-specific profiles covering enrolment, device management, application distribution and client integration. Android is the first such profile. Future versions of this White Paper will add profiles for additional operating systems.

Abbreviations & Terms

Table 3. Abbreviations and terms

Abbreviations & Terms	
3GPP	The 3rd Generation Partnership Project
ATEX	Atmosphère Explosive
D2D	Device-to-Device
DMO	Direct-Mode Operation
eMBMS	Evolved Multimedia Broadcast Multicast Services
EMM	Enterprise Mobility Management
E2EE	End-to-End Encryption
eSIM	a digital SIM built into the device
GALILEO	European Global Satellite-Based Navigation System
GPS	Global Positioning System
GCF	Global Certification Forum
GNSS	Global Navigation Satellite Systems
GSM	Global System for Mobile Communications
GSMA	GSM Association
IMEI	International Mobile Equipment Identity
IP	Ingress Protection
IoT	Internet of Things
MC	Mission Critical
MC PTT	Mission-Critical Push-to-talk
MCX	Mission-Critical services
MBS	Multicast Broadcast Services
NIST	National Institute of Standards and Technology
NFC	Near-Field Communication
NR	New Radio
NTN	Non-Terrestrial Networks
NCCOM	Nordic Critical Communication Operators Meeting
OTA	Over-the-Air
OS	Operating system
Pogo pin	Spring-loaded, electrical connector pin
PRS	GALILEO Public Regulated Service
PPDR	Public Protection and Disaster Relief
PTT	Push-to-talk
QCI	QoS Class Identifier
QoS	Quality of Service
RF	Radio Frequency
RF OTA	RF performance Over-the-Air
RSRP	Reference Signal Received Power
SIM	Subscriber Identity Module
TETRA	TETRA | Terrestrial Trunked Radio – ETSI
TRP	Total Radiated Power
TRS	Total Radiated Sensitivity
USB-C	Universal Serial Bus Type C
UX	User experience

Appendix A - RF OTA for devices with internal antenna

Table 4. RF OTA Required TRP Values for LTE Bands

ITU Region 1 Frequency Band LTE	Required Values for TRP [dBm]		
	BHH	Browsing	Free Space
Band 1 (2100 MHz)	13.5	15.5	18.5
Band 3 (1800 MHz)	13.5	15.5	18.5
Band 7 (2600 MHz)	13.5	15.5	18.5
Band 8 (900 MHz)	14	16	20
Band 20 (800 MHz)	14	16	20
Band 28 (700 MHz)	14	15,5	18,5
Band 31 (450 MHz)	14	16	20
Band 38 (2600 MHz)	14	15,5	18,5
Band 40 (2300 MHz)	13.5	16	20
Band 68 (700 MHz)	14	15,5	18,5

Table 5. RF OTA Required TRS Values for LTE Bands

Frequency Band LTE	Required Values for TRS [dBm]		
	BHH	Browsing	Free Space
Band 1 (2100 MHz)	-89	-91	-93
Band 3 (1800 MHz)	-89	-91	-93
Band 7 (2600 MHz)	-89	-91	-93
Band 8 (900 MHz)	-92	-93	-95
Band 20 (800 MHz)	-92	-93	-95
Band 28 (700 MHz)	-92	-93	-95
Band 31 (450 MHz)	-92	-93	-95
Band 38 (2600 MHz)	-89	-91	-93
Band 40 (2300 MHz)	-89	-91	-93
Band 68 (700 MHz)	-92	-93	-93

Table 6. RF OTA Required TRP Values for NR Bands

Frequency Band NR	Required Values for TRP [dBm]		
	BHH	Browsing	Free Space
n1 (2100 MHz)	13,5	15,5	18,5
n3 (1800 MHz)	13,5	15,5	18,5
n7 (2600 MHz)	13,5	15,5	18,5
n8 (900 MHz)	14	16	20
n20 (800 MHz)	14	16	20
n28 (700 MHz)	14	16	20
n31 (450 MHz)	14	16	20
n38 (2600 MHz)	13,5	15,5	18,5
n40 (2300 MHz)	13,5	15,5	18,5
n68 (700 MHz)	14	16	20
n75 (1500 MHz)	13,5	15,5	18,5
n77 (3700 MHz)	13,5	15,5	18,5
n78 (3500 MHz)	13,5	15,5	18,5

Table 7. RF OTA Required TRS Values for NR Bands

Frequency Band NR	Required Values for TRS [dBm]		
	BHH	**Browsing**	**Free Space**
n1 (2100 MHz)	-89	-91	-93
n3 (1800 MHz)	-89	-91	-93
n7 (2600 MHz)	-89	-91	-93
n8 (900 MHz)	-92	-93	-95
n20 (800 MHz)	-92	-93	-95
n28 (700 MHz)	-92	-93	-95
n31 (450 MHz)	-92	-93	-95
n38 (2600 MHz)	-89	-91	-93
n40 (2300 MHz)	-89	-91	-93
n68 (700 MHz)	-92	-93	-95
n75 (1500 MHz)	-89	-91	-93
n77 (3700 MHz)	-89	-91	-93
n78 (3500 MHz)	-89	-91	-93

Appendix B - RF OTA for devices with external antenna

Table 8. RF OTA Required TRP Values for LTE Bands

ITU Region 1 Frequency Band LTE	Required Values for TRP [dBm]		
	BHH	Browsing	Free Space
Band 1 (2100 MHz)	13.5	17	20
Band 3 (1800 MHz)	13.5	17	20
Band 7 (2600 MHz)	13.5	17	20
Band 8 (900 MHz)	14	18	20
Band 20 (800 MHz)	14	18	20
Band 28 (700 MHz)	14	18	20
Band 31 (450 MHz)	14	18	20
Band 38 (2600 MHz)	14	18	20
Band 40 (2300 MHz)	13.5	17	20
Band 68 (700 MHz)	14	18	20

Table 9. RF OTA Required TRS Values for LTE Bands

Frequency Band LTE	Required Values for TRS [dBm]		
	BHH	Browsing	Free Space
Band 1 (2100 MHz)	-89	-93	-95
Band 3 (1800 MHz)	-89	-93	-95
Band 7 (2600 MHz)	-89	-93	-95
Band 8 (900 MHz)	-92	-99	-102
Band 20 (800 MHz)	-92	-96	-102
Band 28 (700 MHz)	-92	-96	-102
Band 31 (450 MHz)	-92	96	-102
Band 38 (2600 MHz)	-89	-93	-95
Band 40 (2300 MHz)	-89	-93	-95
Band 68 (700 MHz)	-92	-96	-102

Table 10. RF OTA Required TRP Values for NR Bands

Frequency Band NR	Required Values for TRP [dBm]		
	BHH	Browsing	Free Space
n1 (2100 MHz)	13,5	17	20
n3 (1800 MHz)	13,5	17	20
n7 (2600 MHz)	13,5	17	20
n8 (900 MHz)	13,5	20	20
n20 (800 MHz)	13,5	20	20
n28 (700 MHz)	13,5	20	20
n31 (450 MHz)	13,5	20	20
n38 (2600 MHz)	13,5	17	20
n40 (2300 MHz)	13,5	17	20
n68 (700 MHz)	13,5	20	20
n75 (1500 MHz)	13,5	17	20
n77 (3700 MHz)	13,5	17	20
n78 (3500 MHz)	13,5	17	20

Table 11. RF OTA Required TRS Values for NR Bands

Frequency Band NR	Required Values for TRS [dBm]		
	BHH	Browsing	Free Space
n1 (2100 MHz)	-90	-93	-95
n3 (1800 MHz)	-90	-93	-95
n7 (2600 MHz)	-90	-93	-95
n8 (900 MHz)	-93	-99	-102
n20 (800 MHz)	-93	-99	-102
n28 (700 MHz)	-93	-99	-102
n31 (450 MHz)	-93	-99	-102
n38 (2600 MHz)	-90	-93	-95
n40 (2300 MHz)	-90	-93	-95
n68 (700 MHz)	-93	-99	-102
n75 (1500 MHz)	-90	-93	-95
n77 (3700 MHz)	-90	-93	-95
n78 (3500 MHz)	-90	-93	-95

Appendix C – UX requirements on Ruggedized devices

To facilitate an easy and intuitive hardware platform, on the primary talk group in an MC PTT application, the device shall feature a dedicated push-to-talk button that is tactile, easily identifiable, and easy to operate, including while wearing protective gloves.	
	When the PTT button is operated, the device design shall prevent accidental activation of secondary buttons on the opposite side of the device, allowing the user to initiate critical communication without unintended interference. This shall apply to all standard operational grips, whether the device is handheld or mounted on a vest or belt.
	All hardware buttons shall be reachable and operable with the thumb or fingers of the hand holding the device, allowing the user to maintain a secure grip while operating the device, even when it is attached to a vest or belt.
	The PTT button shall be intuitively identifiable by physical feel through distinct texture, elevation, or tactile edges, allowing the user to locate the control instantly without visual aid, even while wearing thick protective gloves.
	The dedicated PTT button shall provide a clear tactile or haptic feedback upon activation, allowing the user to receive positive confirmation of the transmission by physical feel, even while wearing thick protective gloves.
	The PTT button shall be placed on the upper half left (seen from the front side of the device) long side of the device.
	The PTT button shall be sized to accommodate two adjacent fingers, allowing the user to apply sufficient pressure and maintain reliable control, even while wearing thick protective gloves.

	The device shall support full PTT functionality without requiring interaction with the display, allowing the user to initiate communication rapidly.
To facilitate an easy and intuitive hardware platform, using the emergency function in an MC PTT application, the device shall feature a dedicated emergency button that is tactile, color-coded, e.g. red, and placed at the top of the device. The design shall support usage of the emergency button even while wearing protective gloves.	
	The dedicated emergency button shall provide distinct tactile or haptic feedback when pressed, allowing the user to receive immediate and positive confirmation that the button was pressed, even through thick protective gloves.
	The dedicated emergency button shall be easily identifiable when visually inspecting the device. For example, being color-coded in a contrasting and distinct color.
	The emergency button shall be located at the geometric center of the device's top surface, allowing the user to access the control intuitively with either hand when the device is oriented in its intended use position.
	The Emergency button shall have clear texture, elevation and/or edges, allowing the user to intuitively identify the emergency button without looking, by physical feel alone, even while wearing thick protective gloves.
The device shall feature easy-to-operate, by touch alone button(s), for easy and seamless toggling between talk groups. The button(s) shall be protected from unintentional use, manageable while wearing protective gloves, and without the need for visual assistance.	
	The device shall feature dedicated or programmable physical controls for talk group selection, allowing the user to toggle or switch between at least two pre-selected talk groups, even while wearing thick protective gloves.(Note: If multiple channels are monitored simultaneously, this control may refer to switching the active talk

	group while maintaining passive monitoring of others.)
	The talk group controls shall be intuitively identifiable by physical feel alone, allowing the user to locate the correct control without visual aid, even while wearing thick protective gloves.
	The talk group controls shall be designed for effortless physical operation (e.g., press or rotate), allowing the user to perform the switch reliably under stress, even while wearing thick protective gloves.
	The talk group controls shall provide distinct tactile or haptic feedback for each step, position, or activation, allowing the user to receive positive confirmation of the change by physical feel, even while wearing thick protective gloves.
	The talk group controls shall be protected by design against accidental rotation or activation, allowing the user to move freely in demanding environments without unintended channel changes.
The display and resolution shall be sized in a way that supports effective interaction with MCX applications. **It shall also be scratch-resistant and readable in both bright sunlight and complete darkness.** **To conserve battery, the display shall automatically adjust to changing lighting conditions and it shall also be possible to have the display switched off during PTT operations.** **Users shall be able to operate the touch screen in wet conditions and while wearing gloves.**	
	The display should be of a size that is easily operated with one hand, allowing the user to access all parts of the screen while maintaining a secure grip, even when the device is mounted on a vest or belt.
	Users should be able to read and comprehend content shown on the display when glancing at the device screen without unmounting it from standard positions (such as vest or belt) and handling the device with minimal effort.

	The device shall prevent involuntary touch display interactions when mounted in standard positions (display inwards and outwards), allowing the user to operate the PTT and move freely without risking unintended display inputs.
	Users shall be able to easily use the PTT functionality while the display is off, preventing unintended touch display inputs and avoiding light emission that could compromise the user's position when operating in stealth conditions.
Speaker and microphone **To ensure effective communication in all typical environments, the device should include speakers and microphones that allow for clear audio whether held to the ear or worn on the shoulder.** **The speaker/microphone setup shall be designed to account for factors such as wind or loud sirens and have the capability to produce intelligible and clear audio allowing for clear audio input and output for participants in a call, even in blue light/siren situations. Additionally, the device and its accessories shall protect users from sudden high-volume bursts of audio and provide warnings when selected output levels could potentially expose users to such bursts.**	
	It should be easy for the user to adjust the volume up/down with dedicated or programmable button(s)/rotary, even while wearing thick protective gloves.
	The provided warning for potentially harmful sound pressure levels should be intuitive, easy dismissible, and offer a possibility to be disabled.
The device shall have a front camera with at least 2 Megapixel resolution and a back camera with at least 8 Megapixel resolution and flash. **These cameras shall be capable of capturing high-quality photos and videos with the details and clarity needed for identification purposes of individuals and objects such as license plates.**	

The camera system shall be able to operate both in bright daylight and under low lighting conditions.	
	Image capturing and the start/stop of video recording shall be easily executable entirely with one hand.
	The device's surface and the camera placement shall be designed to ensure that fingers do not unintentionally obscure the lens or the flash when the device is held in a steady one-handed grip, even while wearing thick protective gloves.
The device manufacturer shall be able to provide or support several accessories for the device: • **single- and multi-docking stations and charger** • **earphone with PTT button connected to device via side connector using robust locking mechanism to avoid accidental disconnections and, e.g., USB-C or audio jack.** **All accessories shall be waterproof, robust and designed for heavy-handed use and able to use the device's robust, easy-to-use, secure locking mechanism to avoid accidental disconnections.**	
	The device shall be intuitive and easy to dock and charge using a supported docking station or charger.
	The device or supported charger/docking station needs to clearly communicate charging status to the user.
	The supported wired accessories should be easy to attach/detach and lock into place, via the side connector, even while wearing thick protective gloves.
	It should be clear to the user that the wired accessory is attached securely on the side connector.
	Hot swapping the device's battery should be intuitive and easy for the user.
	It should be clear to the user that the battery is attached securely after hot swapping it out for a new one.

Appendix D – Gloves

Purpose

This document defines the baseline profile for the reference protective gloves used across all end-user scenarios, and mentions in requirement descriptions. Using a standardized glove profile ensures that all hardware is evaluated against the same realistic operational constraint, regarding glove material thickness and touchscreen compatibility. This ensures an accurate context of use, and a fair evaluation between the devices.

Standardization

EN 659:2003+A1:2008 is a specialized European standard that defines the requirements and test methods for protective gloves for firefighters. It ensures that gloves provide adequate hand protection during normal firefighting operations, including search and rescue missions. This standard builds upon and references foundational testing procedures from other standard glove specifications, primarily EN 420 (general requirements), EN 388 (mechanical risks), and EN 407 (thermal risks).

Dynamic Selection and Reference Examples

The models detailed below represent verified field examples provided by the Greater Stockholm Fire Brigade (Storstockholms brandförsvar - SSBF) and the Swedish Police Authority (Polismyndigheten). They serve as the guiding benchmark for the material properties required.

Operational Boundaries (Exclusions)

This framework evaluates manual interaction with the terminal during standard tactical field operations (e.g., traffic accidents, patrolling, frisking/search operations, handling detained individuals, and checkpoint duties).

It explicitly excludes extreme environments like active smoke diving (rökdykning). In those scenarios, personnel utilize mask-integrated communication (e.g., Spirocom) or external PTT units (e.g., INVISIO) connected via routing cables. Operatives configure their talk groups before entry, and direct manual interaction with the terminal chassis is operationally prohibited due to extreme thermal and environmental hazards. Therefore, Hardware usability is not benchmarked against smoke-diving glove profiles.

Evaluation Focus Areas

Regardless of the exact brand or model selected in cooperation with the user organization, the reference glove must enforce the following testing dynamics:

- **Physical Control Accessibility:** The glove's bulk and material composition (such as heavy leather or insulation) must actively challenge whether the device's PTT, Emergency button, and talk group controls can be identified and operated by physical feel alone, without visual aid.
- **Touchscreen Error Prevention:** The widened fingertip footprint caused by the glove's insulation or reinforced seams must test the device's user interface target sizes and its ability to suppress accidental touch inputs
- **Mechanical Operation:** Material stiffness must be tested to determine whether the user can securely execute tactical actions, attach wired side accessories, or complete battery hot swaps without utilizing tools.