Feasibility study on deployment and implementation of a Cell Broadcast Service (CBS) solution for sending Alert Messages

MD-ALERT

December 2023

Table of Contents

Acronyms

3GPP	3rd Generation Partnership Project
AMF	Access and Mobility Function
ATIS	Alliance for Telecommunications Industry Solutions
BEREC	Body of European Regulators for Electronic Communications
BSC	Base Station Controller
CAP	Common Alerting Protocol
CB	Cell Broadcast
CBC	Cell Broadcast Center
CBE	Cell Broadcast Entity
CBS	Cell Broadcast Service
CMAS	Commercial Mobile Alert System
ETSI	European Telecommunications Standards Institute
EU	European Union
EW4A	Early Warning for All initiative
EWS	Early Warning System
GIES	General Inspectorate for Emergency Situations of Moldova
GSM	Global System for Mobile Communications
ITU	International Telecommunication Union
LB-SMS	Location-Based SMS
LTE	Long Term Evolution
MME	Mobility Management Entity
MNO	Mobile Network Operator
PWS	Public Warning System
RFQ	Request for Quotation
RNC	Radio Network Controller
STISC	Information Technology and Cyber Security Service of Moldova
SMS	Short Message Service
UMTS	Universal Mobile Telecommunications Systems

Introduction

Worldwide, the occurrence of natural disasters has been increasing since the 1940s, from an average of eight disasters per year to nearly 300 in the last decade.[1] Moldova has not been the exception and since its constitution in 1991, it has had sixteen natural disasters such as floods, extreme temperature, storms and droughts. The number of Moldovans affected by these disasters in the last three decades is near to 2,9 million, a considerable number compared to Moldova's population estimated at 2,5 million in 2023.[2]

Table 1. Natural disasters in Moldova (1994-2023)

Disaster Type	Number of events	Total Deaths	Number of Affected	Number of Homeless
Flood	7	61	51.108	849
Extreme temperature	3	23	12.834	
Storm	2	3	2.600.000	25.500
Drought	3	2	216.194	
Epidemic	1		1.647	
Total	**16**	**89**	**2.881.783**	**26.349**

Source: EM-DAT: The Emergency Events Database. Université Catholique de Louvain (UCL) - CRED, D. Guha-Sapir - www.emdat.be, Brussels, Belgium.

The increasing trend of natural disasters in the following years will not slow down. Thus, the need for tools that improve the response to such disasters, reducing the likelihood of human and material loss, is critical. One such tool is an Early Warning System (EWS) or Public Warning System (PWS).[3] An EWS is a cost-effective tool that saves lives, reduces economic losses, and provides a nearly tenfold return on investment, given that it provides timing warnings to the people regarding imminent emergencies and disasters.[4]

Due to the imperative need for an EWS in every country, the United Nations (UN) has launched the Early Warnings for All (EW4A) Initiative,[5] with the aim of having every person in the world covered by an EWS by 2027.[6] Under the EW4A framework, the International Telecommunication Union (ITU) is leading the "Warning Dissemination and Communication" pillar to ensure that warnings reach the people at risk in time to take action.[7] Because of the diversity of the

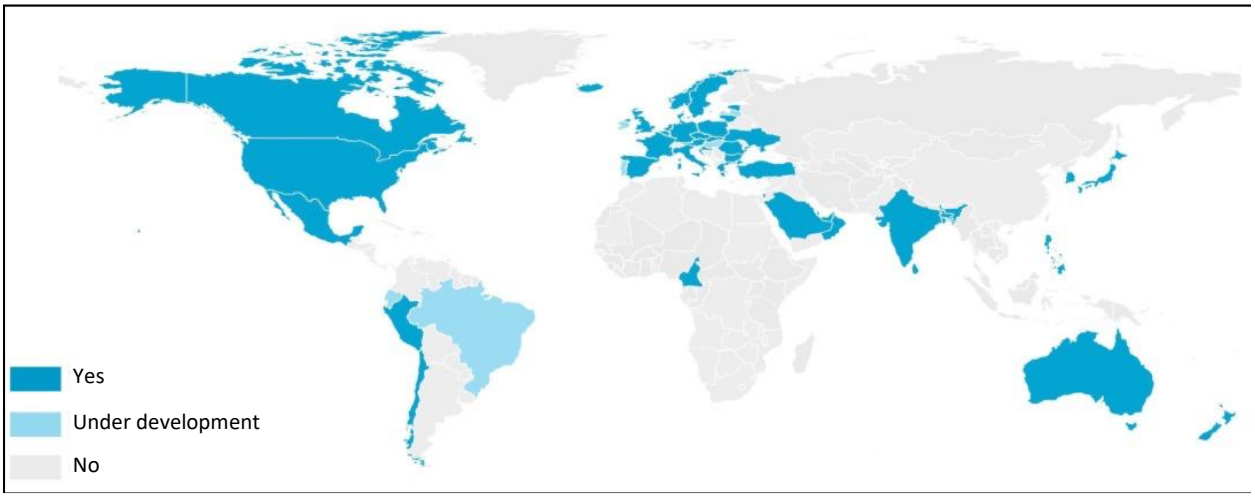
[1] EM-DAT: The Emergency Events Database. Université Catholique de Louvain (UCL) - CRED, D. Guha-Sapir - www.emdat.be, Brussels, Belgium.
[2] Id.
[3] Early Warning System (EWS): an integrated system of hazard monitoring, forecasting and prediction, disaster risk assessment, communication and preparedness activities systems and processes that enables individuals, communities, governments, businesses and others to take timely action to reduce disaster risks in advance of hazardous events. Source: United Nations General Assembly Resolution 69/284 from 1 December 2016.
[4] See: https://www.un.org/en/climatechange/early-warnings-for-all.
[5] Id.
[6] United Nations (2022) Early Warning for All Initiative Executive Action Plan 2023-2027.
[7] The ITU is leading the "Warning Dissemination and Communication" pillar jointly with the IFRC, REAP, UNDP and WMO.

communities at risk, the ITU promotes a multi-channel approach, i.e., using different communication channels such as radio, television, social media, sirens, mobile phones, satellite devices, among others, to reach such communities.[8]

However, given that ninety-five percent of the world's population has access to mobile broadband networks, and close to seventy-five percent of the population owns a mobile phone, mobile networks are a powerful communication channel to deliver alerts to people at risk of imminent hazard.[9] Therefore, the implementation of a geo-located mobile-based EWS using Cell Broadcast Service (CBS) or Location-Based SMS (LB-SMS) must be prioritized. In the second phase, additional communication channels like the ones mentioned above, can be added to the EWS. In fact, the Directive (EU) 2018/1972 of the European Parliament and of the Council required Member States to transmit public warnings through providers of mobile number-based interpersonal communication services (i.e., MNOs) to the end-users concerned.[10]

CBS and LB-SMS are proven technologies implemented by governments and MNOs in several countries (see worldwide deployment in Figure 1).[11]

Figure 1: Countries with mobile EWS in place (using CBS and/or LB-SMS*)



*Note from the source: work in progress, based on ITU research.
Source: ITU

The mobile network landscape in Moldova is no different from the world's trend. Currently, there are three mobile network operators (MNO) covering almost 100% of the population with 3G and

[8] See: https://www.itu.int/en/ITU-D/Emergency-Telecommunications/Pages/Early-Warnings-for-All-Initiative.aspx.
[9] Id. ITU (2022) Measuring digital development: Facts and Figures 2022.
[10] Article 110 of the Directive (EU) 2018/1972 of the European Parliament and of the Council of 11th December 2018 establishing the European Electronic Communications Code (EECC): "Public warning systems – 1. By 21 June 2022, Member States shall ensure that, when public warning systems regarding imminent or developing major emergencies and disasters are in place, public warnings are transmitted by providers of mobile number-based interpersonal communications services to the end-users concerned. 2. Notwithstanding paragraph 1, Member States may determine that public warnings be transmitted through publicly available electronic communications services other than those referred to in paragraph 1, and other than broadcasting services, or through a mobile application relying on an internet access service, provided that the effectiveness of the public warning system is equivalent in terms of coverage and capacity to reach end-users, including those only temporarily present in the area concerned (…)."
[11] 3GPP: 3rd Generation Partnership Project.

4G technologies. Mobile services penetration is 160%, i.e., 160 subscriptions per 100 inhabitants.[12] In addition, 5G networks are planned to be rolled out by 2024.

Table 2: Mobile telecommunications in Moldova

Mobile Network Operator	Technologies deployed	Total subscriptions (millions)	% of population coverage with mobile networks
Orange	2G, 3G, 4G	2,7	2G: not available 3G: 99% 4G: 99%
Moldcell	2G, 3G, 4G	1,7	2G: not available 3G: 99,9% 4G: 92%
Moldtelecom	3G, 4G	0,7	3G: 99,7% 4G: 41,2%

Source: ANRCETI

Considering the need of a PWS, as recommended by the UN, the coverage of mobile networks in Moldova above 99% of the population at least for 3G and 4G technologies, and the EU Directive prioritizing mobile networks to transmit public warnings, **we strongly recommend the implementation of a PWS based initially on mobile networks to deliver alert and warning messages to the people at risk of an imminent hazard in Moldova**. In future upgrades, the PWS should include other means or channels of communication such as broadcasting radio or television, mobile applications, and sirens, among others, to deliver alert and warning messages.

Cell broadcast and location-based SMS

Although the General Inspectorate for Emergency Situations of Moldova (GIES) has already decided to implement a CBS solution for the PWS, we still find it relevant to include a comparison between the two main mobile network technologies available, CBS and LB-SMS, to support and strengthen GIES' decision.

Table 3 presents a comparison between CBS and LB-SMS on specific characteristics.

Table 3: CBS and LB-SMS comparison

Characteristic	Cell broadcast Service (CBS)	Location-Based SMS (LB-SMS)
Mobile networks supported	2G, 3G, 4G, 5G	2G, 3G, 4G, 5G
Devices supported	Smartphone and feature phones	Smartphone and feature phones
Transmission type	Point-to-area messaging (broadcast)	Point-to-point messaging
Bi-directionality	Indirect (message should include a URL or web links or number to reply)	Direct (users can respond to the sender via SMS)

[12] ANRCETI (2022) Statistical yearbook development of electronic communications in the Republic of Moldova.

Characteristic	Cell broadcast Service (CBS)	Location-Based SMS (LB-SMS)
Geographic alerting capability	Inherent to the technology	Needs a Mobile Location Center (MLC) for location-based capability
Alert dissemination	Most devices in the region of interest will receive the alert	Subscription needed (SIM)
Visitor devices (roaming)	Alert messages are received by visitor devices	Roaming agreements needed, rate might be charged
Alert dissemination	Few seconds (less than 10 s)	Could take up to several minutes
Alerting mechanism	Unique standardized ringtone and vibration	Not standardized
Network congestion	Not affected by network congestion (during network congestion alerts still go through and are received by the device)	Affected by network congestion (during network congestion alerts do not go through and are not received by the device)
	Alerts do not contribute to network congestion	Alerts do contribute to network congestion
Privacy (location)	Subscriber location not needed for alert dissemination	Subscriber location needed for alert dissemination
Privacy (mobile number)	Does not require mobile numbers to be known	Does require mobile numbers to be known
Security	Higher (only MNO can broadcast a message)	Lower (source cannot be verified)

Source: vendor information on CBS and LB-SMS

In 2012, the 3GPP standardized CBS; therefore, today, CBS is supported on practically all devices and is commonly available in different operating systems (Android and iOS), without the need to download any application or the requirement to register. CBS alert messages are automatically displayed on the screen device, requiring users to acknowledge the message before they can continue using their device. In addition, the standard requires a worldwide unique ringtone and vibration, only used for emergency alert messages; therefore, the message is recognizable as an emergency alert anywhere.

CBS alert messages are disseminated or broadcasted to a specific geographic area reaching all devices within such area, from a few thousand devices (e.g., small towns) to millions (e.g., nationwide), in a few seconds. Devices, no matter if they are residents or visitors (e.g., roaming devices), will receive the CBS alert messages. In addition, since messages are repeated at a pre-defined interval, any new device (person) entering the geographic area will automatically receive the CBS alert message. However, devices within the geographic area that have already received the alert message, will not receive it again.

One of the key characteristics of CBS is that CBS is not affected by mobile network congestion during emergencies or in crowded areas. Since CBS utilizes a separate channel, different from the one used by regular SMS traffic, SMS traffic congestion does not affect the dissemination of CBS alert messages. For the same reason, CBS alert messages do not contribute to mobile network congestion. Even more, since CBS is a point-to-area (or point-to-multipoint), one-way transmission technology, the alert message sent only once can be received by all devices within the geographic area of interest.

Another key characteristic of CBS is security. Emergency alert messages disseminated through mobile networks using CBS can only be originated by a government-authorized alerting authority. No one can forward or modify the alert sent, nor can anyone not authorized originate an alert.

Finally, CBS does not need to know specific device or user information to send the CBS alert messages. As mentioned before, CBS broadcasts emergency alerts to a specific area, not knowing any specific information about the devices receiving the alert within such area (e.g., mobile number or specific location). Therefore, the privacy of the mobile operator's customers is protected.

Contrary to CBS, LB-SMS utilizes the well-known SMS text message technology and the SMS channel to deliver alert messages. Therefore, several key characteristics of LB-SMS make this option less attractive for delivering emergency alerts. For example:

- Alert messages are sent on a point-to-point basis as individual messages. This means that the alert message is delivered to each device on a one-by-one basis, through the commercial SMS channel, and not broadcasted through a different channel.
- LB-SMS alert messages are affected by network congestion, even if alert messages are prioritized. If multiple mobile users are sending SMS text messages in an area of concern (e.g., sending messages related to an emergency), it could take several minutes, and even a few hours, before the LB-SMS alert message reaches all the people in such area. In addition, LB-SMS alert messages can increase network congestion as well.
- LB-SMS does not have a standardized ringtone and vibration alert since LB-SMS messages are like SMS text messages, and therefore, the ringtone and vibration are identical to any other regular SMS text message, i.e., there is no distinction.
- LB-SMS cannot guarantee that the emergency alert message has been seen by the mobile user. It can only guarantee that the message was delivered to the device (once a receipt acknowledgment of the alert message is received).
- LB-SMS needs to track mobile devices to be able to send messages location-based, and it also needs the mobile number to send LB-SMS messages. Privacy concerns can arise if there are no proper regulations in place.

Although there are some advantages for LB-SMS, such as knowing the number of recipients of the alert message (receipt acknowledgment) or the capability of 2-way communications by sending back an SMS text message to the alert originator, and despite network capacity increasing in recent years for 4G and 5G mobile networks reducing the risk of network congestion, **a CBS solution for a PWS has certainly more advantages as described above and should be prioritized over an LB-SMS solution**. Therefore, we agree with GIES' decision to implement a CBS solution for Moldova's PWS. In future upgrades, a complementary LB-SMS solution might be implemented if needed.

* * *

This document is divided into five chapters including the introduction. Chapter two presents the objective and scope of the document. Chapter three provides a general overview of the CBS solution. Chapter four presents specific recommendations for Moldova to implement a CBS solution. Finally, chapter five (separate Word document) provides a detailed description of the

Terms of Reference (ToR) to open a procurement process to purchase a CBS solution, including support and maintenance for a number of years to be specified (10 years is recommended).

Objective and scope

The objective of this document is to provide a feasibility study to implement a Cell Broadcast Service (CBS) solution for Moldova's Public Warning System (PWS) to send early warning and alert messages to the people in Moldova.

The scope of the study is to provide advice and recommendations on the following topics:

- Estimated cost to implement a CBS solution
- Architecture of the CBS solution
- Management of the CBS solution
- Procurement process
- Terms of Reference (ToR) for the procurement process
- Legal and regulatory framework modifications needed to implement the CBS solution

Cell Broadcast General Overview

Cell Broadcast (CB) is a technology used to broadcast text messages via mobile networks to mobile end-users in a specific geographical area. Since messages are broadcasted from the cell site (point-to-multipoint message distribution), all mobile devices within the coverage area of the cell site receive the message. Messages can be delivered through all cell sites in the mobile network reaching millions of mobile end-users nationwide in few seconds, or to specific cell sites reaching mobile end-users in a specific geographic region of interest, also in few seconds.

In the following sections the following topics are addressed:

- The two main elements of a CBS solution: Cell Broadcast Center (CBC) and Cell Broadcast Entity (CBE)
- The two architectures to implement a CBS solution: centralized CBC and distributed CBC
- Examples of CBS implementations
- CBS standards

Cell Broadcast Center (CBC) and Cell Broadcast Entity (CBE)

A Cell Broadcast Service (CBS) consists of two main elements:

1) Cell Broadcast Center or CBC
2) Cell Broadcast Entity or CBE

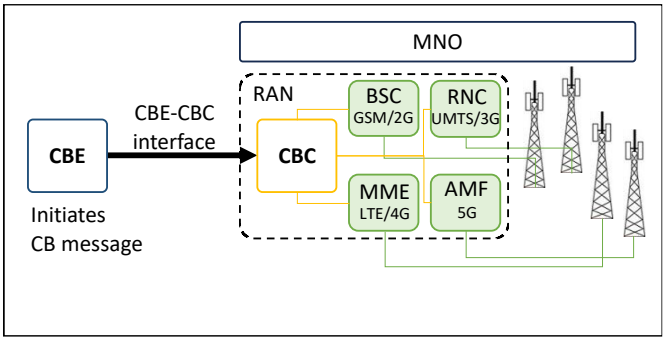
The CBC, standardized by the 3GPP, is a network element in the mobile core network connected to the Radio Access Network (RAN) controller (i.e., connected to the BSC for 2G or GSM networks, RNC for 3G or UMTS networks, MME for 4G or LTE networks, and AMF for 5G networks). It is

responsible for the management of the CB message, for example: creating and managing all CB messages, modifying, or deleting CB messages, replacing the content of a currently broadcasting CB message, eliminating CB messages currently being or waiting to be broadcasted, and listing the pending or currently broadcasting CB messages and their actual status, among others. The CBC is also responsible for determining the set of cells from which the CB message should be broadcast.

The CBE is an application connected to the CBC and is responsible for creating and formatting CB messages. The CBE can also receive alert messages from alerting authorities and forward them to the CBC once the messages have been verified. CB messages, including information such as target locations, message identifier, start time, end time and repetitions of CB messages to be delivered, should be provided by the CBE to the CBC. It is the responsibility of government alerting authorities (e.g., meteorological and seismology authorities) to create the CB message.

CB messages are sent by the CBE and received by the CBC. The CBC then relays the CB messages to mobile devices within the target area in near real-time through the RAN controllers of the MNO core network that broadcast the message to the end user's device. The CBE-CBC interface is not defined within the 3GPP standard. However, Common Alerting Protocol (CAP) could be used for such an interface, among other protocols offered by vendors of the CBS solution.

Figure 2. CBE-CBC implementation



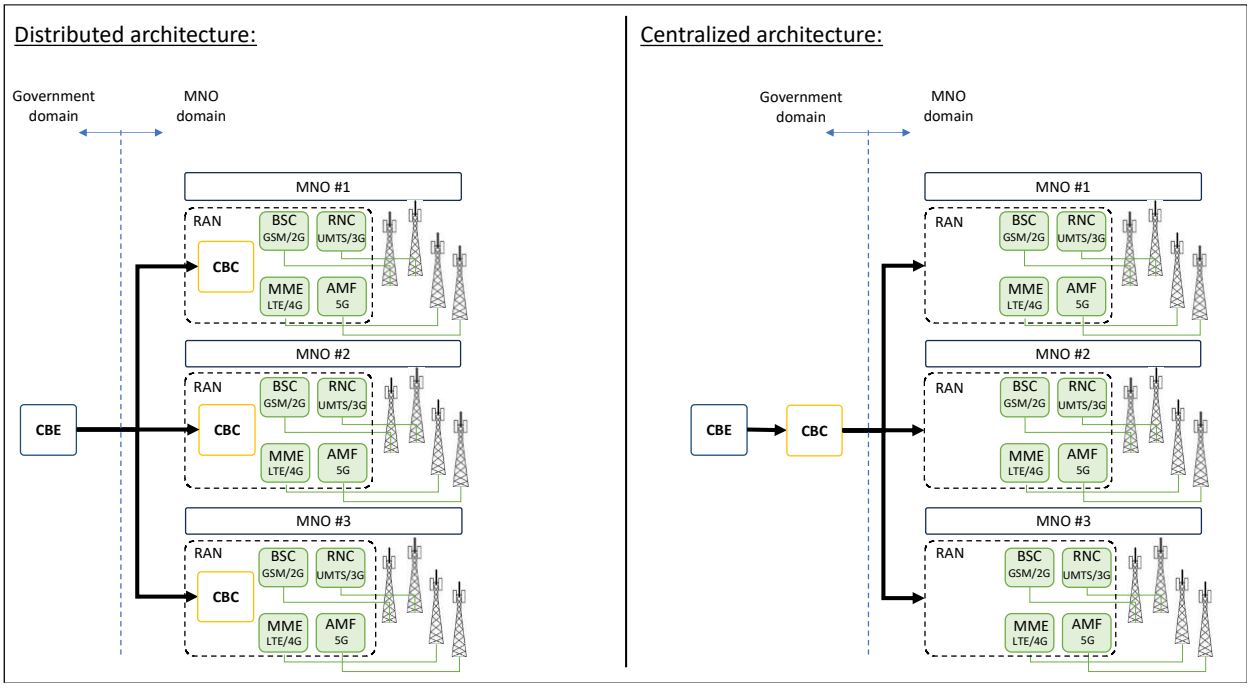
Cell broadcast architecture

There are two architectures for deploying the CBC:

(1) Distributed or decentralized architecture
(2) Centralized architecture

In the distributed architecture, a CBC is implemented for each MNO, while in the centralized architecture, one CBC is shared by all MNOs (see Figure 3). Since each MNO has its own CBC in the distributed architecture, the CBCs are managed by the MNOs, i.e., the CBC is within the MNO domain. On the contrary, in the centralized architecture, the CBC is owned and managed by the government, i.e., the CBC is within the government's domain.

Figure 3. Distributed CBC and centralized CBC architecture



Note: CBC: Cell Broadcast Center; CBE: Cell Broadcast Entity; RAN: Radio Access Network; BSC: Base Station Controller; RNC: Radio Network Controller; MME: Mobility Management Entity; AMF: Access and Mobility Function.

Centralized Cell Broadcast Center

The CBC is installed on the government's premises and is hosted and managed by the government. The MNO's radio access networks are all connected to this centralized CBC via a secure connection (e.g., VPN); therefore, the MNO must provide access to its infrastructure and share information from its network with the government. Sharing information might be of concern to privately owned MNOs; hence, the government must provide assurance that such information will be securely treated.

Distributed Cell Broadcast Center

Each CBC (one per MNO) is installed in the MNO's radio access network. Each MNO hosts and manages its own CBC with its own technical specificities. MNOs do not need to share any network information with a third party (e.g., the government); therefore, they keep control of their sensitive infrastructure and information.

Advantages and disadvantages: centralized CBC vs distributed CBC

Table 4 presents a summary of the general advantages and disadvantages of a centralized architecture versus a distributed architecture for the CBC.

Table 4: Advantages and disadvantages of a centralized CBC vs a distributed CBC

	Centralized CBC	Distributed CBC
Advantages	• Single CBC to purchase, lower capex and operational expenditure costs, and quicker installation time. • Government can take control of the whole Cell Broadcast functionality across all networks in the whole country in case of national emergency and if necessary, take the whole of the capacity for national needs. • Only one team of qualified expert technicians is needed to maintain the facility.	• Network takes full control of the CB channel and all its capabilities as the CBC can control access and use of the facility. • Confidential cell database does not leave the firewall of the network. • Network can exploit any commercial applications of CB. • Network can choose a favoured CBC vendor who supports their system technology and RAN vendor.
Disadvantages	• Government must bear the costs of installation and maintenance of the CBC. • Government must identify and train technicians with the skills and knowledge to maintain the CBC to a high state of readiness and availability. • Government needs to choose a vendor that can support all RAN vendors and system technologies applicable across all networks in the country. • Government needs to arrange for the cell data files to be updated in near real-time from the network's data centers.	• Overall cost of the project is multiplied by the number of different operators all needing their own CBC. • Networks need to identify and train suitable maintenance staff to maintain the CBC and ensure high availability as a matter of high priority particularly in times of national emergency.

CBS implementations

CBS solutions, both centralized and distributed architecture, have been deployed worldwide. Both architectures can comply with all CBS requirements and are technically feasible. For example, in countries like Bulgaria, Greece, Latvia, Peru, and Ukraine, a centralized CBC has been implemented and managed by the government. In other countries such as Germany, the Netherlands, Spain, and the United Kingdom, a distributed CBC has been implemented and managed by the MNOs.

In Greece, the CBC hosts three MNOs, i.e., supports direct connectivity to RAN controllers of all three MNOs. To avoid sharing information related to the mobile networks of any of the three

MNOs, a common database with distinct tables for each MNO's data is required. Thus, each database table will contain the respective MNO's data.

Similar to Greece, Latvia implemented (or is implementing) a centralized CBC architecture connected to the RAN equipment of all three MNOs. The CBC is managed by the Information Center of the Ministry of the Interior, while the CBE is managed by the State Fire and Rescue Service.

Cell Broadcast Standards

The system requirements for a PWS using the CBS must follow the ETSI TS 102 900 V1.4.1 (2023-06) standard "Emergency Communications (EMTEL); European Public Warning System (EU-ALERT) using the Cell Broadcast Service".

Additionally, the CBS solution must comply with the standards presented in Table 5.

Table 5: Standards the CBS solution must comply with

Standard	Description
CAP V1.2	Common Alerting Protocol (CAP) Version 1.2 – OASIS Standard (01 July 2010)
ATIS-0700006	CMAS via GSM-UMTS Cell Broadcast Service Specification
ATIS-0700008	CBE-CBC Interface Specification
ATIS-0700010	CMAS via EPS Public Warning System Specification
ATIS-0700013	Implementation Guidelines for Mobile Device Support of Multi-Language CMAS
ATIS-0700037	Enhanced Wireless Emergency Alert (EWEA) Federal Alert Gateway To CMSP Gateway Interface Specification (A Revised Version Of J-STD-101)
ATIS-0700043	Wireless Emergency Alert (WEA) 3.0 via 5G Public Warning System Specification
ETSI TS 102 182	Emergency Communications (EMTEL); Requirements for communications from authorities/organizations to individuals, groups or the general public during emergencies
ETSI TS 102 900	Emergency Communications (EMTEL); European Publica Warning System (EU-ALERT) using the Cell Broadcast Service
ETSI TS 122 268	Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; 5G; Public Warning System (PWS) requirements
ETSI TS 123 038	Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; Alphabets and language-specific information
ETSI TS 123 041	Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications Systems (UMTS); LTE; 5G; Technical realization of Cell Broadcast Service (CBS)
ETSI TS 125 419	Universal Mobile Telecommunications System (UMTS); UTRAN Iu-BC interface: Service Area Broadcast Protocol (SABP)

Standard	Description
ETSI TS 129 168	Universal Mobile Telecommunications System (UMTS); LTE; 5G; Cell Broadcast Centre interfaces with the Evolved Packet Core; Stage 3 (3GPP TS 29.168 version 17.1.0 Release 17)
ETSI TS 129 518	5G; 5G System; Access and Mobility Management Services; Stage 3
ETSI TS 148 049	Digital cellular telecommunications system (Phase 2+) (GSM); Base Station Controller - Cell Broadcast Centre (BSC-CBC) interface specification; Cell Broadcast Service Protocol (CBSP)
3GPP TS 22.268	Public Warning System (PWS) requirements
3GPP TS 23.038	Alphabets and language-specific information
3GPP TS 23.041	Technical realization of Cell Broadcast Service (CBS)
3GPP TS 25.419	UTRAN Iu-BC interface: Service Area Broadcast Protocol (SABP)
3GPP TS 29.168	Cell Broadcast Centre interfaces with the Evolved Packet Core; Stage 3
3GPP TS 29.518	5G System; Access and Mobility Management Services; Stage 3
3GPP TS 48.049	Base Station Controller - Cell Broadcast Centre (BSC-CBC) interface specification; Cell Broadcast Service Protocol (CBSP)

Cell Broadcast for Moldova

This chapter presents the recommendations related to the implementation of CBS in Moldova in the following topics:

- Estimated cost to implement a CBS solution
- Architecture of the CBS solution
- Management of the CBS solution
- Redundancy
- Procurement process
- Legal and regulatory framework modifications needed to implement the CBS solution

Cost comparison

Quotes based on a draft of the terms of reference (ToR) for a CBS solution were requested from three different CBS vendors. The ToR included options for both, centralized and distributed architectures for the CBC and with geographic redundancy, both for the CBC and the CBE. Table 6 provides an average of these quotes.[13]

[13] Since Non-Disclosure Agreements (NDA) were signed with the different vendors, information specific to each vendor cannot be provided.

Table 6. Cost comparison cell broadcast solution: centralized and distributed architectures

Item	Centralized architecture Values in €	Distributed architecture (1) Values in €	Distributed architecture (2) Values in €
Implementation (CAPEX – one time)			
Purchase CBE software	[redacted]	[redacted]	[redacted]
Purchase CBC software	[redacted]	[redacted]	[redacted]
Installation, integration, training	[redacted]	[redacted]	[redacted]
Total implementation (CAPEX – one time)	[redacted]	[redacted]	[redacted]
Support and maintenance (OPEX – annual)			
CBE and CBC software (annual)	[redacted]	[redacted]	[redacted]
5-year project OEPX (3)	[redacted]	[redacted]	[redacted]
10-year project OPEX (3)	[redacted]	[redacted]	[redacted]
5-year project (CAPEX + OPEX)	[redacted]	[redacted]	[redacted]
10-year project (CAPEX + OPEX)	[redacted]	[redacted]	[redacted]

Notes:
Prices provided by vendors are list prices, which normally are between 30% to 40% above sales prices.
(1) Distributed architecture – one vendor provides all three CBCs, one to each MNO.
(2) Distributed architecture – each CBC to each MNO is provided by a different vendor.
(3) For 5-year and 10-year projects, first year "support and maintenance" is included in the cell broadcast implementation cost.
Source: CBS vendors

Based on the information provided by different vendors, the centralized architecture is overall more cost-effective compared to the distributed architecture (1) by € [redacted] and € [redacted] less investment for a 5-year and 10-year project, respectively. And it's even more cost-effective compared to the distributed architecture (2), by € [redacted] to € [redacted]. Evidently, a CBS solution where each MNO must purchase its own CBC independently is more costly.

The business model used by the software provider for the above cost comparisons is to offer software for purchase.[14] In this business model, the software provider or vendor of the CBS solution, provides a permanent or perpetual software license. However, updates to the software are included in the support and maintenance annual fee.

We recommend **structuring a procurement process for a centralized CBC architecture for at least a 10-year provision of support and maintenance of the software acquired**. This means that funding for a 10-year CBS solution, i.e., € [redacted], should be secure when the procurement process is launched. It is important to mention that the above costs do not include the funding for the hardware which is provided by the government, the connection between the

[14] Other business models used by software providers is Software-as-a-Service or SaaS and software lease. However, for emergency services, these business models are not used often.

CBE and the CBC, and between the CBC and the three MNOs, and the human resources needed to run the CBS solution.

Architecture of the CBS solution

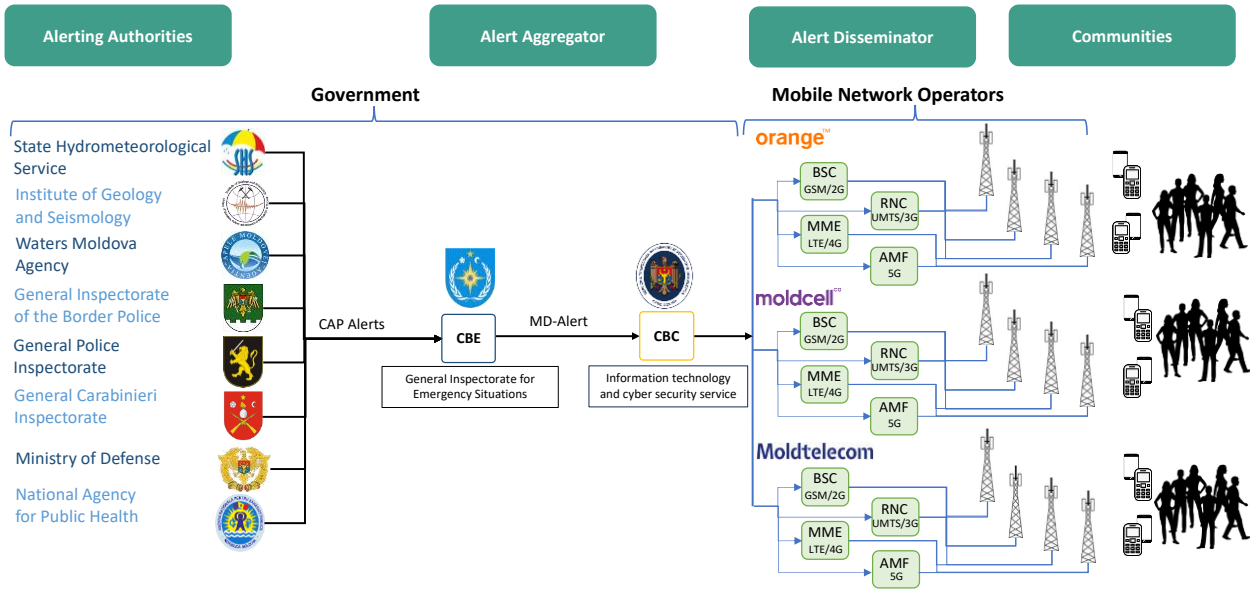
Based on the analysis of the advantages and disadvantages presented in section 0 and the cost comparison presented in section 0, a **centralized architecture for the CBS solution is recommended for Moldova**.

A centralized architecture is relatively a simpler solution and quicker to implement since it requires the installation of a single CBC. In addition, the government has full control of the CBS solution (CBE and CBC); therefore, there are lower risks related to the delivery of emergency messages. The centralized architecture is more cost-effective basically because one CBC is installed, the CBE connects only to one CBC, and the support and maintenance fee is lower. Finally, only one team of managers for the CBC needs to be trained; thus, reducing the cost of running the CBS solution (estimated not included).

Management of the CBS solution

The overall centralized architecture of the CBS solution recommended for Moldova is depicted in Figure 4. Both the General Inspectorate for Emergency Situations of Moldova (GIES) and the Information Technology and Cyber Security Service of Moldova (STISC) must coordinate between them and with alerting authorities and MNOs, respectively.

Figure 4. Cell broadcast overall centralized architecture solution for Moldova



Note: Alerting Authorities are for reference only and not in order of priority.

The CBE will be managed by the GIES and the CBC by the STISC. It is recommended that the CBE is scalable and designed under the basis of a future PWS, i.e., with the possibility to add

and connect other means or channels to deliver alert messages, such as broadcasting radio and television, mobile applications, and sirens, among others.

GIES, as the CBE manager, should be responsible for:

- Leading the procurement process to implement the CBS solution
- Funding the overall CBS solution
- Implementing, jointly with STISC and the MNOs, the overall CBS solution
- Coordinating, jointly with STISC, MNOs in the implementation of the CBE-CBC and MNO RAN network interface
- Determining the Service Level Agreement (SLA)
- Approve, create, confirm, send, and monitor the status of CBS alert messages
- Authorizing the alerting authorities with the right to send alert messages through the CBE and coordinating the interface needed
- Ensure funding for the operation of the CBE
- Adding new dissemination channels in the future (TV and radio broadcasters for example)

STISC, as the CBC owner and manager, should be responsible for:

- Provide the necessary infrastructure for running the CBC and the connection from the CBE-CBC to the MNOs networks
- Ensure the CBC is up and running
- Monitor the fulfillment of the SLA
- Ensure funding for the operation of the CBC

Finally, alerting authorities should be able to prepare alert messages directly in the CBE, as well as to send alert messages from their system to the CBE through a secure connection. For the latter, alerting authorities should develop an Application Programming Interface (API) to ensure integration with the authorities' system and the CBE.

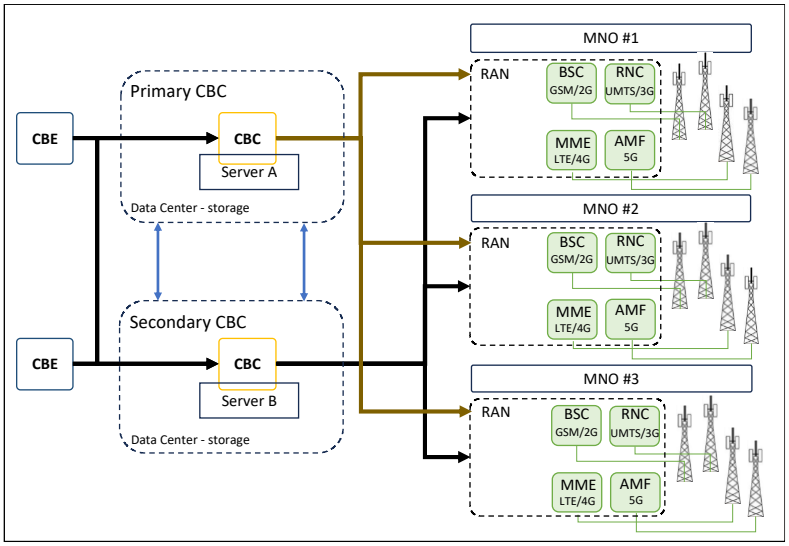
Redundancy

We strongly recommend that **geographic redundancy is included in the overall design of the CBS solution for both the CBC and the CBE**. GIES and STISC should have available physical space (to run the software and databases in different servers, for example) in separate locations for 2 CBEs and 2 CBCs, respectively, to add geo-redundancy to the CBS solution.

STISC must ensure the availability of infrastructure resources (data center and storage, servers) in two different locations for the CBCs. These primary and secondary identical CBCs, including their data centers and servers, must have a secure data connection (two connections) between them. In addition, MNOs must also have separate secure connections to each primary and secondary CBC (see Figure 5).

CBS solution redundancy provides a second option for all technical elements of the centralized architecture, avoiding the formation of a single point of failure. In case of failure of the primary CBC (data center) or CBE, the CBS solution must automatically operate with the secondary CBC.

Figure 5. Geo-redundancy with two CBE-CBCs



Procurement process

Since the CBS solution recommended is a centralized architecture, **the CBE and the CBC should be purchased under a single procurement process that will allow an integrated end-to-end solution**. This single procurement process will avoid the risk of integration that might arise when the CBE and the CBC are purchased separately (e.g., the CBE-CBC interface).

Thus, as a result of the single procurement process, one vendor should provide and be responsible for the implementation and initial testing of the CBE-CBC, as well as future support and maintenance.

Legal and regulatory framework

Often, in the implementation of a CBS solution, legal and regulatory modifications to the existing framework are necessary. These modifications ensure a successful implementation of the CBS solution. The following table suggests some modifications to the legal framework.

Table 7. Proposed modifications to the legal framework

Law	Modification
93/2007 on the General Inspectorate for Emergency Situations	The concept and definition of “Notification” should be added. The concept and definition of “warning” should be added. The responsibility of notifying or warning the population through the national early warning system during emergencies or exceptional situations should be granted to GIES

Law	Modification
271/1994 on Civil Protection	Not only “notices”, but also “warnings” should be included in the legislation. “Emergencies” should also be a reason to notify central and local public administration authorities as well as the population. Such notification should be sent through the national early warning system.
241/2007 on Electronic Communications	Obligations for MNOs for the implementation of a CBS solution must be included in the Electronic Communications code. Such obligations should require MNOs to: a. Ensure the uninterrupted transmission of public warnings received from the national early warning system. b. Ensure the dissemination of warning messages in all available technologies, without altering the content. c. Prioritize warning messages received from the national early warning system. d. Update all hardware and software of their networks, including configuration and activation of licenses, to allow the dissemination of warning messages. e. Collaborate with government authorities and institutions involved in order to promptly resolve any malfunction and incompatibilities related to their network when transmitting warning messages. f. Provide technical information about their networks to the competent public authorities/institutions relevant to the transmission of warning messages (e.g., cell sites database). g. Collaborate with government authorities in the implementation and deployment of the national early warning system, specifically providing a secure connection to the government authorities’ locations (e.g., data center / CBC) to receive the warning message. h. Allow sharing of physical infrastructure elements to connect to the national early warning system Alerts and warning messages shall be transmitted to mobile devices connected to MNO automatically for free.

In addition to the above modifications, regulations should be adopted to:

a. Authorize a government agency to become an Alerting Authority
b. Trigger emergency warnings and alerts
c. Define the EU-Alert levels or hierarchy complying with the ETSI EU-Alert standard
d. Create format emergency alert messages

Terms of reference

See Annex.

ANNEX

Technical Specifications
Terms of Reference

Feasibility study on deployment and implementation of a Cell Broadcast Service (CBS) solution for sending Alert Messages

MD-ALERT

December 2023

Acronyms

3GPP	3rd Generation Partnership Project
AMF	Access and Mobility Function
ATIS	Alliance for Telecommunications Industry Solutions
BSC	Base Station Controller
CAP	Common Alerting Protocol
CB	Cell Broadcast
CBC	Cell Broadcast Center
CBE	Cell Broadcast Entity
CBS	Cell Broadcast Service
CMAS	Commercial Mobile Alert System
ETSI	European Telecommunications Standards Institute
GIES	General Inspectorate for Emergency Situations of Moldova
GSM	Global System for Mobile Communications
LTE	Long Term Evolution
MME	Mobility Management Entity
MNO	Mobile Network Operator
MVNO	Mobile Virtual Network Operator
PWS	Public Warning Systems
RFQ	Request for Quotation
RNC	Radio Network Controller
STISC	Information Technology and Cyber Security Service of Moldova
UMTS	Universal Mobile Telecommunications Systems

Table of Contents

Introduction

This Terms of Reference (ToR) describes the technical specification required to develop and implement a Cell Broadcast Service (CBS) solution in Moldova for public warning and alert messages (MD-ALERT) in compliance with ETSI TS 102 900. The main goal to develop and implement a CBS solution is to deliver alert and warning messages to Moldovans or people from other countries visiting Moldova through mobile devices within a target area (national, regional or local) in near real time.

The General Inspectorate for Emergency Situations (GIES) of Moldova is seeking for an integrated end-to-end CBS solution; thus, the vendor will provide both the Cell Broadcast Center (CBC) and the Cell Broadcast Entity (CBE).

This ToR is composed of six chapters in addition to this introductory chapter. In the second chapter the standards the CBS solution must comply with are listed. In the third chapter, the CBS architecture is described. Chapter five through seven present the requirements the Provider of the CBS solution must comply with.

Standards

The CBS solution must comply with the European Telecommunications Standards Institute (ETSI), the 3rd Generation Partnership Project (3GPP), and OASIS standard listed in Table 5.

Table 8: Standards the CBS solution must comply with

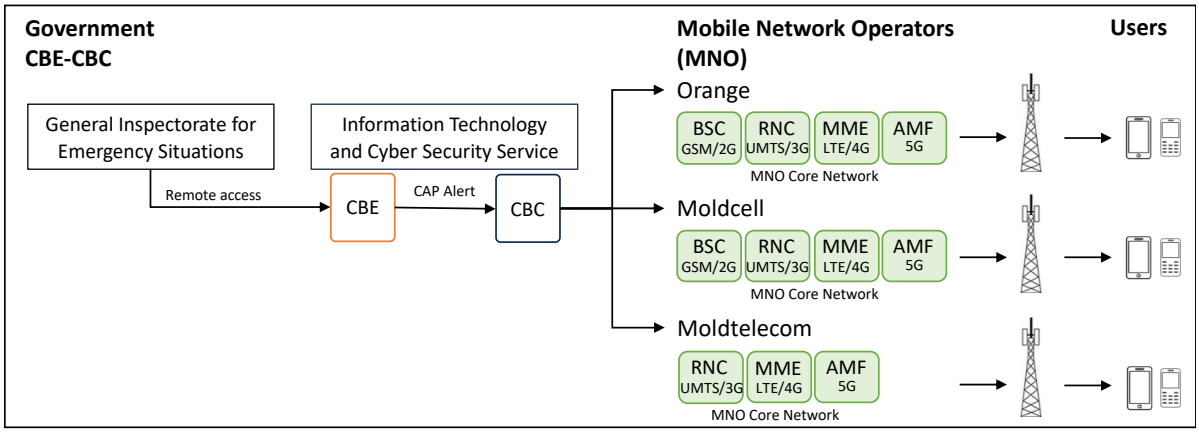
Standard	Description
CAP V1.2	Common Alerting Protocol (CAP) Version 1.2 – OASIS Standard (01 July 2010)
ETSI TS 102 182	Emergency Communications (EMTEL); Requirements for communications from authorities/organizations to individuals, groups or the general public during emergencies
ETSI TS 102 900	Emergency Communications (EMTEL); European Publica Warning System (EU-ALERT) using the Cell Broadcast Service
ETSI TS 122 268	Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; 5G; Public Warning System (PWS) requirements
ETSI TS 123 038	Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; Alphabets and language-specific information
ETSI TS 123 041	Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications Systems (UMTS); LTE; 5G; Technical realization of Cell Broadcast Service (CBS)
ETSI TS 125 419	Universal Mobile Telecommunications System (UMTS); UTRAN Iu-BC interface: Service Area Broadcast Protocol (SABP)

Standard	Description
ETSI TS 129 168	Universal Mobile Telecommunications System (UMTS); LTE; 5G; Cell Broadcast Centre interfaces with the Evolved Packet Core; Stage 3 (3GPP TS 29.168 version 17.1.0 Release 17)
ETSI TS 129 518	5G; 5G System; Access and Mobility Management Services; Stage 3
ETSI TS 148 049	Digital cellular telecommunications system (Phase 2+) (GSM); Base Station Controller - Cell Broadcast Centre (BSC-CBC) interface specification; Cell Broadcast Service Protocol (CBSP)
3GPP TS 22.268	Public Warning System (PWS) requirements
3GPP TS 23.038	Alphabets and language-specific information
3GPP TS 23.041	Technical realization of Cell Broadcast Service (CBS)
3GPP TS 25.419	UTRAN Iu-BC interface: Service Area Broadcast Protocol (SABP)
3GPP TS 29.168	Cell Broadcast Centre interfaces with the Evolved Packet Core; Stage 3
3GPP TS 29.518	5G System; Access and Mobility Management Services; Stage 3
3GPP TS 48.049	Base Station Controller - Cell Broadcast Centre (BSC-CBC) interface specification; Cell Broadcast Service Protocol (CBSP)

Cell Broadcast Service Architecture

The GIES has designed the CBS centralized architecture (one CBC for all three MNOs currently providing mobile services in Moldova) presented in Illustration 1.

Illustration 1: CBS solution – centralized architecture (one CBC for all three MNOs)



As depicted in Illustration 1, both, the CBE and the CBC will be managed by the government:

- The centralized CBC for all three mobile network operators (MNOs) and the CBE will be hosted by the Information Technology and Cyber Security Service (STISC)

- The General Inspectorate for Emergency Situations (GIES) will access and manage the CBE remotely over a secure connection. Alerting authorities, authorized by GIES will access the CBE remotely over a secure connection.

Messages and target locations for messages to be delivered are sent by the CBE and received by the CBC. The CBC then relays the messages to mobile devices within the target area in near real time through the radio access network (RAN) controller of each MNO's core network.

The CBE is remotely accessed by the GIES through a secure connection. The GIES is responsible for the CBE management and the delivery of CB messages, centralizing the alert messages sent by other government alerting authorities, such as the State Hydrometeorological Service, the Institute of Geology and Seismology, among others. The GIES should be able to approve all CB messages sent to the CBC and then broadcasted through the MNO's network.

STISC will host both the CBE and the CBC and will be responsible for the technical administration of both, including but not limited to security and network elements, i.e. hardware. It will also coordinate with the MNOs the interface between the CBC and RAN elements of the MNO's core network.

Currently, MNOs provide 2G, 3G and 4G mobile services in Moldova. However, soon 5G will be deployed. Therefore, the CBS solution should be able to send CB messages through all three existing networks (2G, 3G and 4G – see Table 9), as well as be scalable to 5G mobile networks and future mobile generations.

Table 9: Mobile subscriptions and technology deployed by MNOs

Mobile Network Operator	Technologies deployed	Total MNO subscriptions	Population coverage* (%)
Orange Moldova	2G, 3G, and 4G	2,7 million	2G: Not available / 3G: 99% / 4G: 99%
Moldcell	2G, 3G, and 4G	1,7 million	2G: Not available / 3G: 99,9% / 4G: 92%
Moldtelecom	3G and 4G	0,7 million	3G: 99,7% / 4G: 41,2%

* Total population in Moldova: estimated 2,5 million in 2023 (National Bureau of Statistics of the Republic of Moldova).

Source: ANRCETI (2022), ANRCETI (2021).

Moreover, the proposed CBS solution should be able to integrate in the future with other means or channels of dissemination of warnings and alert messages, such as television and radio broadcasting, sirens and social media, among others. Currently, there are no early warning systems implemented in Moldova.

The following table describes general characteristics of the CBS solution must comply with to be implemented and developed in Moldova.

Table 10: General characteristics the CBS solution must comply with

Characteristic	Description
National solution	Delivery of messages must be available nationally.
Geographically targeted	Ability to geographically target areas of the community: regional and local delivery of warning and alerts must be possible.
Near real time	Warnings and alerts must be delivered in near real time.
Intrusive	Intrusive audible and visible alert to the user, differentiated from existing messaging.
No opt-in and no opt-out	Receiving alerts does not require pro-active action from users. Users do not have to opt-in to the service, and do not have the capability to opt-out of the service – highest priority level.
Reports	Defined reporting, including performance and delivery metrics from CBE, CBC and the telecommunications network.
Rich information	Capability to send richer information as part of the warning or alert message. This may include longer text messages, the ability to attach an image, URL, map, video or a link.
Secure and trusted	Mechanisms to prevent hacking and spoofing for warning and alert messages.
Reliable	Solution must be technically reliable, and it must consider the impacts of catastrophes.
Upgradable	Solution has a defined roadmap, can be upgraded to provide new features, and scalable to future mobile technologies.
Multilingual	Provides support for multiple languages and scripts.
Diverse community support	Supports diverse community groups and considers the elderly, the deaf and hearing impaired, impoverished and remote communities, etc.
Message recipients/devices	Messages are intrusive and sent to the screen of the devices.
Hierarchy of messages	Comply with EU-Alert message types (EU-Alert level 1 ‘National Alert’, level 2 ‘Extreme Alert’, level 3 ‘Sever Alert’, level 4 ‘Public Safety Alert, EU-Info, EU-Amber, etc.). GIES will be responsible for determining the message priority.
Privacy and confidentiality	No requirement to store recipient (end-user) data.
Security	Protections to control against fraudulent use / spoofing.
CBE	CBE hosted by STISC data center and accessed by GIES. There must be at least one geo-redundant CBE.

Technical requirements

This chapter presents technical requirements related to management and network, security and audit, and messaging and performance.

Management and network

Table 11 presents the management and network technical requirements.

Table 11: Management and network technical requirements

#	Category	Requirement
1	Message format	The language/format used to send a request to the CBC from the CBE must be CAP-XML (v1.2).
2	Manual or backup process	Capability to send a CAP XML (v1.2) file manually. A disaster recovery process set up to send in plain text (in XML format) the content of the message and the area(s) to which it applies, and to be able to enter the message into the CBC. This is the fall-back option if requirement 1 above is not available.
3	Test messages	Capability to generate regular/annual test CB messages.
4	Network broadcast	Support CBS on 2G, 3G and 4G, and allow future integration of 5G SA mobile networks.
5	Message reach	a. CB messages must be received by all customers in the target area, including those without home network coverage, MVNO customers, international roaming customers and devices capable of receiving CB messages. If one MNO is unavailable, the end-user must receive the CB message via another MNO if available. b. CB messages must be received by all devices without a SIM (or expired SIM/Contract), but capable of making emergency calls. c. CB messages shall be received in areas of low coverage.
6	Standards	Compliance with ETSI, 3GPP, ATIS and OASIS standards (see Chapter 0). Possibility to update the CBC platform as new standards are adopted.

Security and audit

Table 12 presents the security and audit technical requirements.

Table 12: Security and audit technical requirements

#	Category	Requirement
7	User authentication	a. Only the GIES and authorized government agencies can generate a CB message(s) and send it to the CBC. GIES processes and systems need to be in place to control access and approval of CB messages content and distribution requirements, including those sent by other government authorized agencies. b. Deploy normal security processes and systems to control access to CBC. c. User authorization should be managed in the CBE application.
8	CBE-CBC connectivity	The communications between the CBE and the CBC shall be secured, e.g., VPN approach. Network connectivity shall be over encrypted channels with guaranteed Quality of Service and High Availability.

#	Category	Requirement
9	Reporting	Reporting should include message event, real time statistical and system status reports.
10	Audit trail	Capability to log and record all CB messages sent and provide an audit trail for up to 5 years. Log of each request to broadcast a CB message to enable GIES/STISC to assure that the message was received by the MNO, broadcast and a measure of the success of the broadcast. The log shall contain as a minimum: a. CAP XML message b. Time it took to broadcast the message c. Time the message was received from GIES d. Each cell site in the MNOs network the message was sent to e. Time the message was broadcasted
11	Protection against spoofing / DDoS / DoS attacks	CB messages must be protected against spoofing and DDoS / DoS attacks. Only CB messages from the authorized CBE (GIES) should be accepted.
12	Logged events	The following CBE and CBC events must be logged: ALL logon, failed logon and logoff events FOR OPERATING SYSTEMS - access to important data and processes - application crashes and any error messages - attempts to use special privileges - changes to accounts - changes to security policy - changes to system configurations - Domain Name System (DNS) and Hypertext Transfer Protocol requests - failed attempts to access data and system resources - service failures and restarts - system start-up and shutdown - transfer of data to and from external media - user or group management - use of special privileges FOR WEB APPLICATIONS - attempted access that is denied - crashes and any error messages - search queries initiated by users FOR DATABASES - access to particularly important data - addition of new users, especially privileged users - any query containing comments - any query containing multiple embedded queries

#	Category	Requirement
		- any query or database alerts or failures - attempts to elevate privileges - attempted access that is successful or unsuccessful - changes to the database structure - changes to user roles or database permissions - database administrator actions - database logons and logoffs - modifications to data - use of executable commands
13	Event log details	For each event logged, the date and time of the event, the relevant user or process, the event description, and the ICT equipment involved are recorded.
14	Event log protection	Event logs must be protected from unauthorized access, modification and deletion.
15	Log forwarding	All event logs must be able to be securely forwarded to GIES (and authorized government entities) in near real time if requested.
16	CB Platform secure by design	The end-to-end CBS solution shall be 'Secure-by-Design'. Secure interfaces must be implemented between the CBE/s and CBCs. The design shall include secure links between the GIES and the STISC. CBC platforms shall be securely managed and maintained with controlled access. The system shall be secure and resilient against malicious attack.

Messaging and performance

Table 13 presents the messaging and performance technical requirements.

Table 13: Messaging and performance technical requirements

#	Category	Requirement
17	Message Performance	CB messages will be sent to end-users within seconds [to be defined] of the request from the GIES CBE or in case of manual fallback option being used, from the request of the nominated contact point. CB messages will be sent at any time.
18	End to End Performance	End-to-end testing to ensure end-to-end performance can be measured against the criteria 5(a) Table 11 and time for CB message to be delivered to the cell.
19	Broadcast Geographical area	a. CB messages will be broadcasted to a pre-defined known or target geographic area. The message shall be sent for the duration defined by the CBE and if required a repeat interval defined by the CBE. The target area will be pre-defined for known geographic area, e.g. national, regional or local, and the area will be communicated in the message. The areas are mobile coverage areas not locations of cell sites. b. CB messages will be broadcasted to a geographically specific 'target area' or pre-defined known geographic area for a period defined by the CBE. This could range from a small area (single cell tower, or a sector of a tower), to up to the whole of

#	Category	Requirement
		Moldova. The target area will either be defined in the CAP message or by a pre-defined known geographic area.
20	Concurrent campaigns	Independently transmit CB messages for different campaigns across multiple locations. Multiple events or incidents can occur simultaneously. MNOs need to be able to cater for this scenario with no impact on service delivery. This includes potentially multiple messages (and different languages) in overlapping locations.
21	User Experience	a. Concurrent message broadcast by all MNOs – CB messages should be delivered to customers at the same time regardless of network. Target tolerance is 10 minutes. However, customers travelling through intermittent coverage (e.g. tunnels and in and out of their home network) may not receive the same message at the same time. This is to ensure community/group reaction occurs and recipients can validate the message. b. CB messages shall include information that identifies the sender (Moldovan Government department or agency) of the CB message and the contact details of the Moldovan department or agency.
22	Message updates	Capable of broadcasting updated messages to the same location. Each CB message shall have a unique identifier to enable tracking, reporting and audit. Basic requirement should support the cancelling of any existing message which has not yet expired and stop further transmission. As the situation changes, advice may change so there is a requirement to issue a new message or 'all clear' message to the same location.
23	Broadcast duration	Start time and end time. The CB message shall be broadcast for the entire duration of the broadcast time specified in the CAP message.
24	Broadcast cancellation	If a cancellation CB message is received during the broadcast period, the CBC shall stop broadcasting the message. Time between cancellation message received and the cancellation message being implemented to be agreed.
25	Repeat Period	The CB message shall be broadcast and repeated at time intervals pre agreed with GIES.
26	Reliability of message broadcast	Success broadcast rate from CBC to cell site (RAN) would be greater than 99.8% on average network wide for cells and CBC in service.
27	Display of message on handset	Provide the expected number of hand-held devices (i.e., mobile devices with the capability to receive a CB message) that can be reached once the CBS solution is fully implemented.

Non-technical requirements

Table 14 presents non-technical requirements.

Table 14: Non-technical requirements

#	Category	Requirement
1	CB platform availability	Availability of 99.99% of the time, unless the STISC and GIES have agreed to a planned downtime or other scheduled timings.
2	CB platform unavailability	No more than four (4) hours of unplanned outages per month.
3	Logs retained for audit	Performance/downtime reports of CBC. Monthly reporting of performance and details of service/fault investigations and responses. Reports of service outages should be provided to STISC/GIES.
4	Testing and trials	Support testing and trials in advance of service go live. Expectation that this would be a combination of lab testing and public trials by each MNO and coordinated by STISC/GIES.
5	Message content	CB messages will be easily understood and interpreted by recipients in a high-stress scenario, and targeted to maximize user action. The requirement is for the GIES and government agencies to focus on CB messages. This should be tested as part of any trials.
6	Notification of platform downtime	Any CBC planned downtime by the STISC will be communicated to the GIES with at least a seven (7) day notice. This will apply to the CBC, any communications links (IP VPNs) towards the CBE, and any equipment in the critical path of the CBS solution.
7	Fault categorization and priority	Any unplanned CBS outage should be treated as high priority.
8	Fault resolution times	Fault priorities will be categorized into the following resolution times: - Priority 1 – 4 hours - Priority 2 – 8 hours - Priority 3 – 5 working day - Priority 4 – 1 month
9	Fault response times	Fault priorities will be categorized into the following response times: - Priority 1: 30 minutes - Priority 2: 60 minutes - Priority 3: 1 day - Priority 4: 4 days
10	Privacy	Neither the CBE nor CBC will store recipient information.
11	CBE	The CBE must reside in a server at STISC premises and will be accessed remotely by GIES through a secure connection.

Cell Broadcast Center specifications

Table 15 presents the CBC specifications.

Table 15: CBC specifications

#	Requirement	Description
1	Description of Architecture, Features and Capabilities	The architecture of the CBS system for content submission must be completely separated from the topology of the network. Figure 1 presents the high-level architecture of the CBS solution and its interfaces. The CBS solution provider (from now on, the Provider) shall inform and briefly describe all the constituent components presented in the CB platform. The Provider shall submit the list of features available for any part of the CB platform, indicating, where appropriate, the basic features, options and those that were listed and necessary for the operation of this solution. These features should be included in the unit prices. The Provider shall describe and illustrate all interfaces (physical and logical) to 2G, 3G, 4G and 5G networks supported in the CB platform presented. The Provider must submit / inform: - The throughput license required to enable messages to reach individuals in near real time. Moreover, the Provider should outline the type of throughput licenses to increase the number of messages per minute without a hardware expansion. - Provider should provide how many Cell Controllers (BSC, RNC, MME, AMF) the system needs in total, as well as how many cells for 2G, 3G, 4G, 5G network in simultaneously, as well as the maximum number of radio cells that the CBC solution can be expanded to continue expanding the coverage the cell broadcast can reach. - The Provider should define how many interfaces can be supported, responding with (i.e., the CBC can support at least [number] CBE connections, can be expandable up to [number] CBE concurrently). The CBC shall support ASN.1 and HTTPS/XML interface protocol with the CBE connections. - The CBC interfaces shall support at least [number] CBE-CBC connections based upon Common Alerting Protocol (CAP v1.2). - The CBC must guarantee availability of capacity on the air-interface to the mobile device for public warning type messages. - The proposed solution must support 2G, 3G and 4G connectivity according to the standards. - The proposed solution must support 5G connectivity (future deployment) according to the standards. - Provide a list of vendors (2G, 3G, 4G, 5G) that is already integrated into the CBS solution network (if any). The CBC system shall support High Availability and Geographic Redundancy: - The Provider shall propose active/standby redundant architecture for the CBC. The Provider shall detail the

#	Requirement	Description
		architecture and recovery mechanisms in case of failure of server and signaling links. - The Provider shall detail the architecture and mechanisms (i.e. active/active or active/hot-standby or active/passive) to support dual node geographic redundancy at different geographic locations (distance > 50 km – to be defined). The systems arranged in geographical redundancy should not, in the case of switching from one site and another, causing an interruption or loss of services. - Changes to the configuration of parameters of the CBC can be performed at run time.
2	Security	The CBC shall support two methods of CBE access authentication: - A CBE accessing the CBC must have a unique network address, which must be registered in the CBC for this CBE. - CBE-name and password checking when logging into the CBC.
3	External Interfaces (1)	Cell Controller (CC) Interface. GSM and UMTS: Provider should define if CBC will support GSM and UMTS. The Provider should outline the CBC solution support for the cell controller interfaces. When a CB message is stopped, the cell controller must report the number of broadcasts per radio cell in the statistics interface. ETSI/ATSI/3GPP standards must be supported (see chapter 0). If the solution supports another standard interface, please list. The interfaces to cell controllers BSC, RNC, MME and AMF must be compliant. The mapping of geographical area information to cells can be a task of the CBC in-line with the user interface of the CBE. Information about the topology of the MNOs networks (i.e., association between radio cells and cell controllers) is imported automatically in the CBC. After import into the database, new issued requests will use the updated cell information.
4	External Interfaces (2)	Cell Broadcast Entity (CBE) interface in CBC: - The CBE interface must be able to access the functions of the CBC. - The CBC will accept calls from CBE and addresses cell controllers without operator intervention. - The CBE interface will accept requests, process them and transmit error-messages or confirmations to the CBE. - CBE interface must support ASN.1 and HTTP/XML based protocols. - CBE incoming traffic throughput will be controlled from the CBC platform. - The CBE shall provide a map to define the target area. - The CBC must be able to report to the CBE on the success of message broadcast within 3 minutes after the message was submitted.

#	Requirement	Description
		- The CBE and CBC interfaces must follow the 3GPP standard and functionality that support via vendor implementation.
5	External Interfaces (3)	The CBE–CBC interface should support the following primitives: - CBC Login. - CBC Logout. - Change Password. - Create New Message. - Create Message using Predefined Area. - Change Message Contents. - Kill Message. - Kill Message Cell. - Kill All Message Cell. - Message Information. - Predefine Area. - Remove Predefined Area. - Command Information. - New Message Cells. - New Message Cell Controllers. - New PLMN-wide message. - Retrieve Areas. - Network Availability. (Where a cell broadcast message can reach) - Message Network Cell Count. - Retrieve Information Providers. - Index Message

#	Requirement	Description
6	External Interfaces (4)	CB Message Scheduling - The CBC allows CB messages to be sent directly or to be given a specified start time. - Immediate Execution: the CBE requests without a start time will be executed as soon as possible. - Deferred Delivery: is possible for CBE requests containing a start time later than current local time. - The CBC will internally schedule the message and send it out to the PLMN at the message start time. The CBC should support Index Messages The CBC should support Blacklist Functionality for 'blacklisted words. Load Management: The CBC should provide load management. The CBC manages allocation of resources in the Cell Controllers and cells. Air Capacity Limitations (to be provided, if any, buy the Provider) Storage Capacity Limitations - The capacity for the storage of messages can be limited within a Cell Controller or cell. - A reserved capacity and a maximum capacity may be configured. - The CBC should take into account limitations on capacity of Cell Controllers and cells: • Air Capacity: only 1 message may be broadcast at a time. • Storage: the number of active CB messages or pages in a Cell Controller or cell.

#	Requirement	Description
7	External Interfaces (5)	Prevent Cell and BSC Overload. The CBC internally stores status information regarding BSCs and cells. This information includes: - Usage state: idle, active or busy. - Administrative state: unlocked, shutting down or locked. - Operational state: enabled or disabled. - The air capacity in use (for cells). - The storage capacity in use. - The rate of commands sent to BSC. PLMN Network Fault Handling - The CBC is responsible for managing possible failure conditions regarding CB within the PLMN. These failure conditions include: • Configuration mismatches between CBC and Cell Controllers or cells. • Communication link failures between CBC and Cell Controllers. • Error reports from Cell Controllers - Common Alerting Protocol Gateway (CAP GW) as optional: CAP Gateway must support active-active, active/standby and active–passive redundant configuration.

#	Requirement	Description
8	External Interfaces (6)	Operation & Maintenance Centre (OMC) Interface The following management interfaces must be available and managed by the MNO: - SNMP compliant remote management interface. - A web interface for general CBC OAM. - Locally, via a Command Line Tool (CLT). - The CBC must be managed by an OMC through a GUI interface. - The following functions should be provided by the GUI interface: • Starting and stopping the CBC or parts of it • Entering basic system data (e.g. the position of a radio cell or which cell controller controls a specific radio cell). • Monitoring the CBC activity - All Operator and Maintenance functionality is also provided through a Command Line Tool (CLT). - In case of CBC malfunctions, the operator is notified by SNMP alarms. - Backups: • The CBC contains a backup facility for application data, message data and for a full backup. • Backups can be made on-line and stored on disk and copied to external backup devices. - History Logging: • The MNO must be able to trace the sender of a particular message in case of a (legal) dispute. • The CBC must store each command and each response in a history log file. • The History Logging option must be configured per content provider.

#	Requirement	Description
9	External Interfaces (7)	Traffic Logging - The traffic log provides the operator with information about the status history of the individual messages and of individual network elements (cells and Cell controllers). - The traffic log information consists of events that are generated at state changes of messages. Possible message states are: • Planned • Starting • Running • Killing • Finished • Skipped - Network entities (cells and Cell Controllers), network states are: • Enabled • Disabled • Unlocked • Locked - Per event, some relevant parameters for the event are also logged. For example, for the 'Network Element enabled' event, the parameters timestamp (UTC), network element type, network element id and network element name are logged.

#	Requirement	Description
10	External Interfaces (8)	Off-line reporting For off-line report generation aggregated reports in ASCII CSV format should be available, including below mentioned: - Number of successful incoming test messages - Number of successful incoming heart beat messages - Number of successful incoming normal messages - Number of failed incoming test messages per error cause - Number of failed incoming heart beat messages per error cause - Number of failed incoming normal messages per error cause - Number of status report requests for test messages - Number of status report requests for heart beat messages - Number of status report requests for normal messages - Number of 2G, 3G, 4G, 5G cells addressed to broadcast test messages - Number of 2G, 3G, 4G, 5G cells addressed to broadcast heart beat messages - Number of 2G, 3G, 4G, 5G cells addressed to broadcast normal messages - Number of 2G, 3G, 4G, 5G cells actually have broadcasted test messages - Number of 2G, 3G, 4G, 5G cells actually have broadcasted heart beat messages - Number of 2G, 3G, 4G, 5G cells actually have broadcasted normal messages - Number of test messages failed to broadcast per error cause type - Number of heart beat messages failed to broadcast per error cause type - Number of normal messages failed to broadcast per error cause type - Number of enquire message status requests - Number of replace message request - Number of cancel requests Graphical representation To enable a graphical representation of the cell availability within the network, the CBC shall have a feature in which aggregated reports in ASCII format (above) can be visualized in a KML layer file, which can be imported in most GIS systems in order to be overlaid onto a map.
11	Public Warning Support	Public Warning Support - The CBC must support priority messages. - When a priority message is submitted all non-priority messages that are currently being broadcast in the area where the warning message shall be broadcast, will be stopped temporarily.

#	Requirement	Description
12	Architecture and Hardware Requirements	The hardware architecture should be based on a server [located at STISC]. - The system operating system should be [to be defined]. o The CB Platform should allow software upgrade without freezing up of equipment. - The CB Platform should enable upgrade / downgrade software licenses without loss of connectivity, records of users, active sessions, etc. - The CB shall detail these mechanisms. - The CB Platform should allow full recovery and 100% automatic (without any human intervention) after failure and recovery. - The failure of any element of the solution may result in failure of availability of any features, except during periods of automatic fail-over within the 99.999% availability. - o The Provider should detail the total time required for recovery in case of fail-over, depending on the number of active sessions.
13	Support	The Provider must provide 24 x 7 product support. Provide the details of the support that can be provided and the location of the support centers. Provide the number of staff in your support organization.
14	Training	Include training for at least ten (10) staff members. Training must be provided on-site at customer facilities.
15	Roadmap	The Provider must submit its policy and vision for the evolution of the products / features presented. It will include: - The roadmap of features for the next two - five years - The roadmap and adherence versions (releases) of 3GPP and other standards if necessary
16	Experience	The Provider must have a proven track-record in live CBC deployments: - Have customer systems in live service for at least five (5) years - Have customer systems in use for Cell Broadcast Emergency Alerts - Have customer systems in use for Common Alerting Protocol (CAP) emergency alerts - Have customer systems in use for Commercial Cell Broadcast Applications - Have at least five (5) references for live systems - Have at least five (5) references for geographic redundant CBC - Have at least five (5) references for geographic redundant CAP Gateways - Have at least three (3) references for system used for EU-Alert - Have at least two (2) references for system used for CMAS
17	Standards Compliance	Comply with standards listed in chapter 0.

Cell Broadcast Entity specifications

Table 16 presents the CBE specifications.

Table 16: CBE specifications

#	Requirement	Description
1	Architectural requirements	- It shall be possible to deploy the system in a single node environment; in a cluster environment; in a geo-redundant architecture; in a private environment; and in a virtual environment. - Virtual machine deployment shall be possible. - The CBE shall by default provide a secure HTTPS interface towards connected browsers. - The CBE shall provide a secure HTTPS interface towards all input and output connections. - CBE users will access the CBE through a browser (the CBE solution must not require any CBE related code to be installed on a user desktop)
2	Output adapter requirements	- The CBE interface towards the CBC shall support the Common Alerting Protocol Version 1.2, also called CAP v1.2. - The CBE interface towards the CBC shall support XML CBE-CBC protocol. - The CBE interface towards the CBC shall support the ATIS-0700037 and its predecessor J-STD-101 CMAS interface protocol. - The CBE shall provide a secure HTTPS interface towards the CBC. - The CBE shall provide an interface for publishing public warning messages using the CAP v1.2 interface. - The CBE shall support a generic CAP V1.2 output adapter which can easily be adapted for deviations from the CAP v1.2 standard as sometimes is required by national and regional authorities or commercial companies. - The CBE shall send periodic IP based heartbeat signals to the channels to check if the channels are reachable. - The CBE shall support link test messages. Link test message shall be used to check at regular intervals if the link between the CBE and the input and output channels are still available. - Provide a list of international standards (relevant cell broadcast standards and other emergency alert standards) the CBE will be compliant with.
3	Alarm and Performance management requirements (1)	- The CBE shall generate alarms for all service affecting issues and warnings for issues that are not service affecting but do require attention. - The CBE shall provide a central Fault Management and Performance Management function. - The CBE shall provide alarm types according to severity: Critical / Major / Minor / Warning / Info. - The CBE Platform must provide a set of alarms regarding:

#	Requirement	Description
		• CBE application unavailability or malfunctioning • Connectivity issues to other applications • Connectivity issues to input alert channels • Connectivity issues to output (dissemination) channels • Database issues (e.g. if platform has a database layer with a replication mode for recovery procedure) • Security issues • Failed login attempts - The CBE shall expose functionalities to push information (Alarms, Counters, Logs, etc.) towards customer reporting systems. - The CBE shall support alarm that are to be tracked into a history log file, with additional information: • Time of alarm • Severity • Alarm Text • Time of the clearing of the event
4	Alarm and Performance management requirements (2)	Networking Functionality (e.g. switch, router, firewall etc.) integrated into the CBE shall have their own alarms management traps and alarm forwarding. An alarm shall be sent when the connection to one or several communication channel(s) is down. An alarm shall be sent when the system cannot perform an operation due to lack of resources (e.g. disk space). If the situation that caused an alarm is cleared an automatic clear alarm shall be generated. It shall be prevented that a storm of alarms is generated for a single event. The CBE shall support alarms in SNMP v2c and or SNMP V3 format. The alarms shall be stored for a configurable amount of time and retrievable via SNMP. MIB files shall be provided for all alarms. The severity and description of each alarm shall be editable. It shall be possible to clean the system of old alarms. The CBE must provide a set of clearly defined and measurable KPI in order to monitor availability, performance, capacity, congestion, service quality, load conditions. The CBE shall include effective Antivirus and Malware protection and in case of detection of virus or malware detection an appropriate alarm will be raised.

#	Requirement	Description
5	Logging requirements (1)	All CBE activities shall be logged in an audit-trail which shows what users and administrators have done on the system by capturing all the actions between logging into and logging out of the system for each user. The CBE must have a reporting function. The following reports shall be available in the reporting function of the CBE: - Alert Messages - System User Accounts - System Usage - Notification and Notified Contacts - Predefined Messages - Predefined Areas In the reporting function after the time period has been selected, the results shall be filtered by entering (part of) the desired entry in the field in the table header. It shall be possible configure the level of detail of the logging. A log rotation policy must be defined and configurable. Log files must be totally configurable: it must be possible to decide in a parametric way the detail level, the history policy and the retention of the log.
6	Logging requirements (2)	The log file must be stored on a configurable directory. This path must be configured through one or more parameters. A specific log shall contain a description of every transaction handled by the application (Exit code, Response Time, Exceptions, etc.). Audit log files of user activity in the system shall be supported. Logging of all messages related events shall be supported. The system shall support the integration with an external SIEM/SOC server where all authenticated log files of the CBE can be processed. The CBE must have a reporting function based upon the log files. The following reports shall be available in the reporting function of the CBE on all the activities in CBE: - Alert Messages - System User Accounts - System Usage - Notification and Notified Contacts - Predefined Messages - Predefined Areas The CBE reporting function shall support filtering based upon time period, incident, user, location. The system shall support extensive logging to support troubleshooting.

#	Requirement	Description
7	Input adapter requirements	The CBE shall have an input adapter to receive threat and hazard related messages (from, for example, a sensor network or national weather agency). The CBE shall support a Common Alerting Protocol v1.2 (CAP v1.2) based input adapter. The CAP profile implementation shall support any customer specific CAP profile. The CBE input adapter shall be capable of taking new warning messages from all threat and hazard related systems (e.g. Earthquake Warning systems, flood gauges, sensor networks and monitoring stations). The CBE input adapter shall be capable of taking new warning messages from the GIES. The CBE input adapter shall support advanced Alert authentication, Alert verification, Alert filtering, and Alert routing logic for the incoming connected alert streams. The CBE shall support a generic CAP V1.2 input adapter which can easily be adapted for deviations from the CAP v1.2 standard. The CBE input adapter functionality shall support secure connection based upon HTTPS or VPN connections. The CBE input adapter functionality shall support the detection of duplicate CAP messages. The CBE input adapter functionality shall support CAP encrypted digital signatures to validate the originator of the threat and hazard related messages. The encryption algorithms used must be compliant with Transport Layer Security 1.3 (TLS 1.3). The CBE shall be able to support at least [number] different input channels connected to the system. The CBE should be able to support [number] of different input channels.
8	Generic GUI requirements (1)	The CBE System shall support the possibility of branding the GUI according to the user's needs (header, footer, pictures, fonts, and color). The CBE shall have at least two modes of use, one for real production and one for testing and on the Login page it must be made explicit in which mode one is using. The CBE shall support multiple languages. All text presented in the GUI shall be contained in a (configuration) file. This allows the possibility to translate the text in that file into any language desired by the customer. The CBE shall be able to authenticate and authorize users based on username and password and must be able to grant Users rights in the CBE based on roles. The CBE shall be able to grant users rights in the CBE based on roles. User access to the CBE shall be through the GUI in a web browser using the secure HTTPS connection.

#	Requirement	Description
		The Provider should define the number of roles the CBE is able to support, whereby each role is linked to the right to create, modify, delete and distribute alert messages in a specific region or nationwide. The Provider should define the number of regular CBE users provisioned in the system. The CBE shall keep a real-time log of who has access to the system, and when they accessed the system.
9	Generic GUI requirements (2)	The Provider should define how many concurrent users connect to the system the CBE can support. The CBE shall be able to assign any right to every role. The allocation must be fully configurable and must be able to be adjusted instantaneously and in groups by the Client. CBE users can be assigned one or more roles, such as: - Viewer - Author - Approver - Group administrator - System administrator The CBE shall support two factor authentication mechanisms for successful login. The CBE shall support advanced and complex password policies. The CBE shall support an account lockout mechanism to prevent successful automated password attacks. The CBE shall support the functionality that after a certain number of consecutive failed login attempts within a specified time any further login attempt is prevented. The CBE shall support the functionality to unblock accounts after a certain period. A user shall be able to access the system after entering a valid, registered username and password. The user shall be able to request a new password on the login page. A user shall be allowed to have only a single active session. The system shall be able to provide users with temporary passwords via email.
10	Message Creation GUI (1)	The creation of the alert in the GUI shall be simple, with limited steps, giving priority to speed and security in creating alert messages. The message creation page in the GUI is preferably limited to one (1) screen to give the author of the alert message the full control and overview. It shall be possible to create, modify and stop an alert message from the GUI. The CBE must provide a summary of the alert before the final submission of the message. The CBE must support to create an alert Message in multiple languages. The CBE creation must support a spelling checker in order to reduce the risk of making mistakes in the alert message text. CBE shall support the functionality to show a warning when a spelling mistake is observed in the Message creation screen.

#	Requirement	Description
		The CBE must enable the author of the alert message to select a Broadcast Area on the basis of fixed areas predefined in the CBE, being a [Region, District, Municipality, City / Town, and Village].
11	Message Creation GUI (2)	The CBE must support a library that contains all [Region, District, Municipality, City / Town, and Village] in Moldova. The CBE must support a free selection of a Broadcast Area based on at least an oval, circle, square and polygon. The CBE shall support the functionality for a nationwide alert message without providing the country area polygon or predefined area. The CBE shall support the functionality for a nationwide alert message to the CB channel by specifying a specific Geocode that is recognized by the Cell Broadcast System as a national message (PLMN wide). The CBE shall support maximum number of characters that can be entered in the GUI for the Alert message. The CBE shall support the functionality to show the number of characters used. The number of characters is displayed at the bottom of the Alert Creation screen. The CBE message creation GUI screen shall support the functionality to show a warning when the maximum number of characters is exceeded for one of the communication channels and message will not be sent. The CBE shall support the functionality to display the summary of the created message before the message is being submitted. The CBE shall support the functionality to request for Approval of created warning message before message is being submitted.

#	Requirement	Description
12	Message Creation GUI (3)	The CBE Message creation screen needs to support CB technology related fields that can be set including: - Message Identifier (sometimes referred to as 'CB channel') or severity of the Alert - Serial Number - Data Coding Scheme - Schedule - Repetition Rate (CB message broadcast is repeated at the Repetition Rate) - Broadcast Area - Cell-ID - Cell- Name - Individual CB Channel number - Device Based Geo Fencing (DBGF) flag The CBE creation screen need to support the possibility to enable the use of CAP Digital signatures. The CAP Digital Signatures provide an additional level of assurance that only authorized personnel are sending messages and also ensure that the implications of sending such critical information are well understood. Digital signatures use cryptographic techniques to protect the integrity of information. The key used to sign data is typically controlled by a Certificate Authority (CA) and so the creation of a signature can be directly traced to the owner of the key. The CBE shall support pre-defined template or canned warning messages and pre-defined areas, based on pre-defined text with placeholders where specific elements need to be populated, including the CAP alert category codes. The CBE shall support the functionality to display a warning when place holders in the alert message text are not filled in and the alert message cannot be sent. The CBE shall support predefined message. The CBE shall support pre-defined areas. The CBE shall support to group multiple alerts per incident (crisis management). The CBE must support the functionality to make Text fields of the CBE mandatory. If the User does not fill in such a Text field, a notification must be displayed, and the alert message cannot be sent.

#	Requirement	Description
13	Message Creation GUI (4)	The CBE shall support selecting one or multiple dissemination channels with simple selection. The CBE shall support easy adaptable CAP profiles that are typically defined by the responsibility of government entities (e.g., meteorological agency). The CBE shall support CAP link test messages. The CBE shall support a reporting back functionality from the CBC towards the CBE to indicate the success rate of the alert message sent for each CBC used. It shall be possible to enter the start time of the message. The start time is optional. It shall be possible to enter the end time of the message. The end time can be configured to be optional or mandatory. It shall be possible to enter the message text. It shall be possible to select the language; the language list shall be a configurable list of languages and the configured default language shall be displayed as the first language in the list. If the user doesn't select any other language the default language shall be selected. An empty message shall not be allowed. A counter shall show the number of characters that are used while entering the content and it shall not be possible to enter more characters than is configured. The maximum number of characters that may be entered for a message will be the lowest maximum amongst the configured adapters. It shall be possible to select the severity level for the public warning message. The user shall be forced to select the severity level (no default). If only a single severity level is configured the choice of severity levels shall not be presented to the user. It shall not be allowed to enter an end-time which lies further into the future than the configured amount of time from the current moment on. It shall not be allowed to enter an end-time which lies in the past or not to enter an end-time if the end time is configured to be mandatory.

#	Requirement	Description
14	Message Creation GUI (5)	It shall be possible to define the target area(s) by drawing one or multiple polygons on a map. It shall be possible to define the target area by using one or multiple circles. It shall be possible to define the target area(s) by selecting one or multiple predefined areas which are allocated to the group. It shall be possible to explicitly select the entire country for distribution. The selected or defined areas shall be automatically corrected to the area where the group is allowed to disseminate warning messages. If the user is a member of multiple groups, then the selected or drawn areas are corrected to the areas where all the groups of which the user is a member are allowed to disseminate warning messages. The area where the user is authorized to disseminate messages shall be highlighted. If the system knows one or more CBC's, the location of CB towers will be displayed on the map during selection. The system shall raise a warning to the user if the selected area contains no cells. It shall be possible to load a map from OpenStreet Map and Google Maps. The user will be able to search for a location using a search bar, after which the map will navigate to and zoom into that location. After a user leaves the page that showed a map, the view (center and zoom factor) shall be stored, and when this user enters a page that shows the map again, the initial view shall be the view that was stored. It shall be possible to modify a polygon after the polygon has been completely drawn. The system configured default map view (location and zoom level) shall be presented when the user defines a new message. If possible, the system will generate suggestions on the type of content to fill an empty field with. It shall be possible to create a message based on a predefined/canned message. It shall be possible to modify a selected predefined message before sending it.

#	Requirement	Description
15	Message Creation GUI (6)	The message creation page shall display a ‘send message’ button. After clicking "send message" the system shall validate input on completeness and correctness and display errors in the message creation screen. Checks: - Start date/time should be before end date/time - Content field may not be empty - Description field may not be empty - End date/time may not be empty If message type is a polygon, the Provider should define how many coordinates should be selected on the map. After the ‘send message’ button has been clicked a pop-up should be displayed asking confirmation that message should be sent and inform on to which adapters the message will be sent. It shall be possible to modify parameters by clicking on the "cancel" button, which closes the dialog and returns control to the current Message Creation page. All time stamps should be UTC format
16	Dashboard GUI	The visualization CBE dashboard shall be simple, with limited steps, giving priority to control and security. The CBE shall support a Dashboard GUI. The Dashboard shall provide an overview of the Active, Approval, Completed, Rejected, Duplicates and Draft alert messages. This data is shown to the CBE user on the Dashboard in a clear, time (UTC) stamped list and or in a geographic way (Map). The CBE dashboard shall be an interactive map showing all active, rejected, completed, waiting for approval, duplicates, and draft warning messages. The message status page shall show an overview of all alert messages as part of a list. It shall be possible to modify a message from the Dashboard. This should switch to the Message modify screen filled with all data from the selected message. All fields shall be modifiable, including the area. Activating the creation of a new message shall open the Message Creation/modify screen. It shall be possible to stop messages immediately from the Dashboard. It shall be possible to remove completed or stop messages from the Dashboard. It shall be possible to display the message status and success rate of a message for each of the connected communication channels. If a status update from a communication channel fails, for example because the link to the channel is down, then a notification shall be displayed to the user and an audible alert on the Dashboard GUI and SNMP alert is raised. When the Dashboard is displayed after a message has been sent to the communication channels then the number of channels that acknowledged successful receipt of the message shall be displayed,

#	Requirement	Description
		alongside the total amount of configured communication channels. A user can choose to display a more detailed list of failures if they occur. This status on the Dashboard shall be updated at a configurable interval (1 second at minimum). It shall be possible to display all details of an active, completed, draft, duplicate, rejected, waiting of approval message (such as complete content and target area on a map). When updating a message, the user needs to be presented with polygons of the initially selected areas, unless nationwide message was selected.
17	Predefined Message support	The CBE shall show a list of the current predefined messages. The CBE shall offer the functionality to create a new predefined message. The CBE shall support the functionality to create a new predefined message out of the message creation screen. It shall be possible to notify users of the CBE that a new pre-defined message has been created or modified. The predefined message can only be created, modified, and deleted by users with the correct role. It shall be possible to create predefined messages per language. It shall be possible to create a predefined message including the message text for a number of languages. It shall be possible to create a predefined message set per group. It shall be possible to create a predefined message from an existing message. It shall be possible to import a list of predefined messages from s file (CSV, ASCII). It shall be possible to export a list of predefined messages to an ASCII or CSV file. It shall be possible to modify a predefined message. It shall be possible to delete a predefined message. It shall be possible to include the severity level of each predefined message. It shall be possible to include the duration of each predefined message. It shall be possible to include the number of dissemination channels used for each predefined message. It shall be possible to include a URL or Web link in each predefined message. It shall be possible to include multi-media content in each predefined message.

#	Requirement	Description
18	Predefined Area support	The CBE GUI shall show a list of the current predefined areas. The CBE GUI shall support the bulk import and export of predefined areas via a file interface (CSV format). The CBE must support the bulk upload of all predefined areas in a country including all [Region, District, Municipality, City / Town, and Village] using a file. The CBE shall support the functionality to create a new predefined area. It shall be possible to enter a name for the predefined area. It shall be possible to enter a CAP Geocode for each predefined area. The predefined area can only be created, modified, and deleted by users with the correct role. It shall be possible to create a predefined area from an existing message. It shall be possible to create a predefined area from one or more polygons. It shall be possible to create a predefined area from one or more circles. It shall be possible to import a list of predefined areas to a file. It shall be possible to export a list of predefined areas to a file. It shall be possible to modify a predefined area. It shall be possible to remove a predefined area. It shall be possible to create a predefined areas per group and per area of authorization.
19	Notifications support	The CBE shall support notified contacts. The Provider should outline how many different contacts that can be notified by the system can be supported by the CBE. The page shall offer a button which displays a page to create new contact (name, organization, function, cell phone number, e-mail address). The notified contacts can only be created, modified by users with the correct role. It shall be possible to notify between the regular users of the CBE. It shall be possible to notify users of the CBE that a new concept/draft message is ready. It shall be possible to notify users of the CBE that a message is waiting for approval. It shall be possible to notify users of the CBE that a message has been sent. It shall be possible to indicate per contact if this contact needs to be notified when a new message is sent. It shall be possible to indicate per contact if this contact needs to be notified when an update on a running message is sent. It shall be possible to indicate per contact if this contact needs to be notified when a running message is stopped. It shall be possible to indicate per contact if this contact needs to be notified via e-mail.

#	Requirement	Description
		It shall be possible to indicate per contact if this contact needs to be notified via SMS. It shall be possible to indicate per contact if this contact needs to be notified in the CBE application. It shall be possible to import a list of contacts. It shall be possible to export a list of contracts. It shall be possible to modify contacts. It shall be possible to remove contacts. It shall be possible to assign contacts to groups and these contacts will be notified on message events for the group that sends the message. Government will manage the update of contacts in conjunction with Provider support.
20	User Management functionality	The user management functionality shall only be accessible to users with admin privileges. An Administrator shall be able to create, modify and delete Users. The system shall be able to store at least username, password (in encrypted format), organization, email address, role, status (account enabled/disabled), password unchanged flag, last login date-time. An Administrator shall not be able to remove his own account. An Administrator shall be able to disable / enable a user to access the system. CBE users can be assigned one or more roles, such as: - Viewer - Author - Approver - Group administrator - System administrator An Administrator shall be able to provide Regular Users with Read Only (Viewer) or Read/Write (Regular User) rights, the latter will allow creation, update, stop and deletion of warning messages for the Group(s) the user is assigned to. A Group Administrator can only do this for the group(s) he is assigned to. When a new user has been created, a system generated temporary password shall be sent to the email address of the new user. A Viewer shall only be able to view the messages and message status of the messages of his own group. A Regular user shall be able to create, update and stop messages for his own group and update and stop those of all other users in his group. An Approving user shall be able to approve or reject a message before it will be sent by the portal. A System Administrator shall be able to create Groups. A (System and Group) Administrator shall be able to add and remove Users from a Group. A Group Administrator can only do this for the group(s) he is assigned to.

#	Requirement	Description
		A System Administrator shall be able to assign a predefined Area(s) as Jurisdiction Area to a Group (the area(s) a user in this Group may send messages to). A System or Group Administrator shall be able to assign Predefined Area's to a Group. A Group Administrator can only do this for the group(s) he is assigned to. A System or Group Administrator shall be able to assign Predefined Messages to a Group. A Group Administrator can only do this for the group(s) he is assigned to. A System Administrator shall be able to assign Channels to a Group. A System or Group Administrator shall be able to assign Contacts that need to be notified to a Group. A Group Administrator can only do this for the group(s) he is assigned to.
21	Workflow/ approval requirements	If a group has a minimum number of required Approving Users configured, it requires approval from this configurable number of Approving Users of the group of the regular user that created the message before the message is sent by the CBE. An e-mail request for approval/rejection containing the area and all message parameters (start time, end time, message name, message text, severity, and language) shall be sent as clickable links (one for approval, one for rejection) to the Approving User(s) of the group the creator of the message belongs to. If a configurable number of users approve the warning message for distribution, then the warning message is distributed for dissemination over the selected channels. An approval user is not able to approve warning messages that have been created by him or herself. A user that has overriding approval rights overrides any decision taken by users with regular approval rights. In case there are multiple users with overriding approval rights, then the first issued vote is applied immediately. It shall be possible to configure for each group the minimum number of approval users that need to give their approval for a message to be disseminated. The CBE shall have a mechanism to authenticate approval emails that are received from approval users. The CBE shall support an Approval mechanism of the alert message by giving confirmation in a separate pop-up window, possibly by entering an approval password.

#	Requirement	Description
22	System management requirements (1)	The provision of system parameters shall be based on a configuration file(s) and can also be supported by a GUI. The CBE shall support two factor authentication mechanisms for successful login of the system administrator. Actions and changes users make within the system shall be logged. For example, the creation of a new user or public warning message. See chapter "Logging requirements" for the corresponding specific requirements. Passwords used shall be stored in a suitably encrypted format. It shall be possible to configure the external OpenStreet Map or Google Maps. It shall be possible to configure the OpenStreetMap server. It shall be possible to configure a default view for a map (coordinates and zoom level). It shall be possible to translate the selected alert area into GPS coordinates. It shall be possible in the CBE to support map overlays, for example to show the cell sites of mobile service providers. This map overlay may help determine the broadcast area and to make sure one or more cells are inside the broadcast area. It shall be possible to configure adapters for communication channels. It shall be possible to configure the name of each communication channel that is displayed. It shall be possible to configure maximum, minimum, or possible values of parameters used to create messages. It shall be possible to configure the maximum duration of a message. It shall be possible to configure the maximum number of characters allowed in a message. It shall be possible to configure a list of languages. It shall be possible to configure a default language for creating messages. It shall be possible to configure and submit messages in multiple languages at the same time.

#	Requirement	Description
23	System management requirements (2)	It shall be possible to configure list of severity levels - EU-Alert Level 1: National Alert - EU-Alert Level 2: Extreme Alert - EU-Alert Level 3: Severe Alert - EU-Alert Level 4: Public Safety Alert (For other type of alerts see ETSI TS 102 900 – Message Identifiers) It shall be possible to configure minimum repetition interval per Message Identifier for each CBC adapter. It shall be possible to configure maximum number of days of inactivity before a user is disabled. It shall be possible to configure for each Message Identifier if the target area for messages with that Message Identifier will implicitly be PLMN-wide. It shall be possible to configure mapping of severity levels onto Cell Broadcast Message Identifiers. It shall be possible to configure for CB for each language if the message in that language is mandatory-to-display or optional-to-display. The severity level list shall be a configurable list of severity levels. The initial severity levels will be at least EXTREME, SEVERE and TEST. It shall be possible to configure if the end time of a message is optional or mandatory. It shall be possible to configure the maximum amount of time the end time of a message can be in the future. It shall be possible to configure the minimum number of approving users per group that needs to approve a message before it is sent out. If the number of approving users in a group is lower than the configured minimum number of required approving users for the group, a warning message should be flagged to the administrator of the group.
24	System management requirements (3)	The CBE shall support integration with an official time (UTC) server to be in line with the official time of the country, ensuring that this is maintained throughout the year and considering time changes. The CBE shall come with the following documentation: - User Manual - Installation and Configuration Manual - Upgrade Manual - Release notes - Acceptance Test Plan Document The CBE product shall have an active product roadmap for the coming three (3) years.

#	Requirement	Description
25	System security requirements (1)	Passwords must be stored in a secure manner using an industry validated password hashing mechanism. Access to functionality is restricted unless the user has been explicitly granted access to it. Communication to API's must be done in a secure manner. Cross site scripting should be prevented. HTML and SQL injection should be prevented. The password policy shall support minimum password size (minimum acceptable size for the new password). The password policy shall support to: - Set a limit for the number of digits in the password. - Set a limit for the number of capital letters in the password. - Set a limit for the number of lowercase letters in the password. - Set a limit for the number of other characters in the password. The password policy shall have a maximum duration (e.g. 3 months) that the same password can be used. The CBE shall support an inactivity / session timer. The CBE shall support functionality to automatically log a user out after a period of inactivity. It shall not be possible for a user to login when the last login has occurred more than a configurable number of days ago. It shall not be possible for a user to request a new password when the last login has occurred more than a configurable number of days ago. It shall be possible for a user to have a username and/or password containing any UTF-16 encoded characters. The system shall perform an automatic log out of the user after a configurable period of user inactivity.
26	System security requirements (2)	The system shall support Multifactor authentication/Security interface SAML 2.0. User access to the system shall be implemented with a web browser which uses a secure HTTPS connection with the GUI layer of the CBE. The CBE shall support secure connection and can be secured via VPN tunnels (site-to-site VPN using IPsec or a client-to-site using TLS 1.2 / TLS 1.3 encryption). The CBE must support security hardening. The CBE must support Role Based Access Control. The CBE must support Backup and Restore procedure and solution
27	Support	The Provider must provide 24 x 7 product support. Provide the details of the support that can be provided and the location of your support centers. Provide the number of staff in your support organization.
28	Training	Include training for at least ten (10) staff members for the proposed product. Training must be provided on-site at customer facilities.
29	Roadmap	The Provider must submit its policy and vision for the evolution of products. It will include: - The roadmap of features for the next two - five years

#	Requirement	Description
		- The roadmap and adherence versions (releases) of 3GPP
30	Public Warning Support	Public Warning Support - The CBC must support priority messages. - When a priority message is submitted all non-priority messages that are currently being broadcast in the area where the warning message shall be broadcast, will be stopped temporarily.
33	External Interfaces	The CBE–CBC interface should support the following primitives: - CBC Login. - CBC Logout. - Change Password. - Create New Message. - Create Message using Predefined Area. - Change Message Contents. - Kill Message. - Kill Message Cell. - Kill All Message Cell. - Message Information. - Predefine Area. - Remove Predefined Area. - Command Information. - New Message Cells. - New Message Cell Controllers. - New PLMN-wide message. - Retrieve Areas. - Network Availability. (Where a cell broadcast message can reach) - Message Network Cell Count. - Retrieve Information Providers. - Index Message
34	Standards Compliance	Comply with standards listed in chapter 0.