Body of European Regulators for Electronic Communications

BEREC

BoR (19) 255

BEREC guidelines on how to assess the effectiveness of public warning systems transmitted by different means

December, 2019

Contents

Executive Summary **3**

1. Introduction **5**

1.1. What are Public Warning Systems? 5

1.2. Description of the task & addressees of the Guidelines & non-binding character 5

2. BEREC's interpretation of the scope of article 110 EECC **6**

2.1. Legal considerations 6

2.1.1. Aim of article 110 EECC 6

2.1.2. Obligation of article 110 EECC 6

2.1.3. Equivalence of 110(2)-PWS' 6

2.1.4. Parallel roll-out of multiple ECS-PWS' in a member state 7

2.2. Systems falling under 110(1) EECC for the purpose of benchmarking 7

2.2.1. Introduction 7

2.2.2. Cell Broadcast (CB) implemented according to ETSI EU-ALERT standard 8

2.2.3. Location Based SMS (LB-SMS) 10

2.2.4. Automatic Voice Calling (AVC) 11

2.2.5. Conclusion 12

2.3. Systems falling under 110(2) EECC 12

2.3.1. Introduction 12

2.3.2. IAS Mobile Application Based PWS 12

3. Methodology **15**

3.1. Criteria & sub-criteria for evaluating ECS-PWS performance 16

Coverage 16

3.1.1. Geographical coverage 16

3.1.2. Population Coverage 17

Capacity to reach end-users 17

3.1.3. Support of inbound roamers 17

3.1.4. Supported devices 17

3.1.5. Supported languages 18

3.1.6. Managing longer messages 18

3.1.7. Steps required for recipient to enable receiving warning messages 18

3.1.8. Accessibility for end-users with disabilities 18

3.1.9. Reliability 18

3.1.10. Geographical targeting 19

3.1.11. Scalability 19

3.2. Establishing the Benchmark 20

3.2.1. Analysing the performance of Cell Broadcast as implemented according to ETSI EU-ALERT standard 20

3.2.2. Analysing the performance of Location based SMS 23

3.2.3. Overview of 110(1) performance 27

3.3. Assessing the equivalence of the effectiveness of IAS-PWS 30
3.3.1. Analysing IAS-PWS performance 30
3.3.2. Comparing IAS-PWS performance with 110(1)-PWS performance 32
Annex 1 37
Annex 2 39
Annex 3 41

Executive Summary

These guidelines are provided by BEREC in response to the task set in article 110(2) of the Directive (EU) 2018/1972 of the European Parliament and of the Council of 11th December 2018 establishing the European Electronic Communications Code[1] (hereinafter EECC), to assist member states in assessing the effectiveness of alternative Public Warning Systems (hereinafter PWS) using means of electronic communications services (hereinafter ECS-PWS).

The document has the following structure:

- Chapter 1 sets out the relevant background on ECS-PWS' and a detailed description of the task provided by article 110 EECC, focusing on BEREC's requirement to publish guidelines on how to assess whether the effectiveness of public warning systems under article 110(2) EECC are equivalent to the effectiveness of those under article 110(1) EECC.
- Chapter 2 illustrates BEREC's interpretation of the scope of article 110 EECC, including legal considerations as well as information on the relevant ECS-PWS' (Cell Broadcast, Location-based SMS and ECS-PWS' using an on-device application making use of an internet access service, hereinafter IAS-PWS').
- Chapter 3 describes the methodology BEREC proposes, which is essentially a guideline of steps to conduct an assessment of the equivalence of effectiveness of ECS-PWS'. It is divided into three main sections.
    - Section 3.1 describes the criteria derived from the EECC the methodology proposes to assess the performance of each type ECS-PWS in order to make them comparable. It does so by describing the two main-criteria mentioned by the EECC (coverage and capacity to reach end-users) and a set of sub-criteria which can be summarised under the main-criteria, and in BEREC's view help to substantiate them.
    - Section 3.2 describes how competent authorities may establish a benchmark for the assessment of the equivalence of relevant ECS-PWS falling under article 110(2) EECC (IAS-PWS). To create the benchmark BEREC proposes analysing the performance of the relevant ECS-PWS falling under article 110(1) EECC (Cell Broadcast and Location-based SMS) by assessing them against the proposed criteria and sub-criteria established in section 3.1. For the assessment by the competent authorities BEREC has compiled an initial assessment for each sub-criterion. The level of detail in the assessment of each sub-criterion varies as for some sub-criteria the performance of an ECS-PWS depends on national circumstances like the network-structure or the geographic dispersion of end-users in a Member State.
    - Section 3.3 then describes how competent authorities may assess their envisioned IAS-PWS against the benchmark created in section 3.2. In this section BEREC provides general information for the consideration of competent authorities when assessing the performance of their envisioned IAS-PWS against the criteria and sub-criteria[2] and for the final step of the methodology - when assessing the envisioned IAS-PWS against the benchmark[3].

The document is supported by the following annexes:

[1] https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1564053148824&uri=CELEX:32018L1972

[2] See section 3.3.1

[3] See section 3.3.2

- Annex 1 sets out an overview of desk research / NRA questionnaires
- Annex 2 sets out a glossary of terms.
- Annex 3 contains the text of article 110 EECC

1. Introduction

1.1. What are Public Warning Systems?

PWS' are systems which authorities may use to notify citizens regarding imminent or developing major emergencies and disasters.[4] Such warnings may be transmitted e.g. through sirens, publicly available electronic communications services, broadcasting services, mobile applications relying on an internet access service, or any combination of the above. In these guidelines sirens or TV/radio broadcast are referred to as "legacy-PWS'" and PWS' using means of electronic communications technology are referred to as "ECS-PWS". Article 110 EECC (see Annex 3) introduces an obligation to roll out ECS-PWS' where PWS' are already in place.

There is a wide diversity of practices in Europe regarding ECS-PWS'. Member States appear to have taken different approaches as to which systems to implement (see Annex 1). Also, NRAs are often not the competent authority in relation to implementing PWS and in many cases there are multiple stakeholders involved like ministries and public safety authorities.

1.2. Description of the task & addressees of the Guidelines & non-binding character

According to article 110(2) subparagraph 2 EECC BEREC shall publish guidelines on how to assess whether the effectiveness of ECS-PWS' according to paragraph 2 of article 110 EECC (hereinafter – 110(2)-PWS) is equivalent to those according to paragraph 1 (hereinafter – 110(1)-PWS). This means that BEREC is asked to provide guidance on an assessment to be made by the competent authorities in the respective Member States, which in most cases will not be a NRA. BEREC interprets this task as to provide a toolbox to support Member States in fulfilling their obligations arising from article 110 EECC. The purpose of this document is not to rank ECS-PWS' according to their performance but to provide Member States with the means to compare the effectiveness of the relevant systems keeping in mind their respective national circumstances and envisioned purpose for the ECS-PWS.

After national ECS-PWS' are deployed, the European Commission will be responsible for the assessment of Member States' compliance with article 110 EECC where Member States have rolled out a stand-alone 110(2)-PWS for a specific purpose. These Guidelines could serve as an input to the Commission's assessment of a Member State's compliance, however the Commission is not bound by these guidelines. In this regard, the guidelines may assist Member States to identify reasons to support a decision to roll out a certain 110(2)-PWS.

[4] It is up to each Member State to determine for which type of emergencies/disasters it wants to alert its citizens.

2. BEREC's interpretation of the scope of article 110 EECC

2.1. Legal considerations

2.1.1. Aim of article 110 EECC

According to Recital 293 the aim of article 110 EECC is to approximate the diverging national law in the area of the transmission of public warnings by electronic communications services regarding imminent or developing major emergencies or disasters. Diverging national law could lead to big differences regarding the effectiveness of rolled-out ECS-PWS. To counter such a development article 110(1) EECC prescribes a common level of minimum effectiveness – the performance of the ECS-PWS' mentioned in article 110(1). However, because the article 110 EECC is technologically-neutral article 110(2) EECC provides for a Member State to roll-out alternative ECS-PWS as long as they are as effective as the systems mentioned in article 110(1) EECC, thus ensuring Member States' compliance with the envisioned level of minimum effectiveness of ECS-PWS'.

2.1.2. Obligation of article 110 EECC

Article 110(1) EECC requires that Member States *"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."*

Therefore, article 110 of the EECC does not place any obligation upon Member States without existing PWS, to develop or deploy a legacy or ECS-PWS.

However, article 110(1) EECC obliges Member States with existing PWS (be it legacy-PWS or an early version of ECS-PWS) to implement an ECS-PWS. Whether or not a Member State has to perform such an update is beyond the scope of the BEREC guidelines.

2.1.3. Equivalence of 110(2)-PWS'

Article 110(2) EECC states that Member States may determine that public warnings can be transmitted via alternative publicly available ECS (including an IAS-based mobile app) as long as it has equivalent effectiveness *"in terms of coverage and capacity to reach end-users, including those only temporarily present in the area concerned"* and is "*easy for end-users to receive".*

With regard to the roll-out of ECS-PWS' the EECC considers the obligation of article 110 fulfilled when a system according to article 110(1) EECC is rolled out by a Member State. It does so without requiring further prerequisites recognising the effectiveness of 110(1)-PWS' as a benchmark for alerting the population in case of imminent or developing major emergencies and disasters. With regard to the roll-out of "stand-alone" systems according to article 110(2) the EECC prescribes prerequisites because Member States have to assess these systems against the effectiveness of 110(1)-PWS', measuring the equivalence *in terms of coverage and capacity to reach end-users*.

BEREC considers that Recital 294 EECC explains what is meant by "*easy for end-users to receive"* when it states that "w*here a public warning system relies on an application, it should not require end-users to log in or register with the authorities or the application provider*".

2.1.4. Parallel roll-out of multiple ECS-PWS' in a member state

With regard to the roll-out of several systems in parallel, BEREC considers that this is possible under the EECC since having one ECS-PWS is only the minimum requirement of article 110 EECC. Also, the EECC does not require that one single system must be available across the entire Member State. BEREC thus considers that several regional systems – operating next to each other – can also fulfil the obligation under Article 110 if they meet its requirements.

Furthermore the EECC does not specify that an ECS-PWS has to be fit for all purposes. BEREC considers that Member States may also roll-out several ECS-PWS' in parallel that cover different purposes (e.g. an ECS-PWS specifically tailored to alert participants of a mass event).

Additionally, BEREC considers that if a Member State decides to roll out a 110(2)-PWS for the same purpose as an existing 110(1)-PWS, the 110(2)-PWS would not need to be measured against the equivalence requirements of coverage and capacity to reach end-users as described in the BEREC guidelines because in such a case the Member State would be introducing an additional ECS-PWS on top of the system which already fulfils its obligation from the EECC.

The logic behind this interpretation is supported in the case where a Member State might want to supplement an existing 110(1)-PWS with a 110(2)-PWS with limited functionality, developed to deliver warnings to a certain subset of the public (e.g. visually impaired end-users), or for some other special use case, without rolling out a fully-fledged, "stand-alone" 110(2)-PWS.

An example of this would be a 110(2)-PWS' which could provide better solutions for citizens with disabilities. In this case the Member State might want to complement its 110(1)-PWS with this specialist 110(2)-PWS. Thus, the MS would be going beyond the obligation stemming from article 110 EECC as it would like to roll-out even more than its existing 110(1)-PWS, even if it is not a stand-alone additional 110(2)-PWS. If this "supplemental-110(2)-PWS" needed to be measured against the prerequisites of article 110(2) and the BEREC guidelines, the supplemental 110(2)-PWS would most likely not perform equivalently compared to the benchmark and the Member State might conclude that the roll-out of an additional fully-fledged 110(2)-PWS would be too costly/demanding and could in consequence refrain from improving its overall ECS-PWS capability. In practice this would encourage rolling out less-effective ECS-PWS' which would not be in line with the aim of Article 110.

Therefore BEREC considers that these guidelines should only apply in those cases where a Member States wants to roll-out a stand-alone 110(2)-PWS for a specified purpose. Where Member States want to roll-out a 110(1)-PWS and supplement it with aspects of a 110(2)-PWS the latter would not need to be measured against the guidelines. However, BEREC recommends using the guidelines as a reference point in such cases in order to identify possible areas of improvement in the supplemental-110(2)-PWS.

2.2. Systems falling under 110(1) EECC for the purpose of benchmarking

2.2.1. Introduction

The following sections provide a general description of 110(1) based systems which are implemented in live deployments and which BEREC considers relevant for the purpose of these guidelines. While it would be possible to deliver public warnings using other methods on an NB-ICS[5] (number-based interpersonal

[5] E.g. USSD Push

communications service as defined by article 2(6) EECC), this document is not intended to describe every conceivable method.

An essential component of each ECS-PWS is the “alerting gateway”. This document uses the term “alerting gateway” to refer to the entity which provides an interface to public authorities to submit warning messages. There may be a single alerting gateway per MNO, or a member state might have a single alerting gateway which interfaces to all MNOs. It is the alerting gateway that interfaces with the relevant network equipment to deliver the ECS-PWS messages.

2.2.2. Cell Broadcast (CB) implemented according to ETSI EU-ALERT standard

CB is a technology which was standardised in the early 2G GSM networks, although it was rarely deployed due to the lack of a commercial business case.

For the purpose of these guidelines BEREC uses EU-ALERT as an example for CB implementation as it is a well-known and tested system. There are other CB-systems available which might not share all functions of EU-ALERT but are built on the same technology.

The EU-ALERT standard (ETSI TS 102 900) is equivalent to the American CMAS/WEA system, which also builds upon the CB technology, standardising certain aspects to suit its use as an ECS-PWS. These aspects include the definition of various warning message types which have different severities, with the highest severity (EU-Alert Level 1 – Presidential Alert[6]) being displayed on all compatible devices regardless of the users’ opt-in/opt-out status.

CB is, as the name suggests, a broadcast technology operating at the default minimum granularity of a single cell up to any size of cell group (e.g. all cells in a particular region). In this scenario the alerting gateway interacts with the CBC (Cell Broadcast Centre) which sends a message to the destination cell (BTS/NodeB/eNB/gNBs), which forwards this message over the air interface only in pre-defined time intervals until it is not needed any more. Therefore, even users that arrive in the affected area later (or have been in that area but have not been in coverage of mobile network) could be warned by CB. All attached mobile devices connected to the cell listen for these broadcasts and display the message on the users’ mobile devices where appropriate. Each warning has got its unique serial number. The mobile device remembers the serial number of the CB message, so the CB message is shown only once on each mobile device but can be called up again by the end-user.

[6] The Presidential Alert level is the only level that doesn't allow opt-out. Extreme and Severe Threats should be opted-in by default, but allow the user to opt-out.

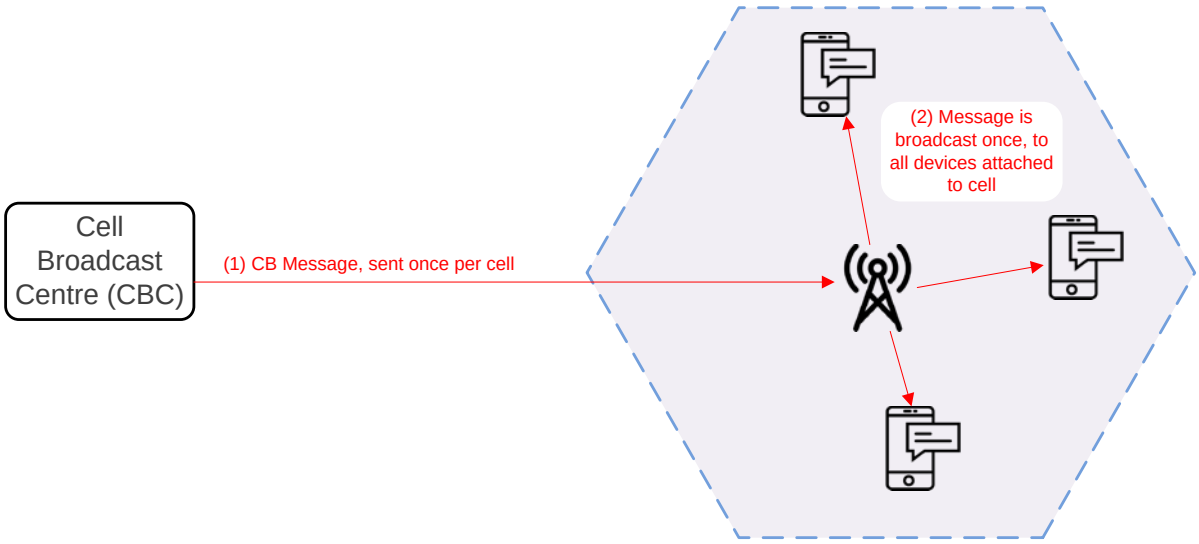

Figure 1 - Cell Broadcast

As can be seen from the diagram above, because a CB message is sent only once from the CBC to each cell, and from each cell it is broadcast repeatedly to all attached mobile devices, the network load for a given warning message is very low. In addition, over the radio interface CB traffic is either carried with the highest priority (3G/4G) or is carried on a dedicated channel (2G). For all these reasons CB works well during times of network congestion.

The ability to avoid network congestion and the ease of targeting specific geographical areas using cell level granularity without any additional mobile device tracking function were identified as key benefits of CB in several NRA's responses to BEREC's questionnaire (The Netherlands, Romania, Greece, Italy, Norway and Sweden).

Device Based Geo-fencing

An enhancement to the CB service is the device based geo-fencing (DBGF) feature, which will enable the CBC to include some geographic information within the CB message. Mobile devices which support this feature will be able to determine if they are currently situated within the geographic area indicated by the CB message, and display the message only if appropriate. For this the mobile device uses its own positioning capability to add an additional filter on the geo-targeting polygon which was previously sent to the mobile device.

This feature was originally specified at the request of the Federal Commission for Communications (FCC, US authority) for use in North America, however it has (in 2019) been added to the relevant 3GPP specifications for worldwide availability. At the time of writing this feature is not yet available in Europe, although it can be reasonably anticipated to be available in the future. Therefore, competent authorities are advised to verify the current situation in terms of network and device[7] support at the time of ECS-PWS implementation in order to ensure the correct capabilities of available CB technology are used when creating their benchmark according to section 3.2.

[7] Note that the level of device support for DBGF will likely increase over time and will depend on the specific profile of devices in a given member state's mobile market

When answering to BEREC's questionnaire some Member States (The Netherlands and Sweden) have mentioned this feature in view of a possible future implementation.

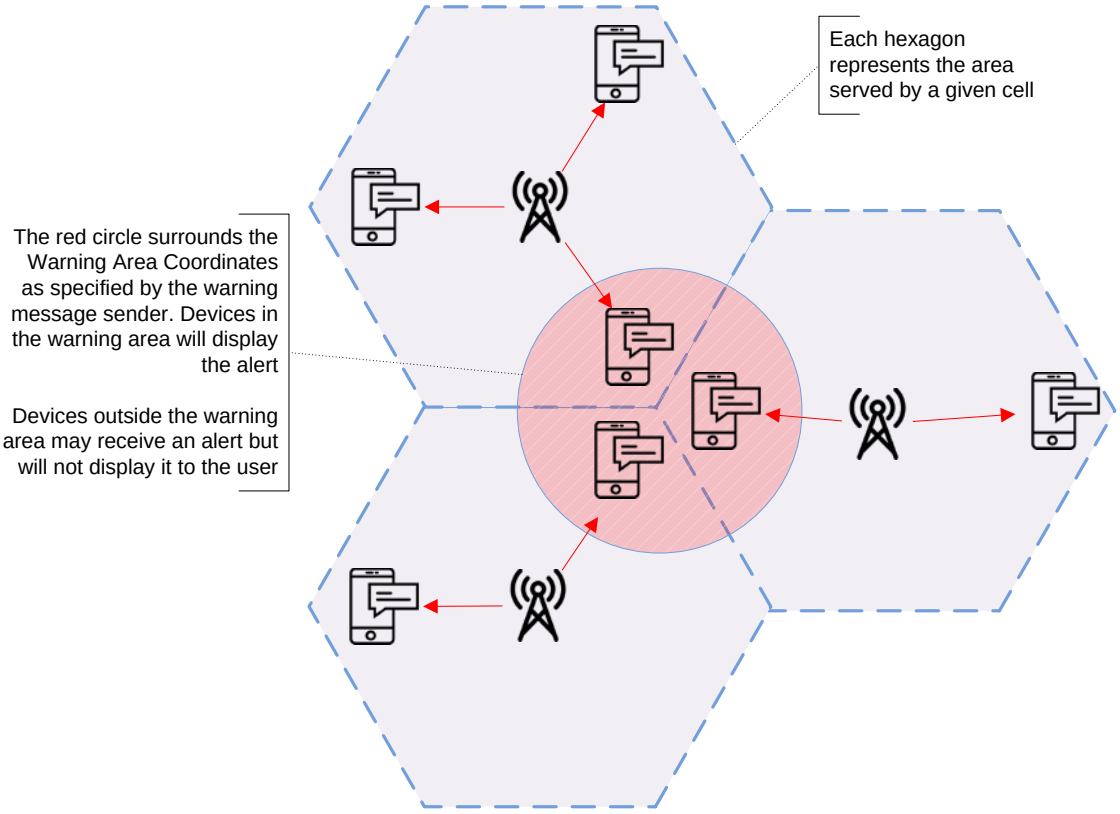

Figure 2 - Device Based Geo-fencing

In the diagram above every mobile device shown in the 3 cells will receive the warning message containing the warning area coordinates. However only mobile devices within that area (denoted by the red circle) will display the message, while mobile devices outside the area will not display it.

2.2.3. Location Based SMS (LB-SMS)

As far as the network[8] and the end user is concerned, an LB-SMS message is simply a normal SMS message which is sent to a subset of the Mobile Network's attached devices, which happen to be in a particular geographical area.

In order to achieve this for some mobile network topologies however, the network must maintain a database of all mobile devices in the target location for potential PWS messages. In other words, for all areas that the MNO

8 It's possible that some integrated SMSCs may simply deliver the SM using the MAP *Forward Short Message* operation, and skip the MAP *Send Routing info for SM* step, if the location is already known; however in other respects an LB-SMS message is no different to a Mobile Originated SMS message.

anticipates potentially delivering LB-SMS messages into, a list of all users currently located in those areas must be kept up to date at all times[9].

It should be noted that while mobile networks require knowledge of subscribers' locations for normal operation, this is usually not maintained at all times at the granularity of the single cell level. Therefore, an LB-SMS implementation will usually require the deployment of a MLC (Mobile Location Centre). The methods used by the MLC to track mobile devices as they move around the network are not standardised, and are subject to a certain level of inaccuracy, as stated by some Member States (Portugal and Sweden). Some MLCs track device location to the cell level, whereas other MLC providers claim to fix device location to a greater level of accuracy. Depending on the level of location granularity stored in the MLC, the precision of targeting will vary. There may be privacy implications in tracking user locations in this manner that should be considered, as mentioned by Croatia, Cyprus and Portugal.

The diagram below attempts to show a high level call flow for a typical LB-SMS implementation.

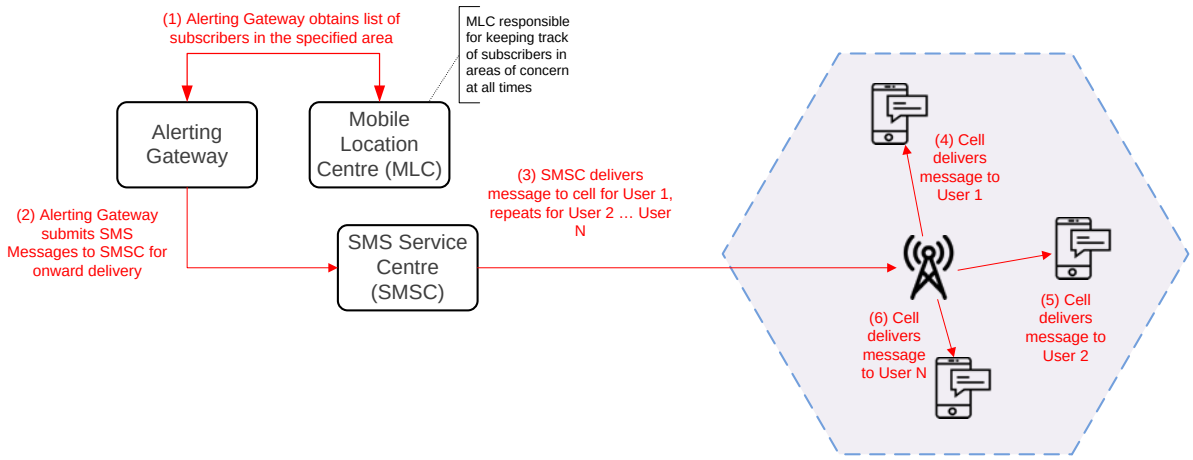

Figure 3 - LB-SMS

Aside from the location specific aspect, the principle difference between CB and LB-SMS services is that for LB-SMS the mobile network must carry each recipient's message separately, since the SMS standards do not have a 'one-to-many' or a broadcast capability.

2.2.4. Automatic Voice Calling (AVC)

In some national cases (Bulgaria and some regions of Spain), automatic voice calling is used to supplement other ECS-PWS facilities. In this situation the network might detect users in the area of interest and make a mobile-terminated voice call to those users' numbers, or might initiate calls to fixed numbers based on pre-provisioned information. This mobile terminated voice call would likely play a recording upon connection before disconnecting, although more advanced Interactive Voice Response (IVR) type use cases are conceivable.

9 The alternative to this approach is to not maintain any list of subscribers and their current cell, but instead to page the network to ascertain which subscribers are in a given cell. The time to execute this paging is likely to be significant, and could make such an approach inadequate for emergency usage.

Given that these AVC deployments are supplemental to other ECS-PWS systems, generally performing a specific niche, BEREC does not consider AVC based PWS as being a benchmark against which 110(2) systems should be measured.

2.2.5. Conclusion

Consequently, as a basis for discussion and to ensure consistent feedback from stakeholders, BEREC considers that for the purpose of the guidelines CB and LB-SMS fall under article 110(1) EECC.

2.3. Systems falling under 110(2) EECC

2.3.1. Introduction

Article 110(2) EECC refers to public warnings which may be delivered "*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*". BEREC interprets this sentence to include "mobile applications relying on an internet access service" (IAS based PWS') as services falling under article 110(2) EECC because the wording used is "or" rather than "other than" which is used for the first two examples of article 110(2) EECC. Consequently the third example describes a specific use case for services falling under article 110(2) EECC.

Article 110(2) EECC allows for the development of future services which cannot yet be conceived of, while also referring to the possibility of a mobile application based PWS, which is covered in the following section. As IAS based PWS' are currently the only existing systems BEREC considers falling under article 110(2) EECC they are used as a reference for 110(2)-PWS throughout these guidelines. In case other 110(2)-PWS will be developed in the future that would not qualify as IAS-PWS the basic methodology for their assessment as described in these guidelines may usefully apply, even though section 2.3.2 and the IAS-PWS specific content of section 3.3.1 are specific to the present IAS-PWS example. Competent authority responsible for considering the system against BEREC's guidelines could contemplate making a description of the new 110(2)-PWS in a similar way as done in section 3.3.1 for IAS-PWS, and proceeding along similar lines to make their assessment.

2.3.2. IAS Mobile Application Based PWS

This section briefly sets out an example of an implementation of a hypothetical IAS-PWS[10] . While individual implementations may differ, many of the following details will be common to any deployment.

Any IAS-PWS will rely on an OTT application server which communicates with its associated app, running on the device of users that have installed it. This also extends to other devices than mobile devices such as smartTVs or PCs that have the app installed on them. Due to the nature of IP networks, each device must be addressed separately as it's not possible to broadcast[11] these warnings. Competent authorities could work with fixed and mobile network operators to model the impact of such traffic where many users are being addressed with small amounts of data.

[10] In this context "OTT" refers to services running "Over the Top" of the IAS, not requiring any special handing by the underlying transport network.

[11] IP Multicast, while complex, may be possible with prior agreement between national ISPs

When a warning is received from the alerting gateway for a specific warning area, the OTT application server is responsible for deciding which of the currently attached devices to send it to. There are a number of approaches to this:

Approach Description	Comment
Option 1: Send the warning message to all attached devices, irrespective of current location. Each device decides whether to display the warning message depending on its location[12]	Doesn't require real-time user location tracking, within the network, but will consume network resources to deliver warning messages which are not subsequently displayed on recipient devices. The behaviour of devices with an inaccurate location fix should be considered.
Option 2: Maintain a real time user-location database and send the warning message only to attached devices currently located in the warning area	This approach minimises the number of warning messages sent to devices which are subsequently discarded, but this comes at the cost of greatly increased network load and possible user privacy implications. The behaviour in the event of a device's location being stale or potentially out of date should be considered.

Table 1 - IAS Mobile Application Based PWS

In addition to the above options it would be possible to send the warning message to an additional subset of attached devices that have subscribed to receiving warning messages for a set of specific locations of interest (see section 3.3.2.2 "support of absent residents").

The following is a description of the sequence of events in an IAS-PWS for devices on which the on-device app has been installed.

Step number	Description	Comment
0	Registration with mobile or fixed network	Consideration should be given to DHCP[13] lease time for long running connections
1	Registration with OTT application server	Devices running the on-device app will register with the OTT application server to notify of their IP addresses and ensure that the device can be reached from the OTT application server. User credentials, preferences and cryptographic certificates may be exchanged at this stage also.

[12] The German NINA application uses this feature.

[13] Dynamic Host Configuration Protocol

Step number	Description	Comment
2	**Option 2 only:** Device keeps OTT application server informed of its location	The OTT application server maintains a user-location database of currently connected devices and their current locations. When the device moves within the mobile network, the on-device app updates the OTT application server with information of its current location[14], which is updated in the user-location database. The frequency of these updates will depend on the implementation (e.g. upon movement of a distance greater than X, every Y minutes etc.). Note that the location information provided is based on the devices' inbuilt Global Navigation Satellite System (GNSS) capability (E.g. GPS, Galileo), rather than detected by the mobile network.
3	Alerting Event	The alerting gateway, upon request of the authority tells the OTT application server to warn all users in a particular area.
4a	**Option 1 only:** Recipient selection	The OTT application server does not make a pre-selection. It transmits the warning message containing the relevant location to **all** devices.
4b	**Option 2 only:** Recipient selection	The OTT application server extracts from its user-location DB a list of users in the specified area. Warning messages are only sent to devices of users in the specified area.
5	Warning message Delivery	Each applicable device is notified individually over the mobile data/fixed line connection.
6	**Option 1 only**	Each device checks autonomously whether it is currently situated in the relevant area and only then portrays the warning message.
7	Acknowledgement (optional)	The devices respond to acknowledge receipt of the warning message.

Table 2 – IAS-PWS Steps

[14] Note that the location update referred to here is in addition to the regular standardised Location Updating procedures implemented in the mobile network control plane, used to facilitate user mobility and roaming etc.

The following diagrams attempt to show these steps in a graphical manner.

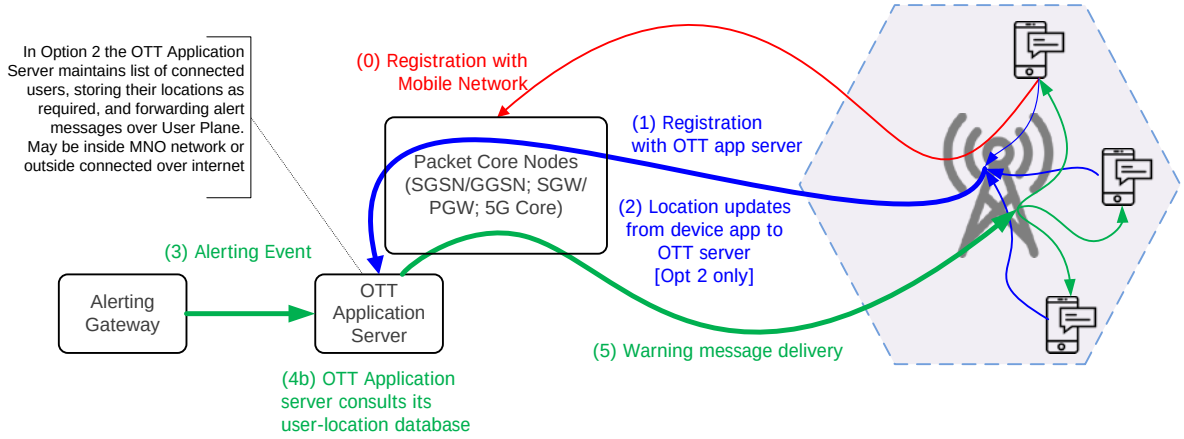

Figure 4 - Operation of an IAS-PWS using a mobile network

It is also possible for an IAS-PWS to operate over fixed network as shown below. In this case the call flow is more straightforward

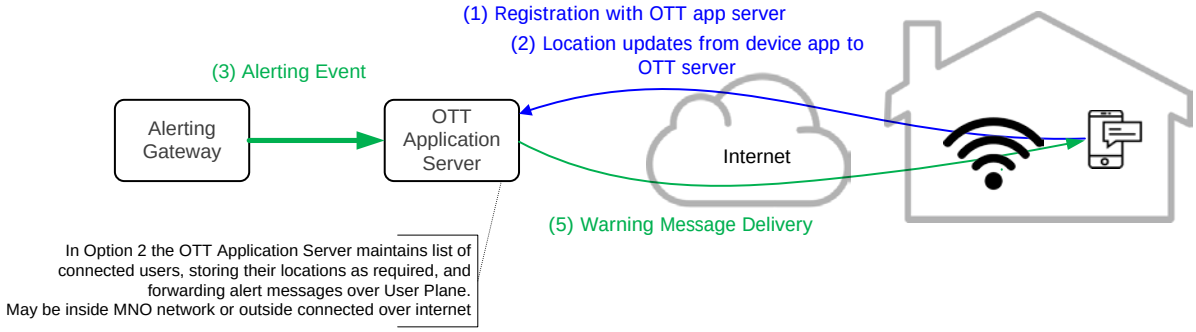

Figure 5 - IAS-PWS using fixed line WiFi

3. Methodology

As explained in section 2.1 these Guidelines apply for cases in which a competent authority of a Member State has to assess the equivalence of the effectiveness of an IAS-PWS it wishes to roll-out as a stand-alone system for a specific purpose compared to an article 110(1)-PWS. In order to enable competent authorities to similarly assess the effectiveness of their IAS-PWS BEREC proposes a methodology consisting of the following steps.

1. The competent authority identifies the purpose for and gathers requirements of the IAS-PWS they intend to deploy (e.g. What size geographical area it intends to address; How many devices need to be alerted in a given area per specified time interval; Does it need to address the whole population or only a specific group of citizens? etc.).
2. Secondly, the EECC defines main-criteria (coverage & capacity to reach end-users) to be used in the assessment. As the EECC does not specify the content of these main-criteria which makes them less tangible, BEREC considers competent authorities should also identify sub- criteria they consider relevant for their assessment of equivalent effectiveness, which can be summarised under the main

criteria mentioned by the EECC. For this a competent authority could make use of BEREC's list of sub-criteria (see section 3.1) and verify whether it needs to add further relevant sub-criteria.

3. Benchmark creation: BEREC proposes that competent authorities identify the performance of standardized 110(1)-PWS as described in sections 2.2.2 and 2.2.3 having regard to their national circumstances and identified use cases in order to create the benchmark for the assessment of the equivalence of their envisioned IAS-PWS. In other words, competent authorities should check how the hypothetical 110(1)-PWS' would perform in their Member State in order to create the benchmark.

   In section 3.2 of these guidelines BEREC sets out its analysis of the performance of 110(1)-PWS (CB & LB-SMS) for each sub-criterion from section 3.1 which may serve as a starting point for the assessment by the competent authority. The level of detail provided by BEREC in the initial assessment of each sub-criterion varies as for some sub-criteria the performance of an ECS-PWS depends on national circumstances e.g. the network-structure or the geographic dispersion of end-users in a Member State. Competent authorities should carefully consider BEREC's analysis and supplement it with their own assessment, in particular where they identified further relevant sub-criteria for the list from section 3.1.

4. Assessing the equivalence of IAS-PWS effectiveness: As a first step in the assessment BEREC proposes that competent authorities should analyse the performance of the envisioned IAS-PWS using the EECC's main criteria (coverage and capacity to reach end users) and the already identified sub-criteria. In this regard BEREC suggests points to consider in section 3.3.1 that could facilitate a reasonable assessment of such sub-criteria. The second element in this step would be comparing the performance of the IAS-PWS with the performance of the 110(1)-PWS (see section 3.3.2.1). Additionally, competent authorities may want to take into account further considerations in their assessment that have an impact on the overall effectiveness of an ECS-PWS. BEREC has listed these in section 3.3.2.2.

BEREC considers this four step approach can be easily replicated in each Member State allowing competent authorities to objectively assess the effectiveness of IAS-PWS and help them in their decision making process. Due to the nature of the criteria this approach ensures that Member States perform the assessment in a similar fashion but it necessarily also enables them to take national circumstances and the envisioned use case into consideration. What is important is that the steps themselves are harmonised, as this may increase certainty about the implementation of article 110 EECC for competent authorities.

3.1. Criteria & sub-criteria for evaluating ECS-PWS performance

Coverage

The EECC mentions "coverage" as one of the two mandatory main-criteria to be taken into account in the assessment of the equivalence of effectiveness. The aim of coverage is to ensure that as many end-users as possible can be effectively reached by the ECS-PWS. Thus, BEREC considers there are two aspects of coverage which are relevant in the assessment of the competent authorities – geographical coverage and population coverage. Depending on the national circumstances BEREC understands one may be more relevant than the other, also concerning the specific use-case the competent authority has in mind for the ECS-PWS.

3.1.1. Geographical coverage

In general this criterion refers to the ability of an ECS-PWS to reach all end-users concerned currently present in the relevant area. 100% geographical coverage of the relevant area is generally desirable, however when assessing national needs, competent authorities could take into account a number of factors:

- Whether the system in question is the only ECS-PWS facility in use, or whether it is complimentary to other ECS-PWS systems with the same purpose but targeting another geographical area. In cases where multiple systems are deployed for the same purpose, a competent authority could consider the total coverage of a combination of different systems potentially delivered over a combination of fixed and wireless networks.
- If there is a limited set of alerting use cases that the PWS will be used for - E.g. Tsunami type warning messages require only coastline coverage; Avalanche type warnings are only relevant in mountainous regions.

3.1.2. Population Coverage

Some Member States may not have 100% geographical coverage but are still able to reach a larger amount of the population than other Member States with higher geographical coverage, due to the distribution of the population within their territory. This applies in particular to Member States where large areas of the country are only sparsely populated (e.g. the north-western part of Sweden). In such cases it may be a viable option to concentrate on the population coverage rather than the geographical coverage in the assessment of a systems effectiveness.

Capacity to reach end-users

"Capacity to reach end-users" is the other mandatory main-criterion to be taken into account in the assessment of the equivalence of effectiveness. The EECC sheds some light on the aspect which end-users are meant in recital 293 which clarifies that "The end-users concerned should be considered to be those who are located in the geographic areas potentially being affected by imminent or developing major emergencies and disasters during the warning period, as determined by the competent authorities". However, it does not specify what is exactly meant by "capacity to reach" which makes this main-criterion rather vague. BEREC considers the following sub-criteria can be summarised under "capacity to reach end-users" making this criterion easier to assess for competent authorities.

3.1.3. Support of inbound roamers

Article 110(2) EECC explicitly refers to the need to provide warning messages to *"those only temporarily present in the area concerned".* Also recital 294 states that "*end-users entering a Member State*" shall be informed "*on how to receive public warnings*". This is the only sub-criterion explicitly mentioned by the EECC, thus BEREC considers it to be of specific importance for the legislator. This should be reflected accordingly in the competent authority's assessment.

This sub-criterion may need to be assessed in conjunction with other sub-criteria in this section (e.g. Sections 3.1.5, 3.1.7 and 3.1.10

3.1.4. Supported devices

Depending on the type of ECS-PWS and the envisioned addressees (Competent authority decides whether it wants the ECS-PWS to potentially address the whole population or only a subset of it), the question of whether all end users' devices can support the service is an important one.

ECS-PWS' which are based on long standardized network services (such as CB and SMS) have a greater likelihood of being supported by default, whereas ECS-PWS' which rely on an on-device app which is not supported by older mobile devices, also introduce questions about how many different platforms it must be developed for and which app stores to use.

Competent authorities should consider the penetration of supported devices when planning a new ECS-PWS implementation.

3.1.5. Supported languages

This sub-criterion refers to the ability of the ECS-PWS to ensure that recipients can receive warning messages in the language of their choice. An ideal implementation would automatically deliver a single warning message in the appropriate language to a given user, while a less than ideal implementation might deliver multiple versions of a warning message in different languages or require end users to pre-select the preferred language.

3.1.6. Managing longer messages

As part of the requirements gathering phase of the ECS-PWS deployment project[15], competent authorities should consider the minimum length of warning message that will suffice for that member state's needs. In the event that special characters are to be used, this could cause a message encoding to be used which results in fewer characters being available in a single message.

Competent authorities should take into account the message concatenation features which exist in some 110(1) systems, considering the possibility and user experience of lost or delayed message segments, for example a scenario when parts 2 and 3 are received by a device while part 1 is delayed or missing.

3.1.7. Steps required for recipient to enable receiving warning messages

This sub-criterion refers to the possible necessity for an end user to take some action to enable the receipt of warning messages. This could range from no human interaction required, to a minor setting change on the device, up to the need to download an on-device app or to create an account on the ECS-PWS potentially specifying details such as the user's location or language.

Given that the requirement for any steps to be taken in advance by the end users will result in a reduced take-up rate, competent authorities should consider the impact on these steps when selecting an ECS-PWS.

3.1.8. Accessibility for end-users with disabilities

Competent authorities should take into account the user experience for end users with disabilities when considering alternative ECS-PWS'.

3.1.9. Reliability

The reliability (sometimes also referred to as 'resilience' or 'robustness') of any Telecoms or IT system will be influenced to a large extent by its complexity. Put simply, the greater the number of nodes, links or components that are involved in the handing of a particular operation, the greater the chance that a failure could occur in that operation's execution.

[15] Step one of the methodology introduced in section 3.

When assessing an ECS-PWS' reliability, competent authorities could seek network design information from the operators of those networks, including details of the nodes which are involved in the delivery of the ECS-PWS.

Some questions that could be asked, include:

- To what extent has this system been end-to-end load tested?
- What is a guaranteed minimum performance level that the network operator is willing to commit to?
- What level of redundancy is built into the critical network elements to allow the service to continue in the event of a node failure?
- How has this redundancy been verified?
- Are real fail-over tests executed on a regular basis?
- What was the measured level of uptime each of the nodes/links involved in the ECS-PWS in recent months/years? How is this measured?
- What was the measured level of uptime for the end-to-end ECS-PWS service in recent months/years? How is this measured?
- In cases where the ECS-PWS is delivered via multiple networks (e.g. both wireless and fixed)
    - In the event of a problem with one delivery network (e.g. the wireless network), does the ECS-PWS have a coherent method to detect this and deliver warning messages via the other network? (e.g. the fixed network)
    - How is the combined uptime measured and assured?

3.1.10. Geographical targeting

Each delivery mechanism (and indeed each specific implementation, depending on the MNO network design) has a different level of granularity, the ability to target end users in a specific location. Details for each ECS-PWS are explained in sections 2.2.2 (CB), 2.2.3 (LB-SMS) and 2.3.2 (IAS-PWS).

Competent authorities should consider during their requirements capture phase[16], the alerting use cases they wish to support, and therefore the level of granularity required.

Another aspect that should be considered is whether the ECS-PWS contains a functionality which ensures that end-users are warned when they enter a hazardous area, in which they were not present at the time the warning message was issued.

3.1.11. Scalability

Any ECS-PWS system will have an upper limit of the number of devices to which it can send warning messages per second, or per minute in a given area or indeed across the entire network. This upper limit will be based somewhat on the capacity of the underlying network, although it should be noted that some ECS-PWS implementations consume more network resources than others.

When assessing this sub-criterion, competent authorities could first consider the warning message use cases which are anticipated, and based on this, a target number of addresses for a given area.

In the responses to the BEREC survey, Croatia raised a general concern about the capacity of mobile networks, which are built for day to day traffic, to alert large populations in real time.

[16] See step one of the methodology introduced in section 3.

3.2. Establishing the Benchmark

When the EECC states in article 110(2) that the effectiveness of 110(2)-PWS needs to be "*equivalent in terms of coverage and capacity to reach end-users*" it conclusively implies, that the effectiveness of a system falling under article 110(1) is the benchmark the 110(2)-PWS needs to be assessed against. In the following sections BEREC analyses the performance of generic CB and LB-SMS systems, which can later be used as a benchmark. BEREC also sets out a number of points of note which competent authorities may take into account when establishing the benchmark for the assessment the equivalence of effectiveness of their envisioned IAS-PWS. This initial assessment needs to be tailored to the national circumstances in the respective Member State as well as to the specific purpose the competent authority has in mind for its ECS-PWS. Therefore, depending on the purpose of their envisioned IAS-PWS competent authorities will have to supplement BEREC's initial assessment with their own considerations. Also, national circumstances will influence the performance of the assessed ECS-PWS especially with regard to sub-criteria that depend on network specific intricacies of each Member State.

3.2.1. Analysing the performance of Cell Broadcast as implemented according to ETSI EU-ALERT standard

Coverage

3.2.1.1. Geographical Coverage

The information needed for the assessment of CB performance with regard to geographical coverage depends largely on the network topology and its capabilities. Such information at the detail required is not available to BEREC. Furthermore BEREC considers that for the assessment the information should be as recent as possible, due to the constant changes made to national networks. BEREC can therefore not provide an in depth assessment for each Member State.

CB as described by ETSI EU-ALERT standard is supported on 2G and each subsequent generation beyond. Specific mobile network features and interfaces (to interact with the CBC) need to be deployed to enable CB on each access network technology. Thus, to assess CB coverage BEREC recommends that competent authorities consult with MNOs to receive information about both radio coverage and CB capabilities for each access technology.

In the responses to the BEREC survey Italy, Romania, Slovenia and Turkey positively mentioned the coverage provided by CB on their respective mobile networks. More specifically the Netherlands provided an estimate that 99% of people with a mobile phone would be reached due to the current architecture of their mobile network.

3.2.1.2. Population Coverage

Similarly to the assessment of the geographical coverage BEREC has no access to the information required to assess population coverage in each Member State Competent authorities should therefore contact the relevant authorities in their Member State that have access to data on the geographic dispersion of the population and analyse which amount of population can be reached under the current state of mobile network deployment relevant for the performance of CB.

Capacity to reach end-users

3.2.1.3. Support of inbound roamers

BEREC considers that the performance of CB with regard to the support of inbound roamers depends rather on technical limitations than on differences in the Member States.

If the mobile devices of inbound roamers have been pre-configured to receive CB messages, then these devices will also receive CB message while roaming (corresponding practical experience is reported by the Netherlands). Therefore BEREC considers that CB excels at performing this criterion.

3.2.1.4. Supported devices

The basic CB service is potentially supported by all mobile devices, whereas the EU-ALERT aspects have been commonly available on Android, iOS and Windows mobile devices since 2012.

It should be noted that while iOS mobile devices support EU-ALERT, Apple have indicated that MNOs should work with them to enable the feature on iOS mobile devices before implementing it.

Slovenia positively noted the amount of devices supported by CB in their response to the BEREC survey.

3.2.1.5. Supported languages

CB supports messages in any language provided by the warning message originator. There is facility in the EU-ALERT standards for warning messages to be sent in multiple languages.

Selecting the language is device dependent and, using an appropriate MMI[17], the user is able to choose the preferable language to be additionally displayed on his mobile device (as stated by the Netherlands and Romania).

A CB structure is required to accommodate the requirement to broadcast messages in multiple languages virtually simultaneously in order not to disadvantage any recipient of a message in a particular language.[18]

As standard, if the user has opted-in to receiving EU-ALERT messages, these will be presented in the local language. However, the mobile device shall be able to maintain user EU-ALERT language preferences in case the user wishes to receive messages in other languages than the local language as well. Such pre-selection only works if messages are broadcast in other languages next to messages in the local language.

3.2.1.6. Managing longer messages

CB messages are sent in ‘pages’. Each page can carry up to 93 characters, with the possibility to concatenate up to 15 pages for a maximum of 1395 Latin characters (e.g. English, French) and fewer characters if Unicode or extended character sets are used.

Before sending multi-page (greater than 93 characters) warning messages, competent authorities should consider the possibility and impact of partial message delivery. Usually if multi-page warning messages are

[17] The Man Machine Interface (MMI) code - include numbers entered on the dial pad which activate different capabilities of the device

[18] See ETSI TS 102 900 V1.3.1 (2019-02) clause 5.1

sent, mobile devices wait until they have received all parts before they display the message. Thus the risk of partial message delivery is low but it may take longer for the full message to be displayed.

3.2.1.7. Steps required for recipient to enable receiving warning messages

Currently three options exist regarding the receipt of CB messages in end-user's mobile devices:

- Pre-configuration by the manufacturer
- Opt-in/Opt-out menu in the settings of the device
- No option to enable CB.

These options are subject to local regulations, requests from government or operators to the mobile device manufacturers. In some Member States (e.g. Germany) CB is currently not used. Consequently, mobile devices sold in such Member States may neither be pre-configured to receive CB messages, nor may they offer a menu to enable CB. ETSI confirms that in other Member States and depending on the use of CB mobile devices can be pre-configured by the manufacturer to receive CB messages by default. Alternatively, a menu is available that allows users to opt-out and to opt-in to message categories that were not pre-configured at the point-of-sale.

In CEPT's and RO Alert's experience there might be devices for which some of the alerts need to be activated manually; furthermore, end-users can opt out for most of the alerts the Netherlands and ETSI indicate that for apple devices recipients have to opt-in. Mobile devices which support EU-ALERT will receive and display all messages sent with the 'EU-Alert Level 1 (Presidential Alert)' severity, as it is not possible to opt-out of these. Users can choose whether to see messages sent with lower severity levels.

For the assessment by the competent authorities BEREC recommends to check the steps required to enable CB on mobile devices currently available on their national market.

3.2.1.8. Accessibility for end-users with disabilities

CB itself does not provide functionality which supports the specific needs of disabled end-users. E.g. the support for text to speech on incoming CB messages is dependent on the end user's mobile device's capabilities (confirmed by ETSI, CEPT and RO ALERT). Thus, if the mobile device does not support text-to-speech for visually impaired end-users, CB does not have a back-up functionality to compensate for this.

Competent authorities are advised to check the level of support against the popular mobile devices in their national market. For mobile devices that do support CB, the CB-message comes with a specific ring-tone which was designed for maximum effectiveness to reach hearing-impaired people. It also comes with a specific vibration cadence which allows the recipient to feel that this is an extraordinary message and not an incoming SMS or messenger message.

3.2.1.9. Reliability

Following the information in section 2.2.2, it can be said that CB is not a complex service involving a large number of nodes/links or components. This all contributes to the high level of reliability of this service which solely depends on the mobile network. Consequently, the robustness of each Member States mobile network plays into the reliability of CB and should be assessed accordingly by the competent authority.

One indicator of robustness is (geo-) redundancy of network functions meaning if a radio cell is down, mobile devices connect to another cell.

In the responses to the BEREC survey Italy, Norway, Slovenia and the Spanish region of the Canary Islands considered the reliability of the CB solution to be suitable for the delivery of PWS messages.

3.2.1.10. Geographical targeting

CB is an anonymous technology and is unaware of its recipients. All (activated) mobile devices that are in coverage of a radio cell that broadcasts a message will receive that message irrespective of whether they have an active subscription (SIM card) or not. The mobile stations may broadcast CB messages as long as the warning is active and as such be received by end-users entering the targeted geographical area at any time. Due to an alert identification feature of EU-ALERT each message will only be portrayed one time on each device (but can be re-opened) to avoid spam while the broadcast is active.

In the event that the Device Based Geo-fencing feature described in section 2.2.2 is available, it would be possible to define a target area with accuracy in the range of tens of meters.

In the responses to the BEREC survey Romania and Greece expressed their satisfaction with the geographical targeting capabilities of CB.

3.2.1.11. Scalability

As mentioned previously in section 2.2.2, CB based warning systems scale very well due to the lack of duplication of message handling. ETSI pointed out that the mobile network only needs to carry a single message per cell to reach every mobile device that is connected to that cell, and consequently the network load of CB messaging is independent of the number of devices that receive the message.

ETSI add that CB, being based on a broadcast technology, does not cause or contribute to mobile network congestion and the CB service always has the highest priority in the mobile network (as per 3GPP specifications) so it remains unaffected by existing congestion. Consequently, the system efficiently avoids network congestion issues in case of an emergency/disaster (CEPT, RO ALERT).

In practice CB messages are quickly delivered. In the Netherlands CB messages are regularly delivered in less than the 3-minute target. Both Romania and Turkey stated that the message can be received in a few seconds or up to 30 seconds. The speed of delivery of CB messages was positively mentioned by Latvia, Norway, Portugal and Turkey, in their responses to the BEREC survey

3.2.2. Analysing the performance of Location based SMS

Coverage

3.2.2.1. Geographical coverage

The information needed for the assessment of LB-SMS performance with regard to geographical coverage depends largely on the network topology and its capabilities. Such information at the detail required is not available to BEREC. Furthermore, BEREC considers that for the assessment the information should be as recent as possible, due to the constant changes made to national networks. BEREC can therefore not provide an in-depth assessment for each Member State.

As mentioned before, a LB-SMS message is simply a normal SMS message which is sent to a subset of the Mobile Network's attached devices, which happen to be in a particular geographical area. Receiving an LB-

SMS message will be possible while end users stay within the coverage of a 2G or 3G mobile network. LB-SMS coverage is identical to regular SMS coverage for a given mobile network.

According to the responses to BEREC's survey, in assessing their PWS plans Czechia, Hungary, Norway, Slovenia, Slovakia, and Portugal considered coverage to a positive factor when using LB-SMS due to the current architecture of their respective mobile network.

3.2.2.2. Population Coverage

Similarly, to the assessment of the geographical coverage BEREC has no access to the information required to assess population coverage in each Member State. Competent authorities should therefore contact the relevant authorities in their Member State that have access to data on the geographic dispersion of the population and analyse which amount of population can be reached under the current state of mobile network deployment relevant for the performance of LB-SMS.

Capacity to reach end-users

3.2.2.3. Support of inbound roamers

While the delivery of a LB-SMS to an inbound roamer presents no challenge for normal messages, the location specific aspect introduces some challenges as mentioned in section 2.2.3. Given that there are various non-standard approaches to locating end users, and that each MLC operates in a different way, it's not possible to make any definitive statements on the support for inbound roamers in this context. It is also possible that the different MLCs operating in each MNO network operate in different ways, therefore BEREC recommends that competent authorities consult with the MNOs operating in their territory when considering this criterion. Nevertheless, several Member States do consider sending SMS warning messages to inbound roamers (Belgium, Portugal, Sweden, Croatia and Slovakia). In any case, including information on how to receive LB-SMS PWS messages could be described in the welcome messages/SMS (this possibility is being considered by Slovakia). A potential challenge of notifying inbound roamers by welcome SMS is that many welcome SMS implementations focus on sending messages from the home network (HPLMN) to the roaming user, although the reverse scenario of the visited network (VPLMN) sending welcome SMS messages to roamers as they arrive is also possible and commonly implemented. Therefore, a competent authority wishing to use welcome SMS to notify inbound roamers of the existence of an ECS-PWS should investigate whether the VPLMN approach is possible, or request that the home MNOs of the inbound roamers customise the message sent to their customer.

3.2.2.4. Supported devices

LB-SMS public warning messages are supported on every mobile device available using an active subscription (SIM card).

This aspect was considered to be a key advantage by Czechia, Poland and Portugal in selecting a LB-SMS system.

3.2.2.5. Supported languages

The SMS standards support extended characters from some languages[19], and in any case Unicode characters can be used so all languages can be supported. It is recommended that competent authorities consult with MNOs and define the character sets used to encode SMS warning messages.

Since LB-SMS requires the network to deliver an individual message to each recipient, it is possible to send different text content in each message. In practise this allows the competent authority to support multiple languages for in-bound roamers by detecting their MCC (mobile country code) and using this to decide which version of the message to send to the end user. In this scenario, the PWS operator would need to submit one version of the same message in each language used. This would however not provide a solution for end-users that have a local MCC but do not properly understand the national language (e.g. immigrants).

3.2.2.6. Managing longer messages

An SMS message is limited to a default of 160 characters, however in the event that special characters or Unicode encoding is used, the single message character limit can drop to as little as 70 characters.

SMS messages can be concatenated, where the PWS system splits text into multiple segments which are reassembled by the receiving device. This has an obvious impact on the network load of any alerting event.

In the situation where all segments are not received together, some devices will await the arrival of the complete set before notifying the user, whereas others might display the received parts of the message with an indication that it is incomplete. The latter could lead to the delivery of confusing messages in rare cases. Competent authorities should consider the behaviour of the receiving device for the most common devices used in that market.

3.2.2.7. Steps required for recipient to enable receiving warning messages

The receipt of LB-SMS messages requires no human interaction, and it can be safely assumed that messages will be displayed as intended on the recipient device. This is supported by the experience of SOS Alarm, UMS and the General Directorate of Fire Rescue Service of the Czech Republic.

The configuration of LB-SMS by the end-user is possible but not a necessary feature. Member states that intend to implement a LB-SMS PWS which invites the end user to use SMS to register or configure the service to their needs, or even to opt-out of receiving warning messages should consider whether sending these configuration messages should be free of charge for the end-user.

It should also be noted that this SMS-based self-configuration would by default be impossible for inbound roamers to use, due to the nature of SMS routing.

3.2.2.8. Accessibility for end-users with disabilities

The support for text to speech for visually impaired end users on incoming LB-SMS messages is dependent entirely on the end user's mobile device's capabilities. Similarly to CB, LB-SMS itself does not provide specific functionality to support the needs of disabled end-users. If the mobile device does not support text-to-speech, LB-SMS does not have a back-up functionality to compensate for this.

[19] For a full description of the languages and character sets supported, see 3GPP TS 23.038

Competent authorities are advised to check the level of support against the popular devices in their national market.

In selecting the PWS in Denmark it was decided to implement a LB-SMS which is limited to hearing impaired users only.

3.2.2.9. Reliability

SMS as a service is dependent on the mobile network and generally very stable, with much attention given by MNOs to ensuring it works reliably under normal conditions. Consequently, the robustness of each Member State's mobile networks SMS service forms a significant aspect of the reliability of LB-SMS and should be assessed accordingly by the competent authority.

One indicator of robustness is (geo-)redundancy of network functions meaning if a radio cell is down, mobile devices connect to another cell.

In their response to the BEREC survey, Malta highlighted the stability of LB-SMS as one of the reasons for its selection as future PWS.

3.2.2.10. Geographical targeting

The granularity of a LB-SMS warning message will depend on the accuracy of the MLC in the MNO's network (usually a single cell) and thus on national and even regional circumstances. See section 2.2.3 for more information.

Competent authorities need to be aware of the fact that LB-SMS messages are not broadcast but sent individually to each mobile device in the respective area of the warning. Therefore, end-users entering the area after the initial warning message has been sent would not receive the warning message unless it is repeatedly sent to all mobile devices in the affected area. This can be corroborated with the explanation given by some Member States (Portugal and Slovakia) that the system uses the mobile network devices location information the moment it is triggered.

Another possible functionality of LB-SMS is the ability to continue to notify users that have left the area in order to keep them informed as highlighted by EENA in its report on PWS'[20].

3.2.2.11. Scalability

While mobile networks are dimensioned to carry millions of messages per day, MNOs assume a relatively flat distribution across the network in terms of both time and location. In other words, the average number of messages per second in a given cell is relatively low even in a busy network.

In some alerting use cases however (for example notifying all users in a densely populated area by SMS, e.g. in large cities) it would be possible for the radio access network to be flooded by SMS messages. In this case, messages which cannot be delivered on the first attempt are usually queued up on the MNO SMSC for further delivery attempts. In the worst case, the mobile network could take hours to deliver all queued warning messages.

[20] Page 14 of version 3.0 published 30.09.2019.

In the experience of the respondents to the BEREC questionnaires the time to deliver messages is highly dependent on the size of the targeted area and the number of end-users within (Portugal); on mobile network load (Romania) or number of devices targeted (BE-Alert); if it is a rural or urban environment (Sweden) regarding the number of base stations (SOS Alarm), and is also depending if prioritisation mechanism are in place in case of vast area incident (Bulgaria).

Regarding the time to deliver the warning messages, Portugal reported that its experience from 2018 showed that it took around one hour to reach 80%-90% for 300k people or 40%-50% for 1M of the recipients. Bulgaria considers real time tests are needed to determine scalability. Poland reported it takes from a few minutes to a few hours.

Competent authorities should work closely with MNOs to establish which volume of LB-SMS messages can be carried in the desired time interval in order to identify whether LB-SMS performs sufficiently well in regard to the purpose foreseen for the ECS-PWS. It is recommended that load testing or a simulation is undertaken of a high volume of warning messages, and the behaviour of SMS retried delivery attempts.

3.2.3. Overview of 110(1) performance

Where possible the following table summarises the results from sections 3.2.1 and 3.2.2 for the assessed sub-criteria. As mentioned in the introduction to section 3.2 BEREC's assessment should be supplemented by competent authorities' considerations of specific national circumstances and also having regard to the purpose and objectives of their envisioned ECS-PWS.

Column 1 in the following table sets out a list of the relevant sub-criteria taken from section 3.1.

Columns 2 and 3 summarise BEREC's initial assessment of the performance of CB-PWS and LB-SMS systems for each sub-criterion, using the notations "++", "+" and "-", as an illustrative measure of performance levels. BEREC denotes a highly effective performance using the "++" icon, and lower levels of performance using "+" and "-" icons respectively. Please note that the purpose of the table is to outline potential high-level differences between systems. BEREC does not consider it appropriate to attach numerical values or to assign a score to the performance of systems as that approach would be highly subjective. Further the EECC does not require BEREC to set out metrics to quantify differences between PWS' but only asks for the distinction whether a system performs better, worse than or as well as another system, without the need to quantify the level of diverging performance. Thus, the actual reasoning for the competent authorities' assessment should to be provided similarly to the description in sections 3.2.1 and 3.2.2.

Column 4 provides a brief explanation for the performance values awarded in columns 2 and 3, taken from the previous sections. Where necessary it should be amended according to the competent authority's assessment in those sections.

1. Sub-criteria	***2. CB (EU-ALERT)***	***3. LB-SMS***	***4. Explanation***
Coverage			
Geo. Coverage	*To be assessed by*	*To be assessed by*	

1. Sub-criteria	2. CB (EU-ALERT)	3. LB-SMS	4. Explanation
	competent authorities	*competent authorities*	
Pop. Coverage	*To be assessed by competent authorities*	*To be assessed by competent authorities*	
Capacity to reach end-users			
Support of inbound roamers	++ To be amended by competent authorities where necessary	*To be assessed by competent authorities*	
Supported devices	+ To be amended by competent authorities where necessary	++ To be amended by competent authorities where necessary	In general, both systems are supported by all mobile devices from mobile phone to smartphone. However, in the case of CB not all devices support the functionality as per default. Therefore, MNOs or even Member States might have to intervene at the manufacturer level in order to enable CB support.
Supported languages	++ To be amended by competent authorities where necessary	+ To be amended by competent authorities where necessary	Both systems allow sending of warning messages in different languages. CB with the EU-ALERT standard even automatically displays the correct language when receiving a warning message in several languages.
Managing longer messages	+ To be amended by competent authorities where necessary	+ To be amended by competent authorities where necessary	Even though LB-SMS outperforms CB in this regard as longer messages are possible, both systems need to concatenate several messages once a certain length is reached. Therefore, there is a risk of receiving the messages in the wrong order or missing parts of messages.
No human interaction needed	+ To be amended by competent authorities	++ To be amended by competent authorities	In order to receive a standard LB-SMS warning message no specific human action is needed apart from turning on the mobile device. This is why LB-SMS excels at fulfilling this sub-criterion. In the case of CB, depending on national regulation or on the standards set by manufacturers for the specific country, human

1. Sub-criteria	2. CB (EU-ALERT)	3. LB-SMS	4. Explanation
	where necessary	where necessary	interaction may be needed to receive all CB warning messages. This is why CB only fulfils this sub-criterion.
Disabled end-users	- To be amended by competent authorities where necessary	- To be amended by competent authorities where necessary	There is no system-inherent support of disabled end-users for either system. Both systems are dependent on the end-user's device's capabilities in order to support disabled end-users.
Reliability	++ To be amended by competent authorities where necessary	+ To be amended by competent authorities where necessary	CB is a more robust technical solution than LB-SMS as it uses less complex components and utilises the minimum network capacity when sending warning messages; Whereas LB-SMS requires the operation of an MLC to track the locations of users in the areas of concern and then requires the network to carry each message individually. The risks introduced by his additional complexity for LB-SMS are somewhat mitigated by the level of attention operators generally pay to stability of the SMS service.
Geo. Targeting	+/++ To be amended by competent authorities where necessary	+ To be amended by competent authorities where necessary	Under normal circumstances both 110(1)-PWS' have a maximum geographical targeting value of a single cell, although both CB (via DBGF) and LB-SMS (via the use of an MLC) offer enhancements which improve on this. Depending on the cell size the actual geographical granularity may vary, which should be considered when comparing to an IAS-PWS. Where DBGF is available for CB BEREC considers its granularity ++.
Scalability	++ To be amended by competent authorities where necessary	To be assessed by competent authorities	

\- = does not fulfil sub-criterion

\+ = fulfils sub-criterion

++ = excels at fulfilling the sub-criterion

Table 3

3.3. Assessing the equivalence of the effectiveness of IAS-PWS

As a first step in the assessment of the actual IAS-PWS, BEREC proposes that competent authorities should analyse the performance of the envisioned IAS-PWS using the set of criteria & sub-criteria from section 3.1. In the following section 3.3.1 BEREC has provided several points to note for competent authorities in their assessment of IAS-PWS performance.

In a second step BEREC proposes comparing the overall performance of the envisioned IAS-PWS with the performance of the hypothetical 110(1)-PWS serving as benchmark (see section 3.3.2.1). Additionally, competent authorities may want to take into account further considerations in their assessment that have an impact on the overall effectiveness of an ECS-PWS. BEREC has listed these in section 3.3.2.2.

3.3.1. Analysing IAS-PWS performance

In this section some points of note are set out to assist competent authorities in defining IAS-PWS requirements and assessing performance with regard to each sub-criterion.

Article 110(2) EECC requires that "*Public warnings shall be easy for end-users to receive".* Recital 294 explains what is meant by "*easy for end-users to receive"* when it states that "w*here a public warning system relies on an application, it should not require end-users to log in or register with the authorities or the application provider*". In other words, when rolling-out an IAS-PWS Member States need to ensure that an end-user can receive warning messages after installing the application on his device without further need for registration or log-in.

The implementation of IAS-PWS may also differ depending on

- the system developer/manufacturer and
- the needs according to the circumstances of a specific geographical region and requirements of a specific Member State with regard to the use-case of the envisioned IAS-PWS.

Therefore, it is not appropriate for BEREC to include a baseline performance analysis. However, there are some general potential merits of IAS-PWS', for example: their display capabilities (e.g. text, pictures, sounds, receiving warnings on other than mobile devices etc.), having no fixed limit to message lengths, specific features that can be included to assist disabled end-users and the possibility of subscribing to an area of interest. Also, both CB and LB-SMS excel at being robust solutions, but some may argue that IAS-PWS are even more robust because they do not rely solely on mobile networks and have WIFI hotspots as an alternative data path.

The following sub-sections provide further sub-criteria-specific points of note:

3.3.1.1. Coverage

A device using an IAS-PWS will be within coverage as long as a data connection exists to enable the communication with the IAS application server, as mentioned in section 2.3.2. Apart from the mobile Internet access service IAS-PWS' benefit from additional WIFI Internet access where available which may increase geographical as well as population coverage.

To assess mobile network coverage for data services it is advised that competent authorities contact MNOs keeping in mind that it may differ from SMS and CB coverage.

It should also be noted that unlike receiving an SMS or a CB message, the mobile internet access service is generally charged-for by MNOs, although a zero-rating mechanism for traffic related to PWS warnings could be implemented. In the situation where a user's data bundle is exhausted, different MNOs handle this in different ways, ranging from the throttling of internet traffic to entirely blocking it. In the latter case end-users will not

receive warning messages unless a suitable zero-rating mechanism is in place, or the device is connected via WiFi.

3.3.1.2. Support of inbound roamers

Although IAS-PWS will work exactly the same way on every device end-users need to take action to enable it. Competent authorities should raise the awareness of the available IAS-PWS to end-users only visiting temporarily. One possibility is to make use of the welcome SMS service capabilities available in most MNOs as described in recital 294 EECC. BEREC considers this to be the minimum functionality that should be ensured by IAS-PWS'.

A potential challenge of notifying inbound roamers by welcome SMS is that many welcome SMS implementations focus on sending messages from the home network (HPLMN) to the roaming user, although the reverse scenario of the visited network (VPLMN) sending welcome SMS messages to roamers as they arrive is also possible and commonly implemented. Therefore, a competent authority wishing use welcome SMS to notify inbound roamers of the existence of an IAS-PWS should investigate whether the VPLMN approach is possible, or request that the home MNOs of the inbound roamers customise the message sent to their customer.

It should also be noted that, in most cases, mobile Internet access relies on an architecture in which data traffic is always routed through the home MNO to reach the Internet. This means that the OTT application server will need to reach IP addresses from foreign countries and cope with the additional communication latency.

3.3.1.3. Supported devices

On-device applications may have two versions, one for Apple and another for Android handsets, (this version must take into account different android versions and processor architectures). These two mobile operating systems together make up over 98% of the smartphone market. It is nevertheless relevant to assess the number of feature phones in use that do not support on-device applications and cannot receive warning messages.

It is also possible to have IAS-PWS applications running on other devices such as Apple and Android tablets and smart TVs and PCs that have the app installed on them.

3.3.1.4. Supported languages

Apart from having warning messages transmitted in multiple languages, something that can be easily accomplished, the whole on-device application (e.g. the menus and settings) could also be developed to be used by visiting end-users in their preferred language.

The warning message display language may be automatically selected by the operating system of the device, mirroring the operating system's language settings.

3.3.1.5. Steps required for recipient to enable receiving warning messages

Although an easily accomplished task for most end-users, the use of IAS-PWS requires downloading and installing an application and granting the necessary permissions (e.g. enable GPS location). Competent authorities should consider how best to maximise the number of end-users that install the on-device application e.g. by raising end-users' awareness on the benefits of having an ECS-PWS available to them.

Competent authorities must be aware that the EECC forbids a necessary registration or log-in, meaning that after the download of the application the default settings should enable receiving warning messages that target the end-user's current location.

The currently deployed IAS-PWS' come equipped with diverging settings in this regard. In Austria, Germany, Portugal and some regions of Spain the IAS-PWS is pre-configured in a way that warnings for the current location can be received after the installation if GPS is activated. In Austria, Germany and Poland additional features can be activated e.g. by entering specific locations the end-user wishes to monitor or filters for specific warning types. Current systems in other countries need further configuration in order to receive warnings (Finland).

3.3.1.6. Accessibility for end-users with disabilities

IAS-PWS could introduce innovation regarding the accessibility for disabled end-users (e.g. visually impaired end-users). Where CB and LB-SMS are dependent on the functionality of the end-users mobile device (e.g. its text-to speed capability) application providers could add improved text-to-speech capabilities or additional features programmable into an app if demanded by the competent authority.

3.3.1.7. Geographical targeting

As mentioned in section 2.3.2, there are several options as how the IAS-PWS might target the end-users in a specific location. The adopted solution will have direct impact on the system's scalability.

With regard to end-users entering a hazardous area after the initial warning message has been issued an IAS-PWS may contain a feature that ensures the mobile device displays the warning message once the end-user enters the affected area. Such a feature is currently under construction for the German IAS-PWS and will be implemented in the near future. Thus, BEREC encourages competent authorities to pursue the implementation of such a feature in case they consider rolling-out an IAS-PWS.

Competent Authorities should also consider that end-users could effectively turn off one of the main functionalities of their IAS-PWS by not allowing geo-location in the device's settings. To avoid unintended non-use of the geo-location feature BEREC encourages competent authorities to ensure end-users are made aware during the installation process that the IAS-PWS can only provide full functionality if the application is granted access to the geo-localisation feature of the device.

3.3.1.8. Scalability

Triggering the IAS-PWS application usually involves sending data packets containing the warning message to be displayed to each end-user individually. Additional information might also be sent (e.g. target geographic area, type of warning, validity of the message, etc.) to allow some remote control of the on-device application.

Although data volumes are relatively low, the OTT application server and underlying transport network must be able to cope with a very high number of connections especially if it is designed to send warning messages to all attached devices, irrespective of their current location. This corresponds to "Option 1" described under section 2.3.2 in which it is the device that decides whether or not to display the warning message depending on its location.

3.3.2. Comparing IAS-PWS performance with 110(1)-PWS performance

3.3.2.1. Comparison with regard to the criteria mentioned in the EECC

When the EECC states in article 110(2) that the effectiveness of 110(2)-PWS needs to be "*equivalent in terms of coverage and capacity to reach end-users*" it clearly implies, that the effectiveness of a system falling under

article 110(1) is the benchmark the 110(2)-PWS needs to be assessed against. Thus, an IAS-PWS only needs to perform as well as the one of the two 110(1)-PWS alternatives.

For the overall assessment BEREC proposes that competent authorities take the outcomes from sections 3.2 which shall be aggregated in Table 3 and compare them with the assessed performance of their envisioned IAS-PWS based on section 3.3.1 (benchmark). BEREC considers that to "greenlight" an IAS-PWS it is necessary that, it performs overall at least as well as the one of the 110(1)-PWS with regard to coverage and capacity to reach end-users.

BEREC also considers that "greenlighting" is possible even if, for several sub-criteria, the IAS-PWS' performance is behind the benchmark-110(1)-PWS, as long this is compensated by an outperformance by a sufficient extent, or in a sufficient amount of other sub-criteria under the same main-criterion (coverage or capacity to reach end-users). For example, a superior performance with regard to "support of disabled end-users" could offset an inferior performance regarding "supported languages" but not with regard to "geographical coverage" as the latter falls under another main-criterion (coverage). With regard to offsetting inferior performances with superior performances BEREC considers that competent authorities should highlight the underlying considerations very clearly, explaining in detail why they consider the particular compensation appropriate for their national circumstances and ECS-PWS use-case. BEREC recognises the fact that it is impossible to quantify any comparison of sub-criteria in this case. However, on a case-by-case basis it can be argued why the superior performance regarding one sub-criterion may offset the inferior performance of another sub-criterion. Otherwise an IAS-PWS which outperforms a 110(1)-PWS in all, but one sub-criterion could not be rolled-out even though it would be more effective in the overall view. Such an outcome would contradict the aim of article 110.

Importantly, with regard to the main-criteria the EECC explicitly states that the IAS-PWS needs to be equally efficient regarding the main-criteria. Therefore, a superior performance of "capacity to reach end-users" cannot offset an inferior performance of "coverage".

BEREC considers competent authorities could also take into account using another line of reasoning, hand in hand with the concept of offsetting an inferior performance regarding one sub-criterion of an IAS-PWS with a superior performance regarding another sub-criterion. Competent authorities may also want to highlight certain sub-criteria as particularly relevant, giving them more weight in their overall assessment. Such a weighting should always be linked with either the particular purpose of an envisioned IAS-PWS or with particular national circumstances.

Some examples:

- A Member State that wants to roll-out an ECS-PWS for a specific mass event (e.g. the Olympic Games in a city) and wants it to be as timely and accurate as possible with regard to geographical targeting in order to be able to evacuate concerned end-users in groups to avoid a mass panics. In this situation, due to the increased presence of end-users in relatively small areas, the Member State should be able to give the sub-criteria of "geographical targeting" and "scalability" more weight in its assessment consequently ranking them very high on its requirements list for the envisioned ECS-PWS.
- A Member State with a very reliable mobile network which all ECS-PWS would effectively use would most likely not focus as much on "reliability" but could instead focus on other sub-criteria more relevant to it.

BEREC considers that Member States should use the weighting option in particular when explaining why they intend to offset an inferior performance regarding one sub-criterion of an IAS-PWS with a superior performance regarding another sub-criterion.

BEREC stresses that according to its interpretation of the EECC, main-criteria cannot be weighted higher or lower because the EECC does not differentiate regarding the importance of either "coverage" or "capacity to

reach end-users". In the same vein BEREC considers that "support of inbound roamers" should be considered as one of the most important sub-criteria by the competent authorities as it is the only sub-criterion which is explicitly mentioned by the EECC. Consequently BEREC considers less than minimum performance of this sub-criterion as described in section 3.3.1.2 could not be offset by the superior performance of another sub-criterion.

3.3.2.2. Comparison with regard to further considerations in line with the aim of article 110 EECC

Even though the following "best effort functionalities" cannot be derived from the actual wording of the EECC BEREC considers them being in line with the aim of article 110 as they contribute to creating more effective ECS-PWS'. Competent authorities could consider them in relation to their specific system.

Display capabilities

A competent authority might wish to include more than plain text in the warning messages. This could include text formatting, pictograms (or Emoji) and/or images. The use of pictograms or extended character sets could make the message more universally understood, and also quicker to understand but could result in fewer characters being available in the message, depending on the ECS-PWS used.

Cell Broadcast

CB distributes text only warning messages (as mentioned by The Netherlands, Romania, Greece, Croatia, Italy and Turkey). It is mobile device dependent if this text can be displayed in another font (larger characters or higher contrast) or could be played out as a voice message if the device supports this. CB does not currently support the inclusion of Emoji or multimedia content such as pictures. Nonetheless, some Member States (The Netherlands and Norway) are studying the possibility of adding multimedia support to the system by including URLs in the broadcasted message.

CB messages generally result in an audible notification from the recipient mobile device, which is different to an incoming SMS, making the warning message recognisable as an important warning.

LB-SMS

By default, LB-SMS messages are composed of text only. It is possible for some receiving devices to display Emoji glyphs, but this cannot be relied upon. LB-SMS warning messages will not produce notifications sounds or a ringtone different than an ordinary SMS message (referred by Slovenia as a limitation), thus end users could easily overlook warning messages. The sender of the warning message has the possibility of sending "Class 0" SMS messages[21] which will appear on the end user's device without any human interaction, however it should be noted that these are not stored on the mobile device and could be accidentally missed.

IAS-PWS

IAS-PWS on the other hand can be set-up to display all sorts of pictures or pictograms.

Authenticity (Can messages be faked? How easily?)

In order to ensure public trust in the integrity of ECS-PWS messages, all reasonable steps should be taken to prevent fake messages from being sent, or genuine ECS-PWS message being tampered with. This need goes beyond simply restricting access to, or otherwise securing the alerting gateway.

[21] See 3GPP TS 23.038 section 4 for more information

All IT systems could be subjected to attacks by hackers, or compromised by malware, and network operators should put in place steps to prevent unauthorised access to their network.

Beyond the normal IT security questions, the underlying ECS-PWS delivery mechanism should be considered. In general, delivery mechanisms based only on the control plane (SMS, CB) use more obscure protocols, are considered to be 'deeper' in the network, and therefore protected by more layers of security; whereas delivery mechanisms which are based on the user plane (e.g. IAS services) are more easily reached from the internet, based on commonly used protocols and therefore more difficult to secure.

In addition, the possibility of advanced attackers using specialist equipment to emulate a network cell thereby acting as a man-in-the-middle, should also be considered.

The above are only general statements, and given the importance and complexity of this functionality, BEREC recommends a specialist security review to support the assessment of this functionality.

Cell Broadcast

Regarding the authenticity of CB warning messages, the following additional information should be considered: Only authorized and authenticated warning message originators should have access to the alerting gateway or CBC and both need to be sufficiently protected against hacking attempts.

It should be noted that there have been some reports of vulnerabilities in the LTE/4G signalling protocols which could allow a determined attacker to create a fake eNodeB which could be used to send fake warning messages to end users within the limited range that device. In this context the number of end users within range of the attacker's fake eNB would be relatively small thereby limiting the number of victims. MNOs should assess the scale of this risk and consider mitigation strategies if appropriate.

LB-SMS

Regarding the authenticity of LB-SMS messages the following additional information should be noted: Given the wide availability of commercial SMS gateways on the internet which allow the user to set an arbitrary source Mobile Subscriber ISDN Number (MSISDN), it would be straightforward for an unauthorised 3rd party to create SMS messages which appear to come from a LB-SMS PWS. These messages will appear to come from a different "service centre" if the receiving device displays this information[22], although the average user is unlikely to check this.

It's also the case that the underlying SS7 protocols used to deliver SMS messages into other networks have some weaknesses which could enable a skilled hacker to generate fake warning messages which would be indistinguishable from genuine warning messages on the device.

The above risks can be mitigated by MNOs that install security devices (e.g. an "SMS Firewall") at their interconnection signalling links, to inspect incoming traffic and reject malformed or messages with an inauthentic service centre address etc.

In the responses to the BEREC survey PL made particular reference to the threat of inauthentic LB-SMS based alerts being sent to end users.

[22] In age of the smartphone, the originating service centre information is not available as it was in the pre-smartphone era. iOS devices, for example provide no visibility of this information.

IAS-PWS

With regard to IAS-PWS implementations it should be ensured they should include cryptographic signatures to verify the identity of the message originator and ensure no modification has occurred to warning messages.

Support of absent residents or users subscribing to an area of interest

This functionality can be considered as having two parts – (1) support for absent residents and (2) support for users subscribing to an area of interest. In this scenario, the ECS-PWS would send warning messages to users that are (temporarily or otherwise) *outside* the area pertaining to a warning message.

Absent residents

> An example of such use case would be an individual wishing to receive warnings related to their home area, while they are at their place of work.

Residents subscribing to an area of interest

> An example for this case would be a parent wishing to receive warnings relating to their child's school.

In the event that a competent authority opts to include these two features, consideration should be given for how these messages will look (e.g. *how will the recipient know that the message does not apply to their current location?* Or *will a given warning message need to be written for two audiences, the end users both within and outside the area of concern?*), and how to facilitate registration of users to enable them to 'subscribe' to receiving warning messages for a given area irrespective of their location.

Cell Broadcast

Absent residents, or residents subscribing to an area of interest are not supported as the CB message is only sent to recipients in the relevant area (confirmed by Netherlands & Romania).

LB-SMS

The same applies to LB-SMS (confirmed by Poland and Sweden). Austria, Belgium, Denmark and Romania have supplemented their LB-SMS PWS with an opt-in functionality to receive an alerting SMS even if outside of the area. Gedicom explains that people can register several addresses in the online subscription form, which permit subscribers to receive the alert when they are outside a regional warning area (concerning their family for example). This is however not a standard for LB-SMS.

IAS-PWS

For IAS-PWS this is a common feature, as warnings for predefined locations can be received from anywhere as long as there is an internet connection (e.g. Austria, Denmark, Germany and Poland).

Annex 1

1. Report on the data basis used for the Guidelines

a. Questionnaires to NRAs

On 11th February 2019, BEREC issued a general questionnaire requesting relevant input by 1st March 2019 from the authorities competent for ECS-PWS in the Member States. The answers to this general questionnaire provide an important insight into the situation and future plans from each Member State which responded. Totally BEREC received a total of 28 replies, of which 25 were from EU Member States (Austria, Belgium, Bulgaria, Cyprus, Czechia, Germany, Denmark, Estonia, Spain (replies from 10 different institutions), Finland, France, Greece, Croatia, Hungary, Ireland, Italy, Latvia, Malta, Netherlands, Poland, Portugal, Romania, Sweden, Slovenia, and Slovakia) and three from non-EU Members States (Norway, Serbia, and Turkey).

At the same time BEREC issued a detailed questionnaire requesting in depth input by 18 April, 2019 from the competent authorities in the Member States to be used for drafting these guidelines. To this detailed questionnaire BEREC received 24 replies, of which 22 from EU Members States (Austria, Belgium, Bulgaria, Cyprus, Czechia, Germany, Denmark, Spain (replies from 4 different institutions), Finland, Greece, Croatia, Hungary, Ireland, Italy, Malta, Netherlands, Poland, Portugal, Romania, Sweden, Slovenia, and Slovakia) and two were from non-EU Members States (Norway and Turkey).

b. Call for input

In order to collect stakeholders' input on the design and capabilities of existing public warning systems on the market, BEREC WNE WG on 19th June 2019 launched an early general call for inputs asking stakeholders to describe the capabilities of existing systems. In total BEREC received 14 contributions (ETSI SC EMTEL, RO - ALERT, BE ALERT, KATWARN, SOS ALARM, Ericsson AB & Mobilaris NS AB, General Directorate of Fire Rescue Service of the Czech Republic, Directorate "National 112 system"- Ministry of Interior of Bulgaria, The Special Telecommunications Service Romania, GEDICOM, Google LLC, Apple, UMS, and PSC Europe) representing different aspects and types of ECS-PWS solutions:

- Cell broadcast based solutions (ETSI SC EMTEL, RO–ALERT, The Special Telecommunications Service Romania, and Apple); and
- SMS based solutions (BE ALERT, KATWARN, SOS ALARM, Ericsson AB & Mobilaris NS AB, General Directorate of Fire Rescue Service of the Czech Republic, Directorate "National 112 system"- Ministry of Interior of Bulgaria, GEDICOM, Google LLC, UMS, and PSC Europe).

For example, Ericsson provides mobile positioning system using Mobilaris products (application server with CIWS: Civil Information Warning System). GEDICOM has described a platform for public warnings similar to the alerting gateway as described in section 2.2.1.

2. General overview of ECS-PWS status quo in EU MS

With regard to the answers to the general questionnaire the following conclusions can be drawn:

Nearly all respondents have implemented some sort of legacy-PWS in their Member State.

Out of the 24 respondents nine have already rolled-out an ECS-PWS covering the whole country. Out of those, one Member State uses stand-alone 110(1)-PWS' (The Netherlands using CB), two Member States use stand-alone 110(2)-PWS' (Germany and Finland using IAS-PWS) and six Member States have rolled out a combination of 110(1) and 110(2)-PWS' (Austria, Denmark, Poland and Portugal are using IAS-PWS and LB-SMS, Romania is using CB and IAS-PWS, but Sweden is using LB-SMS, AVC and IAS-PWS). For the latter cases these Member States often use their IAS-PWS' to supplement their existing 110(1)-PWS', e.g. to receive

national warning messages even when abroad (Poland) or to relay important public announcements (Sweden). Denmark on the other hand uses its SMS-based 110(1)-PWS to supplement its IAS-PWS.

The use cases for which the systems which are already rolled out are deployed differ greatly among Member States. E.g. in Denmark their SMS-based System is limited to messages from the national police to hearing-impaired subscribers. The IAS-PWS in Germany and Denmark on the other hand can be downloaded by anyone and deliver warning messages for multiple purposes.

Only in two Member States (Bulgaria and some regions of Spain) the functions of this system include sending of automated voice messages. For instance, in Spain automated voice calls are sent to citizens in need of specific assistance that have previously registered for the service.

Seven respondents (Cyprus, France, Ireland, Serbia, Slovakia, Slovenia, Norway) have not yet finished their assessment on what kind of system to roll-out, with the remaining respondents currently preparing their own deployments. Five Member States (Czechia, Estonia, Croatia, Greece, and Malta) are planning to introduce a 110(1)-PWS and one is preparing the roll-out of a 110(2)-PWS (Cyprus). Turkey plans to roll out several systems in parallel (110(1) & 110(2)-PWS') and in Spain each region has its own plan regarding the implementation of an ECS-PWS.

The respondents provided a wide range of answers to the question about their expectation of the cases in which the future ECS-PWS should be used, in their opinion. The most common scenarios were natural disasters, terrorist attacks, accidents in industrial complexes with hazardous emissions and war. These could be categorized as threats for health, life or property of citizens.

Annex 2

List of Acronyms

Acronym	Definition
3GPP	3rd Generation Partnership Project
AVC	Automatic Voice Calling
BEREC	The Body of European Regulators for Electronic Communications
BTS	Base Transceiver Station
CB	Cell Broadcast
CBC	Cell Broadcast Centre
CIWS	Civil Information Warning System
CMAS	Commercial Mobile Alert System
DB	Database
DBGF	Device Based Geo-Fencing
ECS	Electronic Communication Services
EECC	European Electronic Communications Code
EENA	European Emergency Number Association
EMTEL	Emergency Communications
ETSI	European Telecommunications Standards Institute
EU	European Union
FCC	Federal Communications Commission
GPS	Global Positioning System
GSM	Global System for Mobile communications
HPLMN	Home Public Land Mobile Network
IAS	Internet Access Service
iOS	iPhone Operational System
IP	Internet Protocol
ISDN	Integrated Services Digital Network

Acronym	Definition
IVR	Interactive Voice Response
LB-SMS	Location based SMS
MCC	Mobile Country Code
MLC	Mobile Location Centre
MMI	Man Machine Interface
MNO	Mobile Network operator
MS	Member State
MSISDN	Mobile Subscriber ISDN Number
NB ICS	Number Based Interpersonal Communications Service
NRA	National Regulatory Authority
OTT	Over The Top
PSAP	Public Safety Answering Point
PWS	Public Warning System
SMS	Short Messaging Service
SMSC	Short Messaging Service Centre
TBD	To Be Decided
VPLMN	Visitor Public Land Mobile Network
WEA	Wireless Emergency Alert
WG	Working Group
WIFI	Family of radio technologies commonly used for wireless local area networking (WLAN) of devices
WNE	Wireless Network Evolution

Annex 3

Article 110 - Public warning system

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, taking utmost account of BEREC guidelines. Public warnings shall be easy for end-users to receive.

By 21 June 2020, and after consulting the authorities in charge of PSAPs, BEREC shall publish guidelines on how to assess whether the effectiveness of public warning systems under this paragraph is equivalent to the effectiveness of those under paragraph 1.