Body of European Regulators
for Electronic Communications
BEREC

BoR (20) 115

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

12 June, 2020

Contents

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 whether the effectiveness of alternative Public Warning Systems (hereinafter PWS) using means of electronic communications services (hereinafter ECS-PWS) as described in Article 110(2) is equivalent to the effectiveness of ECS-PWS falling under Article 110(1).

The methodology set out by BEREC in these Guidelines would only apply to Member States which intend to deploy ECS-PWS according to Article 110(2) EECC (hereinafter 110(2)-PWS). In such case, the methodology set out by BEREC suggests that competent authorities establish a performance benchmark on the basis of a hypothetical ECS-PWS that meets the requirements of Article 110(1) EECC (hereinafter 110(1)-PWS). The envisaged 110(2)-PWS will then have to be assessed against the benchmark so established.

BEREC's methodology is based on a qualitative assessment of factors defining coverage and affecting the ability to reach concerned end-users. BEREC proposes that competent authorities step through the methodology in order to assess the equivalence of effectiveness of the envisaged 110(2)-PWS against the benchmark 110(1)-PWS as follows:

- Preliminary step (identifying suitable hypothetical benchmark systems): The competent authority identifies at least one hypothetical 110(1)-PWS that would comply with the legal requirements of Article 110(1) EECC
- Step 1 (benchmark creation): The competent authority assesses the performance of the hypothetical 110(1)-PWS' identified at the preliminary step in terms of coverage and capacity to reach concerned end-users
- Step 2 (110(2)-PWS assessment): The competent authority assesses the performance of the envisaged 110(2)-PWS in terms of coverage and capacity to reach concerned end-users, and
- Step 3 (equivalence assessment): The competent authority compares the performance of the envisaged 110(2)-PWS with the benchmark (i.e. the performance of the hypothetical 110(1)-PWS from step 1)

BEREC considers that this three step approach can be easily replicated in each Member State allowing competent authorities to objectively assess the equivalence of effectiveness of envisaged 110(2)-PWS and help them in their decision making processes.

This approach ensures that competent authorities 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.

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

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.[2] 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). For example, Member States reported that in the next two years they are considering to deploy various public warning systems: location based SMS (in 8 Member States), Cell Broadcast (in 7 Member States) or Mobile Application (in 1 Member State). Currently the technologies deployed are: sirens in 16 Member States; TV, radio or social media alerts in 14 Member States; specific applications in 5 Member States; LB SMS alert in 6 Member States and Cell Broadcast in 4 Member States.

Also, NRAs are often not the competent authorities in relation to implementing PWS and in many cases there are multiple stakeholders involved like ministries and public safety authorities. Hence the evaluation of ECS-PWS effectiveness according to these Guidelines should be carried out by the relevant competent authorities in each Member State. Which authority is competent depends on the respective national law.

1.2. Purpose of the Guidelines

According to Article 110(2) subparagraph 2 EECC, by 21 June 2020, 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 ECS-PWS' envisaged under paragraph 1 (hereinafter – 110(1)-PWS). BEREC considers that typical 110(1)-PWS are systems that are embedded in the mobile network functionalities (e.g. cell broadcast and/or location based SMS) provided that they are in compliance with prerequisites of Article 110(1) discussed in more detail below. BEREC considers that 110(2)-PWS are systems which are not embedded in the mobile network functionalities (e.g. over the top applications).

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 in case they do not deploy a 110(1)-PWS. 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 21 June 2022, it will be the European Commission's task to assess Member States' compliance with Article 110 EECC where Member States have rolled out a stand-alone 110(2)-PWS. BEREC considers 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.

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

1.3. Structure of this document

The document has the following structure:

- Chapter 2 sets out 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 BEREC's methodology, which is essentially a guideline of steps on how competent authorities could conduct an assessment of the equivalence of effectiveness of ECS-PWS'.
- Chapter 4 describes the criteria derived from the EECC which are coverage and capacity to reach concerned end-users and provides for a set of factors representing aspects of either coverage or capacity to reach concerned end-users which BEREC considers to be non-exhaustive.
- Chapter 5 describes example initial analyses of the performance of 110(1)-PWS' (Cell Broadcast and Location-based SMS) and of IAS-PWS' using the factors described in Chapter 4.
- Chapter 6 provides general information for the consideration of competent authorities when assessing the envisaged IAS-PWS against the benchmark 110(1)-PWS.
- Chapter 7 describes additional functionalities competent authorities might want to consider implementing as well in order to make their ECS-PWS more effective. Also, these are not falling under the wording of Article 110 EECC and could thus not be considered in the equivalence assessment.
- The document is supported by the following annexes:
  - 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 and recitals 293 and 294.

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 significant differences regarding the effectiveness of ECS-PWS'. To counter such a development, Article 110(1) EECC prescribes a common level of minimum effectiveness: the performance of the ECS-PWS' fulfilling the legal requirements of Article 110(1).

Article 110(2) EECC provides a further means to reach the aim of Article 110(1) EECC, by allowing Member States to roll out alternative ECS-PWS as long as they are as effective in terms of coverage and capacity to reach end-users concerned as systems envisaged by Article 110(1) EECC.

This aims to ensure Member States' compliance with the envisioned level of minimum effectiveness of ECS-PWS'.

2.1.2. Obligations under Article 110(1) 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."* Recital 293 explains *that "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"*. Consequently Member States are under the obligation to set such functional requirements for their chosen ECS-PWS that ensure that the rolled-out ECS-PWS is able to send the public warnings in the targeted geographic areas potentially being affected by imminent or developing major emergencies during the warning period.

The EECC therefore considers a sufficient level of granularity of the geographical targeting capability of an ECS-PWS a legal requirement for the roll-out of any ECS-PWS. BEREC considers that the same applies to being able to warn concerned end-users of "imminent" emergencies, as also mentioned by recital 293. Thus requiring the Member States to roll out a system which is able to alert concerned end-users on short notice. Also, visiting end-users including inbound-roamers are explicitly mentioned by the EECC when stating in Article 110(2) EECC that end-users concerned include *"those only temporarily present in the area concerned"* and recital 294 specifies that *"end-users entering a Member State"* need to be informed *"of the existence of such a public warning system"*.

Because of the sentence *"when public warning systems [..] are in place"*, 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.

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 that complies with the legal requirements of Article 110(1). But, Article 110(2) provides an exemption from this rule, also accepting IAS-PWS instead provided their effectiveness is equivalent to an ECS-PWS complying with Article 110(1) EECC in terms of coverage and capacity to reach concerned end-users and the warnings are easy to receive.

Whether or not a Member State has to perform an update of its existing legacy or ECS-PWS is beyond the scope of the BEREC Guidelines.

Recital 293 of the EECC mentions that public warnings should be transmitted to “all” end-users concerned. BEREC observes that due to the risk for a control failure somewhere in a PWS system there may be practical reasons why this requirement may not be achievable / realisable for any ECS-PWS in every warning event in practice e.g. there might be another unplanned situational limitation such as temporary terrain shielding of signals due to cranes or other temporary obstructions in the vicinity of warning transmission or the end-user could be in a basement without reception or his device could be out of power. For the purpose of these Guidelines BEREC therefore understands recital 293 encourages Member States to ensure that ECS-PWS’ reach as many concerned end-users as technically possible.

2.1.3. The requirement of equivalence of 110(2)-PWS’ with 110(1)-PWS

Article 110(2) EECC sets out specific provisions allowing 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”.*

Once the obligation under Article 110 (1) is fulfilled (see section 2.1.2) the EECC does not require further prerequisites recognising the effectiveness of 110(1)-PWS’ as a benchmark for alerting the end-users concerned 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 does prescribe prerequisites because Member States have to assess these systems against the effectiveness of 110(1)-PWS’ (that fulfil the obligation of Article 110(1)), measuring their equivalence in terms of coverage and capacity to reach end-users concerned. An additional prerequisite is that 110(2)-PWS have to ensure that the public warning shall be easy for end-users to receive.

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.

BEREC notes that the EECC also does not forbid the roll-out of hybrid ECS-PWS consisting of any combination of 110(1)-PWS and/or 110(2)-PWS. BEREC encourages Member States to analyse whether such a combination would best fit their purpose and whether it has benefits over a stand-alone roll-out. However, for the purpose of these Guidelines BEREC needs to focus on the analysis of stand-alone roll-outs as Article 110(1) EECC considers them sufficient which makes them the benchmark for the analysis of 110(2)-PWS' equivalence of effectiveness.

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

2.2.1. Introduction

The following sections provide a general description of 110(1)-type-PWS that could potentially fulfil the requirements of Article 110(1), which are currently implemented in live deployments and which BEREC considers relevant for the purpose of these Guidelines. It is still up to the respective competent authorities to assess whether such systems would fulfil the requirements of Article 110(1) under the national circumstances. BEREC therefore stresses that it cannot assess whether the existing deployments of 110(1)-type-PWS fulfil the requirements of Article 110(1) EECC.

While it would be possible to deliver public warnings using other methods on an NB-ICS[3] (number-based interpersonal communications service as defined by Article 2(6) EECC), this document is not intended to describe every conceivable method.

When describing the different ECS-PWS', BEREC describes an example hypothetical deployment of these systems mentioning their standard functionalities at this point in time. BEREC does not make reference to a specific software generation or on-top functionalities that could be provided additionally e.g. by a combination of systems, even if they would be more effective. However, some additional functionalities associated with different ECS-PWS' are set out for information. Pursuant to Article 110 EECC rolling-out a stand-alone system is sufficient and therefore Member States need to be enabled to compare each system independently.

When competent authorities assess hypothetical 110(1)-PWS for the purpose of creating a benchmark for the assessment of the hypothetical IAS-PWS BEREC considers they should take into account the standard

[3] E.g. USSD Push

functionalities of the 110(1)-PWS' at the time of the assessment. These may by then have evolved from the standard functionalities as described in the following sections.

Finally, this document uses the term "alerting gateway" to refer to an entity which provides alerting functionality, potentially executing business logic for more advanced use cases. BEREC considers that an alerting gateway might simply provide an interface within the MNO to public authorities to submit warning messages, or there might be a national alerting gateway which is operated by or on behalf of the competent authority. There may be a single alerting gateway per MNO which interfaces with the relevant network equipment to deliver the ECS-PWS messages, or a member state might have a single alerting gateway which interfaces to all MNOs, or both.

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. A consequence of this is that the implementation of CB for the purpose of PWS is likely to require the deployment of a CBC (Cell Broadcast Centre) node in each MNO.

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[4]) 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 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 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.

[4] 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.

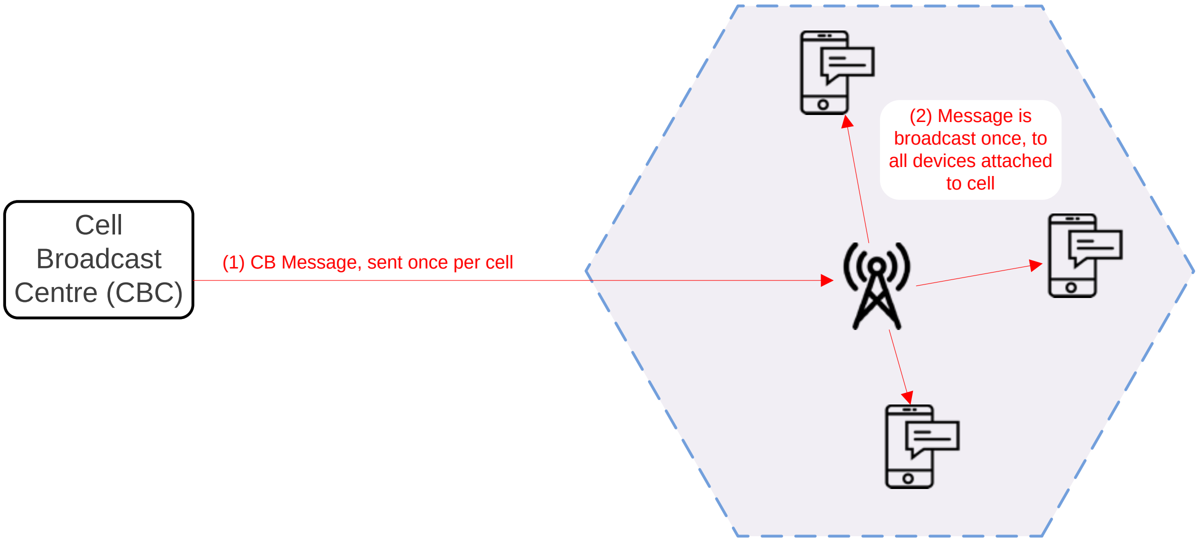

Cell Broadcast Centre (CBC)
(1) CB Message, sent once per cell
(2) Message is broadcast once, to all devices attached to cell

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[5] 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 step 1 of the methodology described in chapter 3.

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

[5] 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

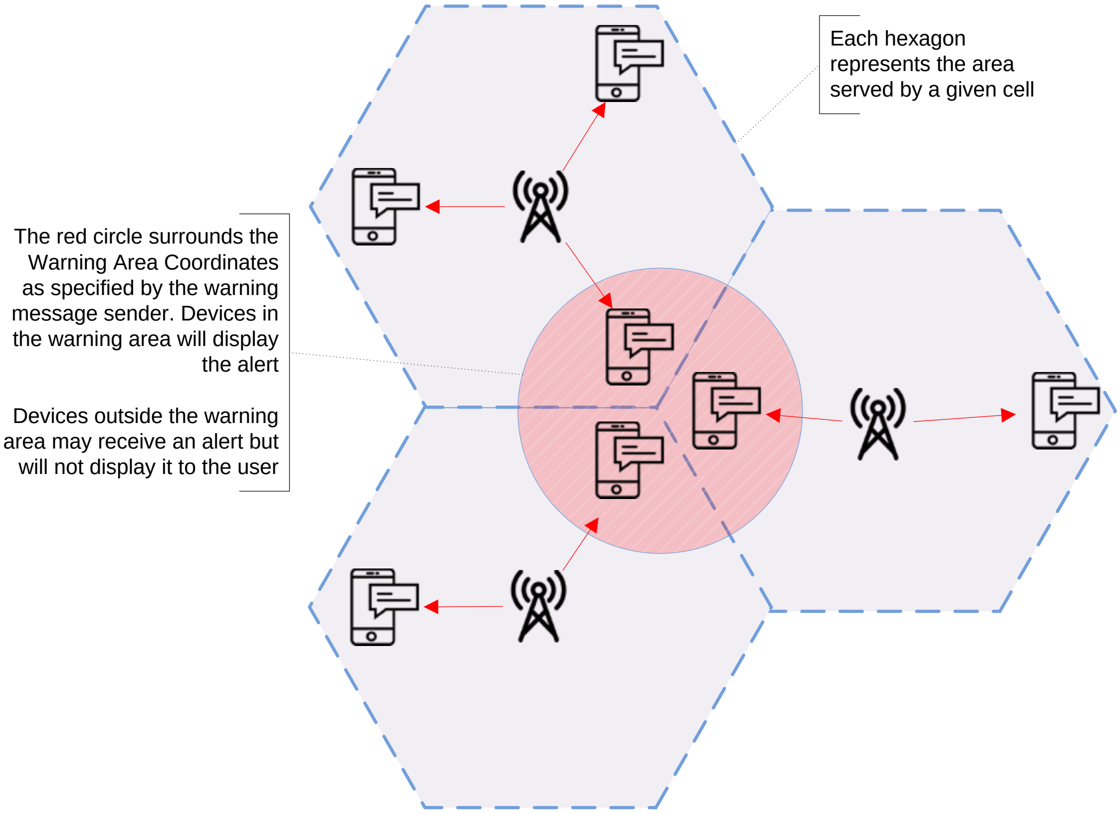

Each hexagon represents the area served by a given cell
The red circle surrounds the Warning Area Coordinates as specified by the warning message sender. Devices in the warning area will display the alert
Devices outside the warning area may receive an alert but will not display it to the user

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. Thus, the DGBF characteristic would allow to more accurately address only the end-users concerned as defined in recital 293 of the EECC.

2.2.3. Location Based SMS (LB-SMS)

As far as the network[6] 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 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[7].

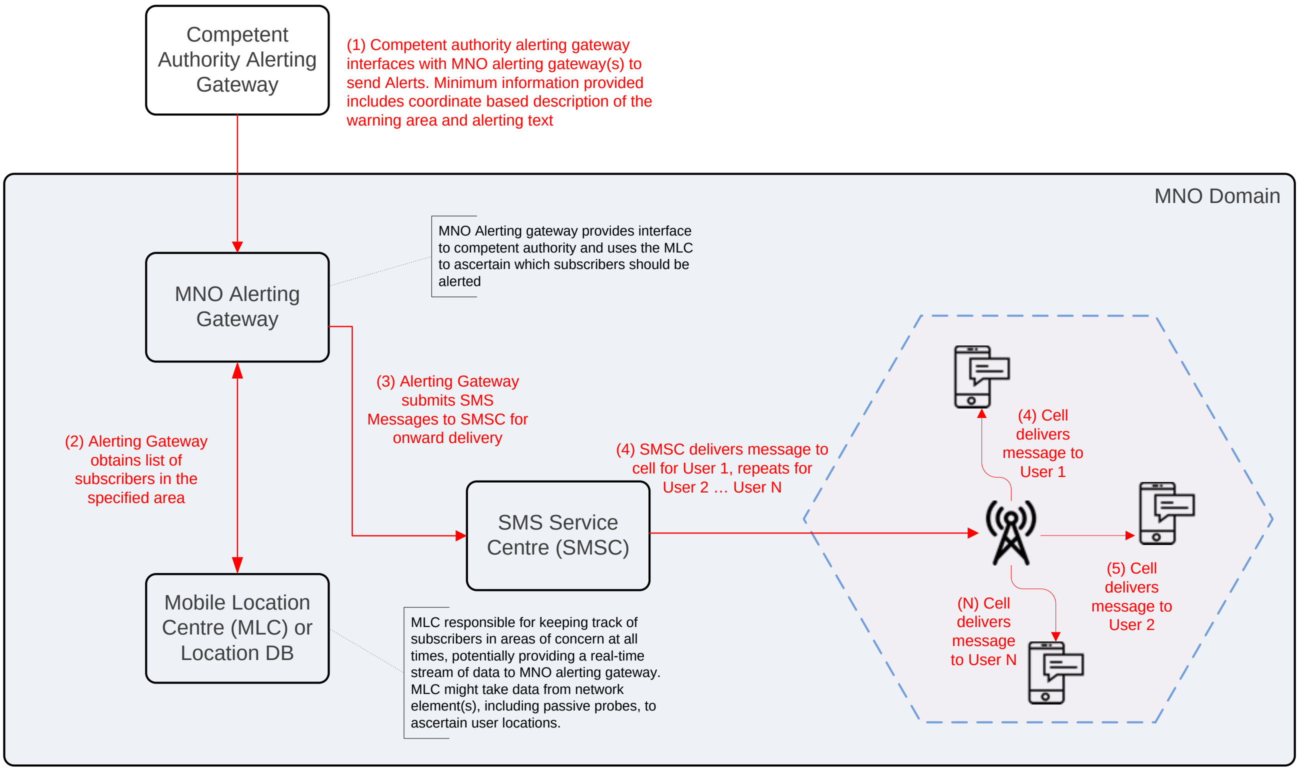
It should be noted that while mobile networks require knowledge of subscribers' locations for normal operation, this is usually not maintained at all times at the granularity of the single cell level. Therefore, an LB-SMS

[6] 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.

[7] The alternative to this approach, not recommended by BEREC, is to not maintain any list of subscribers and their current cell, but instead to retrieve the real-time location from the network (often via paging) to ascertain which subscribers are in a given cell. The time to execute any paging of a large number of users is likely to be significant, and could make such an approach inadequate for emergency usage.

implementation will usually require the deployment of a Location Database or an MLC (Mobile Location Centre). The methods used by the MLC to track mobile devices as they move around the network vary, and some are not standardised. As stated by some Member States (Portugal and Sweden) these location services are subject to a certain level of inaccuracy, because their functionality is based on many variables, including the location technology used and the network topology.. 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. It should also be noted that the location data held in the MLC would be mostly based on network activity from a point in time in the past[8]. Finally, there may be privacy implications in tracking user locations in this manner that should be considered, as mentioned by Croatia, Cyprus and Portugal.

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



Competent Authority Alerting Gateway
(1) Competent authority alerting gateway interfaces with MNO alerting gateway(s) to send Alerts. Minimum information provided includes coordinate based description of the warning area and alerting text
MNO Domain
MNO Alerting Gateway
MNO Alerting gateway provides interface to competent authority and uses the MLC to ascertain which subscribers should be alerted
(3) Alerting Gateway submits SMS Messages to SMSC for onward delivery
(2) Alerting Gateway obtains list of subscribers in the specified area
(4) SMSC delivers message to cell for User 1, repeats for User 2 … User N
(4) Cell delivers message to User 1
SMS Service Centre (SMSC)
(5) Cell delivers message to User 2
(N) Cell delivers message to User N
Mobile Location Centre (MLC) or Location DB
MLC responsible for keeping track of subscribers in areas of concern at all times, potentially providing a real-time stream of data to MNO alerting gateway. MLC might take data from network element(s), including passive probes, to ascertain user locations.

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 and deliver 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 (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

[8] The subscribers’ location may a “last known location” which could be derived from normal network activity, or a “real time” location could be based on network actively locating the device, perhaps via paging.

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.

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 as they would typically not fulfil the requirements of Article 110(1) EECC as a stand-alone roll-out.

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 solutions potentially fall under Article 110(1) EECC. BEREC also concludes that these systems may require certain additional components to be added to existing mobile network infrastructure, so that public warnings could be transmitted effectively in order to fulfil the requirements of Article 110(1) EECC. In terms of additional technical equipment, BEREC observes that CBC would be necessary for CB (see section 2.2.2) and MLC might be necessary for LB-SMS (see section 2.2.3).

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[9]. 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[10] 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.

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 that have the IAS-PWS application downloaded to them it will send the message 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. The IAS-PWS application on each device decides whether to display the warning message depending on its location[11]	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 3.4.3 "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.

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

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

[11] The German NINA application uses this feature.

Step number	Description	Comment
0	Registration with mobile or fixed network	Consideration should be given to DHCP[12] 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.
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[13], 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.

[12] Dynamic Host Configuration Protocol

[13] 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.

Table 2 – IAS-PWS Steps

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

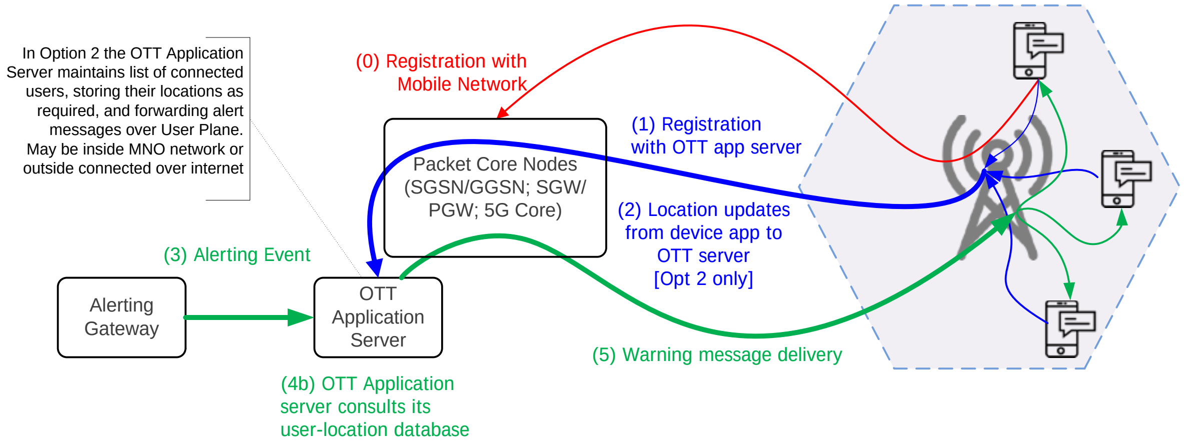

In Option 2 the OTT Application Server maintains list of connected users, storing their locations as required, and forwarding alert messages over User Plane. May be inside MNO network or outside connected over internet
(0) Registration with Mobile Network
Packet Core Nodes (SGSN/GGSN; SGW/ PGW; 5G Core)
(1) Registration with OTT app server
(2) Location updates from device app to OTT server [Opt 2 only]
(3) Alerting Event
Alerting Gateway
OTT Application Server
(5) Warning message delivery
(4b) OTT Application server consults its user-location database

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

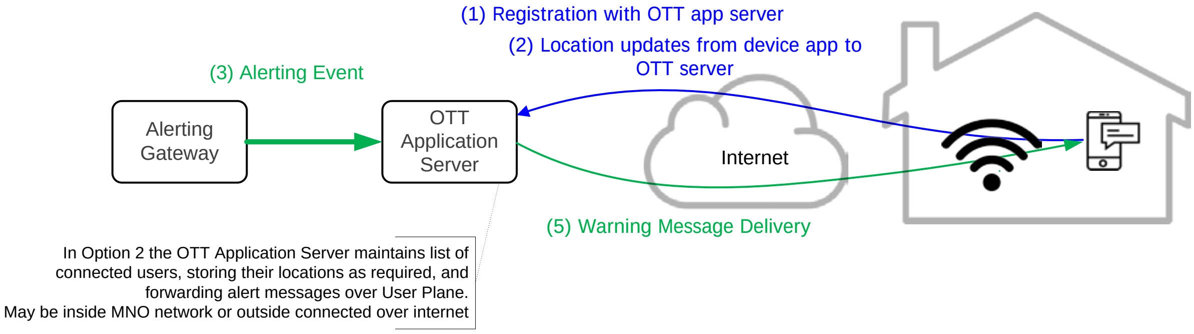

(1) Registration with OTT app server
(2) Location updates from device app to OTT server
(3) Alerting Event
Alerting Gateway
OTT Application Server
Internet
(5) Warning Message Delivery
In Option 2 the OTT Application Server maintains list of connected users, storing their locations as required, and forwarding alert messages over User Plane. May be inside MNO network or outside connected over internet

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 (envisaged IAS-PWS) compared to an Article 110(1)-PWS that fulfils the requirements of Article 110(1). In order to help competent authorities perform the equivalence assessments of their envisaged IAS-PWS, BEREC sets out a methodology consisting of the following steps.

0. Preliminary step (identifying suitable hypothetical benchmark systems):

   The competent authority identifies at least one hypothetical 110(1)-PWS that would comply with the legal requirements of Article 110(1) EECC, because only such 110(1)-PWS may be the benchmark system. BEREC considers that the legal requirements translate into geographical targeting, scalability and support of visiting end-users (which would include inbound roamers) as described in section 2.1.2. BEREC does not provide for any specific performance levels for these requirements which it considers are outside of its remit pursuant to paragraph 110(2). BEREC would therefore also encourage competent authorities to seek their own legal advice on whether the systems which they contemplate could satisfy the prerequisites of Article 110(1) of the EECC.

   For this purpose, the competent authority may take into account the description of the potential 110(1)-PWS' as described in sections 2.2.2 and 2.2.3.

1. Step 1 (benchmark creation)

   The competent authority assesses the performance of the hypothetical 110(1)-PWS' identified at the preliminary step in terms of coverage and capacity to reach concerned end-users.[14]

   First, the competent authority identifies which factors would properly define coverage and probably affect the capacity to reach concerned end-users. For this purpose, the competent authority may take into account the factors described at section 4 bearing in mind that the list of factors is non-exhaustive.

   Second, the competent authority assesses how the identified hypothetical 110(1)-PWS' performs with regard to the factors identified. For this purpose, the competent authority may take into account sections 5.1, 5.2 and 5.3, which sets out an example preliminary analysis of the performance of hypothetical 110(1)-PWS'.

   The benchmark created on the basis of the analysis of the 110(1)-PWS' serves as the minimum performance to be achieved by the envisaged IAS-PWS. BEREC considers that, where more than one hypothetical 110(1)-PWS that fulfil the requirements of Article 110(1) EECC under the respective national circumstances have been identified, the competent authority might choose any of the identified 110(1)-PWS' as the benchmark for the envisaged IAS-PWS.

2. Step 2 (IAS-PWS assessment)

   First, the competent authority verifies that the envisaged IAS-PWS does not require login or registration (see section 2.1.3).

   Second, the competent authority assesses how the envisaged IAS-PWS performs with regard to the factors identified in the previous step. For this purpose, the competent authority may take into account section 5.4, which sets out an example preliminary analysis of the performance of hypothetical IAS-PWS'. This means basically repeating the assessment already performed for the

[14] BEREC considers that coverage and capacity to reach concerned end-users need to be part of the competent authorities' assessment of the hypothetical 110(1)-PWS because, in the following step of the methodology, the hypothetical IAS-PWS needs to be compared to the established benchmark performance in terms of coverage and capacity to reach concerned end-users.

benchmark 110(1)-PWS' in step 1, only this time with the focus on the performance of the envisaged IAS-PWS.

3. Step 3 (equivalence assessment)

BEREC considers that this assessment should be performed factor-by-factor and needs to result in reaching a conclusion of an overall assessment of equivalence of the IAS-PWS with 110(1)-PWS in terms of coverage and capacity to reach end-users. For this purpose, the competent authority may take into account chapter 6 which sets out several examples for decision-making in an equivalence assessment.

In general, BEREC considers the following three cases:

Case A: If the performance of the envisaged IAS-PWS is at least equivalent to the performance of the benchmark for each factor, then the envisaged IAS-PWS fulfils the obligation of Article 110 EECC because it would be equivalent to the benchmark in terms of both coverage and capacity to reach concerned end-users.

Case B: If the envisaged IAS-PWS fails to be equivalent to the performance of the benchmark with regard to either geographic targeting, scalability or support of visiting end-users, it does not fulfil the obligation of Article 110 EECC.

Case C: If the envisaged IAS-PWS fails to be equivalent to the performance of the benchmark with regard to at least one of the other identified factors, it does not fulfil the obligation of Article 110 EECC unless an overall assessment of coverage and capacity to reach concerned end-users shows that the performance of the envisaged IAS-PWS is equivalent to the performance of the benchmark.

BEREC considers this exception from the need to comply with each factor under coverage and capacity to reach concerned end-users is needed in order to take into account differing national circumstances in Member States. Furthermore, without such an overall assessment an envisaged IAS-PWS that would outperform the benchmark system in the majority of factors would have to be dismissed as it would underperform with regard to at least one factor, even though in the overall assessment it would be more effective.

For this exemption to be applied, i.e. for the envisaged IAS-PWS to fulfil the obligation of Article 110(1) EECC even though it underperforms with regard to at least one factor, the envisaged IAS-PWS needs to be at least equivalent to the performance of the benchmark in the overall assessment of both "coverage" and "capacity to reach concerned end-users. For this purpose, BEREC considers that:

- The IAS-PWS do not underperform with regard to either geographic targeting, scalability or support of visiting end-users.
- The competent authority demonstrates that the underperformance of any other factor is compensated for by the outperformance with regard to other factors that have a bigger positive impact on the overall performance of the IAS-PWS regarding coverage or regarding the capacity to reach concerned end-users under the national circumstances.
- The IAS-PWS still provides a sufficient level of performance according to the Member State with regard to the underperforming factor (i.e. if it would fail to provide any performance with regard to that factor, it would not fulfil the obligation of Article 110 EECC).
- It is not possible to compensate the underperformance of a factor falling under "coverage" with the outperformance of a factor falling under "capacity to reach concerned end-users".

BEREC considers that this three step approach can be easily replicated in each Member State allowing competent authorities to objectively assess the equivalence of effectiveness of envisaged IAS-PWS and help them in their decision making processes. In applying this methodology, BEREC considers that competent authorities request information on already deployed ECS-PWS' in other jurisdictions, from other Member States, and from relevant expert groups such as the Early Warning Systems Expert Working Group organised by the Commission, or similar bodies. BEREC considers that this may enhance their assessments and would enable them to rely on information about relevant state of the art technologies.

This approach ensures that competent authorities 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.

4. Example factors of coverage and capacity to reach end-users

As the EECC does not specify the content of “coverage” and “capacity to reach” (except with regard to the aspect of end-users concerned) which makes them less tangible, BEREC considers competent authorities should identify relevant factors that represent an aspect of “coverage” or “capacity to reach end-users concerned” which they consider to be relevant for their equivalence assessment. The EECC hints at some of these factors e.g. when emphasizing on the importance of geographical targeting in recital 293, the need to warn end-users of imminent emergencies in recital 293 or the support of visiting end-users in Article 110(2) and inbound roamers in recital 294 (see section 2.1.2). However, BEREC considers that there are further – non-binding – factors that also fit under the definitions of or have an impact on coverage or capacity to reach concerned end-users and could thus also be used in the equivalence assessment of competent authorities.

BEREC therefore concludes that there are two types of these factors of coverage and capacity to reach concerned end-users (binding and non-binding). The binding factors are mentioned by the EECC and thus of specific importance for the legislator (“geographical targeting”, “scalability” and “support of visiting end-users including inbound roamers”). They should be the minimum factors a competent authority evaluates when assessing “capacity to reach end-users concerned”. Consequently, BEREC considers them to be of specific importance and to be non-negotiable. It has highlighted this explicitly in the methodology, in the respective sections of this chapter 4 and in chapter 6.

When identifying non-binding factors, BEREC considers that they still need to be an aspect of coverage or capacity to reach end-users concerned. A factor that could not contribute to either would therefore not be fit to play a part in the assessment of IAS-PWS equivalence.

For this purpose, BEREC proposes in this chapter a list of binding and non-binding factors of coverage and capacity to reach concerned end-users. With regard to the non-binding factors, BEREC considers this list to be non-exhaustive. Consequently, competent authorities might want to consider the live performance of ECS-PWS already deployed in the EU and reflect this in their own assessment. Relevant information could be requested on bi-lateral basis from Member States that already deployed such ECS-PWS or from relevant expert groups (e.g.: Early warning systems expert working group organised by the Commission). BEREC considers that it might also be useful to somewhere centralise information on the performance of such systems on the basis of Member States reports.

4.1. Coverage

The EECC mentions “coverage” as one of the two mandatory criteria to be taken into account in the assessment of the equivalence of effectiveness. The aim of coverage is to ensure that warning messages can be sent to the destination of the endangered end-users. 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.

4.1.1. Geographical coverage

In general geographical coverage refers to the ability of an ECS-PWS to transmit alerts anywhere in the areas where concerned end-users may be at. 100% geographical coverage 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.

4.1.2. 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. Competent authorities should keep in mind the aim of recital 293 to cover as many end-users concerned as possible, aiming at all end-users concerned.

4.2. Capacity to reach end-users concerned

“Capacity to reach end-users concerned” is the other mandatory 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 in connection with Article 110(1) 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”*. Hence the PWS capacity to reach end-users has to be assessed in relation to the performance of the PWS to convey the public warning message to end-users in the relevant area and fast enough to warn them of imminent emergencies. However, it does not specify what is exactly meant by “capacity to reach” which makes this criterion rather vague. BEREC considers that “all-end-users” is to be interpreted as “as many end-users as possible” and that the following factors can be summarised under “capacity to reach concerned end-users” making this criterion easier to assess for competent authorities.

4.2.1. Geographical targeting

An intrinsic factor in reaching the end-users concerned is the capability of an ECS-PWS to geographically target a specific area. The capability of sufficient geographical targeting is explicitly mentioned by recital 293 when it explains the meaning of “end-users concerned” (*“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”*). This also means that ECS-PWS’ should not unnecessarily alert end-users that are not in danger (argumentum e contrario). BEREC therefore considers sufficient geographical targeting a necessary factor each ECS-PWS needs to fulfil.

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 the alerting use cases they wish to support, and therefore the level of granularity required. The minimum granularity provided by currently rolled-out ECS-PWS is that of a single cell.

During the public consultation of these Guidelines BEREC enquired about how many end-users were usually alerted per incident. Having considered the responses it seems to BEREC that there is limited practical experience among stakeholders because BEREC only received seven answers that responded to this question in a relevant way. The analysis of submissions indicates that between 80% and 98% of warning messages dispatched are sent to areas with up to 50.000 end-users concerned, however, in areas with up to 5.000 end-users concerned, there was a significant variation in numbers of events (between 50% and 90% of warning messages sent to areas up to 5.000 end-users concerned). Therefore, it may be established that a significant number of use cases to be envisaged by public authorities is limited to less than 5000 end-users concerned.

Cases where up to 500.000 end-users need to be alerted range between 1,5% and 10% and less than 1% of the total warning messages are sent in cases where more than 2 Million end-users are concerned.

The variations in the percentages may to some extent be explained through the different sizes of countries. E.g. naturally countries that have less than 2 Million citizens don't send messages to more than 2 Million end-users and consequently they send a higher percentage of messages to less than 2 Million end-users. Furthermore, BEREC considers that the amount of cases does not reflect on the severity and urgency of use-cases. BEREC believes that even though the total cases of alerts affecting more than 2 Million end-users seems to be less than 1% these cases may well be of great importance to the population due to their severity and geographical reach.

Thus, BEREC observes that these population figures may not constitute a reason for Member States to deploy systems that only deal well with the expected majority of small cases. In line with the EECC, ECS-PWS should be able to address the worst case scenarios, even if they are uncommon.

On the other hand, BEREC observes that in the majority of examples of warnings seem to be only relevant for a small part of the overall population, which might add weight to the benefit of precise geographical targeting as it can be used to avoid unnecessarily alerting end-users. Precise targeting of messages might enhance rescue efforts and/or other relevant measures by the competent authorities.

4.2.2. Scalability

When recital 293 states that "*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[…]*", BEREC considers that this includes successful delivery of messages within a sufficiently short period of time as a relevant factor in order to reach and warn end-users concerned of imminent emergencies. Reaching the end-users concerned in time becomes increasingly difficult the larger the affected area/number of end-users concerned. It is therefore important to assess how well an ECS-PWS scales with increasing numbers of end-users concerned and if it is still able to deliver warning messages on time in worst-case scenarios. Consequently BEREC considers sufficient scalability a necessary aspect of the capacity to reach concerned end-users each ECS-PWS needs to fulfil.

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 factor, 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 to alert large populations in real time, as they are built for day to day traffic.

4.2.3. Support of visiting end-users including inbound roamers

The support of visiting end-users is a necessary factor of the capacity to reach end-users concerned. Article 110(2) EECC explicitly refers to the need to provide warning messages to *"those only temporarily present in the area concerned"* which includes national visitors from other regions but also inbound roamers. Also recital 294 states that "*end-users entering a Member State*" shall be informed "*on how to receive public warnings*".

Consequently, BEREC considers that the support of visiting end-users is a necessary factor each ECS-PWS needs to fulfil. This should be reflected accordingly in the competent authority's assessment.

This aspect may need to be assessed in conjunction with other aspects in this section (e.g. Sections 4.2.5 and4.2.6).

4.2.4. Supported devices

The capacity to reach end-users also depends on whether the public warnings are supported by the end-user's 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.

4.2.5. Steps required for recipient to enable receiving warning messages

This aspect of reaching the concerned end-users 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.

The end-users that do not take the steps needed for enabling their handsets to receive public warnings will not receive the public warnings. Therefore, competent authorities should assess the impact of the steps required for the recipient to enable receiving warning messages on the capacity to reach concerned end-users when comparing the ECS-PWS'. Member States should also consider possible measures to maximise the take-up of the ECS-PWS where available.

4.2.6. Supported languages

BEREC considers that one factor of reaching concerned end-users in the most efficient way is sending the warning messages in the recipient's language. Supported languages refers to the ability of the ECS-PWS to ensure that recipients can receive warning messages in the language of their choice which would help in understanding the content of the messages more quickly and thus lead to faster reaction times of end-users concerned. 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.

4.2.7. Managing longer messages

BEREC considers competent authorities should consider the minimum length of warning message that will suffice for that member state's needs. The potential length of a single warning message may have an impact on the time it needs in order to be displayed. Where warning messages consist of several parts that need to be sent separately and then reassembled on the end-user's device, precious time might be lost, which could be essential in alerting concerned end-users in emergencies where a fast reaction is of the essence.

Competent authorities should therefore 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.

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.

4.2.8. Accessibility for end-users with disabilities

End-users with disabilities are a sub-group of the concerned end-users. Some disabilities (e.g. blindness) may prevent recipients becoming aware of the content of a warning message sent via text which would effectively prevent these end-users from being reached by the ECS-PWS. BEREC therefore considers that competent authorities should take into account the user experience for end-users with disabilities when considering ECS-PWS'.

4.2.9. Reliability

The reliability of an ECS-PWS describes how well an ECS-PWS can submit the warning messages triggered by the competent authorities to the concerned end-users without being postponed or lost due to technical failure of network or ECS-PWS components. Consequently this factor has a significant impact on the ability to reach concerned end-users.

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.

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?

4.2.10. Alerting end-users entering the area after the initial warning

As part of the capacity to reach concerned end-users ECS-PWS should also be capable of reaching end-users that enter the hazardous area after the initial warning has been triggered. The reason being that they did not receive the initial warning message when they were outside of the relevant area. This could be achieved through several different mechanisms e.g. by constantly broadcasting warning messages (ensuring that these aren’t displayed again after they have been received) or by keeping track of the mobile devices in the area and alerting those that enter after the initial alert (being aware of the privacy implications).

5. Example analysis of PWS' performances

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 and fulfilling the requirements of Article 110(1) is the benchmark against which the 110(2)-PWS needs to be assessed.

First, in the following sections, BEREC provides an example initial analysis of the performance of generic CB and LB-SMS systems. Competent authorities could use this analysis as a starting point for their assessment of the benchmark 110(1)-PWS. BEREC considers this example assessment to be non-exhaustive. The level of detail provided by BEREC in this example assessment of each factor varies as for some factors the performance of an ECS-PWS depends more on national circumstances e.g. the network-structure or the geographic dispersion of end-users in a Member State.

Consequently, this initial assessment – if used as a starting point by competent authorities – 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 envisaged ECS-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 factors that depend on network specific intricacies of each Member State.

When competent authorities assess the performance of the hypothetical 110(1)-PWS, BEREC considers they should take into account the standard functionalities of the 110(1)-PWS at the time of the assessment. These may by then have evolved from the standard functionalities as described by BEREC in these Guidelines.

Second, in the last section of this chapter, BEREC provides for several points to note for competent authorities in their assessment of IAS-PWS performance

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

5.1.1. Coverage

5.1.1.1. 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 of their national geographical coverage of 99%. In practice they found out that they usually manage to contact 85% of the concerned end-users directly with their CB system.

5.1.1.2. 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.

5.1.2. Capacity to reach end-users

5.1.2.1. 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.

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.

5.1.2.2. 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.

5.1.2.3. Support of visiting end-users including inbound roamers

BEREC considers the performance of CB with regard to the support of visiting end-users from the same country is not likely to be an issue (see next section on supported devices).

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). With regard to iOS BEREC has observed that a new CB settings menu is activated when roamers enter a country with CB, and notes that stakeholders pointed out that receiving CB messages is activated per default (starting from iOS version 12.3). End-users may decide to turn warnings on or off, except EU Alert Level 1 (equivalent to presidential alert) warnings which are always on.

Cell Broadcast is also supported on Android since Android 4.4 Kitkat, according to BERECs calculations this means that 99.14% of Android devices in Europe support CB, however depending on the manufacturer and the country of origin settings of the device warning message reception may need to be activated manually. Inbound roamers from countries not using CB can be instructed by the welcome SMS of the home network operator when entering roaming, how they can turn on the alerting on their phone of a vendor that might not have it set by default due to a different alerting system implemented in their home country. 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 sometimes possible, subject to the roamers MSISIDN being available to the visited network. 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.

BEREC highlights that Member States can explore this matter when they are specifying their PWS with MNOs and providers of PWS. If required, competent authorities should check the steps to enable CB on mobile devices in their market.

Therefore BEREC considers that CB fulfils this criterion but excels at fulfilling this criterion for phones that come pre-configured in a way to receive CB messages.

5.1.2.4. 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.

5.1.2.5. 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. This needs to be taken into consideration by competent authorities which should assess the impact on the expected percentage of warning messages missed by opting-out of lower severity levels because the reach of CB is intrinsically dependent on the penetration of its messages which can be significantly diminished if end-users opt-out of messages with lower severity levels. Competent authorities could raise end-users' awareness on the benefits of having all alert levels displayed to them e.g. through an information campaign.

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.

5.1.2.6. 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[15], 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.[16]

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.

5.1.2.7. 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 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.

5.1.2.8. 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

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

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

visually impaired end-users, CB does not have a back-up functionality to compensate for this. However, in combination with the devices features CB is able to provide a basic support for end-users with disabilities.

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. BEREC considers a specific siren sound and vibration cadence may only be useful to inform recipients that a warning message has arrived but they do not help with informing recipients about the content of the warning message.

5.1.2.9. 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.

5.1.2.10. Alerting end-users entering the area after the initial warning

The mobile networks may (re)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.

5.2. Analysing the performance of Location based SMS

5.2.1. Coverage

5.2.1.1. 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 national authorities have considered as relevant for the transmission of a public warning. Receiving an LB-SMS message will be possible while end-users stay within the coverage of a compatible 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.

5.2.1.2. 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 LB-SMS.

5.2.2. Capacity to reach end-users

5.2.2.1. 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.

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'[17].

5.2.2.2. 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 or area 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 a 2G/3G radio access network ("RAN") to be flooded by SMS messages. Outside of the RAN domain, other network nodes or links could have unexpected capacity limitations when alerting large numbers of users in a concentrated area.

In these cases, 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 or days to deliver all queued warning messages.

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, although it needs to be mentioned that this was in an early phase of their respective LB-SMS roll-out and since then improvements have been made. Bulgaria considers real time tests are needed to determine scalability. Poland

[17] Page 14 of version 3.0 published 30.09.2019.

reported it takes from a few minutes to a few hours. Competent authorities should work closely with MNOs to establish what 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.

5.2.2.3. Support of visiting end-users including inbound roamers

BEREC considers the performance of LB-SMS with regard to the support of visiting end-users from the same country is not likely to be an issue due to the fact that SMS is standardised throughout the world.

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 sometimes possible, subject to the roamers MSISIDN being available to the visited network. 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.

5.2.2.4. 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.

5.2.2.5. 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.

5.2.2.6. Supported languages

The SMS standards support extended characters from some languages[18], 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). For the time being no roll-out exists that support all EU27 languages.

5.2.2.7. 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.

Longer SMS messages are possible via a feature called concatenation, where the PWS system or the MNO's SMSC splits text into multiple segments which are subsequently reassembled by the receiving device. This approach multiplies the number of SMS messages carried and has an obvious impact on the network load of any alerting event.

In the situation where all message segments are not received together, some devices will await the arrival of the complete set before notifying the user which will delay they display of the warning message, 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 receiving device behaviour for the most common devices used in that market.

5.2.2.8. 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 provide any back-up functionality to compensate for this. However, in combination with the devices features LB-SMS is able to provide a basic support for end-users with disabilities.

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.

5.2.2.9. 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

[18] For a full description of the languages and character sets supported via the use of shift tables, see 3GPP TS 23.038

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.

5.2.2.10. Alerting end-users entering the area after the initial warning

As described in section 2.2.3, 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 by default receive the warning message. This can be corroborated with the explanation given by some Member States (Portugal and Slovakia) that the system uses the mobile network's view of the devices' location at the moment it is triggered. It would be possible however to configure the MLC to notify the alerting gateway of end-users entering the area (subject to issues mentioned in section 2.2.3, of location accuracy and recency), and send individual LB-SMS messages to these users if required.

5.3. Overview of 110(1) performance

Where possible, the following table summarises the results from BEREC's example initial assessment from sections 5.1 and 5.2 for the assessed factors. It does not introduce new conclusions diverging from those sections. As mentioned in the introduction to chapter 5, BEREC's example initial assessment needs to be supplemented by competent authorities' own assessment based on their considerations of specific national circumstances and also having regard to the purpose and objectives of their envisaged ECS-PWS.

Column 1 in the following table sets out a list of the relevant factors a taken from chapter 4.

Columns 2 and 3 summarise BEREC's example initial assessment of the performance of CB-PWS and LB-SMS systems for each factor, 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 did not attach numerical values or assign a score to the performance of systems as it did not have access to suitable information in order to be able do so. 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. Nevertheless competent authorities may attach metrics to the factors to assist their analyses if relevant quantitative data is available to support such an approach. In this aspect, BEREC encourages competent authorities to request information on already deployed ECS-PWS' in other jurisdictions, from other Member States, and from relevant expert groups such as the Early Warning Systems Expert Working Group organised by the Commission, or similar bodies. Thus, the actual reasoning for the competent authorities' assessment should to be provided similarly to the description of their assessment in sections 5.1 and 5.2.

Column 4 provides a brief explanation for the performance values awarded in columns 2 and 3, taken from the previous sections. It only mentions the relevant reasons for the outcome of BEREC's example initial assessment. The competent authority should amend it as necessary based on its own assessment in those sections.

1. Factors	*2. CB (EU-ALERT)*	*3. LB-SMS*	*4. Explanation*
Coverage			
Geo. Coverage	To be assessed by competent authorities	To be assessed by competent authorities	
Pop. Coverage	To be assessed by competent authorities	To be assessed by competent authorities	
Capacity to reach end-users			
Geo. Targeting	+/++ To be assessed by competent authorities and amended as necessary	+ To be assessed by competent authorities and amended as 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 assessed by competent authorities and amended as necessary	To be assessed by competent authorities	
Support of inbound roamers	+ To be assessed by competent authorities and amended as necessary	To be assessed by competent authorities	*Note that the visiting user's MSISDN might not be available to the visited network in some scenarios. BEREC notices that when it comes to iOS devices CB excels at performing this criterion. However, it is unclear whether the same can be said for all android devices. This is why BEREC considers CB does not overall excel at fulfilling this factor.*
Supported devices	+ To be assessed by competent authorities and amended as necessary	++ To be assessed by competent authorities and amended as 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.

1. Factors	*2. CB (EU-ALERT)*	*3. LB-SMS*	*4. Explanation*
Steps required for recipient to enable warning messages / No human interaction needed	+ To be assessed by competent authorities and amended as necessary	++ To be assessed by competent authorities and amended as necessary	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 factor. In the case of CB, depending on national regulation or on the standards set by manufacturers for the specific country, human interaction may be needed to receive all CB warning messages. This is why CB does not excel at fulfilling this criterion
Supported languages	++ To be assessed by competent authorities and amended as necessary	+ To be assessed by competent authorities and amended as necessary	Both systems allow sending of warning messages in different languages. CB with the EU-ALERT standard even automatically displays the correct language as selected by the recipient on their device, when receiving a warning message in several languages.
Managing longer messages	+ To be assessed by competent authorities and amended as necessary	+ To be assessed by competent authorities and amended as 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, resulting in a delay in the display of the complete message.
End-users with disabilities	+ To be assessed by competent authorities and amended as necessary	+ To be assessed by competent authorities and amended as 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. However, in combination with the devices features both systems are able to provide a basic support for end-users with disabilities.
Reliability	++ To be assessed by competent authorities and amended as necessary	+ To be assessed by competent authorities and amended as 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 (or similar) 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.

1. Factors	*2. CB (EU-ALERT)*	*3. LB-SMS*	*4. Explanation*
Messages to end-users entering the warning area late	++ To be assessed by competent authorities and amended as necessary	+ To be assessed by competent authorities and amended as necessary	Both, CB and LB-SMS can provide this functionality. The reason why CB excels at this factor is because it can provide this feature without any downsides such as privacy implications.

-	= does not fulfil factor
+	= fulfils factor
++	= excels at fulfilling the factor

Table 3

5.4. Example analysis of IAS-PWS' performances

In this section some points of note are set out to assist competent authorities in defining functionalities IAS-PWS should possess and assessing IAS-PWS performance with regard to each factor and consequently with regards to coverage and capacity to reach concerned end-users.

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 envisaged IAS-PWS.

Therefore, it is not possible for BEREC to include a baseline performance analysis, which is up to the competent authorities when assessing the envisaged IAS-PWS.

However, the following sub-sections provide specific points of note for all factors, also based on the experience with currently rolled-out IAS-PWS which will be of relevance for the roll-out of future IAS-PWS:

5.4.1. Easy to receive

Article 110(2) EECC introduces an additional general legal requirement for IAS-PWS when stating 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 "*where 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 (for details see section 3.3.1.9). BEREC considers this to be a general legal requirement with regard to IAS-PWS that competent authorities need to ensure when rolling-out an IAS-PWS.

5.4.2. Coverage

5.4.2.1. Geographical 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.

5.4.2.2. Population Coverage

For population coverage the distribution of the population within a Member States' territory is relevant. As already mentioned in the previous paragraphs on population coverage for CB and LB-SMS competent authorities should analyse the distribution of the population in their Member State and consider whether population coverage is superior to geographical coverage in their country. This is an assessment BEREC cannot make.

For population coverage for IAS-PWS competent authorities should keep in mind the aspect that IAS-PWS benefits from additional WIFI Internet access.

5.4.3. Capacity to reach end-users

5.4.3.1. 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.

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. Also competent authorities may require that the geo-location feature is activated by default upon installation of the IAS-PWS application.

5.4.3.2. 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. The feedback received during the consultations in preparation of these Guidelines show that countries using this option did not encounter any issue in the speed of the delivery of the warning messages (e.g. Germany) which were received within a few seconds.

5.4.3.3. Support of visiting end-users and inbound roamers

BEREC considers there to be two potential difficulties of IAS-PWS applications in this regard. The first is that visiting end-users and inbound roamers have to download an application (see section 5.4.3.5). The second is making these users aware about which application to download. Different applications in different regions may also mean that an IAS-PWS could be less effective.

Furthermore, it should be considered that inbound roamers might have difficulties of going through the download process when the application is not available in a language that they can understand.

Competent authorities should raise the awareness of the available IAS-PWS to inbound roamers. Recital 294 recommends 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.

5.4.3.4. Supported devices

On-device applications may need to 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. One handset and base station manufacture is planning to deploy its own operating system in the timeframe leading to the legal deadline provided in Article 110 (21 June 2022). 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. This may be of particular relevance for older people that are not in possession of such devices.

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.

5.4.3.5. Steps required for recipient to enable receiving warning messages

The use of IAS-PWS requires downloading and installing an application and possibly also granting the necessary permissions (e.g. enable location services). However, because the reach of an IAS-PWS is intrinsically dependent on the penetration of its application, the competent authorities should assess the expected take-up of the IAS-PWS application. BEREC considers that in order to ensure broader reach of end-users, 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 through an information campaign or by obliging device manufacturers to have the IAS-PWS app pre-installed.

Similar to the assessment of CB, competent authorities should assess the impact on the expected percentage of warning messages missed by de-installing the application or by withdrawing the necessary permissions.

Recital 294 of the EECC explains that end-users should not need to log in or register with the application provider or the authorities in order to receive the public warning. This means that the end-user may also not be required to enter a username and password in order to use the IAS-PWS (log-in). BEREC thus considers that the manual activation of location services therefore would neither fall under “registration” or “log-in”. However, BEREC recommends that after the download of the application the default settings should enable receiving warning messages that target the end-user’s current location without the need to change any settings.

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 locations services are 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).

5.4.3.6. 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.

For the time being there are no live deployments of an IAS-PWS supporting all EU27 languages.

5.4.3.7. Managing longer messages

IAS-PWS usually don’t come with a fixed limit to message lengths and can be built according to the demands of the competent authorities. Thus, IAS-PWS are able to transmit and display longer messages as one single messages, thus reducing the network load and eliminating the risks that come with message-concatenation.

5.4.3.8. Accessibility for end-users with disabilities

IAS-PWS could introduce innovation regarding the accessibility for disabled end-users (e.g. visually impaired end-users). For example application providers could add improved text-to-speech capabilities or additional features programmable into an app if demanded by the competent authority.

5.4.3.9. Reliability

IAS-PWS are very robust solutions because they do not rely solely on mobile networks and have WIFI hotspots as an alternative data path thus enabling concerned end-users to receive warning messages even when the mobile networks are down and they are within reach of a WiFi.

5.4.3.10. Alerting end-users entering the area after the initial warning

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.

6. Examples of comparing IAS-PWS performance with 110(1)-PWS performance

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 and fulfilling the requirements of Article 110(1) EECC is the benchmark the 110(2)-PWS needs to be assessed against. Where more than one hypothetical 110(1)-PWS that fulfil the requirements of Article 110(1) EECC under the respective national circumstances have been identified, the competent authority might choose any of the identified 110(1)-PWS' as the benchmark for the envisaged IAS-PWS.

For the overall assessment, BEREC proposes that competent authorities take the outcomes from their assessment of the benchmark 110(1)-PWS comparable to the description of BEREC's example assessment in sections 5.1, 5.2 and 5.3 which should be aggregated in Table 3. Next competent authorities should compare this benchmark with the assessed performance of their envisaged IAS-PWS possibly taking into account the points of note in section 5.4.

BEREC considers that when comparing the performances of the benchmark 110(1)-PWS to the assessed IAS-PWS with regard to each factor under coverage and capacity to reach concerned end-users, the factors should lead to an overall assessment of the respective criterion they fall under (coverage or capacity to reach concerned end-users) as explained in the methodology in chapter 3.

In the following paragraphs, BEREC provides examples for the overall assessment needed in the equivalence assessment in case the envisaged IAS-PWS fails to be equivalent to the performance of the benchmark with regard to at least one of the non-binding factors as explained in chapter 3:

> *"The IAS-PWS may not underperform with regard to either geographic targeting, scalability or support of visiting end-users."*
>
> ➔ BEREC considers these three factors mentioned by the EECC to be of particular importance for the legislator. Therefore they may not be subject to compensation if the envisaged IAS-PWS underperforms with regard to one of these factors.
>
> *"The competent authority demonstrates that the underperformance of any other factor is compensated for by the outperformance with regard to other factors that have a bigger positive impact on coverage or on the ability of alerts to reach concerned end-users under the national circumstances"*
>
> ➔ Example 1 (successful compensation): All other factors being equivalent, compared to the benchmark, the IAS-PWS is under-performing with regard to reliability and out-performing with regard to support of end-users with disabilities (i.e. the "accessibility for end-users with disabilities" factor, see also section 4.2.8). The mobile networks in the Member State are very reliable (see section 4.2.9) and the result of the marginal difference in the reliability of the IAS-PWS compared to the benchmark, would have a limited impact on the capacity to reach concerned end-users. On the other hand, compared to the benchmark system, the IAS-PWS would be more effective at reaching disabled end-users and, as a consequence, this factor would be more rewarding than the "reliability" factor in the overall assessment of capacity to reach concerned end-users.[19] The

[19] For example, though the message would be received in the same text format as for Art 110(1) PWS, the IAS PWS could have additional features to attract the attention of the end-user to the alert (e.g. longer vibrating, other specific signal that a warning has been received, etc.). Therefore, the difference would be specifically in the effectiveness of reaching end-users with disabilities.

competent authority, in light of carefully observing factors in this way, and considering the compensation between the performances of these two factors in an overall manner, could demonstrate that the IAS-PWS would be as effective as the benchmark in terms of the capacity to reach concerned end-users.

- ➔ Example 2 (unsuccessful compensation): The IAS-PWS would be expected to be downloaded by only 10% of the population but on the other hand it could provide a length of message exceeding 100 characters and transmit the public warning automatically in 2 non-official languages, representing 12% of the population. Meanwhile, the benchmark ECS-PWS established by the Member State would allow for the effective reach of at least 50% of the population, would only provide 90 characters per message and only be available in the official language of the Member State concerned. The competent authority would establish that the length of one message sent by the benchmark system is shorter than the length of the IAS-PWS message and additional language versions of the public warning would not be available. While the IAS-PWS would outperform with regard to two factors, in an overall assessment of the capacity to reach end-users, these factors could not compensate for the underperformance in terms of reach of concerned end-users because the benchmark system would have the capacity to reach 40% more of the concerned end-users compared to the IAS-PWS.
- ➔ With regard to the compensation of underperforming factors, 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. The quantification of the impact on coverage or on the capacity to reach concerned end-users from each factor may be enhanced through information exchange between authorities and Member States as well as by the use of existing relevant surveys and studies.

"The IAS-PWS still provides a sufficient level of performance according to the Member State with regard to the underperforming factor (i.e. if it would fail to provide any performance with regard to that factor, it would not fulfil the obligation of Article 110 EECC)."

- ➔ If for example the envisaged IAS-PWS would only be able to send 70 characters with a single message whereas LB-SMS is able to send 93 characters, the envisaged IAS-PWS would underperform but still be able to provide a certain level of performance. It would then be up to the competent authority to explain whether it considers this performance by the envisaged IAS-PWS would still be sufficient to fulfil the national needs in terms of minimum performance of the envisaged IAS-PWS.
- ➔ In another example where the envisaged IAS-PWS would not only underperform with regard to "alerting end-users entering the area after the initial warning" but would not provide this functionality at all, BEREC considers this would be a strong indication for the envisaged IAS-PWS failing to comply with the obligation from Article 110 EECC.

"It is not possible to compensate the underperformance of a factor falling under "coverage" with the outperformance of a factor falling under "capacity to reach concerned end-users".

- ➔ Article 110(2) states the envisaged IAS-PWS needs to be equivalent in terms of coverage and capacity to reach concerned end-users thus clearly differentiating between these two criteria. BEREC therefore considers that an overall assessment of factors falling under coverage or capacity to reach concerned end-users can only be done within the respective criterion of either coverage or capacity to reach concerned-end-users. Consequently, BEREC considers that, for example, an outperformance of "reliability" could not compensate an underperformance of either "geographical coverage" or "population coverage".
- ➔ BEREC stresses that according to its interpretation of the EECC, coverage and capacity to reach concerned end-users cannot be subject to compensation because the EECC does not differentiate between the importance of either "coverage" or "capacity to reach concerned end-users".

7. Further functionalities that may improve ECS-PWS' effectiveness

Even though the following functionalities cannot be derived from the actual wording of the EECC, BEREC considers them to be 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 to make it more effective, even if these functionalities could not be used in the equivalence assessment of effectiveness of IAS-PWS according to Article 110 EECC.

It would also be a matter for Member States or competent authorities to ensure that any measures taken to improve the effectiveness of ECS-PWS', comply with other relevant legislations and promote the highest standards in terms of technical security functionalities, e-Privacy requirements, and Open Internet guidance. In this regard, BEREC encourages stakeholders to consult widely and appropriately before committing to deploy functionalities in their ECS-PWS'.

7.1. Free of Charge for the end-user to receive

Recital 294 of the EECC mentions that the SMS explaining the access to the national ECS-PWS and the transmission of public warning messages should be free of charge for end-users. The EECC thus recommends to Member States that these messages are delivered free of charge. BEREC notices that this is not a binding obligation but encourages Member States to ensure that costs for end-users do not pose a disincentive to use ECS-PWS.

Cell broadcast

As far as BEREC is aware in the currently rolled-out CB-systems warning messages are provided free of charge to end-users.

LB-SMS

As far as BEREC is aware in the currently rolled-out LB-SMS-systems warning messages are provided free of charge to end-users.

IAS-PWS

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 IAS-PWS warnings might not be charged.

In the situation where a user's data bundle is exhausted, different MNOs handle this in different ways, ranging from the throttling of internet access service traffic to entirely blocking it. In the latter case, end-users will not receive warning messages unless the blocking would exclude IAS-PWS alerts or the device is connected via WiFi.

In any case, the measures taken by the Member States in this regard should be compliant with the open internet regulation.[20]

[20] Regulation (EU) 2015/2120 of the European Parliament and of the Council of 25 November 2015 laying down measures concerning open internet access and retail charges for regulated intra-EU communications and amending Directive 2002/22/EC and Regulation (EU) No 531/2012, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02015R2120-20181220

7.2. 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 and specific ringtones or vibration cadences. 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 that can be clickable, depending on the handset functionalities, and allow further user interaction.

CB messages generally result in an audible notification from the recipient mobile device which cannot be turned off and which is different to an incoming SMS, making the warning message recognisable as an important warning. While this distinct audible notification can generally be seen as a benefit, there are situations (e.g. related to terrorism or shootings) where it is imperative for such a notification be silenced in order to stay hidden.

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. The inclusion of a hyperlink is possible.

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. Nevertheless, end-users have the option to assign customised tones or vibration cadences to the warning message in their device’s settings and also to disable audible alarms. 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 or hyperlinks. It can also be programmed to come with a specific ringtone or vibration cadence or allow the end-user to choose their own in the settings menu, and also to disable audible alarms.

7.3. 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.

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.

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

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 Poland made particular reference to the threat of inauthentic LB-SMS based alerts being sent to end-users.

IAS-PWS

In order to ensure the authenticity of warning messages in an IAS-PWS implementation, since the competent authority is in control of both the client and server side, it would be possible to implement a secure message authentication facility via the use of cryptographic signatures and/or TLS based encryption/authentication.

[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.

7.4. 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).

7.5. Delivery rate tracking for sent messages/Reporting numbers of end-users located in a warning area

This functionality summarises several related functionalities that are based on the end-users device giving back some kind of report to the competent authority. One functionality is sending an acknowledgment of a successful receipt of the warning message thus also giving the competent authority an estimation of the number of end-users concerned. Secondly, competent authorities could use aggregated and anonymised location data from end-user devices to track their movement in the relevant area and react with fine-tuned measures.

Cell broadcast

CB uses broadcasting technology and thus the end-users device does not send a feedback to the competent authority. Therefore, CB supports none of the functionalities mentioned above.

LB-SMS

According to several stakeholders (Nokia, Everbridge and 112 Iceland) LB-SMS can be upgraded with these functionalities, thus enabling competent authorities to react with tailored measures to critical situations. However, functionalities such as the movement tracking come at the cost of having a possible impact on end-users privacy (in particular if there were data protection breaches or other unintended uses of the data) and a negative impact on network load.

IAS-PWS

Similarly to LB-SMS, IAS-PWS could provide feedback-features which might be even more effective when it comes to location tracking as this would be provided based on location services. However, it would also come at the cost of end-user privacy issues privacy (in particular if there were data protection breaches or other unintended uses of the data) and additional network load. This is why in the case of the German IAS-PWS these functionalities were not implemented.

7.6. All-clear messages

Another useful feature, although strictly speaking not a warning message, would be sending all-clear messages once the situation that made issuing the warning message necessary has been resolved. Such a feature would also need to address people who were present in the relevant area when the warning was issued but left the area during the alert (e.g. during an evacuation order). Thus, they would receive a message that it is safe to come back which is of particular importance e.g. when defusing unexploded ordnance.

Cell broadcast

CB does not track end-users that have received a warning. Thus, the all-clear message would not reach end-users that have left the area.

LB-SMS

If combined with the “feedback-functionality” LB-SMS could be upgraded with a feature that keeps track of the devices that have received a warning message and send an all-clear message to them, even if they have left the relevant area.

IAS-PWS

One option to configure IAS-PWS is to broadcast alerts nationwide and then the IAS-PWS checks whether it is in the relevant area and only then displays the warning message (Option 1 in Table 2). This feature could also be used to enable on tracking on the device of whether a warning message has been displayed and if so also display subsequent all-clear messages. Such a feature wouldn’t even have to use the feedback-functionality and thus have no impact on privacy.

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. This call was aiming to get feedback from all competent authorities with regard to ECS-PWS'. In total BEREC received 15 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, , Ministry of Justice and Security of the Netherlands, Directorate-general of Police and Safety Regions (MoJS NL), 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 2.2.3.

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, two Member State uses stand-alone 110(1)-PWS' (The Netherlands using CB and Belgium using LB-SMS), 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.

In of Spain the functions of this system include sending of automated voice messages. For instance, automated voice calls are sent to citizens in need of specific assistance that have previously registered for the service.

In Bulgaria early warning and voice dialling are intended for the executive authorities and the constituent parts of the United Rescue System and does not constitute a system for early warning of the population within the meaning of Directive (EU) 2018/1972, as well as that no early warning system using LB-SMS is established in Bulgaria.

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
GALILEO	Global Navigation Satellite System of the European Union
GNSS	Global Navigation Satellite System
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

Acronym	Definition
ISDN	Integrated Services Digital Network
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
TLS	Transport Layer Security
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.

Recitals 293 & 294

(293) Diverging national law has developed in relation to the transmission by electronic communications services of public warnings regarding imminent or developing major emergencies and disasters. In order to approximate law in that area, this Directive should therefore provide that, when public warning systems are in place, public warnings should be transmitted by providers of mobile number-based interpersonal communication services to all end-users concerned. 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.

(294) Where the effective reach of all end-users concerned, independently of their place or Member State of residence, is ensured and fulfils the highest level of data security, Member States should be able to provide for the transmission of public warnings by publicly available electronic communications services other than mobile number-based interpersonal communications services and other than transmission services used for broadcasting or by mobile application transmitted via internet access services. In order to inform end-users entering a Member State of the existence of such a public warning system, that Member State should ensure that those end-users receive, automatically by means of SMS, without undue delay and free of charge, easily understandable information on how to receive public warnings, including by means of mobile terminal equipment not enabled for internet access services. Public warnings other than those relying on mobile number-based interpersonal communications services should be transmitted to end-users in an easily receivable manner. Where 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. End- users’ location data should be used in accordance with Directive 2002/58/EC. The transmission of public warnings should be free of charge for end-users. In its review of the implementation of this Directive, the Commission could also assess whether it is possible in accordance with Union law, and feasible to set up a single Union-wide public warning system in order to alert the public in the event of an imminent or developing disaster or major state of emergency across different Member States.